Polityka Bezpieczeństwa
Ochrony Danych Osobowych

w Przychodni Leczenia Ran i Pielęgnacji Stóp
"Centrum Stopy"
Kazimiera Urszula Proszkowska
(Dalej „Centrum Stopy")

1. Wstęp

Celem Polityki Bezpieczeństwa jest zapewnienie ochrony DANYCH OSOBOWYCH przetwarzanych przez CENTRUM STOPY przed wszelakiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.

Polityka określa obowiązki administratora danych w zakresie zabezpieczenia danych osobowych, o których mowa w Art. 4 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.

Polityka określa reguły dotyczące procedur zapewnienia bezpieczeństwa danych osobowych w postaci papierowej oraz zawartych w systemach informatycznych w firmie CENTRUM STOPY.

Jako załącznik do niniejszej polityki opracowano i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwaną dalej **„Instrukcją zarządzania systemem informatycznym RODO".** Określa ona sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem zapewnienia ich bezpieczeństwa.

Polityka została opracowana zgodnie z wymogami określonymi w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.
Polityka obowiązuje cały personel CENTRUM STOPY oraz dostawców, podmiotów współpracujących na zasadzie umów, mających jakikolwiek kontakt z danymi osobowymi objętymi ochroną.

Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.

Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

1. poufność danych - rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
2. integralność danych - rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
3. rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
4. integralność systemu rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

Za przestrzeganie zasad ochrony i bezpieczeństwa danych jest odpowiedzialny kierownik Agnieszka Głuszczak

2. Definicje

Przez użyte w Polityce określenia należy rozumieć:

1. Polityka – rozumie się przez to Politykę bezpieczeństwa ochrony danych osobowych w CENTRUM STOPY
2. Administrator Danych Osobowych – CENTRUM STOPY decydujący o celach i środkach przetwarzania danych osobowych;
3. Inspektor Ochrony Danych (IOD) – pracownik, lub inna osoba w CENTRUM STOPY, wyznaczony przez CENTRUM STOPY odpowiedzialny za organizację ochrony danych osobowych.
4. Kierownik – dyrektor, naczelnik, kierownik albo inna osoba pełniąca funkcje kierownicze jednostki bądź komórki organizacyjnej CENTRUM STOPY;
5. Rozporządzenie- rozumie się przez to rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (dalej RODO)
6. 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 takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
7. Zbiór danych – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
8. Usuwanie danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
9. Zgoda osoby, której dane dotyczą – oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
10. Baza danych osobowych – zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci zewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisane dane osobowe;
11. 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;
12. System informatyczny (system) – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
13. Użytkownik – pracownik/współpracownik CENTRUM STOPY posiadający uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych;
14. Zabezpieczenie systemu informatycznego – należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą,
15. Nośnik komputerowy (wymienny) – nośnik służący do zapisu i przechowywania informacji, np. dysk zewnętrzny, płyta CD, płyta DVD, pendrive;

3. Zadania IOD

Administrator i podmiot przetwarzający **wyznaczają inspektora ochrony danych, zawsze gdy**:

a) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
b) główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub
c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10.

Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa poniżej.
Inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług.

Do najważniejszych obowiązków Inspektora Ochrony Danych Osobowych należy:

a) **informowanie administratora**, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
b) **monitorowanie przestrzegania** niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
c) **udzielanie na żądanie** zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;
d) **współpraca** z organem nadzorczym;
e) **pełnienie funkcji punktu kontaktowego** dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

Inspektor Ochrony Danych ma prawo :

1. wstępu do pomieszczeń, w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą,
2. żądać złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego,
3. żądać okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli,
4. żądać udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.

4. Obowiązki Informacyjne Administratora Danych Osobowych.

A) Obowiązek podania tożsamości administratora, danych kontaktowych oraz tożsamości i danych kontaktowych przedstawiciela administratora.

Administrator musi przede wszystkim poinformować osobę, której dane dotyczą, o swojej tożsamości oraz danych kontaktowych. Tożsamość może wymagać podania również numerów publicznych rejestrów (takich jak KRS, NIP, Regon, czy PESEL), aby nie zachodziła wątpliwość co do tożsamości, szczególnie w przypadku osób fizycznych.

Pojęcie „danych kontaktowych" należy rozumieć szeroko, a więc nie tylko jako adres siedziby lub zamieszkania administratora, ale także jego numer telefonu, faxu, poczty elektronicznej, formularza kontaktowego na stronie internetowej etc. Chodzi zatem o maksymalne ułatwienie dostępu osób, których dane dotyczą, do administratora ich danych osobowych.

Analogiczny zestaw informacji podlegających udostępnieniu dotyczy przedstawiciela administratora, o ile taki został ustanowiony. Dotyczy to sytuacji przetwarzania danych osób przebywających na terenie UE przez administratora niemającego jednostek organizacyjnych w Unii, w przypadku oferowania towarów lub usług takim osobom, których dane dotyczą, w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty albo monitorowania ich zachowania, o ile do zachowania tego dochodzi w Unii.

B) Obowiązek podania danych kontaktowych inspektora ochrony danych

Konkluzje w zakresie pojęcia danych kontaktowych w przypadku inspektora ochrony danych są takie same, jak w przypadku administratora i jego przedstawiciela – udostępnieniu podlega nie tylko adres, ale i telefon, adres poczty elektronicznej etc. Nie ma konieczności podania tożsamości inspektora danych osobowych, czyli jego imienia i nazwiska. Informacje te nie powinny być udostępniane osobom, których dane dotyczą.

C) Obowiązek wskazania celów przetwarzania danych osobowych oraz podstawy prawnej przetwarzania.

Administrator powinien wskazać w sposób wyraźny i zrozumiały konkretny cel lub cele przetwarzania danych osobowych. Określenie celów powinno być starannie przemyślane, bowiem przetwarzanie danych w innym celu niż wskazany na początku będzie wymagało podania nowego celu oraz wszelkich niezbędnych rodzajów informacji podawanych już w przypadku przetwarzania w ramach pierwotnego celu, o ile uległy one zmianie w przypadku nowego celu.

Administrator musi także podać podstawę prawną przetwarzania. Oznacza to przede wszystkim wskazanie jednej z przesłanek legalizujących przetwarzanie danych, określonych w art. 6 ust. 1 RODO lub art. 9 ust. 1 RODO w przypadku danych o szczególnym charakterze (na gruncie UODO określonych w art. 27 oraz określanych w literaturze mianem sensytywnych lub wrażliwych). W przypadku, gdy dane osobowe są przetwarzane na podstawie szczegółowych uregulowań prawnych, należy podać zarówno przesłankę legalizującą z RODO, jak i tę szczegółową regulację.

D) Obowiązek wskazania prawnie uzależnionych interesów realizowanych przez administratora lub przez stronę trzecią

Jedną z przesłanek legalizujących przetwarzanie danych jest przypadek, w którym przetwarzanie to jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem. Gdy administrator działa w swojej ocenie w oparciu o przedmiotową przesłankę, to jego obowiązkiem jest nie tylko poinformować, że ta przesłanka jest podstawą przetwarzania danych, ale także wskazać, jakie konkretnie prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią wchodzą w grę. W tym kontekście wskazać należałoby, że jeśli prawnie uzasadniony interes w przetwarzaniu danych ma strona trzecia, to osoba, której dane dotyczą, powinna być poinformowana o tożsamości tej strony.

E) Obowiązek poinformowania o odbiorcach danych osobowych lub o kategoriach odbiorców, jeśli istnieją

Odbiorca danych oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią (strona trzecia oznacza z kolei osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe). Jednakże organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są uznawane za odbiorców.

Jeśli dane mają być przekazywane odbiorcom danych, to administrator musi poinformować osobę, której dane dotyczą, o tożsamości tych odbiorców lub o kategoriach tych odbiorców. Zgodnie z RODO, obowiązek informacyjny w tym zakresie powinien być wypełniony najpóźniej w momencie pierwszorazowego ujawnienia danych temu odbiorcy.

Jako alternatywę do przekazywania informacji o odbiorcach wskazuje się możliwość informowania o „kategoriach odbiorców". Powinno to dotyczyć sytuacji, gdy krąg odbiorców jest znaczny, a ponadto nie jest to krąg zamknięty, ani znany w chwili wypełnienia obowiązku informacyjnego. Mogą to być np. klienci administratora, dostawcy administratora etc.

F) Obowiązek przekazania informacji związanych z zamiarem przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej

Przedmiotowy obowiązek istnieje tylko wtedy, gdy administrator ma w ogóle zamiar przekazać dane do państwa trzeciego lub organizacji międzynarodowej. W takim przypadku administrator musi wskazać, czy doszło lub nie do stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych. Wskazane wyżej artykuły RODO dotyczą sytuacji, w których brak jest decyzji Komisji w zakresie stwierdzenia odpowiedniego stopnia ochrony. W takim przypadku administrator musi zapewnić odpowiednie zabezpieczenia (w tym poprzez ustanowienie wiążących reguł korporacyjnych) oraz że prawa osób, których dane dotyczą, będą egzekwowalne i zostaną im zapewnione skuteczne środki ochrony prawnej.

W razie braku decyzji Komisji stwierdzającej odpowiedni stopień ochrony lub braku odpowiednich zabezpieczeń określonych, w tym wiążących reguł korporacyjnych, dane osobowe mogą być przekazane

do państwa trzeciego lub organizacji międzynarodowej tylko w szczególnych przypadkach wskazanych w art. 49 ust. 1 RODO.

G) Wskazanie okresu, przez który dane osobowe będą przechowywane

Z uwagi na zasadę ograniczenia czasu przechowywania danych do okresu, w jakim są one niezbędne do spełnienia określonego celu przetwarzania, dane po tym okresie powinny być usunięte lub zanonimizowane. Administrator powinien podać albo wprost informację o okresie przetwarzania, a jeśli nie jest to możliwe, kryteria ustalania tego okresu – np. wykonanie umowy, zakończenie okresu świadczenia usługi etc.

H) Podanie informacji o prawach osób, których dane dotyczą

Administrator zobowiązany jest przekazać osobom, których dane dotyczą, informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych. Powyższe obowiązki informacyjne wiążą się w szczególności z zasadą prawidłowości danych oraz ograniczenia przetwarzania.

Prawo do ograniczenia przetwarzania danych w przypadkach związanych z RODO powoduje, że dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

Prawo do przenoszenia danych polega na tym, że osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy.

I) Podanie informacji o prawie wniesienia skargi do organu nadzorczego

Administrator ma obowiązek poinformować osobę, której dane dotyczą, o prawie wniesienia skargi do organu nadzorczego. Należy poinformować tę osobę o pełnej nazwie organu oraz jego adresie.

J) Podanie informacji w zakresie wymogu podania danych

Administrator informuje, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych. Obowiązek ten ma na celu przedstawienie osobie, której dane dotyczą, jej pełnej sytuacji prawnej w zakresie dobrowolności podania przez nią jej danych osobowych. Ta regulacja wynika z faktu, że częstokroć osoby, których dane dotyczą, nie wiedzą, z czego wynika potrzeba przetwarzania ich danych i jakie są konsekwencje ich niepodania. Dotyczy to w szczególności niezbędności podania określonych danych. Dotyczy to w szczególności takich danych, które zwykle nie są niezbędne do większości celów, jak telefon, adres e-mail, czy dane biometryczne.

K) Podanie informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu

Co do zasady, osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa. Profilowanie w świetle RODO 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.
Od prawa niepodlegania decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu RODO przewiduje następujące wyjątki, jeżeli ta decyzja:

a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;
b) jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub
c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

W takim przypadku, gdy podejmowanie decyzji w sposób zautomatyzowany jest prawnie dopuszczalne, administrator powinien przekazać osobie, której dane dotyczą, istotne informacje o zasadach podejmowania decyzji, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

DODATKOWE OBOWIĄZKI W PRZYPADKU POZYSKANIA DANYCH NIE OD OSOBY, KTÓREJ DANE DOTYCZĄ

W razie pozyskania danych osobowych nie od osoby, której dane dotyczą, administrator danych musi dodatkowo poinformować osobę, której dane dotyczą, o:

a) kategoriach odnośnych danych osobowych, które są przetwarzane – a więc rodzaju przetwarzanych danych, np. imię, nazwisko, adres, data urodzenia etc.
b) źródle pochodzenia danych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych.

W przypadku pozyskania danych osobowych od osoby, której dane dotyczą, wszelkie wskazane wyżej informacje powinny być tej **osobie przekazane podczas pozyskiwania danych.**
Z kolei w przypadku pozyskiwania danych osobowych nie od osoby, której dane dotyczą, z oczywistych względów administrator nie ma możliwości spełnienia swoich obowiązków informacyjnych podczas pozyskiwania danych. RODO ustanawia w tym zakresie stosowne terminy w zależności od sytuacji.
Wskazane wyżej informacje administrator podaje:

a) w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych;
b) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub
c) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.

5. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

Szczegółowe rozmieszczenie zbiorów dokumentacji papierowej i elektronicznej, zawierającej dane osobowe, opisane jest w Załączniku A „Wykaz zbiorów danych osobowych”.

6. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Wykaz zbiorów danych osobowych w postaci dokumentacji papierowej i elektronicznej wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opisany jest w Załączniku A „Wykaz zbiorów danych osobowych".

7. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

CENTRUM STOPY nie posiada programów przetwarzających dane osobowe w dniu tworzenia tego dokumentu.

8. Sposób przepływu danych pomiędzy poszczególnymi systemami

CENTRUM STOPY nie posiada programów przetwarzających dane osobowe w dniu tworzenia tego dokumentu.

9. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

A. Środki ochrony fizycznej

1. Podstawowe zabezpieczenia fizyczne opisane są w Załączniku A „Wykaz zbiorów danych osobowych".
2. Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych
3. Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych.
4. CENTRUM STOPY na dzień dzisiejszy nie posiada Kopii zapasowych/archiwalnych zbiorów danych osobowych i z racji tego nie są nigdzie przechowywane.

B. Środki sprzętowe, informatyczne i telekomunikacyjne

1. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.
2. Zbiór danych osobowych prowadzony jest przy użyciu komputera przenośnego i jest zabezpieczony poprzez (np. hasła / szyfrowanie dysku / zabezpieczenia biometryczne)
3. Lokalizacja urządzeń komputerowych (komputerów typu PC, terminali, drukarek) uniemożliwia osobom niepowołanym dostęp do nich oraz wgląd do danych wyświetlanych na monitorach komputerowych.
4. Komputery przenośne, wykorzystywane do przetwarzania danych osobowych, po zakończonej pracy są przechowywane w warunkach zapewniających ich bezpieczeństwo.
5. System operacyjny zapewnia odpowiednie restrykcje w zakresie dostępu do danych i aplikacji

6. Zastosowano urządzenia typu UPS chroniące system informatyczny służący do przetwarzania danych osobowych przed awarią zasilania.
7. Użyto system Firewall do ochrony dostępu do sieci komputerowej.

C. Środki ochrony w ramach oprogramowania urządzeń teletransmisji

1. Proces teletransmisji zabezpieczony jest za pomocą środków uwierzytelnienia.
2. Proces teletransmisji zabezpieczony jest za pomocą środków kryptograficznej ochrony danych osobowych.
3. Zastosowano procedurę oddzwonienia (callback) przy transmisji realizowanej za pośrednictwem modemu.

D. Środki ochrony w ramach oprogramowania systemu

1. Serwery obsługujące bazę danych oraz stanowiska komputerowe służące do przetwarzania danych osobowych dostępne są wyłącznie po przeprowadzeniu prawidłowego procesu autoryzacji (system użytkowników i haseł, ograniczenie dostępu do poziomu poleceń systemowych lub zakaz wykonywania poleceń systemowych (restricted Shell)).
2. Zastosowano oprogramowanie umożliwiające wykonanie kopii zapasowych zbiorów danych osobowych.
3. Zastosowano oprogramowanie zabezpieczające przed nieuprawnionym dostępem do systemu informatycznego.

E. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych

1. Dostęp do zbioru danych osobowych zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
2. Zastosowano mechanizm umożliwiający rejestrację identyfikatora użytkownika wprowadzającego dane osobowe.
3. Wykorzystano środki pozwalające na rejestrację dokonanych zmian w zbiorze danych osobowych.
4. Zastosowano środki umożliwiające określenie praw dostępu do zbioru danych osobowych.
5. Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji.
6. Dla każdego użytkownika systemu jest ustalony odrębny identyfikator.
7. Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.

F. Środki ochrony w ramach systemu użytkowego

1. Zastosowano zabezpieczone hasłem wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika.
2. Zastosowano blokadę klawiatury, w przypadku dłuższej nieaktywności użytkownika.
3. Zastosowano działający w „tle” program antywirusowy na komputerach użytkowników.

G. Środki organizacyjne

1. Opracowano i wdrożono Politykę bezpieczeństwa ODO i Instrukcję zarządzania systemem informatycznym ODO.
2. Wdrożono odpowiedni podział obowiązków i kontroli dostępu.

3. Do danych osobowych mają dostęp jedynie osoby posiadające upoważnienie nadane przez Administratora Danych.
4. Administrator danych prowadzi Ewidencję osób upoważnionych do przetwarzania danych osobowych.
5. Wprowadzono mechanizmy autoryzacji odpowiednio zabezpieczone przed dostępem osób trzecich.
6. Wprowadzono procedury alarmowe i informacyjne.
7. Osoby upoważnione do przetwarzania danych osobowych przed dopuszczeniem do tych danych są szkolone w zakresie obwiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych osobowych. Osoby te są zobowiązane do podpisania stosownego oświadczenia.
8. Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane są do zachowania ich w tajemnicy.
9. Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym.
10. Tymczasowe wydruki z danymi osobowymi są po ustaniu ich przydatności niszczone w niszczarce.
11. Korespondencja w zakresie procedur kadrowo-płacowych prowadzona jest za pomocą listów poleconych.
12. Zapewniono klauzule poufności z wszystkimi podmiotami zewnętrznymi mającymi dostęp do danych osobowych Firmy.
13. Zapewnia się bezpieczne przechowywanie lub niszczenie uszkodzonych nośników zawierających dane osobowe (np dysk twardy), szczególnie, gdy sprzęt, w którym zamontowany jest dany nośnik przekazywany jest do naprawy do firmy zewnętrznej.

10. Obowiązek administratora oceny skutków ryzyka przetwarzania danych osobowych.

Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

Dokonując oceny skutków dla ochrony danych, administrator konsultuje się z inspektorem ochrony danych, jeżeli został on wyznaczony.

Ocena skutków dla ochrony danych, o której mowa w ust. 1, jest wymagana w szczególności w przypadku:

a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10; lub
c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

Ocena zawiera co najmniej:

a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;

b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;

c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1; oraz

d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

11. Instrukcja alarmowa (postępowania w przypadku naruszenia ochrony danych osobowych)

Zdarzenia zagrażające bezpieczeństwu danych osobowych

Do zdarzeń zagrażających bezpieczeństwu danych osobowych należą:

1. próby naruszenia ochrony danych:
    - z zewnątrz – włamania do systemu, podsłuch, kradzież danych,
    - z wewnątrz – nieumyślna lub celowa modyfikacja danych, kradzież danych,
2. programy destrukcyjne:
    - wirusy,
    - konie trojańskie,
    - makra,
    - bomby logiczne,
3. awarie sprzętu lub uszkodzenie oprogramowania,
4. zabór sprzętu lub nośników z ważnymi danymi,
5. inne skutkujące utratą danych osobowych, bądź wejściem w ich posiadanie osób nieuprawnionych.
6. usiłowanie zakłócenia działania systemu informatycznego,

Procedura postępowania w przypadkach naruszenia bezpieczeństwa danych osobowych

1. W przypadku stwierdzenia faktu nieuprawnionego przetwarzania, ujawnienia lub nienależytego zabezpieczenia przed osobami nieuprawnionymi danych osobowych, jak również stwierdzenia istnienia przesłanek wskazujących na prawdopodobieństwo naruszenia ochrony danych osobowych, każdy pracownik/współpracownik CENTRUM STOPY zobowiązany jest poinformować bezpośredniego przełożonego, który powiadamia o zdarzeniu Administratora.
2. W sytuacji, określonej w pkt. 1, ADO/IOD prowadzi postępowanie wyjaśniające w toku, którego:
    - ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,
    - ustala osoby odpowiedzialne za naruszenie,

- podejmuje działania w kierunku ograniczenia szkód oraz przeciwdziałania podobnym przypadkom w przyszłości,

3. sporządza pisemną notatkę z przeprowadzonego postępowania. Administrator zobowiązany jest:
   - W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55 RODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia
   - Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
4. IOD powiadamia o wynikach postępowania wyjaśniającego kierownik Agnieszka Głuszczak
5. W przypadku zaistnienia zdarzenia, określonego w ust. 1, decyzje dyscyplinarne w stosunku do winnych oraz w sprawie wniosku o pociągnięcie ich do odpowiedzialności karnej podejmuje kierownik Agnieszka Głuszczak z własnej inicjatywy lub na wniosek kierownika właściwej jednostki lub komórki organizacyjnej CENTRUM STOPY.

Procedura postępowania w przypadkach zagrożeń (stwierdzenia słabości systemu)

1. W przypadku jakiejkolwiek nieprawidłowości w działaniu systemu, uszkodzenia lub podejrzenia o uszkodzenie sprzętu, oprogramowania lub danych należy bezzwłocznie powiadomić Administratora Systemu.
2. W przypadku włamania lub podejrzenia o włamanie do systemu administrator danego systemu podejmuje działania w celu zabezpieczenia systemu i danych:
   - zmienia hasła administracyjne,
   - określa rodzaj i sposób włamania,
   - podejmuje działania w celu uniemożliwienia ponownego włamania tego samego typu,
   - szacuje straty w systemie,
   - przywraca stan systemu sprzed włamania.
3. W przypadku uszkodzenia sprzętu lub programów z danymi administrator danego systemu podejmuje działania w celu:

- określenia przyczyny uszkodzenia,
- oszacowania strat wynikłych z w/w uszkodzenia,
- naprawy uszkodzeń, a w szczególności naprawy sprzętu, ponownego zainstalowania danego programu, odtworzenie jego pełnej konfiguracji oraz wczytania danych z ostatniej kopii zapasowej.

4. W przypadku uszkodzenia danych administrator systemu podejmuje następujące działania:

- ustala przyczynę uszkodzenia danych,
- określa wielkość i jakość uszkodzonych danych,
- podejmuje działania w celu odtworzenia danych z ostatniej kopii zapasowej.

5. W przypadku stwierdzenia nieprawidłowości w funkcjonowaniu sieci telekomunikacyjnej każdy użytkownik zobowiązany jest niezwłocznie powiadomić administratora sieci, który podejmuje działania w celu ustalenia przyczyn zaistniałej sytuacji oraz wyeliminowania nieprawidłowości.

W przypadku zidentyfikowania osób odpowiedzialnych za wystąpienie któregoś ze zdarzeń zagrażających bezpieczeństwu danych administrator danego systemu zobowiązany jest powiadomić bezpośredniego przełożonego winnej osoby oraz IOD, a ten kierownik Agnieszka Głuszczak

12.Procedura działań korygujących i zapobiegawczych

1. Celem procedury jest uporządkowanie i przedstawienie czynności związanych z: inicjowaniem oraz realizacją działań korygujących i zapobiegawczych wynikających z zaistnienia incydentów bezpieczeństwa lub słabości systemu ochrony danych osobowych.
2. Procedura działań korygujących i zapobiegawczych obejmuje wszystkie te procesy, w których incydenty bezpieczeństwa, zagrożenia lub słabości systemu ochrony danych osobowych mogą wpłynąć na zgodność z wymaganiami RODO, jak również na poprawne funkcjonowanie systemu ochrony danych osobowych.
3. Osobą odpowiedzialną za nadzór nad procedurą jest kierownik Agnieszka Głuszczak
4. , przy czym czynności związane z realizacją poszczególnych zadań / zabezpieczeń wykonuje osoba odpowiedzialna a zatwierdza kierownik Agnieszka Głuszczak

Definicje

1. Niezgodność – niespełnienie wymagania, czyli potrzeby lub oczekiwania, które zostało ustalone, przyjęte zwyczajowo lub jest obowiązkowe.
2. Incydent – naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność.
3. Zagrożenie – potencjalna możliwość wystąpienia incydentu.
4. Słabość systemu – zdarzenie, stan rzeczy zwiększający ryzyko wystąpienia incydentu.
5. Działanie korygujące – jest to działanie przeprowadzane w celu wyeliminowania przyczyny wykrytej niezgodności / incydentu lub innej niepożądanej sytuacji.
6. Działanie zapobiegawcze – jest to działanie, które należy przedsięwziąć, aby wyeliminować przyczyny potencjalnej niezgodności / incydentu lub innej potencjalnej sytuacji niepożądanej.
7. Korekcja – działanie w celu wyeliminowania wykrytej niezgodności lub incydentu.
8. Kontrola (Audit) – systematyczny, niezależny i udokumentowany proces oceny skuteczności systemu ochrony danych osobowych, na podstawie określonych kryteriów, wymagań, polityk i procedur.

Opis czynności

1. kierownik Agnieszka Głuszczak jest odpowiedzialny za analizę incydentów bezpieczeństwa, zagrożeń lub słabości systemu ochrony danych osobowych. Typowymi źródłami informacji o incydentach, zagrożeniach lub słabościach są:

- zgłoszenia od pracowników
- alarmy z systemów informatycznych
- analizy incydentów
- wyniki auditów / kontroli

2. Gdy kierownik Agnieszka Głuszczak stwierdzi konieczność podjęcia działań korygujących lub zapobiegawczych, określa:

- Źródło powstania incydentu / zagrożenia lub słabości
- Zakres działań korygujących lub zapobiegawczych
- Termin realizacji
- Osobę odpowiedzialną

3. Kierownik Agnieszka Głuszczak jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych.
4. Po przeprowadzeniu działań korygujących lub zapobiegawczych, IOD jest zobowiązany do oceny efektywności ich zastosowania.

5. Powyższe czynności kierownik Agnieszka Głuszczak rejestruje w pliku **Załącznik B - zadania ODO.xls.**

13.Kontrola systemu ochrony danych osobowych i przegląd zarządzania

1. Celem procedury jest uporządkowanie i przedstawienie czynności związanych z: kontrolą stanu bezpieczeństwa danych osobowych oraz okresową oceną Systemu Ochrony Danych Osobowych.
2. Procedura obejmuje wszystkie procesy organizacji, gdzie przestrzeganie zasad ochrony danych osobowych jest wymagane.
3. Do kontroli stanu ochrony danych osobowych w CENTRUM STOPY upoważnieni są:

- Kierownik Agnieszka Głuszczak lub osoby przez nich upoważnione,
- Inspektor Ochrony Danych

4. Raz w roku kontroli (auditowi) podlegają wszystkie systemy informatyczne przetwarzające dane osobowe oraz zabezpieczenia fizyczne i bezpieczeństwo osobowe.
5. Inspektor Ochrony Danych przygotowuje plan kontroli uwzględniając zakres oraz potrzebne zasoby fizyczne, czasowe i osobowe.
6. Kontroli podlega warstwa sprzętowa, systemy operacyjne oraz aplikacje, realizacja zabezpieczeń przez pracowników firmy i przestrzeganie polityki bezpieczeństwa. Kontrola (audit przeprowadzana jest z użyciem dokumentu **Załącznik C - lista kontrolna audit ODO**.
7. Po dokonanej kontroli kierownik Agnieszka Głuszczak przygotowuje raport audytowy, którego jeden egzemplarz przekazuje kierownikowi kontrolowanej jednostki lub komórki organizacyjnej. Na jego podstawie informuje Zarząd o konieczności podjęcia właściwych działań korygujących i doskonalących.
8. Raz w roku po przeprowadzonej kontroli kierownik Agnieszka Głuszczak przygotowuje ocenę roczną stanu funkcjonowania systemu ochrony danych osobowych i przedstawia go Zarządowi na Przeglądzie zarządzania ODO. Na jej podstawie informuje Zarząd o konieczności podjęcia właściwych działań korygujących i doskonalących. Potwierdzeniem przeprowadzenia przeglądu zarządzania ODO jest protokół (Patrz **Załącznik D - Przegląd stanu bezpieczeństwa danych osobowych.doc**).

14.Postanowienia końcowe

1. „Polityka Bezpieczeństwa” jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.
2. Prawnicy/współpracownicy są obowiązani zapoznać z treścią „Polityki bezpieczeństwa” każdego użytkownika.
3. Użytkownik zobowiązany jest złożyć oświadczenie o tym, iż został zaznajomiony z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania.
4. Oświadczenie potwierdzające zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania, przechowywane jest w aktach osobowych pracownika.
   - Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
   - Kara dyscyplinarna, orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. nr 101, poz. 926) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
   - Wszystkie regulacje dotyczące systemów informatycznych określone w Polityce Bezpieczeństwa dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
5. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej „Polityce”.
6. W sprawach nieuregulowanych w niniejszej „Polityce bezpieczeństwa” mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (tj. Dz.U. z 2002r., Nr 101, poz. 926 ze zm.) oraz wydanych na jej podstawie aktów wykonawczych.