Załącznik do uchwały KRL-W
Nr 24/2018/VII z dnia 14 czerwca 2018 r.

POLITYKA BEZPIECZEŃSTWA W ZAKRESIE PRZETWARZANIA I OCHRONY DANYCH OSOBOWYCH

Przygotowana dla Krajowej Izby Lekarsko-Weterynaryjnej

Warszawa; maj 2018 rok.

ZAWARTOŚĆ DOKUMENTU

SPIS ZAŁĄCZNIKÓW

WPROWADZENIE

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych stosowanych w Krajowej Izbie Lekarsko-Weterynaryjnej z siedzibą w Warszawie przy Al. Przyjaciół 1 lok. 2. Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę. Dokument zwraca uwagę na konsekwencje jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń. Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym. Dokument „Polityka bezpieczeństwa", wskazuje sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w systemach informatycznych i przeznaczony jest dla wszystkich pracowników Krajowej Izby Lekarsko – Weterynaryjnej, którzy w ramach swoich obowiązków służbowych mają dostęp do danych osobowych. Polityka bezpieczeństwa została opracowana na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE i 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 i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

Polityka bezpieczeństwa określa tryb postępowania w przypadku, gdy:
1) stwierdzono naruszenie zabezpieczenia systemu informatycznego;
2) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.

Polityka bezpieczeństwa obowiązuje wszystkich pracowników zatrudnionych w Krajowej Izbie Lekarsko - Weterynaryjnej. Realizacja postanowień tego dokumentu ma zapewnić ochronę danych osobowych, właściwą ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznych.

Rozdział I
Przepisy wprowadzające

§ 1

1. Użyte w niniejszym dokumencie określania oznaczają:
   1) **Administrator danych osobowych** – Krajowa Izba Lekarsko-Weterynaryjna;
   2) **Baza danych osobowych** – każdy posiadający strukturę zbiór danych o charakterze osobowym, dostępnych według określonych kryteriów;
   3) **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
   4) **Dostępność** – właściwość określająca, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym;
   5) **Folder** – katalog plików;
   6) **Hasło** - ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w Systemie informatycznym;
   7) **Identyfikator** - ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
   8) **Inspektor -** Inspektor Ochrony Danych (IOD);
   9) **Inspektor Ochrony Danych** (IOD) osoba wyznaczona przez Administratora danych osobowych, a gdy osoba taka nie została wyznaczona – Administrator danych osobowych;
   10) **Integralności danych osobowych** - właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   11) **Internet** publiczna sieć telekomunikacyjna w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne;
   12) **KILW** – Krajowa Izba Lekarsko-Weterynaryjna;
   13) **Polityka bezpieczeństwa** – niniejszy dokument;
   14) **Poufność danych osobowych** - właściwość zapewniająca, że dane osobowe nie są udostępniane nieupoważnionym podmiotom;
   15) **Przetwarzanie danych osobowych** – wykonywanie jakiekolwiek operacji na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
   16) **Raport** - przygotowane przez System informatyczny zestawienia zakresu i treści przetwarzanych danych osobowych;
   17) **RODO** – rozporządzenie EU dotyczące ochrony danych osobowych;
   18) **Rozliczalność** - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
   19) **Sieć telekomunikacyjna** - sieć telekomunikacyjna w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.);
   20) **System informatyczny** –zespół powiązanych ze sobą elementów: serwerów z systemami operacyjnymi, systemu zarządzania bazą danych osobowych, baz danych osobowych, oprogramowania (programów użytkowych), urządzeń

końcowych (komputerów, terminali, drukarek) oraz urządzeń służących do komunikacji między sprzętowymi elementami systemu;

21) **System zarządzania bazą danych** – system oprogramowania zawierający mechanizmy zapewniające spójność i bezpieczeństwo danych osobowych, sprawny dostęp do danych osobowych, środki programistyczne służące do przetwarzania danych osobowych, jednoczesny dostęp do danych osobowych dla wielu użytkowników, środki pozwalające na regulację dostępu do danych osobowych, środki pozwalające na odtworzenie zawartości bazy danych osobowych po awarii;
22) **Teletransmisja** – przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
23) **Uwierzytelnianie** - działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
24) **Usuwanie danych osobowych** – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.

§ 2

Polityka bezpieczeństwa jest zgodna z następującymi aktami prawnymi:

1) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (DzUrz L nr 119 z 4.05.2016 r., s. 1; RODO);
2) rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

§ 3

1. Administrator danych osobowych, wyznacza Inspektora Ochrony Danych oraz osobę upoważnioną do zastępowania Inspektora.
2. Inspektor Ochrony Danych realizuje zadania w zakresie ochrony danych, a w szczególności:
   1) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Administratora;
   2) podejmowania stosownych działań w przypadku wykrycia nieuprawnionego dostępu do bazy danych osobowych lub naruszenia zabezpieczenia danych osobowych;
   3) niezwłocznego informowania Administratora danych osobowych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów rozporządzenia o ochronie danych osobowych;
   4) nadzoru i kontroli Systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych;
   5) fizycznego zabezpieczenia danych osobowych oraz obiektów, w których są gromadzone i przetwarzane.
   6) prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych;
   7) nadzoruje funkcjonowanie mechanizmów uwierzytelniania użytkowników w Systemie Informatycznym przetwarzającym dane osobowe oraz kontroli dostępu do danych osobowych;
   8) podejmuje stosowne działania zgodnie z Polityką bezpieczeństwa oraz Instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych, w przypadku otrzymania informacji o naruszeniu zabezpieczeń Systemu informatycznego lub informacji

o zmianach w sposobie działania Systemu informatycznego, programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych osobowych;

9) Osoba zastępująca Inspektora realizuje zadania, o których mowa w ust. 2 w przypadku nieobecności Administratora Bezpieczeństwa Informacji.
10) Osoba zastępująca Inspektora składa Inspektorowi Ochrony Danych relację z podejmowanych działań w czasie jego zastępstwa.

Rozdział II

Podstawowe zasady związane z przetwarzaniem danych osobowych

§ 4

1. Ochrona danych osobowych przetwarzanych w Krajowej Izbie Lekarsko-Weterynaryjnej i Okręgowych Izbach Lekarsko-Weterynaryjnych obowiązuje wszystkie osoby, które mają dostęp do danych osobowych zbieranych, przetwarzanych oraz przechowywanych w programie WetSystems, bez względu na zajmowane stanowisko oraz miejsce wykonywania pracy jak również charakter stosunku pracy.
2. Osoby mające dostęp i przetwarzają inne dane osobowe w KILW niż w programie WetSystem, są zobligowane do stosowania niezbędnych środków zapobiegających ujawnieniu tych danych osobom nieupoważnionym.
3. Zachowanie tajemnicy w zakresie danych osobowych obowiązuje zarówno podczas trwania stosunku pracy jak i po jego ustaniu.
4. Inspektor Ochrony Danych jest odpowiedzialny za tworzenie, wdrażanie, administrację i interpretację Polityki bezpieczeństwa, standardów, zaleceń oraz procedur dotyczących ochrony danych osobowych w Krajowej Izbie Lekarsko-Weterynaryjnej w Warszawie przy Al. Przyjaciół 1 lok. 2.
5. Polecenia Inspektora Ochrony Danych a także innych osób delegowanych i wyznaczonych do działań związanych z ochroną w zakresie ochrony informacji i bezpieczeństwa systemu informatycznego muszą być bezwzględnie wykonywane przez wszystkich osoby, o których mowa w ust. 1 i użytkowników systemu.

§ 5

1. Przetwarzanie danych osobowych może odbywać się wyłącznie w obszarach do tego celu przeznaczonych. Wykaz pomieszczeń, w których dopuszczalne jest przetwarzanie danych osobowych stanowi **Załącznik nr 1** do Polityki bezpieczeństwa.
2. Należy przestrzegać podstawowych zasad przetwarzania danych wg art. 5 RODO:
    - zasady legalności (zgodności z prawem), rzetelności i przejrzystości, zgodnie z którymi dane powinny być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
    - zasada ograniczenia celu, w myśl której dane powinny być 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 za niezgodne z pierwotnymi celami;
    - zasada minimalizacji danych, zgodnie z którą dane powinny być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;

- zasada prawidłowości (poprawności), w myśl której dane mają być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;
- zasada ograniczenia przechowywania, zgodnie z którą dane muszą być 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;
- zasada zapewnienia bezpieczeństwa danych, w tym ich integralności i poufności, zgodnie z którą dane muszą być 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.

3. W szczególnych przypadkach możliwe jest przetwarzanie danych osobowych poza wyznaczonym obszarem (np. na komputerach przenośnych), jednak wymaga to zgody indywidualnej Inspektora Ochrony Danych. Szczegółowe zasady przetwarzania danych osobowych na komputerach przenośnych określa **Załącznik nr 2** do Polityki bezpieczeństwa.
4. Dostęp do pomieszczeń, w których przetwarzane są dane osobowe oraz do pomieszczeń, w których znajdują się serwery baz danych osobowych lub przechowywane są kopie zapasowe mogą mieć wyłącznie osoby, które posiadają do tego upoważnienie nadane przez Inspektora Ochrony Danych.
5. Przetwarzać dane osobowe może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych.
6. Wydanie upoważnienia do przetwarzania danych osobowych następuje na wniosek przełożonego pracownika, który otrzymuje upoważnienie. Wniosek o wydanie upoważnienia składany jest w formie pisemnej do Inspektora Ochrony Danych.

§ 6

1. Aktualny rejestr czynności przetwarzania znajduje się w **Załączniku 3** do Polityki bezpieczeństwa.
2. Załącznik, o którym mowa w ust. 1 powinien być aktualizowany po wprowadzeniu do przetwarzania nowych zbiorów danych osobowych lub nowych programów, które je obsługują.

§ 7

1. Aktualny rejestr kategorii czynności przetwarzania znajduje się w **Załączniku 4** do Polityki bezpieczeństwa.
2. W przypadku istnienia więcej niż jednego zbioru danych osobowych dla każdego zbioru powinien zostać sporządzony odrębny załącznik do Polityki bezpieczeństwa opatrzony odpowiednio numerem 3a, 3b itd.
3. Załącznik powinien być aktualizowany po wprowadzeniu istotnych zmian w strukturze bazy danych osobowych, którą opisuje. W przypadku systemów, które są rozbudowywane wprowadzone zmiany.

§ 8

1. Aktualny opis sposobu przepływu danych osobowych pomiędzy poszczególnymi systemami znajduje się w **Załączniku 5** do Polityki bezpieczeństwa.
2. W przypadku istnienia wymiany danych pomiędzy więcej niż dwoma zbiorami danych dla każdej pary zbiorów wymieniających dane osobowe powinien zostać sporządzony odrębny załącznik do Polityki bezpieczeństwa opatrzony odpowiednio numerem 4a, 4b itd.
3. Załącznik, o którym mowa w ust. 2 powinien być aktualizowany po wprowadzeniu istotnych zmian w sposobie lub zakresie wymiany danych osobowych, którą opisuje. W przypadku systemów, które są rozbudowywane wprowadzone zmiany rejestruje się (aktualizując odpowiedni załącznik) nie rzadziej, niż co 2 miesiące.
4. Administrator dopuszcza możliwość przekazania danych osobowych innym podmiotom. W takim przypadku, przetwarzanie danych osobowych odbywa się na podstawie umowy powierzenia danych osobowych.
5. Umowa, o której mowa w ust. 4 powinna zawierać ściśle określony zakres przetwarzanych danych.
6. Do umowy, o której mowa w ust. 5 stosuje się postanowienia art. 28 RODO.
7. Powierzone dane osobowe podlegają przetwarzaniu i ochronie na takich samych zasadach jak te, które dotyczą Administratora, chyba że umowa określi inne zasady ochrony danych osobowych.
8. Zmiana zasad związana z ochroną danych osobowych oraz ich przetwarzaniem przez inny podmiot, któremu Administrator udostępnił dane osobowe, nie może:
    1) naruszać praw osób, których dane osobowe są przetwarzane;
    2) naruszać zasad związanych z ochrona danych osobowych przewidzianych we właściwych przepisach prawa;
    3) zmieniać celu przetwarzania danych osobowych;
    4) udostępniać danych osobowych innym podmiotom bez zgody Administratora.
9. Zmiana zasad związanych z przetwarzaniem danych osobowych może dotyczyć nadawania uprawnień do przetwarzania danych osobowych.
10. Dostęp do powierzonych danych osobowych z sieci zewnętrznej musi odbywać się z zachowaniem odpowiednich zabezpieczeń.
11. Dostęp do danych musi być chroniony Identyfikatorem oraz Hasłem, a połączenie sieciowe realizujące dostęp do danych musi być odpowiednio szyfrowane.

Rozdział III
Opis zdarzeń naruszających ochronę danych osobowych

§ 9

1. Podział zagrożeń:
    1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu) - ich występowanie może prowadzić do utraty integralności danych osobowych, ich zniszczenia i uszkodzenia infrastruktury technicznej Systemu informatycznego; ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych osobowych;
    2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania, pogorszenie jakości sprzętu i oprogramowania) - może dojść do zniszczenia danych osobowych, może zostać

zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych osobowych;

3) zagrożenia zamierzone - świadome i celowe działania powodujące naruszenia poufności danych osobowych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na:
   a) nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
   b) nieuprawniony dostęp do systemu z jego wnętrza,
   c) nieuprawnione przekazanie danych osobowych,
   d) bezpośrednie zagrożenie materialnych składników systemu (np. kradzież sprzętu).

2. Naruszenie lub podejrzenie naruszenia Systemu informatycznego, w którym przetwarzane są dane osobowe następuje w sytuacji:
   1) losowego lub nieprzewidzianego oddziaływania czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, itp.;
   2) niewłaściwych parametrów środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych;
   3) awarii sprzętu lub oprogramowania, które wyraźnie wskazuje na umyślne działanie w kierunku naruszenia ochrony danych osobowych;
   4) pojawienia się odpowiedniego komunikatu alarmowego;
   5) podejrzenia nieuprawnionej modyfikacji danych osobowych w systemie lub innego odstępstwa od stanu oczekiwanego;
   6) naruszenia lub próby naruszenia integralności systemu lub bazy danych w tym systemie;
   7) pracy w systemie wykazującej odstępstwa uzasadniające podejrzenie przełamania lub zaniechania ochrony danych osobowych - np. praca osoby, która nie jest formalnie dopuszczona do obsługi systemu;
   8) ujawnienia nieautoryzowanych kont dostępu do systemu;
   9) naruszenia dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (np. nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, itp.).

3. Za naruszenie ochrony danych osobowych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia fizycznego miejsc przechowywania i przetwarzania danych osobowych np.
   a) niezabezpieczone pomieszczenia;
   b) nienadzorowane, otwarte szafy, biurka, regały;
   c) niezabezpieczone urządzenia archiwizujące;
   d) pozostawianie danych osobowych w nieodpowiednich miejscach – kosze, stoły itp.

Rozdział IV
Zabezpieczenie danych osobowych

§ 10

1. Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w systemach informatycznych, a w szczególności:
   1) zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym;
   2) zapobieganie przed pobraniem danych przez osobę nieuprawnioną;

3) zapobieganie zmianie, utracie, uszkodzeniu lub zniszczeniu danych osobowych;
4) zapewnianie przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa.

2. Zadanie określone w ust. 1 pkt 2 wykonuje w imieniu Administratora danych osobowych Inspektor Ochrony Danych.

§ 11

1. Zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe:
   1) wszystkie pomieszczenia, w których przetwarza się dane osobowe, są zamykane na klucz;
   2) w przypadku opuszczenia pomieszczenia przez ostatniego pracownika upoważnionego do przetwarzania danych osobowych – także w godzinach pracy, dane osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej (na zewnętrznych nośnikach np. pendrive, płyta CD/DVD, dyskietka) po zakończeniu pracy są przechowywane w zamykanych na klucz meblach biurowych, a tam, gdzie jest to możliwe – w szafach metalowych lub pancernych. Klucze od szafek należy zabezpieczyć przed dostępem osób nieupoważnionych do przetwarzania danych osobowych;
   3) nieaktualne lub błędne wydruki zawierające dane osobowe niszczone są w niszczarkach;
   4) budynek, w którym zlokalizowane są zbiory danych osobowych, jest nadzorowany przez firmę ochrony fizycznej oraz posiada instalację alarmową.

2. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych osobowych następuje poprzez:
   1) podłączenie urządzenia końcowego (komputera, terminala, drukarki) do Sieci informatycznej dokonywane jest przez informatyka;
   2) udostępnianie użytkownikowi zasobów sieci (programów i baz danych osobowych), następuje na podstawie upoważnienia do przetwarzania danych osobowych;
   3) identyfikacja użytkownika w systemie następuje poprzez zastosowanie podwójnego uwierzytelnienia;
   4) przydzielenie indywidualnego identyfikatora każdemu użytkownikowi Systemu Informatycznego i rejestrowanie przez system czasu logowania użytkownika i rodzaju wprowadzonych przez niego danych osobowych;
   5) udostępnianie kluczy od centrum przetwarzania danych osobowych (serwerowni) tylko upoważnionym pracownikom;
   6) przechowywanie kopii zapasowych w zamykanej szafie metalowej, ognioodpornej umiejscowionej poza pomieszczeniami Administratora;
   7) stosowanie programu antywirusowego z zaporą antywłamaniową na komputerach;
   8) zabezpieczenie hasłami kont na komputerach, używanie kont z ograniczonymi uprawnieniami do ciągłej pracy;
   9) szyfrowanie dysków w komputerach przenośnych;
   10) ustawienie monitorów stanowisk przetwarzania danych osobowych w sposób uniemożliwiający wgląd w dane osobom nieupoważnionym.

3. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych osobowych poprzez Internet:
   1) logiczne oddzielenie Sieci informatycznej (lokalnej), uniemożliwiające uzyskanie połączenia z bazą danych osobowych spoza Systemu Informatycznego, jak również uzyskanie dostępu z Systemu do sieci rozległej Internet,
   2) zastosowanie dwustopniowego zabezpieczenia Sieci lokalnej:
      - pierwszy stopień ochrony stanowią listy dostępu ACL (Acces Control List) na głównym routerze uniemożliwiające nawiązanie połączenia z jakimkolwiek niewskazanym jawnie komputerem w sieci;
      - drugi stopień ochrony stanowi lokalna brama sieciowa z zainstalowanym systemem typu firewall z funkcją analizy charakteru ruchu sieciowego, uniemożliwiającym nawiązanie połączenia do chronionych komputerów i blokującym ruch o charakterystyce niepożądanej lub mogącej zostać uznanej za szkodliwą.
4. Zabezpieczenia przed utratą danych osobowych w wyniku awarii realizowane jest poprzez:
   1) odrębne zasilanie sprzętu komputerowego;
   2) ochronę serwerów przed zanikiem zasilania poprzez stosowanie zasilaczy zapasowych UPS;
   3) ochronę przed utratą zgromadzonych danych poprzez cykliczne wykonywanie kopii zapasowych, z których w przypadku awarii odtwarzane są dane osobowe i system operacyjny;
   4) ochronę przed awarią podsystemu dyskowego poprzez używanie macierzy dyskowych,
   5) zapewnienie właściwej temperatury i wilgotności powietrza dla pracy sprzętu komputerowego, poprzez zastosowanie klimatyzatorów;
   6) zastosowanie ochrony przeciwpożarowej poprzez umieszczenie w serwerowni gaśnic, okresowo kontrolowanych przez specjalistę;
   7) zwiększenie niezawodności serwerów i urządzeń sieciowych poprzez logiczne rozmieszczenie ich w szafach serwerowych.

Rozdział V
Kontrola przestrzegania zasad zabezpieczenia danych osobowych

§ 12

1. Inspektor Ochrony Danych sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikający z RODO oraz zasad ustanowionych w Polityce bezpieczeństwa.
2. Inspektor Ochrony Danych sporządza roczne sprawozdanie i przedstawia je Administratorowi danych osobowych.
3. Inspektor Ochrony Danych osobowych zobowiązany jest pełnić funkcję punktu kontaktowego dla organu nadzorczego.

Rozdział VI
Postępowanie w przypadku naruszenia ochrony danych osobowych

§ 13

1. W przypadku stwierdzenia naruszenia:
   1) zabezpieczenia systemu informatycznego
   2) technicznego stanu urządzeń;
   3) zawartości zbioru danych osobowych;
   4) jakości transmisji danych osobowych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych;
   5) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, kradzież itp.) każda osoba jest zobowiązana do niezwłocznego powiadomienia o tym fakcie Inspektora Ochrony Danych i bezpośredniego przełożonego.
2. Po wykonaniu czynności określonych w ust. 1 należy:
   1) 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;
   2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia;
   3) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę zdarzenia;
   4) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego lub aplikacji użytkowej;
   5) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku;
   6) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Inspektora Ochrony Danych lub osoby upoważnionej.
3. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Inspektor Ochrony Danych lub osoba go zastępująca:
   1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy;
   2) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem;
   3) w razie potrzeby powiadamia o zaistniałym naruszeniu Administratora danych osobowych;
   4) jeżeli zachodzi taka potrzeba zleca usuniecie występujących naruszeń, oraz powiadamia odpowiednie instytucje.
4. Inspektor Ochrony Danych dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego **Załącznik nr 6** do Polityki bezpieczeństwa.
5. Raport, o którym mowa w ust. 4, Inspektor Ochrony Danych niezwłocznie przekazuje Administratorowi danych osobowych, a w przypadku jego nieobecności osobie uprawnionej.
6. Naruszenie ochrony danych osobowych ma być zgłoszone przez administratora danych organowi nadzorczemu. Niezależnie od zgłoszenia naruszenia organowi nadzorczemu

administrator danych może również mieć obowiązek zawiadomienia o takim naruszeniu osób, których dane dotyczą.

7. Administrator Danych lub Inspektor Ochrony Danych jest obowiązany zgłosić niezwłocznie organowi nadzorczemu (UODO) incydent naruszenia systemu, bazy danych lub wycieku danych osobowych nie później niż w terminie 72 godzin od stwierdzenia naruszenia.
8. Zaistniałe naruszenie może stać się przedmiotem szczegółowej analizy prowadzonej przez zespół powołany przez Inspektora Ochrony Danych.
9. Analiza, o której mowa w ust. 6, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Rozdział VII
Postanowienia końcowe

§ 14

1. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w Polityce bezpieczeństwa, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, wszczyna się postępowanie dyscyplinarne.
2. Inspektor Ochrony Danych zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z Polityką bezpieczeństwa i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego **Załącznik nr 7** do Polityki bezpieczeństwa.