UCHWAŁA NR 231/I KRF
KRAJOWEJ RADY FIZJOTERAPEUTÓW
z dnia 29 maja 2018 r.
w sprawie Procedur z zakresu ochrony danych osobowych

Na podstawie art. 70 i art. 77 pkt 10 ustawy z dnia 25 września 2015 r. o zawodzie fizjoterapeuty (Dz. U. z 2018 r. poz. 505 i 1000) oraz 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 (ogólne rozporządzenie o ochronie danych) uchwala się, co następuje:

§ 1. Krajowa Rada Fizjoterapeutów ustala:

1) Politykę Ochrony Danych Osobowych, stanowiącą załącznik nr 1 do uchwały;
2) Procedurę uwzględnienia ochrony danych w fazie projektowania i domyślnej ochrony danych, stanowiącą załącznik nr 2 do uchwały;
3) Procedurę konsultacji z organem nadzorczym, stanowiącą załącznik nr 3 do uchwały.

§ 2. Uchwała wchodzi w życie z dniem podjęcia, z mocą od dnia 25 maja 2018 r.

Prezes
Krajowej Rady Fizjoterapeutów

dr hab. n. med. Maciej Krawczyk

Załączniki do uchwały Nr 231/I KRF
Krajowej Rady Fizjoterapeutów

Załącznik nr 1

POLITYKA OCHRONY DANYCH OSOBOWYCH

KRAJOWA IZBA FIZJOTERAPEUTÓW

Zatwierdzam:

....
Miejscowość, data

.....
Podpisy zgodnie z reprezentacją

SPIS TREŚCI

1. Definicje

1.1. **Dane osobowe** – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora. Może być nim przykładowo identyfikator stanowiący dane takie jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

1.2. **Atrybuty bezpieczeństwa:**

- Poufność - zapewnienia, że dane osobowe są udostępniane jedynie osobom upoważnionym
- Integralność – zapewnienie zupełnej dokładności i kompletności danych osobowych oraz metod ich przetwarzania.
- Dostępność - zapewnienia, że osoby upoważnione mają dostęp do danych osobowych tylko wtedy, gdy istnieje taka potrzeba.

1.3. **Naruszenie ochrony danych osobowych** - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

1.4. **Administrator** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

1.5. **Pseudonimizacja** - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

1.6. **Dane genetyczne** - oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;

1.7. **Dane biometryczne** - oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;

1.8. **Nośnik danych** – wszelkie przedmioty fizyczne na których możliwe jest zapisanie informacji, w tym danych osobowych (np. pendrive, dyski, karty magnetyczne);

1.9. **Ograniczenie przetwarzania** – oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

1.10. **Przetwarzanie** - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

1.11. **Profilowanie** - oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

1.12. **Personel** - osoby zatrudnione na podstawie stosunku pracy, umów cywilnoprawnych (umowa o dzieło, umowa zlecenia), przedsiębiorcy wykonujący działalność osobiście i jednoosobowo, osoby odbywające praktyki, stażyści, osoby skierowane do pracy w ramach umów z agencjami pracy tymczasowej wykonujące prace związane z przetwarzaniem danych osobowych u ADO, mogą być to również członkowie KIF.

1.13. Wykaz skrótów:

- **Administrator** – Krajowa Izba Fizjoterapeutów z siedzibą w Warszawie (00-511) przy ul. Siennej 39,
- **UODO** – Urząd Ochrony Danych Osobowych - organ powołany do spraw ochrony danych osobowych,
- **RODO** - Rozporządzenie 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,
- **Polityka** – niniejsza Polityka Ochrony Danych Osobowych.

2. Wprowadzenie

2.1. Zgodnie z art. 32 RODO (Sekcja 2 „Bezpieczeństwo danych osobowych") Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa danych osobowych odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych.

2.2. Podczas doboru środków technicznych i organizacyjnych uwzględnia się charakter, zakres, kontekst i cele przetwarzania danych osobowych.

2.3. Środki, o których mowa powyżej, obejmują wdrożenie przez Administratora odpowiednich polityk ochrony danych.

2.4. Celem niniejszej polityki ochrony danych osobowych jest zapewnienie odpowiedniego poziomu bezpieczeństwa przetwarzanych danych, tak aby zapobiegać przypadkowemu lub niezgodnemu z prawem zniszczeniu, utraceniu, zmodyfikowaniu, nieuprawnionemu ujawnieniu lub nieuprawnionemu dostępowi do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

2.5. Polityka zatwierdzana jest przez kierownictwo i podawana do wiadomości jako dokument do użytku wewnętrznego Administratora.

2.6. Obowiązki określone w Polityce mają zastosowanie odpowiednio dla wszystkich:

- Danych osobowych przetwarzanych przez Administratora, zarówno w przypadku, gdy jest on administratorem, jak i w sytuacji, gdy przetwarza dane w imieniu innego administratora
- Danych osobowych przetwarzanych bez względu na rodzaj użytego nośnika (zarówno w postaci dokumentacji papierowej, jak i w formie elektronicznej)
- Lokalizacji Administratora, w których dane osobowe są przetwarzane.
- Personelu Administratora.

2.7. Polityka powinna być poddawana regularnym przeglądom nie rzadziej niż raz do roku tak, aby pozostawała przydatna, adekwatna i skuteczna.

2.8. Naruszenia przepisów dotyczących obowiązków Administratora związanych z bezpieczeństwem danych osobowych podlegają zgodnie z art. 83 RODO administracyjnej karze pieniężnej w wysokości do 10 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 2 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

2.9. Naruszenie obowiązków wynikających z niniejszej polityki oraz przepisów o ochronie danych osobowych może być uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz karnym.

3. Obowiązki w zakresie ochrony danych osobowych

3.1. Obowiązki Administratora obejmują:

3.1.1. Zapewnienie środków technicznych i organizacyjnych, aby osiągnąć odpowiedni stopień bezpieczeństwa przetwarzanych danych

3.1.2. Wdrożenie procedur organizacyjnych, w zakresie następujących zasad:

- **zgodności z prawem** – dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby której dane dotyczą.
- **ograniczenia celu przetwarzania** – dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.
- **minimalizacji danych** – dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.
- **prawidłowości danych** – dane osobowe muszą 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.
- **ograniczenia przetwarzanych danych** – dane osobowe muszą być przechowywane w formie umożliwiającej identyfikacje osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.
- **poufności i integralności danych** – dane osobowe muszą być przetwarzanie w sposób zapewniający odpowiednie bezpieczeństwo w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.
- **rozliczalności** – Administrator jest odpowiedzialny za przestrzeganie powyższych zasad i musi być w stanie wykazać ich przestrzeganie.

3.1.3. Wdrożenie procedur organizacyjnych w zakresie respektowanie praw osób, których dane dotyczą w zakresie:

- prawa dostępu do danych
- prawa do sprostowania danych
- prawa do usunięcia danych
- prawa do ograniczenia przetwarzania

- obowiązku powiadomienia odbiorców o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania.
- prawa do przenoszenia danych
- prawa do sprzeciwu
- zautomatyzowanym podejmowanie decyzji, w tym profilowaniu
- prawa do uzyskania informacji o:
    - administratorze
    - inspektorze Ochrony Danych Osobowych - gdy ma to zastosowanie
    - celu przetwarzania danych osobowych oraz podstawie prawnej
    - prawnie uzasadnionych interesach realizowanych przez ADO lub przez stronę trzecią
    - odbiorcach danych osobowych lub kategoriach odbiorców, jeżeli istnieją
    - o zamiarze przekazania danych osobowych do państwa trzeciego – gdy ma to zastosowanie,
    - okresie, przez który dane osobowe są przechowywane
    - informacji o prawie do żądania od ADO dostępu do danych
    - informacji o prawie do cofnięcia zgody w dowolnym momencie
    - informacji o prawie wniesienia skargi do UODO,
    - Informacji czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest obowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych
    - Informacji o zautomatyzowanym podejmowaniu decyzji w tym o profilowaniu

3.1.4. Wdrożenie procedury uwzględnienia ochrony danych osobowych w fazie projektowania oraz stosowanie domyślnej ochrony danych osobowych.

3.1.5. Wdrożenie procedury zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu (UODO) oraz zawiadomienia osoby, której dane dotyczą o naruszeniu ochrony danych osobowych.

3.1.6. Wdrożenie procedury wykonywania oceny skutków dla ochrony danych osobowych oraz wykonywanie uprzednich konsultacji z organem nadzorczym, gdy ma to zastosowanie

3.1.7. Prowadzenie, kiedy ma to zastosowanie rejestru czynności przetwarzania danych osobowych oraz rejestru kategorii przetwarzania.

3.1.8. Powołanie inspektora ochrony danych, gdy ma to zastosowanie

3.1.9. Zawarcia umów z podmiotami przetwarzającymi dane w imieniu Administratora.

3.1.10. Nadzorowanie czy podczas przekazywania danych osobowych do państw poza Europejski Obszar Gospodarczy (EOG) odbywa się na zasadach zgodnych z przepisami prawnymi.

4. Szacowanie ryzyka

4.1. Administrator analizuje i identyfikuje ryzyka związane z przetwarzaniem danych osobowych. Ryzyka oceniane są zgodnie z ustaloną metodyką szacowania ryzyka. Wynikiem szacowania jest raport, identyfikujący procesy przetwarzania najbardziej ryzykowne oraz sposoby postępowania z ryzykiem.

4.2. Jako kryterium wyznaczania poziomu akceptacji ryzyka jest dążenie do wyrównania ryzyk szczątkowych w firmie. Wartość ryzyka akceptowalnego jest każdorazowo ustalana podczas przeglądów analizy ryzyka.

4.3. Analiza ryzyka jest wykonywana cyklicznie, po każdej istotnej zmianie, która może mieć wpływ na bezpieczeństwo przetwarzanych danych, ale nie rzadziej niż raz w roku.

4.4. Proces zarządzania ryzykiem przedstawia się w następujący sposób:

5. Bezpieczeństwo organizacyjne

5.1. Role i odpowiedzialności w zakresie bezpieczeństwa danych osobowych powinny być jasno określone i przypisane do konkretnych osób lub stanowisk.

5.2. Podczas przetwarzania danych należy bezwzględne oddzielić funkcje wykonawcze od funkcji kontrolnych.

5.3. Specjalistyczny Personel Administratora powinien utrzymywać kontakty z grupami specjalistycznymi oraz profesjonalnymi stowarzyszeniami w zakresie bezpieczeństwa informacji.

5.4. Każda osoba, przed uzyskaniem dostępu do danych osobowych powinna zostać zapoznana z obowiązkami i odpowiedzialnościami wynikającymi z przepisów prawa dotyczących ochrony danych osobowych oraz wewnętrznymi procedurami.

5.5. Każda osoba przed rozpoczęciem pracy powinna podpisać dokument o zapoznaniu się z wewnętrznymi regulacjami, zachowaniu poufności oraz przyjęciu odpowiedzialności za wszystkie operacje wykonane przez nią podczas przetwarzania danych.

6. Bezpieczeństwo fizyczne

6.1. Administrator lub wyznaczone przez niego służby ochrony stosują środki zapewniające ochronę fizyczną przed przypadkowym lub niezgodnym z prawem zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem przechowywanych lub w inny sposób przetwarzanych danych osobowych.

6.2. W szczególności Administrator:

- projektuje i stosuje fizyczne zabezpieczenia przed dostępem do pomieszczeń i obiektów ze szczególnym uwzględnieniem wejść
- projektuje i stosuje fizyczne zabezpieczenia przed katastrofami naturalnymi
- sprawuje nadzór nad punktami dostępu do budynków takimi jak obszary dostaw i załadunku oraz innymi punktami przez które nieuprawnione osoby mogą wejść do pomieszczeń

6.3. Właściwy poziom zabezpieczeń określa się w wyniku szacowania ryzyka.

6.4. W szczególności w celu ochrony obszarów przetwarzania stosuje się:

- monitoring wizyjny
- systemy alarmowe
- nadzór służby ochrony
- recepcje
- czujniki przeciwpożarowe
- gaśnice lub automatyczne systemy gaszenia
- zamykane pomieszczenia biurowe
- zamykane szafy i szafki
- karty wejściowe do budynku

- niszczarki dokumentów

6.5. Personel zobowiązany jest do przestrzeganie tzw. „zasady czystego biurka" - na biurku, w trakcie pracy powinny znajdować się jedynie dokumenty potrzebne do wykonania bieżącej pracy a po zakończeniu pracy dokumenty zawierające dane osobowe powinny zostać schowane w szafach lub szufladach.

6.6. Niszczenie zbędnych dokumentów papierowych oraz nośników zawierających dane osobowe należy dokonywać w niszczarkach posiadających stopień 3 lub większy wg normy DIN 66399 lub poprzez umieszczenie ich w specjalnie do tego celu przygotowanych zaplombowanych pojemnikach.

6.7. Należy cyklicznie kontrolować czy dokumenty zawierające dane osobowe są przechowywane w sposób zapobiegający nieuprawnionemu ujawnieniu lub nieuprawnionemu dostępowi do danych.

6.8. Należy wprowadzić zasady, by osoby postronne (np. goście) poruszały się po pomieszczeniach, w których przetwarzane są dane osobowe tylko przy asyście Personelu.

6.9. Personel powinien natychmiast poinformować swoich przełożonych o zauważonych nieprawidłowościach w funkcjonowaniu systemu ochrony fizycznej w szczególności w przypadku zauważenia osoby postronnej bez asysty w obszarze przetwarzania danych osobowych.

6.10. Należy dołożyć szczególnej staranności w przypadku wynoszenia dokumentów papierowych zawierających dane osobowe, aby dokumenty te były należycie zabezpieczone przed zgubieniem lub odczytaniem przez osoby nieuprawnione.

7. Bezpieczeństwo teleinformatyczne

7.1. Zasady ogólne

7.1.1. W celu ochrony systemów informatycznych służących do przetwarzania danych osobowych przed zagrożeniami stosuje się zabezpieczenia umożliwiające zapewnienie poufności, integralności oraz dostępności danych.

7.1.2. Właściwy poziom zabezpieczeń określa się w wyniku szacowania ryzyka.

7.1.3. Zabezpieczenia teleinformatyczne należy na bieżąco aktualizować w celu dostosowania ich do zmian prawnych i uwzględnienia postępującego rozwoju technologii oraz zmieniających się zagrożeń.

7.1.4. Należy wyłączyć niewykorzystywane usługi oraz odinstalować nie użytkowane aplikacje na serwerach i urządzeniach sieciowych w tym w drukarkach.

7.1.5. W celu zapewnienia ciągłości działania procesów biznesowych należy stworzyć plany awaryjne dla ważnych elementów w systemie informatycznym.

7.2. Inwentaryzacja sprzętu i oprogramowania informatycznego.

Należy przygotować i utrzymywać aktualność spisu inwentaryzacyjnego sprzętu i oprogramowania służącego do przetwarzania danych osobowych.

7.3. Wykorzystanie sprzętu

7.3.1. Personelowi nie wolno wykorzystywać sprzętu służbowego do celów prywatnych, chyba, że zostało to ustalone w odrębnych regulaminach.

7.3.2. Personelowi nie wolno wykorzystywać sprzętu prywatnego do celów służbowych, chyba, że zostało to uregulowane w odrębnych regulaminach.

7.4. Zarządzanie dostępem do systemów

7.4.1. Przyznawanie i korzystanie z dostępu do systemów informatycznych jest ograniczone i kontrolowane.

7.4.2. Każdy użytkownik otrzymuje indywidualne poświadczenia (login i hasło) służące do identyfikacji w systemie informatycznym.

7.4.3. Dostęp do zasobów systemu teleinformatycznego podlega ograniczeniom zgodnie z określonym zakresem uprawnień danego użytkownika.

7.4.4. Dostęp do systemów przetwarzających dane osobowe nadawany jest Personelowi wyłącznie na czas realizacji zadań bądź realizacji umowy.

7.4.5. Personelowi nadaje się dostęp jedynie do zasobów wynikających z zakresu obowiązków i umów, które są niezbędne do wykonywania obowiązków w zakresie określonych czynności i odpowiedzialności.

7.5. Oprogramowanie i aktualizacje

7.5.1. Wykorzystywane oprogramowanie w celu zapewnienia ciągłości działania procesów biznesowych musi być wykorzystywane zgodnie z prawami licencji.

7.5.2. Dopuszcza się instalacje oprogramowania wyłącznie zaakceptowanego przez Administratora.

7.5.3. Należy monitorować stan aktualnych poprawek systemowych w szczególności w zakresie bezpieczeństwa.

7.5.4. Należy aktualizować oprogramowanie antywirusowe, definicje wirusów na serwerach, stacjach roboczych i urządzeniach mobilnych.

7.5.5. Zabrania się instalowania oprogramowania pochodzącego z nieznanych źródeł.

7.6. Bezpieczeństwo sieci

7.6.1. Sieć teleinformatyczna powinna być zarządzana w sposób zapewniający utrzymanie bezawaryjnej i niezakłóconej komunikacji systemów.

7.6.2. Urządzenia sieciowe należy konfigurować i monitorować tak, aby zminimalizować zagrożenia.

7.6.3. Należy dążyć do stosowania komunikacji szyfrowanej.

7.6.4. Należy dążyć do separacji sieci w tym w szczególności do użytku gości powinna być stosowana sieć wydzielona.

7.6.5. W przypadku połączenia stacji roboczych z siecią publiczną należy stosować logiczne lub fizyczne zabezpieczenia systemów przed intruzami lub nieautoryzowanym dostępem np. firewall,/ IDS/IPS (wykrywanie/blokowanie ataków w czasie rzeczywistym)/PROXY.

7.6.6. W produkcyjnej infrastrukturze teleinformatycznej powinien być dopuszczony tylko niezbędny ruch sieciowy. Konfiguracja ruchu sieciowego powinna dopuszczać ruch tylko dla konkretnych, niezbędnych adresów IP, tylko dla konkretnych portów źródłowych i docelowych oraz protokołów.

7.7. Urządzenia drukujące/mfp

7.7.1. Należy upewnić się, że wszystkie urządzenia drukujące w sieci zostały zidentyfikowane i są aktywnie zarządzane w celu uzyskania zgodności z zasadami bezpieczeństwa obowiązującymi w firmie tzn. m.in.:

- w regułach firewall'a uwzględnione zostały adresy IP urządzeń drukujących

- zmienione zostały domyślne sposoby logowania i haseł na zgodne z polityką haseł
- wyłączone zostały nieużywane porty takie jak FTP czy Telnet i pozostawione włączenie tylko porty tych usług, które są potrzebne do pracy.

7.7.2. W urządzeniach drukujących należy włączyć automatyczne aktualizacje oprogramowania.

7.7.3. Należy upewnić się, że wszelkie oprogramowanie wbudowane i inne rozwiązania zainstalowane w urządzeniach drukujących są aktualne, posiadają certyfikaty oraz potwierdzoną oryginalność.

7.7.4. Należy wybierać urządzenia drukujące z wbudowaną ochroną systemu BIOS i oprogramowania.

7.7.5. Zaleca się stosowanie szyfrowania w celu ochrony przesyłanych danych (przesyłanie zadań druku lub skanowania do i z urządzenia drukującego) oraz przechowywanych na dysku twardym urządzenia.

7.7.6. Przed wycofaniem urządzeń drukujących z użytkowania lub podczas przekazywania do serwisu należy upewnić się, że dane przechowywane na dyskach twardych urządzeń są usunięte.

7.7.7. Należy wprowadzić ograniczenie komunikacji nieautoryzowanych komputerów z urządzeniem drukującym

7.7.8. Należy stosować autoryzację druku w przypadku drukarek zlokalizowanych w przestrzeniach otwartych tak, by wydruk był dostępny po zalogowaniu się do wybranego urządzenia pinem lub kartą.

7.8. Kryptografia

7.8.1. W celu ochrony poufności stosuje się systemy i techniki kryptograficzne.

7.8.2. Zaleca się szyfrowanie dysków urządzeń mobilnych oraz innych nośników.

7.8.3. Zaleca się, aby dane uwierzytelniające oraz dane osobowe były przesyłane komunikacją szyfrowaną.

7.8.4. W przypadku przekazywania plików zawierających dane osobowe, Personel ma obowiązek zabezpieczenia danych za pomocą szyfrowania.

7.9. Urządzenia mobilne i praca zdalna

7.9.1. Urządzenia takie jak: laptopy, tablety, telefony, nośniki danych, są przyznawane personelowi na stanowiskach wymagających pracy poza przedsiębiorstwem.

7.9.2. Ze względu na typ urządzenia oraz jego specyfikę, zbiór zabezpieczeń dobierany jest adekwatnie do ryzyka i możliwości technicznych.

7.9.3. Ze względu na występowanie specyficznych ryzyk związanych z posługiwaniem się urządzeniami mobilnymi użytkowników obowiązują specjalne zasady minimalizujące te ryzyka.

7.10. Nośniki danych

7.10.1. Do przechowywania i przenoszenia danych osobowych mogą być wykorzystywane tylko i wyłącznie autoryzowane nośniki danych (dyski, pendrive itp.)

7.10.2. Zabrania się przenoszenia danych osobowych na nośniki prywatne.

7.10.3. Przenośne nośniki danych podlegają ochronie w postaci szyfrowania oraz kontroli antywirusowej.

7.10.4. Trwałe i bezpowrotne kasowanie danych zalecane jest w szczególności:

- Zmiany użytkownika komputera
- Zwrotu uszkodzonego nośnika producentowi w ramach gwarancji

7.10.5. Przed przekazaniem do serwisu lub utylizacji urządzeń zawierających dyski lub inne nośniki informacji, należy z nich wymontować nośniki

7.10.6. Sporządza się dokumentację potwierdzająca utylizację sprzętu i nośników danych.

7.11. Kopie zapasowe

7.11.1. Na potrzeby zachowania dostępności wykonuje się kopie zapasowe danych osobowych.

7.11.2. Zasady określające wykonywanie kopii zapasowych danych osobowych powinny być udokumentowane.

7.11.3. Wobec kopii bezpieczeństwa stosuje się następujące zabezpieczenia:

- Nośniki zawierające kopie zapasowe powinny podlegać zabezpieczeniu przed nieuprawnionym dostępem

- Nośniki zawierające kopie zapasowe powinny być przechowywane w sposób minimalizujący ryzyko ich uszkodzenia lub nieuprawnionej modyfikacji
- Kopie zapasowe powinny być przechowywane w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco
- Kopie zapasowe sprawdza się okresowo pod kątem ich dalszej przydatności. Po stwierdzeniu nieprzydatności kopii zapasowych nośnik zostaje pozbawiony danych uniemożliwiający dalszy odczyt danych

7.11.4. Sporządzane kopie zapasowe sprawdza się cyklicznie w celu weryfikacji poprawnego przywrócenia danych znajdujących się na kopii zapasowych

7.12. Rozliczalność działań w systemach informatycznych

7.12.1. Zapewnia się rozliczalność działań użytkowników.

7.12.2. Zapewnienie rozliczalności operacji polega na gromadzeniu informacji o tym kto, kiedy i jakie wykonał operacje w systemie informatycznym.

7.12.3. Zaleca się regularne przeglądanie dzienników systemowych (logów) i ich analizę w celu identyfikacji działań niepożądanych.

7.12.4. Zaleca się ustalenie okresu i sposobu przechowywania dzienników systemowych.

7.12.5. Zaleca się ustalenie właściciela aplikacji (systemu), który odpowiada za funkcjonalność, zawartość, monitorowanie, rozwój systemu oraz jest odpowiedzialny za obsługę awarii i incydentów mających miejsce w systemie informatycznym.

7.12.6. Zaleca się okresową kontrolę uprawnień kont użytkowników.

7.13. Serwerownia

7.13.1. Zaleca się zastosowanie zabezpieczeń serwerów i urządzeń sieciowych przed utratą oraz przerwami zasilania.

7.13.2. Zaleca się, aby serwery oraz urządzenia sieciowe przesyłające ruch sieciowy umieszczone były w specjalnych pomieszczeniach takich jak serwerownie lub węzły.

7.13.3. Zaleca się, aby pomieszczenia te były chronione przed nieupoważnionym dostępem poprzez zastosowanie dodatkowych zabezpieczeń, jak np. wzmocnione drzwi, dodatkowa autoryzacja, wzmocnione lub okratowane okna, system kontroli dostępu.

7.13.4. Serwerownia powinna być odporna na zagrożenia naturalne takie jak pożar, zalanie, przegrzanie – temperatura powinna być kontrolowana oraz powinna spełniać normy dla znajdującego się w niej sprzętu teleinformatycznego.

7.14. Zgłaszanie incydentów i nadużyć związanych z bezpieczeństwem informatycznym

7.14.1. Personel powinien natychmiast poinformować swoich przełożonych o zauważonych nieprawidłowościach w funkcjonowaniu swojego sprzętu teleinformatycznego (np. komputera, telefonu, tabletu, drukarki, itp.) i oprogramowania.

7.14.2. Zaleca się, aby utratę lub kradzież sprzętu komputerowego personel niezwłocznie zgłaszał do przełożonego lub odpowiedniej komórki organizacyjnej.

7.14.3. Zaleca się, aby każdy sprzęt przeznaczony do usunięcia (złomowania) został sprawdzony i przygotowany przez osobę odpowiedzialną za inwentaryzację sprzętu

7.14.4. Zaleca się, aby informacje o awariach sprzętu komputerowego, potencjalnie zagrażających bezpieczeństwu danych osobowych były raportowane i udokumentowane.

7.15. Audyty systemu

7.15.1. Zaleca się przeprowadzanie cyklicznych audytów systemów teleinformatycznych w celu przeglądu tych systemów pod kątem zgodności z ustaloną polityką, przyjętymi wytycznymi i standardami.

7.15.2. Wyniki audytu powinny być podstawą do działań zapobiegawczych spadkowi ustalonego poziomu bezpieczeństwa.

7.16. Obowiązki personelu

7.16.1. Personel odpowiada za zapewnienie bezpieczeństwa swojego stanowiska w zakresie dotyczącym ograniczenia dostępu do niego przez osoby nieuprawnione oraz użytkowania sprzętu teleinformatycznego zgodnie z jego przeznaczeniem.

Personel obowiązany jest do:

- Wykorzystywania zasobów teleinformatycznych wyłącznie w celach służbowych
- Eksploatowania zasobów systemu zgodnie z przydziałem uprawnień a w przypadku nadania szerszych uprawnień niż wcześniej założonych niezwłocznego zgłoszenia tego faktu przełożonym.
- W przypadku urządzeń przenośnych:
    - Zachowania szczególnej ostrożności podczas używania urządzenia w miejscach publicznych, salach spotkań, hotelach (ryzyko podglądania informacji chronionych przez nieuprawnione osoby)
    - Stosowania w miarę możliwości fizycznego zabezpieczenia sprzętu przed kradzieżą np. poprzez nie pozostawanie go bez nadzoru.

- W samochodzie komputer przenośny należy przewozić albo w zamkniętym bagażniku, albo na podłodze w miejscu przeznaczonym na nogi pasażera
- Zabronione jest odstępowanie komputera przenośnego osobom trzecim
- Komputery przenośne powinny być okresowo kontrolowane w celu sprawdzenia bezpieczeństwa
- Należy unikać łączenia się do publicznych sieci Wi-Fi.
- Personel pracujący na urządzeniach przenośnych z innych lokalizacji niż siedziba przedsiębiorstwa powinien uzyskać ograniczony, szyfrowany dostęp do infrastruktury (np. VPN)
- Zapoznania się i stosowania obowiązujących przepisów prawa w zakresie ochrony danych osobowych.
- Chronienia poufności i integralności swojego klucza prywatnego wykorzystywanego w podpisie elektronicznym.
- Przestrzegania tzw. **„zasady czystego biurka"**, która polega na tym, aby na biurku znajdowały się jedynie dokumenty potrzebne do wykonania bieżącej pracy.
- Przestrzegania, aby dostęp do komputera podczas opuszczania stanowiska pracy był zablokowany (np. poprzez włączenie wygaszacza ekranu chronionego hasłem lub wylogowania się z systemu),
- Dokonania bez zbędnej zwłoki zgłoszenia w przypadku podejrzenia, że osoba nieupoważniona weszła w posiadanie elementu uwierzytelniającego (np. karta dostępu, hasło).
- Nieudostępniania haseł innym użytkownikom i osobom trzecim.
- Informowania przełożonych o wszelkich zauważonych nieprawidłowościach skutkujących obniżeniem poziomu ochrony danych osobowych.
- Niepodłączania nieautoryzowanych urządzeń do stanowiska pracy (np. dysków USB, itp.) bez niezwłocznego przeskanowania oprogramowaniem antywirusowym.
- Niszczenia zbędnych dokumentów papierowych oraz nośników zawierających dane osobowe w niszczarkach dokumentów lub umieszczania ich w specjalnie do tego celu przygotowanych pojemnikach.
- Dbania, aby dokumenty zawierające dane osobowe były przechowywane w zamkniętych szafach lub szufladach, lub w inny sposób uniemożliwiający dostęp osobom nieupoważnionym.
- Dbania, aby osoby postronne (np. goście) poruszały się po pomieszczeniach, w których przetwarzane są dane osobowe tylko przy asyście osób zatrudnionych.
- Zmiany haseł dostępowych do systemu operacyjnego lub aplikacji służących do przetwarzania danych osobowych w przypadku podejrzenia, że hasło straciło swoją poufność.
- Stosowania następujących zasad w stosunku do haseł dostępowych:
  - ➔ hasła mogą być zapisywane wyłącznie w postaci zaszyfrowanej,

- ➔ hasła nie mogą być powszechnie używanymi słowami oraz w szczególności nie należy wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów,
- ➔ hasło musi składać się co najmniej z 8 znaków oraz powinno zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

- Wykazywania szczególnej ostrożności przy odbieraniu poczty elektronicznej przychodzącej od nieznanych adresatów lub o podejrzanym tytule e-maila, załącznika,
- Korzystania z funkcji BCC/UDW (adresatów ukrytych wiadomości), w sytuacji kiedy korespondencja jest kierowana do grupy osób, która nie jest sobie znana.
- Dbania, aby komputer wyposażony był w stosowny i na bieżąco aktualizowany program ochrony antywirusowej,
- Dbania, aby ekran monitora był ustawiony w sposób, uniemożliwiający wgląd osób nieuprawnionych.

Załącznik nr 2

PROCEDURA UWZGLĘDNIENIA OCHRONY DANYCH W FAZIE PROJEKTOWANIA I DOMYŚLNEJ OCHRONY DANYCH

KRAJOWA IZBA FIZJOTERAPEUTÓW

PODSTAWOWE DEFINICJE:

RODO – Rozporządzenie 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 (ogólne rozporządzenie o ochronie danych);

Administrator – Krajowa Izba Fizjoterapeutów z siedzibą w Warszawie przy ul. Nowogrodzkiej 31, 00-511 Warszawa;

System informatyczny – oznacza aplikację, system oraz każdy program w których dochodzi do przetwarzania danych osobowych;

Pracownik – każda osoba upoważniona przez Administratora do przetwarzania danych osobowych w Krajowej Izbie Fizjoterapeutów, bez względu na podstawę prawną zatrudnienia, stanowisko, charakter i rodzaj wykonywanej pracy

Osoba – osoba fizyczna, której dane dotyczą, np. fizjoterapeuta, pracownik, kandydat do pracy;

CEL PROCEDURY

1.1. Celem Procedury jest:

1.1.1. Zapewnienie przestrzegania przepisów ochrony danych osobowych przez Krajową Izbę Fizjoterapeutów;

1.1.2. Usystematyzowanie i udokumentowanie realizacji obowiązku uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych Administratora.

2. PODSTAWA PRAWNA

2.1. Podstawą prawną niniejszej procedury są:

2.1.1. Rozporządzenie 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 (ogólne rozporządzenie o ochronie danych);

3. ODPOWIEDZIALNOŚĆ

3.1. Za wdrożenie Procedury odpowiada Krajowa Izba Fizjoterapeutów, będąca Administratorem danych osobowych.

3.2. Za realizację obowiązków wynikających z Procedury odpowiada:

3.2.1. W zakresie uwzględnienia ochrony danych w fazie projektowania: każda wyznaczona osoba odpowiedzialna za poszczególny obszar działalności Krajowej Izby Fizjoterapeutów,

3.2.2. W zakresie domyślnej ochrony danych: każda wyznaczona osoba odpowiedzialna za poszczególny obszar działalności Krajowej Izby Fizjoterapeutów.

3.3. Za aktualizację Procedury odpowiada IOD.

4. ADRESACI PROCEDURY

4.1. Przestrzeganie postanowień Procedury należy do obowiązków:

4.1.1. IOD,

4.1.2. Każdej wyznaczonej osoby odpowiedzialnej za poszczególny obszar działalności Krajowej Izby Fizjoterapeutów,

4.1.3. Pracowników.

5. STOSOWANIE PROCEDURY

5.1. Procedura ma zastosowanie:

5.1.1. przy planowaniu nowych procesów, projektów, podczas których będzie dochodziło do przetwarzania danych osobowych w formie papierowej oraz w systemach informatycznych;

5.1.2.w trakcie przetwarzania danych osobowych.

6. OPIS POSTĘPOWANIA

6.1. **Uwzględnienie ochrony danych w fazie projektowania**

6.1.1. Każdy pracownik planując procesy lub projekty, podczas których będzie dochodziło do przetwarzania danych osobowych jest zobowiązany do poinformowania IOD o planowanych działaniach.

6.1.2. IOD ocenia planowane procesy/projekty w zakresie ochrony danych osobowych.

6.1.3. IOD ma prawo uzyskać wszystkie informacje, które są niezbędne do oceny, czy planowane procesy/projekty uwzględniają ochronę danych.

6.1.4. Podczas oceny, o której jest mowa powyżej IOD bierze pod uwagę:

- stan wiedzy technicznej,
- koszt wdrażania,
- charakter, zakres, kontekst i cele przetwarzania,
- ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania.

6.1.5. IOD opracowuje w formie pisemnej ocenę planowanych procesów/projektów wraz ze wskazaniem ewentualnych naruszeń ochrony danych oraz zaleceń wdrożenia środków technicznych i organizacyjnych, które zapewnią ochronę danych w planowanym procesie/projekcie.

6.1.6. IOD przekazuje dokument oceny osobie odpowiedzialnej za poszczególny obszar działalności Krajowej Izby Fizjoterapeutów,

6.1.7. Osoba odpowiedzialna za poszczególny obszar działalności Krajowej Izby Fizjoterapeutów, na podstawie dokumentu oceny podejmuje decyzję:

- o wdrożeniu/rozpoczęciu planowanych procesów/projektów lub
- o wdrożeniu odpowiednich środków technicznych i organizacyjnych zapewniających ochronę danych w planowanych procesach i projektach.

6.1.8. Dokument oceny planowanych procesów/projektów jest archiwizowany przez IOD .

6.2. Uwzględnienie ochrony danych w trakcie przetwarzania danych osobowych

6.2.1. Raz na rok IOD przeprowadza przegląd procesów/projektów przetwarzania danych osobowych w Krajowej Izbie Fizjoterapeutów w zakresie uwzględnienia ochrony danych przez te procesy/projekty.

6.2.2. Po każdym przeglądzie IOD. sporządza dokument oceny procesów/projektów przetwarzania danych osobowych.

6.2.3. Dokument oceny procesów/projektów przetwarzania danych osobowych jest przekazywany osobom decyzyjnym w zakresie realizowanych procesów.

6.2.4. Osoby decyzyjne w zakresie realizowanych procesów) na podstawie dokumentu oceny podejmują decyzje:

- o przetwarzaniu danych osobowych w dotychczasowy sposób,
- o wdrożeniu dodatkowych środków technicznych i organizacyjnych zapewniających ochronę danych w procesach przetwarzania danych.

6.2.5. Dokument oceny planowanych działań jest archiwizowany przez IOD.

6.3. Domyślna ochrona danych osobowych

6.3.1. Każdy autor projektu nowego systemu informatycznego lub zmian w istniejących systemach informatycznych jest zobowiązany do skonsultowania się w tej sprawie z IOD.

6.3.2. IOD weryfikuje czy w systemie informatycznym będą zapewnione ustawienia zapewniające ochronę danych.

6.3.3. IOD ma prawo uzyskać wszystkie informacje, które są niezbędne do oceny, czy system informatyczny będzie posiadał ustawienia zapewniające ochronę danych osobowych.

6.3.4. IOD oraz upoważniona osoba z działu IT podczas oceny systemy informatycznego bierze pod uwagę:

- czy domyślnie przetwarzane dane osobowe nie były udostępniane bez aktywności osoby, której dane dotyczą nieokreślonej liczbie osób fizycznych,
- czy zbierane dane osobowe są adekwatne do celu ich przetwarzania,
- czy dane osobowe są dostępne Osobie,
- czy termin przechowywania danych osobowych jest adekwatny do celów, w jakich dane są przechowywane.

6.3.5. IOD we współpracy z upoważnioną osobą z działu IT opracowuje w formie pisemnej ocenę systemu informatycznego wraz ze wskazaniem ewentualnych naruszeń ochrony danych oraz zaleceń wdrożenia środków technicznych i organizacyjnych, które zapewnią ochronę danych w ustawieniach systemu informatycznego.

6.3.6. IOD przekazuje dokument oceny systemu informatycznego autorowi projektu.

6.3.7. Autor projektu na podstawie dokumentu oceny systemu informatycznego podejmuje decyzję:

- O wdrożeniu odpowiednich środków technicznych i organizacyjnych zapewniających ochronę danych w pierwotnych ustawieniach systemu informatycznego lub
- O zachowaniu pierwotnej formy projektu.

7. KONTROLA REALIZACJI PROCEDURY

7.1. Administrator oraz IOD może prowadzić kontrolę realizacji Procedury.

7.2. Wszyscy pracownicy naruszający Procedurę mogą zostać pociągnięci do odpowiedzialności porządkowej lub dyscyplinarnej.

Załącznik nr 3

PROCEDURA KONSULTACJI Z ORGANEM NADORCZYM

8. DEFINICJE:

Administrator danych osobowych – Krajowa Izba Fizjoterapeutów z siedzibą w Warszawie (00-511), ul. Nowogrodzka 31

Inspektor Ochrony Danych (IOD) - osoba wyznaczona przez Administratora na stanowisko Inspektora Ochrony Danych w rozumieniu przepisów RODO

Organ nadzorczy – Prezes Urzędu Ochrony Danych Osobowych

Pracownik – każda osoba upoważniona przez Administratora do przetwarzania danych osobowych w Krajowej Izbie Fizjoterapeutów, bez względu na podstawę prawną zatrudnienia, stanowisko, charakter i rodzaj wykonywanej pracy

RODO – Rozporządzenie 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 (ogólne rozporządzenie o ochronie danych);

9. CEL PROCEDURY:

9.1. Celem procedury jest:

9.1.1. Realizacja obowiązujących przepisów prawa dotyczących ochrony danych osobowych,

10. PODSTAWA PRAWNA:

10.1. Podstawą prawną niniejszej procedury jest:

10.1.1. Rozporządzenie 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 (ogólne rozporządzenie o ochronie danych;

11. ODPOWIEDZIALNOŚĆ:

11.1. Za wdrożenie Procedury odpowiada Krajowa Izba Fizjoterapeutów będąca Administratorem danych osobowych.

11.2. Za realizację obowiązków wynikających z Procedury odpowiada osoba wyznaczona przez Administratora.

11.3. Za aktualizację Procedury odpowiada IOD.

12. ADRESACI PROCEDURY:

12.1. Przestrzeganie postanowień Procedury należy do obowiązków:

12.1.1. Administratora,

12.1.2. IOD,

12.1.3. wszystkich Pracowników dopuszczonych do przetwarzania danych osobowych, którzy uczestniczą w procedurze uprzednich konsultacji z organem nadzorczym.

13. ZAKRES STOSOWANIA:

13.1. Procedura ma zastosowanie w przypadku, gdy przeprowadzona wcześniej ocena skutków dla ochrony danych wskaże, że przetwarzanie danych powoduje wysokie ryzyko naruszenia praw i wolności osób fizycznych, których dane dotyczą.

14. OPIS POSTĘPOWANIA

14.1. IOD przygotowuje dokumentację niezbędną do przeprowadzenia konsultacji z organem nadzorczym. Dokumentacja ta zawiera:

14.1.1. Dane kontaktowe Administratora;

14.1.2. Jeśli w Krajowej Izbie Fizjoterapeutów został wyznaczony IOD, to jego dane kontaktowe;

14.1.3. Odpowiednie obowiązki Krajowej Izbie Fizjoterapeutów jako administratora, jeśli ma zastosowanie, to obowiązki współadministratorów oraz podmiotów przetwarzających uczestniczących w przetwarzaniu, szczególnie jeśli przetwarzanie odbywa się w ramach grupy przedsiębiorstw;

14.1.4. Cele i sposoby zamierzonego przetwarzania;

14.1.5. Środki i zabezpieczenia mające chronić prawa i wolności osób, których dane dotyczą;

14.1.6. Dokumentację przeprowadzenia oceny skutków dla ochrony danych, w której zostało wskazane, że przetwarzanie danych powoduje wysokie ryzyko naruszenia praw i wolności osób fizycznych, których dane dotyczą.

14.2. Przygotowaną dokumentację IOD przekazuje do Administratora.

14.3. Administrator po podpisaniu dokumentacji przekazuje ją do Biura Krajowej Izby Fizjoterapeutów w celu wysłania do organu nadzorczego.

14.4. Wysyłka dokumentacji do organu nadzorczego odbywa się sposób pozwalający na jej potwierdzenie np. listem poleconym.

14.5. W przypadku, gdy organ nadzorczy zażąda innych, dodatkowych informacji, IOD niezwłocznie przygotowuje te informacje i dostarcza je Administratorowi do podpisu.

14.6. Administrator przekazuje te informacje do Biura Krajowej Izby Fizjoterapeutów w celu ich wysłania do organu nadzorczego.

14.7. Wysyłka do organu nadzorczego odbywa się sposób pozwalający na jej potwierdzenie listem poleconym.

14.8. Po otrzymaniu odpowiedzi organu nadzorczego IOD przekazuje ją niezwłocznie Administratorowi.

14.9. Dalsze postępowanie w sprawie przetwarzania danych, które podlegało konsultacjom z organem nadzorczym jest uzależnione od zaleceń wskazanych przez organ nadzorczy w otrzymanej odpowiedzi.

15. KONTROLA REALIZACJI PROCEDURY:

15.1. Administrator oraz IOD może prowadzić kontrolę realizacji Procedury.

15.2. Wszyscy pracownicy naruszający niniejszą procedurę mogą zostać pociągnięci do odpowiedzialności porządkowej lub dyscyplinarnej.

16. TERMINY UDZIELANIA ODPOWIEDZI PRZEZ ORGAN NADZORCZY

16.1. Jeżeli organ nadzorczy jest zdania, że zamierzone przetwarzanie stanowiłoby naruszenie przepisów RODO – w szczególności gdy administrator niedostatecznie zidentyfikował lub zminimalizował ryzyko – organ nadzorczy w terminie **do ośmiu tygodni** od wpłynięcia wniosku o konsultacje udziela pisemnego zalecenia.

16.2. Okres ten może zostać **przedłużony o sześć tygodni** ze względu na złożony charakter zamierzonego przetwarzania. Organ nadzorczy informuje o takim przedłużeniu w terminie miesiąca od wpłynięcia wniosku o konsultacje, z podaniem przyczyn tego opóźnienia.

16.3. Bieg tych terminów może zostać zawieszony do czasu aż organ nadzorczy uzyska wszelkie informacje, których zażądał do celów konsultacji.

17. UPRAWNIENIA ORGANU NADZORCZEGO

17.1. Podczas konsultacji organ nadzorczy niezależnie od wydania pisemnego zlecenia może skorzystać z dowolnego ze swoich uprawnień:

17.1.1. nakazanie dostarczenia wszelkich informacji potrzebnych organowi nadzorczemu do realizacji swoich zadań;

17.1.2. prowadzenie postępowań w formie audytów ochrony danych;

17.1.3. dokonywanie przeglądu udzielonych certyfikacji;

17.1.4. zawiadamianie o podejrzeniu naruszenia niniejszego rozporządzenia;

17.1.5. uzyskiwanie dostępu do wszelkich danych osobowych i wszelkich informacji niezbędnych organowi nadzorczemu do realizacji swoich zadań;

17.1.6. uzyskiwanie dostępu do wszystkich pomieszczeń administratora i podmiotu przetwarzającego, w tym do sprzętu i środków służących do przetwarzania danych.

17.1.7. wydawanie ostrzeżeń dotyczących możliwości naruszenia przepisów RODO poprzez planowane operacje przetwarzania;

17.1.8. udzielanie upomnień w przypadku naruszenia przepisów niniejszego rozporządzenia przez operacje przetwarzania;

17.1.9. nakazanie dostosowania operacji przetwarzania do przepisów RODO, a w stosownych przypadkach wskazanie sposobu i terminu;

17.1.10. nakazanie zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych;

17.1.11. wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania;

17.1.12. nakazanie sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania oraz nakazanie powiadomienia o tych czynnościach odbiorców, którym dane osobowe ujawniono;

17.1.13. cofnięcie certyfikacji lub nakazanie podmiotowi certyfikującemu nieudzielania certyfikacji, jeżeli jej wymogi nie są spełnione lub przestały być spełniane;

17.1.14. zastosowanie, oprócz lub zamiast środków, o których mowa w ww. punktach administracyjnej kary pieniężnej zależnie od okoliczności konkretnej sprawy;

17.1.15. nakazanie zawieszenia przepływu danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej.

17.1.16. udzielanie porad administratorowi.