Załącznik do Uchwały Zarządu ŁSARN Nr 3 z dnia 15 maja 2018 r.
w sprawie ochrony danych osobowych w Łódzkim Stowarzyszeniu Analityków Rynku Nieruchomości.

Polityka Bezpieczeństwa Informacji w zakresie ochrony danych osobowych w Łódzkim Stowarzyszeniu Analityków Rynku Nieruchomości (w skrócie: ŁSARN)

I. Wstęp

1. Dokument „Polityka bezpieczeństwa w zakresie ochrony danych osobowych w ŁSARN" – zwany dalej: „Dokumentem" wskazuje sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych i jest w szczególności przeznaczony dla osób pracujących przy przetwarzaniu danych osobowych w Łódzkim Stowarzyszeniu Analityków Rynku Nieruchomości, zwanym dalej w skrócie „ŁSARN".

2. Niniejszy dokument opisuje reguły dotyczące procedur zapewnienia bezpieczeństwa danych osobowych ŁSARN, **w tym danych osobowych zawartych w systemach informatycznych od chwili gdy systemy takie zostaną w Stowarzyszeniu wdrożone**.

3. Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę ŁSARN.

4. Dokument zwraca uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

5. Potrzeba opracowania „Polityki bezpieczeństwa" wynika z przepisów § 3 i 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

II. Postanowienia ogólne

1. Ilekroć w polityce bezpieczeństwa jest mowa o:

1) ustawie - rozumie się przez to ustawę z dnia 29 sierpnia 1997r. o ochronie danych osobowych,
2) rozporządzeniu – rozumie się przez to 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. nr 100, poz. 1024),
3) administratorze danych - rozumie się przez to Zarząd ŁSARN,
4) systemie informatycznym administratora danych - rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer,
4) administratorze systemu - rozumie się przez to wskazanego przez Zarząd ŁSARN współpracownika ŁSARN zatrudnionego na zasadzie umowy powierzenia czynności ds. informatyki lub na innym stanowisku związanym z przetwarzaniem danych osobowych,
5) użytkowniku - rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło,
6) haśle - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi,

7) identyfikatorze - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
8) integralności danych - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
9) odbiorcy danych - rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
   - osoby, której dane dotyczą.
   - osoby upoważnionej do przetwarzania danych,
   - przedstawiciela, o którym mowa w art. 31a ustawy,
   - podmiotu, o którym mowa w art. 31 ustawy,
   - organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,
9) osobie upoważnionej do przetwarzania danych osobowych - rozumie się przez to osobę, która upoważniona została do przetwarzania danych osobowych przez Zarząd ŁSARN,
10) poufności danych - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,

2. „Dokument" określa tryb postępowania w przypadku, gdy:

1) stan urządzenia, zawartość rejestru danego zbioru danych osobowych, ujawnione metody pracy mogą wskazywać na naruszenie zabezpieczeń tych danych;
2) stwierdzono naruszenie bezpieczeństwa przetwarzanych danych w rejestrze danego zbioru danych.

3. „Dokument" obowiązuje wszystkie osoby pracujące przy przetwarzaniu danych osobowych w ŁSARN.

4. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa w danym rejestrze zbioru danych ŁSARN.

5. Niniejsza polityka bezpieczeństwa dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, rejestrach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych.

6. Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych.

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

1. Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst pierwotny: Dz.U. z 1997r. Nr 133, poz. 883; tekst jednolity: Dz.U. z 2016r. poz. 922),
2. Rozporządzeniem 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 służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024),
3. Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. Nr 229, poz. 1536).

III. Organizacja przetwarzania danych osobowych

1. Administrator danych osobowych

Administrator danych osobowych realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:

1) podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji administratora danych oraz technik zabezpieczenia danych osobowych,
2) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi ich obowiązków,
3) może powołać Administratora Bezpieczeństwa Informacji i upoważnić go do przetwarzania wszystkich zbiorów danych osobowych zaewidencjonowanych w „Rejestrze zbiorów danych osobowych przetwarzanych w ŁSARN".
4) wyznacza administratora systemu jako osobę realizującą zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym administratora danych,
5) wyznacza osobę ds. kadrowych jako właściwą do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych oraz pozostałej dokumentacji z zakresu ochrony danych,
6) zapewnia użytkownikom odpowiednie stanowiska pracy umożliwiające bezpieczne przetwarzanie danych,
7) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych.

2. Administrator systemu

Administrator systemu realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym administratora danych, w tym zwłaszcza:

1) zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora,
2) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,
3) na polecenie Zarządu ŁSARN przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników zgodnie z zasadami określonymi w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
4) nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,
5) podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego,
6) wyrejestrowuje użytkowników na polecenie administratora danych,
7) zakłada konta użytkowników w poszczególnych stacjach roboczych nadając hasła dostępu, znane wyłącznie danemu użytkownikowi. Każda stacja robocza winna posiadać niezależne konto administratora zabezpieczone hasłem, znane tylko administratorowi systemu lub w razie konieczności osobie upoważnionej przez administratora danych osobowych,
8) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje Administratora Danych o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia,

9) sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,
10) podejmuje działania służące zapewnieniu niezawodności zasilania komputerów i innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej.

3. Osoba do spraw kadrowych

Osoba ds. kadrowych realizuje przede wszystkim następujące zadania w zakresie ochrony danych osobowych:

1) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych,
2) występuje z wnioskiem do administratora danych o nadanie upoważnienia do przetwarzania danych osobowych,
3) występuje z wnioskiem (zaakceptowanym przez Zarząd ŁSARN) do administratora systemu o nadanie identyfikatora i przyznanie hasła osobie upoważnionej do przetwarzania danych osobowych,
4) występuje z wnioskiem do administratora danych o odwołanie upoważnienia.

4. Osoba upoważniona do przetwarzania danych osobowych

Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana przestrzegać następujących zasad:

1) może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez administratora danych w upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków. Zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie. Odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych bez konieczności jego pisemnego cofnięcia;
2) musi zachować tajemnicę danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u administratora danych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji;
3) zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej polityki i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
4) stosuje określone przez administratora danych wytyczne mające na celu zgodne z prawem przetwarzanie danych;
5) korzysta z systemu informatycznego administratora danych w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników;
6) zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym.

IV. Infrastruktura przetwarzania danych osobowych

1. Obszar przetwarzania danych osobowych

Wykaz budynków i pomieszczeń wchodzących w skład przetwarzania danych osobowych

Łódzkie Stowarzyszenie Analityków Rynku Nieruchomości Adres: 90-608 Łódź ul. Wólczańska 51	Pomieszczenia: biuro ŁSARN – pomieszczenie nr 23 na II piętrze budynku

UWAGA:
Wskazana powyżej siedziba ŁSARN jest współużytkowana z siedzibą Łódzkiego Stowarzyszenia Rzeczoznawców Majątkowych (w skrócie ŁSRM) w ramach udzielonego przez ŁSRM patronatu.
Komputer stacjonarny zlokalizowany w siedzibie ŁSRM nie jest użytkowany przez ŁSARN, zatem niniejsze procedury nie dotyczą tego urządzenia i zainstalowanego na nim systemu informatycznego.

2. Zbiory danych osobowych

Rejestr zbioru danych osobowych przetwarzanych w ŁSARN (stan na dzień 14.05.2018r)

L.p.	Nazwa zbioru danych osobowych	Nazwa programu stosowanego do przetwarzania	Lokalizacja miejsca przetwarzania (budynek, pomieszczenie, nazwa komputera)	Obowiązek zgłoszenia zbioru danych osobowych GIODO* TAK / NIE
1	kadrowo-płacowy	zbiór aktualnie nie jest prowadzony	*nie dotyczy*	*nie dotyczy*
2	członkowie ŁSARN	zbiór prowadzony w formie tradycyjnej	biuro ŁSARN	NIE - art. 43 ust. 1 pkt 4 ustawy
3	rejestr osób upoważnionych do dostępu do pomieszczeń ŁSARN	zbiór prowadzony w formie tradycyjnej	biuro ŁSARN	NIE - art. 43 ust. 1 pkt 4 ustawy
4	rejestr korespondencji	zbiór prowadzony w formie tradycyjnej	biuro ŁSARN	NIE - art. 43 ust. 1 pkt 4 ustawy

Opis struktury zbiorów danych osobowych przetwarzanych w ŁSARN

L.p.	Nazwa zbioru danych osobowych	Nazwa programu stosowanego do przetwarzania	Opis struktury zbiorów – pól zawierających dane osobowe	Poziom bezpieczeństwa
1	kadrowo-płacowy	zbiór aktualnie nie jest prowadzony	*nie dotyczy*	*nie dotyczy*
2	członkowie ŁSARN	zbiór prowadzony w formie tradycyjnej	nazwiska i imiona, nr uprawnień, nr telefonu, adres poczty elektronicznej, liczba członków Stowarzyszenia	Średni
3	rejestr osób upoważnionych do dostępu do pomieszczeń ŁSARN	zbiór prowadzony w formie tradycyjnej	nazwiska i imiona	Średni

4	rejestr korespondencji	zbiór prowadzony w formie tradycyjnej	nazwa podmiotu, adres, sprawa, nr pisma	Średni

V. Strategia zabezpieczenia danych osobowych (określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych)

1. Zabezpieczenie danych osobowych

1. Administratorem danych osobowych zawartych i przetwarzanych w rejestrach zbiorów danych Łódzkiego Stowarzyszenia Analityków Rynku Nieruchomości jest Zarząd ŁSARN.

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

1) zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym,
2) zapobiegania kradzieży danych,
3) zapobiegania przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

3. Do zastosowanych środków technicznych należy:

1) przetwarzanie danych osobowych w wydzielonych, odpowiednio zabezpieczonych i przystosowanych do tego pomieszczeniach;
2) zabezpieczenie wejścia do pomieszczeń, o których mowa w pkt 1;
3) wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji i nośników danych.

4. Do zastosowanych środków organizacyjnych należą następujące zasady:

1) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych przed jej przystąpieniem do pracy przy przetwarzaniu danych osobowych;
2) przeszkolenie osób, o których mowa w pkt 1, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych;
3) kontrolowanie otwierania i zamykania pomieszczeń wymienionych w pkt 3.1, 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.

5. 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 regulacjami określonymi w „Polityce bezpieczeństwa".

6. Niezwykle ważne dla bezpieczeństwa danych jest wyrobienie przez każdą osobę upoważnioną do przetwarzania danych lub użytkownika nawyku:

1) ustawiania ekranów komputerowych tak, by osoby niepowołane nie mogły oglądać ich zawartości;
2) niepozostawiania bez kontroli dokumentów, nośników danych i sprzętu w hotelach i innych miejscach publicznych oraz w samochodach;
3) dbania o prawidłową wentylację komputerów (nie można zasłaniać kratek wentylatorów meblami, zasłonami lub stawiać komputerów tuż przy ścianie);
4) niepodłączania do listew podtrzymujących napięcie przeznaczonych dla sprzętu komputerowego

innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejniki, czajniki, wentylatory);

5) pilnego strzeżenia akt oraz przenośnych nośników danych elektronicznych;
6) kasowania danych na dyskach przenośnych po ich wykorzystaniu;
7) nieużywania powtórnie dokumentów zadrukowanych jednostronnie;
8) niezapisywania na papierze hasła wymaganego do uwierzytelnienia się w systemie;
9) powstrzymywania się przez osoby upoważnione do przetwarzania danych osobowych od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu (szczególnie komputerów przenośnych), nawet gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych;
10) przestrzegania przez osoby upoważnione do przetwarzania danych osobowych swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń administratora systemu (lub administratora bezpieczeństwa informacji - w przypadku gdy zostanie powołany);
11) opuszczania stanowiska pracy dopiero po aktywizowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób;
12) kopiowania tylko jednostkowych danych (pojedynczych plików). Obowiązuje zakaz robienia kopii całych zbiorów danych lub takich ich części, które nie są konieczne do wykonywania obowiązków przez pracownika. Jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane;
13) nie wynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej;
14) wykonywania kopii roboczych danych, na których się właśnie pracuje, tak często, aby zapobiec ich utracie;
15) chowania do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;
16) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych;
17) zachowania tajemnicy danych, w tym także wobec najbliższych;
18) chowania do zamykanych na klucz szaf wszelkich akt zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;
19) umieszczania kluczy do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy;
20) zamykania okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych;
21) zamykania okien w razie opuszczania pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy;
22) zamykania drzwi na klucz po zakończeniu pracy w danym dniu. Jeśli niemożliwe jest umieszczenie wszystkich dokumentów zawierających dane osobowe w zamykanych szafach, należy powiadomić o tym administratora danych.

2. Postępowanie z nośnikami i ich bezpieczeństwo

Osoby upoważnione do przetwarzania danych osobowych powinny pamiętać zwłaszcza, że:

1) dane z nośników przenośnych niebędących kopiami zapasowymi po wprowadzeniu do systemu informatycznego administratora danych powinny być trwale usuwane z tych nośników przez fizyczne

zniszczenie (np. płyty CD-ROM) lub usunięcie danych programem trwale usuwającym pliki. Jeśli istnieje uzasadniona konieczność, dane pojedynczych osób (a nie całe zbiory czy szerokie wypisy ze zbiorów) mogą być przechowywane na specjalnie oznaczonych nośnikach. Nośniki te muszą być przechowywane w zamkniętych na klucz szafach, nieudostępnianych osobom postronnym. Po ustaniu przydatności tych danych nośniki powinny być trwale kasowane lub niszczone;

2) uszkodzone nośniki przed ich wyrzuceniem należy zniszczyć fizycznie w sposób uniemożliwiający ich odtworzenie;

3) zabrania się powtórnego używania do sporządzania brudnopisów pism jednostronnie zadrukowanych kart, jeśli zawierają one dane chronione. Zaleca się natomiast dwustronne drukowanie brudnopisów pism i sporządzanie dwustronnych dokumentów;

4) wydruki zawierające dane osobowe należy po wykorzystaniu codziennie przed zakończeniem pracy zniszczyć w niszczarce. O ile to możliwe, nie należy przechowywać takich wydruków w czasie dnia na biurku ani też wynosić poza siedzibę administratora danych.

3. Wymiana danych i ich bezpieczeństwo

1. Sporządzanie kopii zapasowych następuje w trybie opisanym w § 6 instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

2. Inne wymogi bezpieczeństwa systemowego są określane w instrukcjach obsługi producentów sprzętu i używanych programów, wskazówkach administratora systemu oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

3. Elektronicznie można przesyłać tylko jednostkowe dane, a nie całe bazy lub szerokie z nich wypisy i tylko w postaci zaszyfrowanej. Chroni to przesyłane dane przed przypadkowym rozproszeniem ich w Internecie.

4. Przed atakami z sieci zewnętrznej wszystkie komputery administratora danych (w tym także przenośne) chronione są środkami dobranymi przez administratora systemu w porozumieniu z administratorem danych osobowych. Ważne jest, by użytkownicy zwracali uwagę na to, czy urządzenie, na którym pracują, domaga się aktualizacji tych zabezpieczeń. O wszystkich takich przypadkach należy informować administratora danych lub administratora systemu i umożliwić im monitorowanie oraz aktualizację środków (urządzeń, programów) bezpieczeństwa.

5. Administrator systemu w porozumieniu z administratorem danych dobiera elektroniczne środki ochrony przed atakami z sieci stosownie do pojawiania się nowych zagrożeń (nowe wirusy, robaki, trojany, inne możliwości włamania się do systemu), a także stosownie do rozbudowy systemu informatycznego administratora danych i powiększania bazy danych. Jednocześnie należy zwracać uwagę, czy rozwijający się system zabezpieczeń sam nie wywołuje nowych zagrożeń.

7. Należy stosować następujące sposoby kryptograficznej ochrony danych:

- przy przesyłaniu danych drogą elektroniczną stosuje się protokół szyfrowania SSL,

- przy przesyłaniu danych osobowych, niezbędnych do wykonania przelewów elektronicznych, używa się zabezpieczeń stosowanych przez bank obsługujący ŁSARN.

4. Przeglądy okresowe zapobiegające naruszeniom obowiązku szczególnej staranności administratora danych (art. 26 ust. 1 ustawy)

1. Administrator danych przeprowadza raz w roku przegląd przetwarzanych danych osobowych pod kątem celowości ich dalszego przetwarzania. Osoby upoważnione do przetwarzania danych osobowych, są obowiązani współpracować z administratorem danych w tym zakresie i wskazywać mu dane osobowe, które powinny zostać usunięte ze względu na zrealizowanie celu przetwarzania danych osobowych lub brak ich adekwatności do realizowanego celu.

2. Administrator danych może zarządzić przeprowadzenie dodatkowego przeglądu w wyżej określonym zakresie w razie zmian w obowiązującym prawie, ograniczających dopuszczalny zakres przetwarzanych danych osobowych. Dodatkowy przegląd jest możliwy także w sytuacji zmian organizacyjnych administratora danych.
3. Z przebiegu usuwania danych osobowych należy sporządzić protokół podpisywany przez administratora danych.

5. Kontrola dostępu do systemu

Poszczególnym osobom upoważnionym do przetwarzania danych osobowych przydziela się konta opatrzone niepowtarzalnym identyfikatorem, umożliwiające dostęp do danych, zgodnie z zakresem upoważnienia do ich przetwarzania. Administrator systemu ds. informatyki po uprzednim przedłożeniu upoważnienia do przetwarzania danych osobowych, zawierającego odpowiedni wniosek pracownika osoby ds. kadr zaakceptowany przez Prezesa ŁSARN przydziela osobie upoważnionej do przetwarzania danych konto w systemie informatycznym, dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem. System musi wymuszać zmianę hasła przy pierwszym logowaniu.
Pierwsze hasło wymagane do uwierzytelnienia się w systemie przydzielane jest przez administratora systemu po odebraniu od osoby upoważnionej do przetwarzania danych oświadczenia zawierającego zobowiązanie do zachowania w tajemnicy pierwszego i następnych haseł oraz potwierdzenie odbioru pierwszego hasła.
Do zagwarantowania poufności i integralności danych osobowych konieczne jest przestrzeganie przez użytkowników swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń administratora danych osobowych.

6. Kontrola dostępu do sieci

System informatyczny posiada dostęp do Internetu tylko w przypadku posiadania przez stację codziennie aktualizowanego systemu antywirusowego. Połączenie z siecią zewnętrzną następuje poprzez bezpieczną bramę internetową posiadającą system antywirusowy, firewall, oraz zabezpieczenia typu IDS/IPS.

7. Komputery przenośne i praca na odległość

1. Urządzenia przenośne oraz nośniki danych wynoszone z siedziby administratora danych nie powinny być pozostawiane bez nadzoru w miejscach publicznych. Komputery przenośne należy przewozić w specjalnie dostosowanych do tego celu torbach.

2. Nie należy pozostawiać bez kontroli dokumentów, nośników danych i sprzętu w hotelach i innych miejscach publicznych ani też w samochodach.

3. Informacje przechowywane na urządzeniach przenośnych lub komputerowych nośnikach danych należy chronić przed uszkodzeniami fizycznymi, a ze względu na działanie silnego pola elektromagnetycznego należy przestrzegać zaleceń producentów dotyczących ochrony sprzętu.

4. Wykorzystywanie komputerów przenośnych administratora danych w miejscach publicznych jest dozwolone, o ile otoczenie, w którym znajduje się osoba upoważniona do przetwarzania danych osobowych, stwarza warunki minimalizujące ryzyko zapoznania się z danymi przez osoby nieupoważnione.
W konsekwencji korzystanie z komputera przenośnego będzie z reguły niedozwolone w restauracjach czy środkach komunikacji publicznej.

5. W domu niedozwolone jest udostępnianie domownikom komputera przenośnego należącego do administratora danych. Użytkownik powinien zachować w tajemnicy wobec domowników identyfikator i hasło, których podanie jest konieczne do rozpoczęcia pracy na komputerze przenośnym administratora danych.

6. Administrator systemu w razie potrzeby wskazuje w dokumencie powierzenia komputera przenośnego osobie upoważnionej do przetwarzania danych osobowych konieczność i częstotliwość sporządzania kopii

zapasowych danych przetwarzanych na komputerze przenośnym oraz określa zasady zwrotu sprzętu w razie zakończenia pracy u administratora danych.

7. W zakresie nieuregulowanym w polityce bezpieczeństwa stosuje się do pracy z wykorzystaniem komputerów przenośnych postanowienia instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

8. Udostępnianie danych osobowych

- Udostępnianie danych osobowych na podstawie ustawy:

  Udostępnianie danych osobowych odbiorcom danych może nastąpić wyłącznie po złożeniu wypełnionego wniosku spełniającego wymogi ustawy.

- Udostępnianie danych osobowych na podstawie ustaw szczególnych:

  Udostępnianie informacji Policji, ABW i innym służbom następuje na zasadach wskazanych w ustawie o ochronie danych osobowych lub przepisach szczególnych.

9. Postępowanie w przypadku naruszenia ochrony danych osobowych

1. W przypadku stwierdzenia :
   - ✓ naruszenia zabezpieczeń systemu informatycznego,
   - ✓ naruszenia technicznego stanu urządzeń,
   - ✓ naruszenia zawartości zbioru danych osobowych,
   - ✓ ujawnienia metody pracy lub sposobu działania programu,
   - ✓ jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
   - ✓ innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.)

<u>każda osoba przetwarzająca dane osobowe jest zobowiązana niezwłocznie powiadomić o tym fakcie administratora danych.</u>

2. W razie niemożliwości zawiadomienia administratora danych lub osoby przez niego upoważnionej, należy powiadomić pracownika biura ŁSARN (jeśli takie stanowisko zostało obsadzone).

3. Do czasu przybycia na miejsce naruszenia danych osobowych osoby upoważnionej przez administratora danych należy:
   - ✓ 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;
   - ✓ udokumentować wstępnie zaistniałe naruszenie;
   - ✓ nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia osoby upoważnionej przez administratora danych.

4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, osoba upoważniona przez administratora danych:
   - ✓ zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania, mając na uwadze ewentualne zagrożenia dla prawidłowości pracy stowarzyszenia;
   - ✓ 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;
   - ✓ rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu lub ujawnieniu ochrony danych osobowych administratora danych;

- ✓ nawiązuje bezpośredni kontakt – jeżeli zachodzi taka potrzeba – ze specjalistami spoza stowarzyszenia.

5. Po wyczerpaniu niezbędnych środków doraźnych związanych z zaistniałym naruszeniem/ujawnieniem ochrony danych osobowych, administrator danych zasięga niezbędnych opinii i proponuje postępowanie naprawcze, w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

6. Administrator danych 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.

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

9. Analiza, o której mowa w pkt. 7, 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.

10. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych

Niezastosowanie się do prowadzonej przez administratora danych polityki bezpieczeństwa przetwarzania danych osobowych, której założenia określa niniejszy dokument, i naruszenie procedur ochrony danych może skutkować odpowiedzialnością karną na podstawie art. 51-52 ustawy.
Przykładowo przestępstwo można popełnić wskutek:

1) stworzenia możliwości dostępu do danych osobowych osobom nieupoważnionym albo osobie nieupoważnionej,

2) niezabezpieczenia nośnika lub komputera przenośnego,

3) zapoznania się z hasłem innej osoby upoważnionej wskutek wykonania nieuprawnionych operacji w systemie informatycznym administratora danych.

11. Przeglądy polityki bezpieczeństwa i audyty systemu

Polityka bezpieczeństwa powinna być poddawana przeglądowi przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych administrator danych może zarządzić przegląd polityki bezpieczeństwa stosownie do potrzeb.

Administrator danych analizuje, czy polityka bezpieczeństwa i pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do:

1) zmian w budowie systemu informatycznego,

2) zmian organizacyjnych administratora danych, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych,

3) zmian w obowiązującym prawie.

VI. Postanowienia końcowe

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści.

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

3. Ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych, zobowiązany jest prowadzić administrator danych.

4. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie.

5. Orzeczona kara wobec osoby uchylającej się od powiadomienia administratora danych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst pierwotny: Dz. U. z 1997 r. Nr 133, poz. 883; tekst jednolity: Dz. U. z 2016 r. poz. 922) oraz możliwości wniesienia wobec niej przez stowarzyszenie sprawy z powództwa cywilnego o zrekompensowanie poniesionych strat.

6. Wszystkie regulacje dotyczące systemów informatycznych określone w „Polityce bezpieczeństwa" dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.

7. „Polityka bezpieczeństwa" wchodzi w życie w terminie określonym w treści Uchwały Zarządu ŁSARN. Zmiany w „Polityce bezpieczeństwa" będą wchodzić w życie w terminach określonych w Uchwałach Zarządu ŁSARN dotyczących wprowadzenia zmian w dokumencie.