POLITYKA BEZPIECZEŃSTWA

OCHRONY DANYCH OSOBOWYCH

W GMINNYM OŚRODKU POMOCY SPOŁECZNEJ

W GOSTYCYNIE

SPIS TREŚCI

WPROWADZENIE

Polityka ochrony danych osobowych, zwana dalej Polityką, jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez **Gminny Ośrodek Pomocy Społecznej w Gostycynie z siedzibą na ul. Sępoleńska 12a, 89 – 520 Gostycyn** w związku z wymaganiami 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 – dalej RODO).

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z RODO.

UWAGI DOTYCZĄCE DOKUMENTU

Każda osoba, mająca dostęp do danych osobowych z upoważnienia podmiotu: **Gminny Ośrodek Pomocy Społecznej w Gostycynie** (zwanej dalej Administratorem Danych Osobowych, w skrócie Administratorem lub ADO), została zapoznana z Polityką i zobowiązana do jej przestrzegania, w zakresie wynikającym z przydzielonych zadań. Dotyczy to w szczególności pracowników zatrudnionych przez Administratora. Osoby, o których mowa powyżej złożyły na piśmie oświadczenie o zapoznaniu się z treścią Polityki oraz zobowiązały się do stosowania zawartych w niej postanowień. Wzór treści oświadczenia stanowi załącznik nr 1

Administrator Danych Osobowych przetwarza informacje o osobach fizycznych służące do realizacji celów szczegółowo ujętych w rejestrze czynności przetwarzania danych stanowiący załącznik nr 2 oraz w rejestrze kategorii czynności, który stanowi załącznik nr 3

Informacje są przetwarzane przez Administratora Danych Osobowych w postaci dokumentacji tradycyjnej i elektronicznej.

Z uwagi na użycie do przetwarzania danych osobowych systemów informatycznych, uzupełnieniem treści Polityki jest Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej Instrukcją, stanowiąca załącznik nr 4.

Zakresy ochrony danych osobowych określone przez dokument Polityki i załączników do Polityki mają zastosowanie do:

1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz zbiorów papierowych, w których przetwarzane są dane osobowe;
2) informacji będących własnością Administratora lub podmiotów współpracujących, o ile zostały przekazane na podstawie umów lub porozumień;
3) wszystkich lokalizacji - budynków i pomieszczeń, w których są lub będą przetwarzane dane

osobowe;

4) wszystkich pracowników Administratora w rozumieniu przepisów Kodeksu Pracy konsultantów, praktykantów, stażystów i innych upoważnionych przez niego osób mających dostęp do danych osobowych.

ODPOWIEDZIALNOŚĆ ZA OCHRONĘ DANYCH OSOBOWYCH

SCHEMAT ORGANIZACYJNY PRZETWARZANIA

Za prawidłowość procesów przetwarzania danych osobowych oraz ich ochronę zgodnie z przepisami prawa oraz niniejszej Polityki odpowiadają:

1) Administrator danych osobowych (ADO),
2) Podmiot przetwarzający dane na zlecenie ADO zwany dalej Przetwarzającym (inaczej Procesorem).
3) Inspektor Ochrony Danych Osobowych zwany dalej IOD,
4) Administrator Systemów Informatycznych, którym jest podmiot zewnętrzny świadczący usługi informatyczne na podstawie zawartej umowy, zwany dalej ASI,
5) Każda osoba, wykonująca pracę bądź świadcząca usługi cywilnoprawne na rzecz ADO, która uzyskała upoważnienie do przetwarzania danych osobowych.

SZCZEGÓŁOWY ZAKRES ZADAŃ I ODPOWIEDZIALNOŚCI

Obowiązki Administratora Danych Osobowych

Administratorem danych osobowych jest: Gminny Ośrodek Pomocy Społecznej w Gostycynie.

Wyłączenie w przypadkach wskazanych w załączniku 3 - rejestr kategorii czynności przetwarzania Administrator pełni na podstawie zawartej umowy rolę Przetwarzającego. Zadania i odpowiedzialności w tym względzie wyznaczają szczegółowo zapisy właściwych umów powierzenia.

Administrator danych osobowych odpowiada za:

1) podział zadań i obowiązków związanych z organizacją ochrony danych osobowych w tym podjęcie decyzji o wyznaczeniu IOD,
2) nadzór nad zapewnianiem bezpieczeństwa przetwarzania danych osobowych oraz wspieranie realizacji przedsięwzięć technicznych i organizacyjnych związanych z ochroną danych osobowych
3) zapewnienie odpowiednich do zagrożeń i kategorii danych środków technicznych i rozwiązań organizacyjnych,
4) organizowanie szkoleń w zakresie przetwarzania danych i sposobów ich ochrony,
5) okresowe szacowanie ryzyka przetwarzania danych osobowych,

6) kontrolę przestrzegania zasad bezpieczeństwa przetwarzania i ochrony danych osobowych,
7) wydawanie i anulowanie upoważnień do przetwarzania danych osobowych oraz prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych, z zastrzeżeniem, że ADO może wskazać podmiot bądź osobę, która będzie prowadziła taką ewidencję w jego imieniu.
8) przeglądy i aktualizację dokumentacji przetwarzania danych osobowych,
9) zgłaszanie bez zbędnej zwłoki (nie później niż w terminie 72 godzin po stwierdzeniu wystąpienia zdarzenia) naruszeń ochrony danych osobowych do PUODO z zastrzeżeniem sytuacji, w których jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych,
10) dokonanie oceny skutków planowanych operacji przetwarzania, w przypadku gdy dany rodzaj przetwarzania ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych

Obowiązki Podmiotu Przetwarzającego

Zakres obowiązków i odpowiedzialności każdorazowo jest wyznaczany właściwą umową powierzenia danych osobowych.

Przetwarzający wykonuje operacje przetwarzania na udokumentowane polecenia ADO lub w jego imieniu.

Obowiązki Inspektora Ochrony Danych

Do obowiązków IOD należy:

1) informowanie ADO oraz jego pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych
2) doradzanie ADO w sprawie właściwego wykonywania obowiązków wynikających z przepisów prawa i dokumentu Polityki,
3) monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich oraz niniejszej Polityki, w tym podejmowanie działań zwiększających świadomość, przeprowadzanie szkoleń personelu uczestniczącego w operacjach przetwarzania oraz przeprowadzanie audytów w zakresie zgodności przetwarzania z przepisami RODO i niniejszej Polityki oraz innymi,
4) udzielanie na żądanie ADO zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania,
5) współpraca z organem nadzorczym,
6) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem,

7) pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy rozporządzenia,
8) wspieranie ADO w prowadzeniu rejestru czynności przetwarzania danych osobowych i rejestru kategorii czynności przetwarzania
9) wspieranie ADO w realizacji obowiązku notyfikacji naruszeń (prowadzenie postepowań wyjaśniających, rejestru naruszeń)

Obowiązki Administratora Systemu Informatycznego – podmiot zewnętrzny

Do obowiązków ASI należy:

1) zapewnienie optymalnej ciągłości działania systemu informatycznego,
2) nadzór nad przeprowadzanymi pracami przy naprawach, konserwacjach systemów informatycznych zawierających dane osobowe,
3) nadawanie, zmiana i blokowanie uprawnień do systemów informatycznych w oparciu o upoważnienie nadane przez ADO
4) właściwa konfiguracja systemu informatycznego zapewniająca jego bezpieczeństwo i ograniczenie dostępu do danych osobowych przez osoby nieupoważnione,
5) monitorowanie funkcjonowania zabezpieczeń systemów informatycznych wdrożonych w celu ochrony danych osobowych,
6) nadzór na sprawnym działaniem systemu sporządzania kopii bezpieczeństwa (lub sporządzanie przechowywanie i regularne testowanie kopii bezpieczeństwa)
7) podejmowanie działań w przypadku wykrycia naruszeń bezpieczeństwa w systemie zabezpieczeń lub podejrzenia naruszenia np. pojawienie się wirusa w systemie (w tym niezwłoczne informowanie ADO oraz IOD)
10) instalacja i konfiguracja oprogramowania na poszczególnych urządzeniach służących przetwarzaniu danych (stacjach roboczych, terminalach)
11) świadczenie pomocy technicznej (oprogramowanie i urządzenia) dla pracowników ADO
12) dokonanie okresowej weryfikacji zainstalowanego oprogramowania na stacjach roboczych poszczególnych użytkowników,
13) instalowanie i weryfikację zabezpieczeń urządzeń mobilnych służących do przetwarzania danych osobowych,
14) zapewnienie bezpieczeństwa sieci komputerowej
15) zapewnienie prawidłowej konfiguracji i działania ochrony antywirusowej
16) pozostałe działania przewidziane w załączniku numer 4 (Instrukcji)

Obowiązki Upoważnionych

1) znajomość treści Polityki oraz przepisów powszechnie obowiązującego prawa w obszarze ochrony danych osobowych, przetwarzanych przez ADO,

2) znajomość, zrozumienie i stosowanie w możliwie największym zakresie wszelkich dostępnych środków ochrony danych osobowych oraz uniemożliwienie osobom nieuprawnionym dostępu do przetwarzanych danych,
3) przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa oraz przyjętymi regulacjami, w granicach przyznanego upoważnienia,
4) postępowanie zgodnie z ustalonymi regulacjami wewnętrznymi dotyczącymi przetwarzania danych osobowych,
5) zachowanie w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia, również po ustaniu zatrudnienia lub współpracy,
6) ochrona danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem,
7) niezwłoczne informowanie o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe do ADO lub (IOD jeżeli powołano).

STOSOWANE ZASADY OCHRONY DANYCH OSOBOWYCH

ZASADY OGÓLNE stosowane przez Administratora:

Legalność – ADO dba o ochronę prywatności i przetwarza dane zgodnie z prawem, zapewnia, że dane są legalnie przetwarzane (na podstawie art. 6, 9 RODO),

Bezpieczeństwo - ADO zapewnia odpowiedni do zidentyfikowanych zagrożeń poziom bezpieczeństwa danych, podejmując stałe działania doskonalące w tym względzie,

Przestrzeganie praw jednostki - ADO umożliwia osobom, których dane przetwarza wykonywanie swoich praw i prawa te realizuje,

Rozliczalność - ADO dokumentuje to, w jaki sposób spełnia obowiązki aby w każdej chwili móc wykazać zgodność,

Celowość - ADO przetwarza dane osobowe wyłącznie zgodnie z określonymi celami,

Adekwatność - ADO nie przetwarza danych w zakresie szerszym niż konieczny dla osiągnięcia oznaczonego celu,

Ograniczenia czasowego - ADO nie przetwarza danych osobowych dłużej niż jest to konieczne dla osiągnięcia oznaczonego celu, ADO określił konkretny czas przez jaki przetwarzane są dane (załącznik nr 2 - rejestr czynności przetwarzania).

INNE ZASADY stosowane przez Administratora

ZASADA WIEDZY KONIECZNEJ – oznaczająca, że dostęp do informacji ograniczony jest do tych danych, które są niezbędne do prawidłowego wykonywania obowiązków na danym stanowisku.

ZASADA CHRONIONEGO POMIESZCZENIA – wyrażająca się tym, że pod nieobecność osoby uprawnionej w pomieszczeniach (poza ogólnodostępnymi typu korytarze) nie mogą przebywać osoby postronne. Po opuszczeniu pomieszczenia osoba odpowiedzialna zamyka je na klucz (bez pozostawiania kluczy w zamkach – wyjątek stanowi ewakuacja).

ZASADA NADZOROWANIA KLUCZY – pobrane/posiadane klucze do pomieszczeń powinny być w każdym czasie pod kontrolą. Pracownicy odpowiedzialni są za należyte zabezpieczenie kluczy do ich biurek oraz szaf biurowych, w których przechowywane są dokumenty. Ostatni pracownik opuszczający dane pomieszczenie po zakończeniu pracy zamyka szafy i chowa klucze w bezpieczne, ustalone z pozostałymi współpracownikami miejsce.

ZASADA CZYSTEGO BIURKA – oznaczająca, że zarówno dokumentów papierowych, jak i jakichkolwiek innych nośników informacji (np. pendrive, płyt CD), nie pozostawia się bez nadzoru.

ZASADA CZYSTEGO EKRANU – każdorazowe opuszczenie pomieszczenia w godzinach pracy powinno zostać poprzedzone zablokowaniem komputera. Na wszystkich stacjach aktywny jest wygaszasz ekranu zabezpieczony hasłem, który aktywizuje się automatycznie po przekroczeniu, określonego w minutach, czasu braku aktywności. Każdy użytkownik systemu zobowiązany jest zadbać, aby po zakończeniu pracy sprzęt został poprawnie wyłączony.

ZASADA CZYSTEJ DRUKARKI – wszystkie osoby zobowiązane są do zabierania dokumentów z drukarek zaraz po ich wydrukowaniu (dotyczy to zwłaszcza drukarek usytuowanych w miejscach ogólnie dostępnych).

ZASADA CZYSTEGO KOSZA – nieprzydatne dokumenty, brudnopisy, zbędne kopie muszą zostać trwale zniszczone w sposób uniemożliwiający odtworzenie zawartych w nich informacji. Zasada ta dotyczy również informacji zapisanych w innej niż papierowa formie – na nośnikach elektronicznych. Zabrania się wrzucania do kosza na śmieci płyt CD/DVD oraz innych nośników, które powinny zostać zniszczone w specjalistycznych niszczarkach.

ZASADA LEGALNOŚCI OPROGRAMOWANIA – wyrażająca się zabranianiem pracownikom samodzielnego instalowania oprogramowania a także przechowywania na komputerach stanowiących mienie ADO treści naruszających prawo.

ZASADY DOSTĘPU DO POMIESZCZEŃ PRZETWARZANIA – szczegółowe zasady dostępu do pomieszczeń, w których przetwarza się dane osobowe, zostały określone w załączniku nr 5 „Procedura postępowania z kluczami".

ZASADA MINIMALIZACJI DANYCH – ADO deklaruje, że w ramach wdrożenia zapisów RODO, zweryfikował zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych

danych pod kątem ich adekwatności do rozpoznanych celów przetwarzania. ADO deklaruje, że dokonuje okresowego przeglądu ilości przetwarzanych danych nie rzadziej niż raz w roku.

SYSTEM OCHRONY DANYCH OSOBOWYCH

System ochrony danych Administratora składa się z następujących elementów:

1. ZINWENTARYZOWANE ZASOBY (AKTYWA)

1.1 ADO dokonał identyfikacji zasobów wykorzystywanych w procesach przetwarzania danych osobowych.

Dla każdego zidentyfikowanego i zewidencjonowanego w rejestrze czynności przetwarzania danych procesu ustala się i opisuje następujące parametry: cel przetwarzania, kategorię osób których dane są przetwarzane, kategorie przetwarzanych danych, okresy przechowywania danych, odbiorców danych.

Szczegółowy opis zasobów przetwarzania wraz z zidentyfikowanymi podatnościami, zagrożeniami i zastosowanymi przez ADO zabezpieczeniami został zawarty w załączniku nr 6

W przypadku przetwarzania danych z wykorzystanie systemów informatycznych oznacza się nazwy programów zastosowanych do przetwarzania wraz z oznaczeniem dostawcy oprogramowania (oznaczenie następuje w pozycji opisu oprogramowania).

W załączniku nr 6 w opisie lokalizacji oznacza się wszystkie obszary przetwarzania danych osobowych. Przez obszar przetwarzania rozumie się wydzielone pomieszczenia w których wykonywane są jakiekolwiek operacje na danych osobowych.
Obszar przetwarzania danych stanowią również budynki i pomieszczenia osób trzecich, opisany w zawartych z nimi umowach na przetwarzanie danych osobowych. Za obszar przetwarzania danych rozumie się miejsce, w którym wykonywana jest choćby jedna z operacji na danych a w szczególności: zbieranie, utrwalanie, przechowywanie, opracowywanie, modyfikowanie, udostępnianie i usuwanie.

2. REJESTRY CZYNNOŚCI PRZETWARZANIA i KATEGORII PRZETWARZANIA

2.1 Administrator przy wsparciu IOD, opracowuje, prowadzi, utrzymuje aktualność i udostępnia rejestr czynności przetwarzania danych oraz rejestr kategorii przetwarzania, które stanowią narzędzia rozliczania zgodności z ochroną danych w podmiocie.
2.2 Zakres informacji odnotowywany w ww. rejestrach dla każdej czynności przetwarzania danych, którą ADO uznał za odrębną zawiera załącznik nr 2 oraz załącznik nr 3
2.3 Informacje w rejestrach są na bieżąco aktualizowane przez ADO lub wyznaczoną przez niego osobę/podmiot.
2.4 Rejestry są prowadzone w formie elektronicznej - tabeli Excel.

2.5 W rejestrze czynności przetwarzania zamieszcza się według potrzeby dodatkowe elementy takie jak np. podstawa przetwarzania danych.
Decyzję w sprawie dalszego rozszerzenia pozycji rejestru podejmuje ADO.

3. SPOSÓB OBSŁUGI PRAW JEDNOSTKI W TYM OBOWIĄZKÓW INFORMACYJNYCH

3.1. Administrator ułatwia korzystanie osobom z ich praw poprzez działania takie jak: zamieszczenie na stronie internetowej informacji lub przekierowań (linków) do informacji o prawach osób, sposobie korzystania, wymogach dotyczących identyfikacji, metodach kontaktu z ADO w tym celu.

3.2 ADO dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób, których dane przetwarza.

3.3 ADO wprowadza adekwatne mechanizmy identyfikacji tożsamości osób dla potrzeb realizacji praw osób, których dane dotyczą.

3.4 ADO dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób, których dane przetwarza w formie rejestru stanowiącego załącznik nr 7 .

3.5 ADO informuje osobę o przedłużeniu o ponad 1 miesiąc terminu na rozpatrzenie żądania wskazując przyczynę przedłużenia.

3.6 ADO informuje osobę w ciągu miesiąca od otrzymania żądania o odmowie rozpatrzenia żądania wraz z podaniem przyczyny odmowy i przysługujących osobie związanych z tym prawach.

3.7 Na żądanie osoby, której dane dotyczą ADO wydaje kopię danych jej dotyczących, odnotowując fakt wydania pierwszej kopii. Wprowadza się i utrzymuje się cennik stosowany do pobierania opłat za każdą kolejną (drugą i następną kopii danych). Cena kopii skalkulowana została na podstawie szacowanego jednostkowego kosztu obsługi żądania wydania kopii.

3.8 ADO niezwłocznie dokonuje sprostowania nieprawidłowych danych na żądanie osoby.

3.9 Jeżeli ADO ustali, że nie przetwarza danych osoby, która wystąpiła z żądaniem – powiadamia ją o tym fakcie.

3.10 ADO usuwa dane lub dokonuje ograniczenia przetwarzania danych na żądanie osoby, której dane dotyczą w przypadkach określonych w przepisach prawa

3.11 Na żądanie osoby ADO wydaje w ustrukturyzowanym formacie (tj. xml, csv) lub przekazuje innemu podmiotowi dane dotyczące osoby, które dostarczyła ona ADO, przetwarzane na podstawie zgody lub w celu zawarcia lub wykonania umowy

4 BEZPIECZEŃSTWO

4.1 Administrator zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych

4.2 ADO przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych. W tym celu stosuje metodykę szacowania ryzyka, która stanowi załącznik nr 8.

4.3 W przypadku konieczności przeprowadzenia oceny skutków (Art. 35), wymagane jest wykonanie następujących czynności:

a. opis planowanych operacji przetwarzania i celów przetwarzania
b. ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów
c. ocenę ryzyka
d. środki planowane w celu zarządzenia ryzyku, przedstawione w postaci planu postępowania z ryzykiem

Oceny skutków dokonuje się metodą przyjętą przez Administratora w przypadku wystąpienia wysokiego ryzyka praw i wolności.

4.4 ADO prowadzi wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych

4.5 Wykaz prowadzony jest w załączniku nr 6 i jest aktualizowany po każdej analizie ryzyka ale nie rzadziej niż raz w roku.

4.6 ADO ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa uwzględniając koszt ich wdrożenia.

4.7 U Administratora zabronione jest udzielanie informacji zawierających dane osobowe osobom, których tożsamości nie można zweryfikować. Potwierdzenia tożsamości dokonuje się przez żądanie okazania dokumentu zawierającego zdjęcie lub poprzez wykorzystanie informacji zawartych w dokumentacji ADO, które są znane jedynie osobie, której dane są przetwarzane. ADO w celu weryfikacji tożsamości może stosować metodę pytań bezpośrednich (pozytywna weryfikacja nastąpi w wyniku udzielenia minimum 2 poprawnych odpowiedzi przez respondenta).

4.8 Udostępniając dane osobowe podmiotom, instytucjom czy też organom ADO żąda podania i weryfikuje podstawę prawną dostępu do danych wskazaną przez wnioskujący podmiot, instytucję, organ.

5 ZGŁASZANIE NARUSZEŃ

5.1 Każda osoba upoważniona do przetwarzania danych osobowych i podmiot przetwarzający zobowiązana jest do powiadamiania ADO lub Inspektora Ochrony Danych o stwierdzeniu podatności lub wystąpieniu naruszenia.
Wzór zgłoszenia naruszenia znajduje się w załączniku nr 9.

5.2 W przypadku stwierdzenia wystąpienia naruszenia, ADO (lub w przypadku powołania – IOD) prowadzi postępowanie wyjaśniające w toku, którego:

a. ustala zakres i przyczyny naruszenia oraz jego prognozowane skutki
b. inicjuje ewentualne działania dyscyplinarne
c. działa na rzecz przywrócenia prawidłowego funkcjonowania organizacji po wystąpieniu naruszenia
d. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych naruszeń w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.

5.3 ADO dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze w rejestrze stanowiącym załącznik nr 10.

5.4 W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, ADO lub Inspektora Ochrony Danych, bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, zgłasza je organowi nadzorczemu w sposób szczegółowo określony przepisami prawa krajowego.

5.5 ADO powiadamia o wystąpieniu naruszenia osoby, których dane dotyczą w sposób zindywidualizowany chyba że jest to niemożliwe (duża skala zdarzenia) wówczas stosując inne powszechnie dostępne środki komunikacji (np. publikacja informacja na stronie internetowej, ogłoszenie prasowe).

6 RELACJE Z PODMIOTAMI PRZETWARZAJĄCYMI

6.1 Dane osobowe mogą być powierzone podmiotowi zewnętrznemu wyłącznie na podstawie zawartej w formie pisemnej umowy powierzenia.

6.2 Ewidencję zawartych umów powierzenia prowadzi Administrator lub osoba przez niego wyznaczona. Wzór rejestru umów powierzenia zawiera załącznik nr 11.

6.3 Aby zapewnić maksymalne bezpieczeństwo informacji oraz spójność stosowanych rozwiązań, umowy dotyczące systemu teleinformatycznego, sprzętu, oprogramowania czy dostępu do danych chronionych zawierane z osobami trzecimi powinny być akceptowane przez IOD.

6.4 Wzorcowe zapisy umowy powierzenia zawarto w załączniku nr 12.

7 UPOWAŻNIENIA

7.1 Administrator odpowiada za nadawanie / modyfikowanie i anulowanie upoważnień do przetwarzania danych osobowych.

7.2 Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa.

7.3 Upoważnienia określają zakres operacji na danych, np. tworzenie, usuwanie, wgląd, przekazywanie – patrz załącznik nr 13.

7.4 Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli, audytów, wykonania czynności służbowych, udokumentowanego polecenia administratora, w postaci umowy powierzenia.

7.5 ADO prowadzi rejestr osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych. Rejestr ma charakter pomocniczy i stanowi załącznik nr 14.

7.6 Upoważnienie jest wydawane w 2 egzemplarzach w formie pisemnej. 1 egzemplarz otrzymuje osoba upoważniona, drugi pozostaje w dokumentacji ADO. Osoba

upoważniona potwierdza własnoręcznym podpisem i datą otrzymanie upoważnienia na egzemplarzu administratora.

7.7 Upoważnienie traci ważność w przypadkach:

a) upływu terminu jego ważności

b) zmiany zakresu przetwarzania danych przez użytkownika

c) automatycznie w momencie rozwiązania stosunku pracy, zakończenia odbywania stażu, praktyki, rozwiązania umowy z osobą trzecią

d) przebywania na urlopie macierzyńskim, wychowawczym lub bezpłatnym,

e) zmiany nazwisk i imion osoby upoważnionej.

POSTANOWIENIA KOŃCOWE

Odpowiedzialnym za wdrożenie i utrzymanie niniejszej polityki jest Administrator Danych Osobowych.

Treści zawarte w Polityce i załącznikach do polityki stanowią tajemnicę prawnie chronioną i nie mogą być udostępniane osobom nieupoważnionym w żadnej formie.

Polityka podlega regularnym przeglądom, nie rzadziej niż 1 raz w roku.

Osobą odpowiedzialną za dokonanie przeglądu jest Administrator lub wyznaczona przez niego osoba.

WYKAZ ZAŁĄCZNIKÓW

1. Wzór oświadczenia o poufności
2. Rejestr czynności przetwarzania danych
3. Rejestr kategorii czynności
4. Instrukcja zarządzania systemem informatycznym
5. Procedura postępowania z kluczami
6. Inwentaryzacja zasobów przetwarzania
7. Rejestr obowiązków informacyjnych
8. Metodyka szacowania ryzyka bezpieczeństwa danych osobowych
9. Wzór zgłoszenia naruszenia
10. Rejestr naruszeń
11. Rejestr umów powierzenia
12. Wzór umowy powierzenia
13. Wzór upoważnienia
14. Rejestr upoważnionych
15. Harmonogram wykonywania kopii zapasowych (instrukcja zarządzania)
16. Rejestr nośników elektronicznych