POLSKIE DRUŻYNY STRZELECKIE (PDS)

Warszawa, dnia, 15. 01. 2020 r.

„ZATWIERDZAM”

Jan Grudniewski

NADAWANIE
„UPOWAŻNIEŃ do przetwarzania danych osobowych” tzw.: RODO. Kompendium wiedzy

Rozpoczęto:	15. 01. 2020 r.
Zakończono:	.... 2020 r.
Zawiera stron:	

KATEGORIA ARCHIWALNA: B **– 10**

WARSZAWA

SPIS TREŚCI

ROZDZIAŁ I
POSTANOWIENIA OGÓLNE

1. Nadawanie „Upoważnień do przetwarzania danych osobowych”

1. Komendant Naczelny Stowarzyszenia Polskie Drużyny Strzeleckie (PDS) **–** po wyznaczeniu Inspektora Ochrony Danych Osobowych (w skrócie I ODO) upoważnił Inspektora do działania w problematyce ochrony danych osobowych, w związku z czym na wniosek Komendanta Naczelnego nadaje się określonej Osobie uprawnienia użytkownika systemu informatycznego lub akceptuje zmianę / wycofanie uprzednio nadanych uprawnień, poprzez zatwierdzenie formularza „Upoważnienia…”.

2. Zastępcami w sprawach Ochrony Danych Osobowych w zależności od sytuacji są i mogą być: Członkowie Zarządu, jak i Komendanci (Dowódcy) poszczególnych Oddziałów*; Brygad*; Batalionu*; Regimentu*… PDS, którzy również wykonywać będą zadania ABI, jak i odpowiadać za prawidłowe funkcjonowanie Systemu Informatycznego w ich Oddziale*; Brygadzie*; Batalionie*; Regimencie*… Są oni wyznaczeni w „Zarządzeniu…” .

3. Zakres nadawanych uprawnień musi być uzasadniony charakterem obowiązków służbowych potencjalnego użytkownika systemu.

4. Pracownicy zajmujący samodzielne stanowiska w strukturze organizacyjnej Stowarzyszenia PDS występują osobiście do Administratora o nadanie *(zmianę/wycofanie)* dotyczących ich uprawnień.

5. „UPOWAŻNIENIE…” sporządza się w dwóch (2 Egz.) egzemplarzach:

– pierwszy przekazywany jest po rozpatrzeniu sprawy i po zatwierdzeniu osobie upoważnianej, natomiast

– drugi przekazywany jest Inspektorowi ODO.

6. Administrator Systemu Informatycznego, na podstawie zatwierdzonego „UPOWAŻNIENIA…”, dokonuje czynności związanych z przyznaniem (zmianą /wycofaniem) użytkownikowi uprawnień, a następnie informuje Administratora Bezpieczeństwa Informacji o nadaniu uprawnień określonemu użytkownikowi.

7. Inspektor Ochrony Danych Osobowych, prowadzący „Ewidencję osób upoważnionych do przetwarzania danych osobowych”, dokonuje w niej stosownych adnotacji oraz

– jeśli nadanie uprawnień związane jest z zatrudnieniem po raz pierwszy osoby w Stowarzyszeniu

– przeprowadza szkolenie użytkownika w zakresie zapoznania (zaznajomienia) go z przepisami Ustawy o ochronie danych osobowych oraz obowiązującymi procedurami w zakresie bezpieczeństwa informacji.

8. Komendanci (Dowódcy) Oddziału*; Brygady*; Batalionu*; Regimentu*… zobowiązani są do dokonywania okresowych analiz uprawnień przydzielonych użytkownikom, nadzoru nad wykorzystywaniem tych uprawnień oraz aktualizacji uprawnień, nie później niż w ciągu dwóch dni po zaistnieniu zdarzenia powodującego konieczność aktualizacji.

9. W przypadku rozwiązania stosunku zatrudnienia lub zakończenia okresu stażu / praktyki osoba, której nadano uprawnienia użytkownika systemu informatycznego Stowarzyszenie PDS obowiązana jest do uzyskania na „Karcie obiegowej” podpisu Administratora Bezpieczeństwa Informacji, co jest podstawą do wyrejestrowania osoby z systemu oraz wykreślenia jej z bazy aktualnych użytkowników.

2. Wymagania dotyczące identyfikatorów użytkowników

Identyfikator użytkownika spełnia następujące wymagania:

1. jest kombinacją Imienia i Nazwiska użytkownika systemu,
2. jest niepowtarzalny w skali systemu,
3. jednym identyfikatorem posługiwać może się wyłącznie jeden użytkownik,
4. każdy z użytkowników jest odpowiedzialny za wszystkie czynności wykonywane w systemie przy pomocy identyfikatora, którym się posługuje.

3. Nadawanie dostępu do systemu informatycznego

Ustawodawca bezwzględnie nakazał kontrolę nad tym, kto ma dostęp do danych osobowych. W przypadku jego realizacji za pośrednictwem systemu informatycznego ten wymóg rozliczalności, można spełnić z całą starannością i pełnym zakresem kontroli. Przyznanie osobie możliwości dostępu do danych osobowych przetwarzanych w systemie informatycznym jest procesem dwustopniowym.

1) Nadanie przez Administratora Danych Osobowych dokumentu pod nazwą: „Upoważnienie do przetwarzania danych osobowych", które musi zawierać:

a) wskazanie, że uprawnienie ma być realizowane przy pomocy systemu informatycznego,

b) wskazanie zbioru danych, do którego ma być udzielony dostęp,

c) określenie dopuszczalnych czynności przetwarzania w systemie informatycznym, np.: wprowadzanie, przeglądanie, modyfikowanie, drukowanie, udostępnianie, anonimizowanie, usuwanie, itp.

2) Utworzenie przez Administratora Systemu Informatycznego indywidualnego konta „Użytkownika systemu informatycznego", które charakteryzuje się:

a) niepowtarzalnym „Identyfikatorem", stanowiącym ciąg znaków literowych, cyfrowych lub innych, jednoznacznie pozwalającym na identyfikację osoby upoważnionej do przetwarzania danych osobowych w systemie informatycznym,

b) zakresem dostępu do określonych „Baz danych" oraz uprawnień do ich przetwarzania nie mogącym wykraczać poza ten wyznaczony przez „Upoważnienie do przetwarzania danych osobowych".

Najpopularniejszą metodą weryfikacji praw dostępu do systemu informatycznego, jedyną wskazaną bezpośrednio przez Rozporządzenie ws. warunków technicznych, jest użycie „HASŁA", tj.: unikalnego i poufnego ciągu znaków literowych, cyfrowych lub innych. Siła „HASŁA" wykorzystywanego do uwierzytelnianie użytkowników w systemie informatycznym jest jedynym szczegółowo określonym wymogiem zabezpieczeń:

- Długość: co najmniej 8 znaków;
- Budowa: małe i wielkie litery oraz cyfry lub znaki specjalne;
- Ważność: maksymalnie 30 dni.

Nie ma obowiązku, żeby system informatyczny automatycznie wymuszał na użytkownikach te wymagania, jednak taka funkcjonalność pozwala na skuteczne zarządzanie ich realizacją, uniemożliwiając jawne lub przypadkowe łamanie tego nakazu. Należy w tym miejscu wskazać również, że o poufności hasła nie decyduje wyłącznie jego nieudostępnianie innym osobom, ale również jego treść. Stąd też użytkownik systemu informatycznego ma obowiązek stosować hasła trudne do odgadnięcia.

W szczególności nie mogą nimi być:

- nazwisko, imię, adres, numer rejestracyjny prywatnego samochodu, PESEL, NIP, numer telefonu, itp.;
- słowo w żadnym popularnym języku;
- nazwa geograficzna, termin techniczny lub określenie potoczne;
- sekwencja kolejnych znaków na klawiaturze; a także dowolny spośród wymienionych uzupełnionym na początku lub końcu cyfrą lub znakiem specjalnym.

Omawiając zasady udzielania dostępu do systemu informatycznego nie można pominąć kwestii odbierania tych praw, choć nie została ona wprost opisana w Rozporządzeniu w sprawie warunków technicznych.

Zablokowanie konta użytkownika uniemożliwiające mu jakikolwiek dostęp do systemu informatycznego lub wykonywanie w nim czynności przetwarzania danych osobowych może mieć charakter:

1) trwały, w sytuacji ustania ważności „Upoważnienia do przetwarzania danych osobowych", np.: rozwiązanie stosunku pracy;
2) czasowy, w sytuacjach szczególnych, np.:
   a) nieobecności użytkownika w pracy trwającej dłużej niż 1 miesiąc;
   b) zawieszeniu użytkownika w pełnieniu obowiązków służbowych;
   c) wypowiedzenia użytkownikowi umowy o pracę;
   d) wszczęcia wobec użytkownika postępowania dyscyplinarnego.

4. Wzór „Upoważnienie..." dla osoby funkcyjnej Polskich Drużyn Strzeleckich

WZÓR

....., dnia .....

UPOWAŻNIENIE

Niniejszym:

1. Upoważniam Pana* Panią* ..... do przetwarzania danych osobowych metodami tradycyjnymi w związku z wykonywaniem w Stowarzyszeniu PDS obowiązków pracowniczych / stażysty* / praktykanta* / umowy cywilnoprawnej*, zgodnie z zakresem powierzonych Pani* / Panu* obowiązków służbowych na zajmowanym stanowisku pracy* / programem stażu* / programem praktyki* / postanowieniami umowy cywilnoprawnej*;

2. Upoważniam Panią* / Pana* ..... do obsługi systemu informatycznego i urządzeń wchodzących w jego skład;

3. Nadaję Pani* / Panu* Identyfikator: .....;

4. Zakres uprawnień związanych z powierzonym Pani* / Panu* dostępem do obsługi systemu informatycznego obejmuje:

Nazwa systemu	Opis uprawnienia	TAK	NIE	Uwagi
	Zarządzanie bazą danych			
	Dodawanie i modyfikacje danych			
	Edycja danych *(w tym, drukowanie, usuwanie)*			
	Przeglądanie danych na ekranie			
	Wykonywanie kopii archiwalnych			
	Wypełnianie „Wniosków…" na mianowanie…, odznaczenie… itd.			
	Inne:			

Upoważnienie traci ważność z dniem rozwiązania umowy o pracę* / umowy cywilnoprawnej* / zakończenia stażu* / praktyki* oraz zmiany zakresu upoważnienia.

.....
podpis i pieczęć upoważniającego

** - Niepotrzebne skreślić*

ROZDZIAŁ II
PROCEDURY PRZYDZIELANIA I ZARZĄDZANIA HASŁAMI UŻYTKOWNIKÓW. PRZYDZIELANIE HASEŁ

1. Przydzielanie haseł

Przydzielanie haseł jest kontrolowane przez formalny proces zarządzający, zawierający następujące wymagania:

- Użytkownicy podpisują „Zobowiązania do zachowania w tajemnicy danych osobowych i stosowanych w Stowarzyszeniu Polskich Drużyn Strzeleckich i sposobów ich zabezpieczenia”

  (w tym pojęciu mieści się ochrona haseł osobistych)

  – „Zobowiązania…” przechowywane są w ich można powiedzieć „Aktach osobowych”;
- Administrator Systemu Informatycznego zapewnia natychmiastową zmianę hasła początkowego (instalacyjnego), przydzielonego użytkownikowi, na nowe przez niego wybrane;
- Hasła są przechowywane w systemie informatycznym w postaci chronionej.

2. Zasady posługiwania się HASŁAMI

Na wszystkich użytkownikach systemu informatycznego Stowarzyszenia Polskich Drużyn Strzeleckich spoczywają, w zakresie zasad posługiwania się HASŁAMI, następujące obowiązki:

1. Pierwsze HASŁO (instalacyjne) dla każdego z użytkowników zakłada Administrator Systemu Informatycznego podczas wprowadzania do systemu identyfikatora użytkownika;
2. Użytkownik, w obecności Administratora Systemu Informatycznego, zmienia hasło na własne, samodzielnie wybrane i nie ujawnia tego hasła jakimkolwiek osobom;
3. Hasła generowane są samodzielnie przez użytkowników z cyfr i liter alfabetu łacińskiego.
4. Hasło musi składać się **z co najmniej 8** znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne (np.: !@#<>);
5. Zmiana hasła następuje nie rzadziej niż co 30 dni, a ponadplanowo w przypadku podejrzenia lub stwierdzenia, że z hasłem zapoznać mogły się osoby trzecie;
6. Użytkowników systemu informatycznego obowiązuje utrzymywanie haseł w tajemnicy (również po upływie ważności haseł) oraz unikanie zapisywania haseł na papierze, chyba, że mogą być one przechowywane w sposób bezpieczny.

ROZDZIAŁ III
ZASADY BEZPIECZEŃSTWA W PRACY Z KOMPUTERAMI PRZENOŚNYMI

W trakcie używania przenośnych urządzeń komputerowych typu:

* laptop; * tablet; * notebook; * iPiod;

* smartfon, itp. urządzenia z możliwością dostępu do „Internetu" należy zwracać szczególną uwagę na to, aby nie ujawniać informacji prawnie chronionych.

W Stowarzyszeniu Polskich Drużyn Strzeleckich obowiązują następujące zasady bezpieczeństwa odnoszące się do korzystania z komputerów przenośnych:

- osoba użytkująca komputer przenośny, zawierający dane osobowe lub inne informacje podlegające ochronie, ma obowiązek zachowania szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania poza obszarem administracyjnym Stowarzyszenia Polskich Drużyn Strzeleckich w tym celu stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych;
- w celu ochrony przed nieuprawnionym dostępem stosuje się zabezpieczenie komputera mechanizmem kontroli dostępu do danych:

  (Identyfikator i Hasło);
- w komputerze przenośnym zainstalowane jest oprogramowanie antywirusowe;
- wprowadzono zakaz niekontrolowanego pozostawiania komputerów zawierających informacje podlegające ustawowej ochronie w samochodach i innych środkach transportu, (pokojach hotelowych, centrach konferencyjnych, itp.);
- organizowane są szkolenia dla personelu używającego komputerów przenośnych dotyczące obowiązku stosowania wyżej określonych środków bezpieczeństwa.

ROZDZIAŁ IV
ZABEZPIECZENIE PRZED ZAGROŻENIAMI Z INTERNETU

1. Zagrożenia z Internetu

Systemy informatyczne w związku z ich powszechnym podłączeniem do sieci publicznej (Internet), w sposób szczególny są podatne na różnego rodzaju niepożądane działania, które mogą bezpośrednio lub pośrednio zagrażać bezpieczeństwu przetwarzanych w nich danych osobowych.

W związku z powyższym, zgodnie z dyspozycją Rozporządzenia w sprawie warunków technicznych, Administrator Danych Osobowych jest zobowiązany do zabezpieczenia systemu informatycznego przed działaniem szkodliwego oprogramowania, tzw.: „wirusów", lub innego czynnika – np.: *hacking*, których celem jest uzyskanie nieuprawnionego dostępu do procesu przetwarzania danych osobowych.

2. „Działania niepożądane" w obszarze zagrożeń z Internetu

Za „działania niepożądane" w tym obszarze należy uznać m.in. takie, które:

- powodują nieautoryzowaną samo instalację oprogramowania;
- prowadzą do uszkodzenia lub modyfikacji pamięci komputerowej, plików systemowych lub oprogramowania;
- służą do omijania lub przełamywania zabezpieczeń i / lub praw dostępu;
- wymuszają wykorzystanie większej ilości zasobów niż jest to niezbędne do zapewnienia prawidłowego działania systemu informatycznego;

- powodują zakłócenia w normalnym działaniu systemu informatycznego;
- prowadzą do naruszenia zasad integralności, rozliczalności, dostępności i poufności danych osobowych przetwarzanych w systemie informatycznym.

Zabezpieczenie systemu informatycznego przed podatnością na działania niepożądane może składać się z bardzo wielu elementów zabezpieczających – organizacyjnych, programowych i fizycznych.

Dobór środków ochrony powinien uwzględniać:

- ⇨ rodzaj przetwarzanych danych osobowych, w tym ich „wrażliwość" informacyjną;
- ⇨ organizację systemu informatycznego, w tym jego wielkość, skomplikowanie i rozproszenie;
- ⇨ sposób podłączenia do Internetu;
- ⇨ specyfikę procesu przetwarzania, w tym konieczność przesyłania danych za pośrednictwem „Internetu" i wykorzystywanie komputerowych nośników danych;
- ⇨ dotychczasowe zdarzenia niepożądane, bez względu na to czy pochodziły z „Internetu".

Podstawowym warunkiem ochrony systemu informatycznego przed możliwością wystąpienia sytuacji niepożądanych jest systematyczna aktualizacja oprogramowania.

Wszelkie aplikacje informatyczne mają zamierzone lub przypadkowe błędy, luki w oprogramowaniu, które mogą pozwolić na dostęp do danych bez uwierzytelniania, tzw.: „wejście tylnymi drzwiami". Szczególnie w przypadku oprogramowania pochodzącego z nieznanego źródła może ono zawierać dodatkowo niebezpieczne kody lub ukryte szpiegowskie funkcjonalności.

W związku z powyższym jest niezbędne, aby do przetwarzania danych osobowych wykorzystywać wyłącznie legalne oprogramowanie, gdyż tylko takie umożliwia uzyskiwanie zatwierdzonych przez producenta nowych wersji, poprawek lub aktualizacji usuwających stwierdzone wady i słabości.

3. Sposób przechowywania wydruków z danymi osobowymi

1. Wydruki zawierające dane osobowe, na przykład Kandydatów, Członków PDS, „Osób odznaczonych" i inne przechowywane są w zamykanej(-ych) na klucz w szafie(-ach) znajdujących się w pomieszczeniu(-ach) Stowarzyszenia Polskich Drużyn Strzeleckich. Wydruki o szczególnie istotnym znaczeniu przechowywane są w sejfie lub w metalowej(-ych) szafie(-ach) lub biurku(-ach) zamykanym na klucz.
2. Użytkownik dokonujący wydruku jest właścicielem wytworzonego dokumentu.
3. Użytkownik dokonujący wydruku przy wykorzystaniu drukarki sieciowej zobowiązany jest udać się niezwłocznie do pomieszczenia usytuowania drukarki i przejąć wydrukowany dokument.
4. Każdy pracownik, który napotka wydruk, nośnik elektroniczny, czy inny dokument pozostawiony bez dozoru jest zobowiązany zabezpieczyć go i przekazać Administratorowi Bezpieczeństwa Informacji lub Lokalnemu ABI.

4. Dokumentowanie systemu ochrony danych osobowych

Administrator Danych Osobowych ma ustawowy obowiązek opracowania, wdrożenia i prowadzenia dokumentacji systemu ochrony danych osobowych.

System ochrony danych osobowych to najogólniej zbiór celowo zdefiniowanych elementów organizacyjnych i technicznych, które wzajemnie ze sobą powiązane funkcjonują jako jedna całość, wspólnie realizując jeden cel – zapewnienie niezakłóconego procesu przetwarzania danych osobowych i minimalnego akceptowalnego poziomu ich odporności na działania niepożądane.

5. Wymogi prowadzenia dokumentacji

Na wymóg prowadzenia dokumentacji nie ma wpływu:

- rodzaj przetwarzanych danych osobowych;
- cel przetwarzania;
- wielkość przetwarzanych zbiorów danych osobowych;
- sposób przetwarzania.

Zgodnie z dyspozycją Rozporządzenia w sprawie dokumentacji… w skład obowiązkowej dokumentacji systemu ochrony Danych Osobowych mogą wchodzić:

1) „Polityka bezpieczeństwa”;
2) „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”.

Należy jednak uznać, że nie jest to zbiór zamknięty i powinien być rozszerzony na pozostałe dokumenty określone wprost lub wynikające z przepisów Ustawy:

3) „Upoważnienia do przetwarzania danych osobowych”;
4) „Ewidencja upoważnień do przetwarzania danych osobowych”;
5) „Zobowiązania do zachowania poufności”.

Ponadto ze względów organizacyjnych skład dokumentacji może być jeszcze szerszy i obejmować dokumenty niezbędne do prawidłowego zarządzania procesem przetwarzania danych osobowych w organizacji. Istotna jest przede wszystkim zawartość merytoryczna dokumentacji, a nie liczba jej składników. Przede wszystkim jednak podstawowym wymogiem stawianym dokumentacji systemu ochrony danych osobowych, jest jej przejrzystość i kompleksowość, dzięki której osoby zarządzające, nadzorujące i bezpośrednio przetwarzające dane osobowe będą wiedziały, jak wypełniać obowiązki ustawowe na swoim stanowisku pracy.

6. Zabezpieczenie fizyczne pomieszczeń, w których odbywa się przetwarzanie danych osobowych

Stowarzyszenie Polskich Drużyn Strzeleckich wykorzystuje w celu ochrony obiektu, zgromadzonych w nim dokumentów i mienia oraz zapewnienia bezpieczeństwa pracownikom i interesantom:

- ⇨ całodobową ochronę fizyczną wykonywaną przez pracowników ochrony koncesjonowanego Przedsiębiorcy wykonującego na rzecz Stowarzyszenia Polskich Drużyn Strzeleckich usługę ochrony fizycznej (indywidualne przypadki),
- ⇨ system sygnalizacji włamania – system jest całodobowo monitorowany przez Stację Monitorowania Alarmów koncesjonowanego Przedsiębiorcy wykonującego na rzecz Stowarzyszenia usługę ochrony fizycznej,
- ⇨ system telewizji dozorowej,
- ⇨ środki zabezpieczenia mechanicznego,
- ⇨ procedury wewnątrz organizacyjne, obowiązujące pracowników, mające zapewnić pożądany stan bezpieczeństwa Stowarzyszenia Polskich Drużyn Strzeleckich

Dokumenty i materiały podlegające rygorom przepisów o ochronie danych osobowych lub zawierające inne informacje prawnie chronione są zabezpieczone zgodnie z obowiązującymi w tym zakresie regulacjami Ustawowymi, oraz Dekretami Komendanta Naczelnego Polskich Drużyn Strzeleckich, Uchwałami Stowarzyszenia.

7. Bezpieczeństwo fizyczne

Dane osobowe są przykładem dobra niematerialnego, którego istotą jest przede wszystkim zawartość informacyjna, a nie fizyczny obiekt. To ich treść wyznacza obowiązek ochrony, jej zakres i odpowiedzialność. Niemniej jednak musimy pamiętać o tym, że proces przetwarzania Danych Osobowych dokonuje się poprzez ich materialne nośniki – papierowe, czy elektroniczne. Stąd ochrona danych osobowych przed działaniami niepożądanymi musi uwzględniać także kwestie fizycznego dostępu do tych nośników. Niestety prawie zupełne pominięcie przez ustawodawcę kwestii „bezpieczeństwa fizycznego" powoduje, że w większości publikacji książkowych kwestia ta jest nadmiernie bagatelizowana.

W praktyce można więc spotkać się z takim podejściem, że Administrator Danych Osobowych nie ma żadnych obowiązków w tym zakresie. Nic bardziej mylnego. Wystarczy przypomnieć sobie nakazy „szczególnej staranności" (Art.), oraz „odpowiedniej ochrony", które nie mają ograniczenia rzeczowego. Dotyczą on bezwzględnego obowiązku zabezpieczenia przetwarzanych danych osobowych w odniesieniu do wszystkich rodzajów zagrożeń, dając Administratorowi Danych Osobowych swobodę wyłącznie w kwestii doboru środków bezpieczeństwa.

Zabezpieczenia, a przede wszystkim ich poziom, należy dobierać opierając się na zasadzie adekwatności w stosunku do istniejących zagrożeń, wynikających z:

- specyfiki działalności Firmy;
- lokalizacji „Strefy przetwarzania";
- kategorii przetwarzanych danych osobowych, tj.: zwykłych, czy „wrażliwych";
- sposobu przetwarzania danych osobowych, tj.: wielkości zbiorów tradycyjnych oraz budowy systemu informatycznego.

8. Wyznaczenie strefy przetwarzania danych osobowych

Podstawowym środkiem bezpieczeństwa decydującym o skuteczności ochrony przetwarzanych danych osobowych przed dostępem do nich osób nieuprawnionych jest wyznaczenie miejsc podlegających obowiązkowemu nadzorowi.

Administrator Danych Osobowych zobowiązany jest do określenia „Strefy przetwarzania", tj.: obszaru administracyjnego:

- w których jest możliwy bezpośredni lub pośredni dostęp do danych osobowych;
- dostępnego w sposób nieograniczony wyłącznie dla osób posiadających „Upoważnienia do przetwarzania danych osobowych".

W skład „Obszaru przetwarzania" powinny więc wejść wszystkie pomieszczenia biurowe i techniczne, w których są przetwarzane dane osobowe. Nie są to jednak tylko te pomieszczenia, w których wykonuje się bieżące operacje na danych osobowych, tj.: stanowiska pracy biurowej, ale także te miejsca, gdzie są przechowywane nośniki tych danych osobowych, np.: szafy dokumentacji papierowej, jak również te odpowiadające za funkcjonowanie systemu informatycznego, np.: serwerownia.

W związku z koniecznością zapewnienia dostępu do „Strefy przetwarzania", ograniczonego wyłącznie do osób mających „Upoważnienie do przetwarzania danych osobowych" lub pod ich bezpośrednim nadzorem, jest zasadnym, żeby nie uogólniać jej granic do całego budynku biurowego. Takie pozornie upraszczające podejście może spowodować konieczność zabezpieczenia także tych pomieszczeń, w których nie jest realizowany proces przetwarzania danych osobowych, tj.: pokoi socjalnych, łazienek czy całych ciągów komunikacyjnych.

ROZDZIAŁ V
ZABEZPIECZENIE POMIESZCZEŃ BIUROWYCH

Pierwszym z zabezpieczeń jest system kontroli dostępu, który, w odniesieniu do wskazanego uprzednio obowiązku zabezpieczenia „Strefy przetwarzania" przed dostępem osób nieuprawnionych, uchodzi w istocie za najważniejszy.

Zasadniczo przyjmuje się, że obiekt biurowy powinien mieć, o ile jest to fizycznie możliwe, wydzielone obszary:

OGÓLNODOSTĘPNY i KONTROLOWANY, a przejście między nimi powinno być właściwie nadzorowane. Nie ma konieczności stosowania elektronicznego systemu kontroli dostępu, natomiast nieograniczony dostęp do pomieszczeń biurowych mogą mieć wyłącznie osoby „Upoważnione do przetwarzania danych osobowych", wykonujące w nich swoje obowiązki służbowe. Na nich też ciąży obowiązek kontroli dostępu do tych pomieszczeń, tj.: inne osoby mogą w nich przebywać tylko pod nadzorem.

Przykład z życia. Studium przypadku:

Pracownik marketingu przyjmując klienta, nie może pozostawić go samego w pomieszczeniu biurowym, w sytuacji konieczności udania się do magazynu po materiały reklamowe. Nie może tego zrobić nawet wtedy, kiedy stanowisko komputerowe jest wyłączone, a dokumentacja papierowa umieszczona w zamkniętej szafie.

Z kontrolą dostępu jest nieodzownie związany problem zarządzania kluczami. Powinny być one dostępne wyłącznie dla osób pracujących w konkretnym pomieszczeniu biurowym, a jednocześnie przechowywane w sposób uniemożliwiający ich zabranie przez osoby nieuprawnione.

W przypadku zabezpieczeń przed zagrożeniami związanymi z nieuprawnionym dostępem do „strefy przetwarzania", ale będącym skutkiem działań o charakterze przestępczym (np.: włamanie), należy przeanalizować ich ryzyko i dobrać odpowiednie środki, np.: drzwi i okna o podwyższonej odporności na włamanie lub elektroniczny system alarmowy.

Ponadto należy zabezpieczyć pomieszczenia „Strefy przetwarzania" przed działaniami spowodowanymi siłami przyrody oraz awariami technicznymi, tj.: pożar, czy zalanie. W pierwszym przypadku będzie to przynajmniej właściwe rozmieszczenie ręcznego sprzętu gaśniczego. W drugim zaś unikanie lokalizacji pomieszczeń biurowych w bezpośredniej bliskości instalacji wodociągowych i kanalizacyjnych. Dobór zabezpieczeń jest autonomiczną decyzją Administratora Danych Osobowych, za którą ponosi on samodzielną odpowiedzialność.

Niedopuszczalne jest jednak przetwarzanie Danych Osobowych w pomieszczeniach niemających żadnych, chociażby najbardziej podstawowych, zabezpieczeń fizycznych uniemożliwiających dostęp do nich osób nieuprawnionych oraz ochrony przed skutkami innych działań niepożądanych.

ROZDZIAŁ VI
ZABEZPIECZENIE POMIESZCZEŃ SPECJALNYCH

W przypadku pomieszczeń „specjalnych" ich zabezpieczenia powinny być adekwatne do ich roli w procesie przetwarzania danych osobowych. Przede wszystkim muszą cechować się wyższym poziomem ochrony dla znajdujących się w nich zasobów, niż te stosowane dla zwykłych pomieszczeń biurowych.

Pomieszczenie serwerowni (o ile takie są), to najbardziej newralgiczny punkt systemu informatycznego. Znajdują się w nim wszystkie zbiory danych osobowych oraz urządzenia i aplikacje pozwalające na ich przetwarzania.

Mając na uwadze znaczenie serwera dla całokształtu ochrony danych osobowych oraz jego podatność na różnego rodzaju zagrożenia, należy przyjąć, że pomieszczenie serwerowni powinno być wyposażone w:

1) specjalne drzwi i okna:
    a) antywłamaniowe;
    b) ognioodporne;
2) elektroniczne systemy wspomagające:
    a) kontroli dostępu;
    b) sygnalizacji włamania i napadu;
    c) dozoru wizyjnego;
    d) sygnalizacji pożarowej;
    e) automatycznego gaszenia pożaru;
    f) sygnalizacji zalania;
3) zabezpieczenie przed silnym polem elektromagnetycznym;
4) klimatyzację i wentylację;
5) podłogę techniczną.

Szczegółowy rodzaj i klasę wskazanych zabezpieczeń należy dostosować do oceny zagrożeń i wartości przetwarzanych danych osobowych. Zbliżony poziom zabezpieczeń – dostosowany do innej specyfiki zagrożeń – należy zastosować względem pomieszczeń, w których znajdują pozostałe kluczowe elementy systemu informatycznego tzn.: uszkodzone komputery, dyski i innego rodzaju nośniki, które mogą zawierać nieusunięte bazy danych, a przede wszystkim kopie bezpieczeństwa zbiorów Danych Osobowych i aplikacji służących do ich przetwarzania.

ROZDZIAŁ VII
PRZECHOWYWANIE DOKUMENTACJI TRADYCYJNEJ

Podobnie jak w przypadku zabezpieczeń pomieszczeń „Strefy przetwarzania", tak również w kwestii przechowywania dokumentacji tradycyjnych, tj.: akta, księgi, kartoteki, Administrator Danych / Administrator Bezpieczeństwa Informacji otrzymał całkowitą swobodę w zakresie doboru sposobu ich ochrony przed działaniami niepożądanymi:

- nieuprawnionym przejęciem;
- nieuprawnioną modyfikacją ich zawartości;
- uszkodzeniem uniemożliwiającym odczytanie;
- całkowitym zniszczeniem fizycznym.

W związku z powyższym całkowicie niedopuszczalne jest przechowywanie dokumentacji zawierającej dane osobowe bez jakiegokolwiek ich zabezpieczenia, np.: na otwartych regałach.

Przyjmuje się powszechnie, że dla zachowania ustawowych wymogów oraz faktycznego jej bezpieczeństwa, dokumentację tradycyjną należy umieszczać w zamykanych na klucz szafach i szufladach mebli biurowych. Niemniej jednak część akt papierowych z uwagi na wrażliwość zawartych w nich danych osobowych, np.: dokumentacja medyczna, powinna być przechowywana w szafach metalowych o podwyższonej klasie odporności na włamanie.

ROZDZIAŁ VIII
POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Zasady postępowania w przypadku naruszenia ochrony danych osobowych

Na naruszenie bezpieczeństwa danych osobowych (lub możliwość wystąpienia takiego zagrożenia) mogą wskazywać:

- nietypowy stan pomieszczeń wchodzących w skład obszaru przetwarzania (otwarte pomieszczenia, okna, drzwi od szaf i biurek, włączone urządzenia),
- zaginięcie sprzętu lub nośników informacji,
- nieuzasadnione modyfikacje lub usunięcie danych,
- nieprawidłowe lub nietypowe działanie systemu informatycznego,
- wykrycie wirusa w systemie,
- obecność podejrzanych plików w poczcie elektronicznej,
- nietypowe komunikaty wyświetlane na monitorze,
- ujawnienie przetwarzanych danych lub procedur ochrony przetwarzania osobom nieupoważnionym,
- ujawnienie istnienia nieautoryzowanych kont dostępu do danych,
- przesłanie danych do niewłaściwego adresata,
- znalezienie poza obszarem przetwarzania dokumentów, wydruków, dyskietek i innych nośników informacji,
- niekontrolowany lub niezgodny z obowiązującymi procedurami pobyt w obszarze przetwarzania osoby nieupoważnionej.

2. Postępowanie osób zatrudnionych przy przetwarzaniu danych osobowych

1. Użytkownicy systemu informatycznego po stwierdzeniu (lub podejrzeniu) wystąpienia incydentu naruszenia bezpieczeństwa informacji są zobowiązani do:

a) powstrzymania się od wszelkich czynności w pomieszczeniu przetwarzania danych, mogących zatrzeć ślady naruszenia bezpieczeństwa informacji,

b) niepodejmowania działań w systemie informatycznym, w tym do nieusuwania podejrzanego oprogramowania,

c) stosowania się (po zgłoszeniu incydentu) do poleceń Administratora Systemu Informatycznego,

d) sporządzenia na polecenie Administratora Systemu Informatycznego notatki o incydencie (zdarzeniu).

2. Użytkownicy są zobowiązani do natychmiastowego zgłaszania zaistniałych przypadków naruszenia zasad bezpieczeństwa. Wszyscy użytkownicy są zapoznani z procedurami zgłaszania naruszeń bezpieczeństwa:

a) w każdym pomieszczeniu obszaru przetwarzania dostępny jest wykaz telefonów kontaktowych do Administratora Systemu Informatycznego, Administratora Bezpieczeństwa Informacji, lokalnych ABI oraz osób zastępujących ich w razie nieobecności;

b) kwestie zgłaszania incydentów są przedmiotem szkoleń organizowanych dla pracowników i innych osób dopuszczonych przez:

Administratora Bezpieczeństwa Informacji;

Administratora Systemu Informatycznego do przetwarzania danych.

3. Od użytkowników systemu informatycznego Spółki wymaga się zgłaszania wszelkich zauważonych lub podejrzewanych słabości lub zagrożeń dla systemów. Użytkownicy zobowiązani są zgłaszać takie spostrzeżenia przełożonym lub bezpośrednio Administratorowi Systemu Informatycznego.

4. Użytkownicy są poinformowani, że w żadnych okolicznościach nie powinni usiłować potwierdzać istnienia podejrzanych słabych punktów systemu. Takie zalecenie służy ich własnemu bezpieczeństwu, bowiem testowanie słabych punktów może być interpretowane w systemie jako potencjalne nadużycie.

5. Użytkownicy systemu zobowiązani są do:

a) obserwacji objawów niewłaściwego funkcjonowania oprogramowania i wszelkich komunikatów pojawiających się na ekranie monitora;

b) jeśli to jest możliwe komputer powinien zostać odizolowany, a jego użytkowanie powinno zostać przerwane;

c) konieczne jest natychmiastowe powiadomienie Administratora Systemu Informatycznego.

6. Użytkownicy systemu nie powinni próbować usuwać podejrzanego oprogramowania, wszelkie działania w tym zakresie pozostają w kompetencjach Administrator Systemu Informatycznego.

3. Postępowanie Administratora Systemu Informatycznego po wykryciu lub otrzymaniu zgłoszenia o incydencie

1. Ustala, czy incydent rzeczywiście miał miejsce.
2. Określa, czy istnieje zagrożenie dla dalszego prawidłowego funkcjonowania systemu.
3. Ocenia, czy system powinien zostać odizolowany od sieci i informuje o takim zamiarze Członków Stowarzyszenia Polskich Drużyn Strzeleckich oraz Administratora Bezpieczeństwa Informacji (ABI).
4. Zabezpiecza dowody zdarzenia.
5. Zaleca użytkownikom systemu sposób dalszego postępowania.

4. Postępowanie ABI po otrzymaniu zgłoszenia o incydencie

Informuje Członka Stowarzyszenia Polskich Drużyn Strzeleckich o podjętych działaniach związanych z incydentem, a w razie zaistnienia incydentu o poważnych konsekwencjach sporządza pisemny:

5. „RAPORT o incydencie”

1. Dokonuje analizy skutków incydentu oraz – w razie potrzeby – opracowuje zalecenia mające na celu podniesienie poziomu bezpieczeństwa systemu. Analizując incydent uwzględnia stan zabezpieczeń fizycznych obszaru przetwarzania danych, stan informacji (czy została zmodyfikowana, utracona lub ujawniona), dane o dostępie osób nieupoważnionych do zasobów oraz ocenia celowość lub przypadkowość ewentualnego przekroczenia uprawnień przez osoby dopuszczone do przetwarzania danych.

2. Dokonuje stosownego wpisu do „Ewidencji incydentów naruszenia bezpieczeństwa informacji”:

– Data i godzina wystąpienia incydentu,
– Opis incydentu i okoliczności zdarzenia,
– Opis podjętych działań.

* Zadania określonego charakteru.

„INSTRUKCJA postępowania w sytuacji naruszenia ochrony danych osobowych” zawiera **Załącznik** do „POLITYKI…”.

Za dobrą praktykę należy uznać korzystanie z funkcji automatycznej aktualizacji wszystkich aplikacji w systemie informatycznym, nie tylko tych służących bezpośrednio do przetwarzania danych osobowych.

W przypadku braku takiej możliwości, należy regularnie śledzić informacje udostępniane przez producenta oprogramowania i dokonywać jego „ręcznej” aktualizacji.

Warszawa; dnia 15. 01. 2020 r.

Wykonano w 1 Egz.
- do powielenia w niezbędnej ilości egzemplarzy – wg potrzeb.

ZAŁĄCZNIK

WYKAZ

osób zapoznanych z dokumentem Nadawanie „Upoważnień…”

L. p.	Imię i Nazwisko	Data	Podpis	UWAGI
1	2	3	4	5
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				
21.				
22.				
23.				
24.				
25.				
26.				
27.				
28.				
29.				
30.				

Dokument pod nazwą:

NADAWANIE „Upoważnień…”

zawiera 18

(osiemnaście) stron
(słownie)

ponumerowanych.

Warszawa, 15.01.2020 r.
(Miejscowość i data)