Polityka Ochrony Danych Osobowych

marzec 2021

Wstęp

Niniejsza Polityka Ochrony Danych Osobowych określa zasady zabezpieczania przetwarzania danych osobowych obowiązujących w Pracownia Psychoterapii ZACISZE Anita Sobczak-Kubiak (dalej „Przedsiębiorca") odnosi się do wszystkich osób mających dostęp do bazy danych osobowych gromadzonych w Pracownia Psychoterapii ZACISZE Anita Sobczak-Kubiak, zbiorach wyodrębnionych u Przedsiębiorcy. Zawiera zakres gromadzonych danych osobowych oraz sposób ich zabezpieczenia, jak również opis zastosowanych środków organizacyjnych i technicznych pozwalających na zoptymalizowanie bezpieczeństwa informacji jak również mechanizmy ochrony danych osobowych przetwarzanych zarówno w zbiorach tradycyjnych (papierowych) jak i w infrastrukturze informatycznej. Ponadto normuje sposoby aktualizacji dokumentacji związanej z ochroną danych osobowych, a także wprowadza jednolite zasady wydawania upoważnień do przetwarzania danych osobowych oraz formalizuje proces udostępniania informacji.

Postanowienia ogólne

1) Niniejsza "Polityka Ochrony Danych Osobowych" w Pracownia Psychoterapii ZACISZE Anita Sobczak-Kubiak, z siedzibą w Łodzi przy ul. Słoneczne Zacisze 27, (92-637) oraz praktyką w Łodzi przy ul. Lęborska 9 lok. 7, (92-713), (zwaną dalej „Polityką") zostaje wdrożona, celem ustandaryzowania procesów związanych z przetwarzaniem danych osobowych u Przedsiębiorcy oraz określenia reguł właściwego wykonywania obowiązków administratora danych osobowych oraz prawidłowej ochrony przetwarzanych danych osobowych u Przedsiębiorcy.

2) Niniejsza Polityka odnosi się do zabezpieczenia wszystkich danych osobowych przetwarzanych u Przedsiębiorcy w sposób tradycyjny (na papierze, w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych) oraz przy użyciu infrastruktury informatycznej, również w przypadku przetwarzania danych poza zbiorem danych.

Definicje

1) Użyte w niniejszej Polityce pojęcia oznaczają:

[POLITYKA] - niniejsza Polityka Ochrony Danych Osobowych w Pracownia Psychoterapii ZACISZE Anita Sobczak-Kubiak**.**

[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).

[PUODO] – Prezes Urzędu Ochrony Danych Osobowych, organ nadzorczy powołany do spraw ochrony danych osobowych.

[Dane osobowe] - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, tzn. takiej, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

[Administrator danych osobowych (ADO)] – Pracownia Psychoterapii ZACISZE Anita Sobczak-Kubiak, reprezentowane przez Anitę Sobczak Kubiak, jako podmiot decydujący o celach i środkach przetwarzania danych osobowych u Przedsiębiorcy.

[Przedsiębiorca] – Pracownia Psychoterapii ZACISZE Anita Sobczak-Kubiak.

[Zbiór danych osobowych] - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

[Przetwarzanie danych osobowych] - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w infrastrukturze informatycznej.

[Infrastruktura informatyczna] - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

[Usuwanie danych] - zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą (np. anonimizacja danych).

[Zgoda osoby, której dane dotyczą] - oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być

domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie.

[Odbiorca danych] – każdy, komu udostępnia się dane osobowe, z wyłączeniem:

- osoby, której dane dotyczą,
- osoby, upoważnionej do przetwarzania danych,
- podmiotu, któremu powierzono przetwarzanie danych,
- organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

[Państwo trzecie] – państwo nienależące do Europejskiego Obszaru Gospodarczego; przekazywanie danych osobowych na teren państwa trzeciego wymaga spełnienia dodatkowych obowiązków określonych przepisach prawa.

[Użytkownik Infrastruktury/Użytkownik] - osoba posiadająca uprawnienia do pracy w infrastrukturze informatycznej, zgodnie ze swoim zakresem upoważnienia.

[Osoba upoważniona] - każdy pracownik Przedsiębiorcy, mający nadane pisemne upoważnienie do przetwarzania danych osobowych.

Deklaracja Administratora Danych Osobowych

1) Administrator Danych Osobowych deklaruje, że zbiera i przetwarza dane wyłącznie w uzasadnionych celach, określonych w niniejszej Polityce, stosuje niezbędne środki aby zapobiegać nieautoryzowanym dostępom do danych. W tym celu wprowadza się i na bieżąco aktualizuje zasady przetwarzania danych osobowych u Przedsiębiorcy.
2) Administrator Danych Osobowych zobowiązuje się wdrożyć i stosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, w szczególności zabezpieczające te dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
3) Administrator Danych Osobowych zobowiązuje się do zapewnienia, aby dane osobowe przez cały okres ich przetwarzania, były:
    a) przetwarzane zgodnie z prawem,
    b) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane, przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Główne zasady ochrony danych osobowych

1) Zasady bezpieczeństwa przetwarzania danych osobowych, wprowadzane niniejszą Polityką, w szczególności mają na celu zapewnienie:

    a) poufności, rozumianej jako właściwość zapewniającą, że dane osobowe nie są udostępniane osobom nieupoważnionym,

    b) integralności, rozumianej jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

    c) rozliczalności, rozumianej jako właściwość zapewniającą, że działania podmiotu wobec danych osobowych mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

    d) dostępności, rozumianej jako właściwość zapewniającą, że dane osobowe będą osiągalne i możliwe do wykorzystania na żądanie, w założonym czasie, przez osobę upoważnioną.

2) Zasady określone w niniejszej Polityce oraz w dokumentach powiązanych powinny być znane i stosowane przez pracowników Przedsiębiorcy przetwarzających dane osobowe, w szczególności każdy upoważniony do przetwarzania pracownik ma obowiązek podejmować odpowiednie środki ochrony danych przed utratą lub nieuprawnioną zmianą, dostępem lub ujawnieniem.

3) Pracownicy Przedsiębiorcy mają świadomość możliwości zaistnienia sytuacji naruszenia ochrony danych osobowych, przestrzegają procedur związanych z przebywaniem w obszarze przetwarzania danych osobowych osób nieupoważnionych oraz odpowiednio reagują na sytuacje stwarzające podejrzenie naruszenia bezpieczeństwa informacji i niniejszej Polityki.

4) Każda osoba przetwarzająca dane osobowe u Przedsiębiorcy, przed dopuszczeniem do przetwarzania danych osobowych, otrzymuje pisemne upoważnienie Administratora Danych Osobowych.

5) Przed rozpoczęciem przetwarzania danych osobowych każdy pracownik zostaje zapoznany z obowiązującymi u Przedsiębiorcy zasadami przetwarzania danych osobowych, w szczególności z obowiązującymi przepisami prawa o ochronie danych osobowych, Polityką Ochrony Danych Osobowych oraz z zasadami użytkowania urządzeń i infrastruktury informatycznej służących do przetwarzania danych osobowych, zasadami dostępu do pomieszczeń, w których przetwarzane są dane osobowe, sposobem postępowania w przypadku naruszenia ochrony danych osobowych oraz odpowiedzialnością z tytułu naruszenia ochrony danych osobowych, a także zasadami przetwarzania danych osobowych wprowadzanych przepisami RODO.

6) Osoby, które zostały upoważnione do przetwarzania danych, obowiązane są zachować w tajemnicy gromadzone u Przedsiębiorcy dane osobowe, a także sposoby ich zabezpieczenia.

7) Za bieżącą ochronę danych osobowych odpowiada każda osoba przetwarzająca te dane w zakresie zgodnym z udzielonym upoważnieniem, kompetencjami lub rolą sprawowaną w procesie przetwarzania danych.
8) Pracownicy Przedsiębiorcy są zobowiązani do informowania o wszelkich podejrzeniach lub zauważonych naruszeniach oraz słabościach infrastruktury informatycznej przetwarzających dane osobowe Administratora Danych Osobowych.

Role i odpowiedzialności

Obowiązki i kompetencje Administratora Danych Osobowych

1) Administrator Danych Osobowych jest odpowiedzialny za przetwarzanie i ochronę danych osobowych u Przedsiębiorcy zgodnie z przepisami prawa, w tym wprowadzenie do stosowania procedur postępowania zapewniających prawidłowe przetwarzanie danych osobowych.

2) Do kompetencji Administratora Danych Osobowych należy podział zadań i obowiązków związanych z organizacją ochrony danych osobowych u Przedsiębiorcy, przyjmowanie i zatwierdzanie niezbędnych, wymaganych przez przepisy prawa lub aktualny stan faktyczny, dokumentów regulujących ochronę danych osobowych u Przedsiębiorcy, zapewnia niezbędne zasoby i narzędzia w celu realizacji Polityki w sposób efektywny oraz monitoruje jej przestrzeganie.

3) Administrator Danych Osobowych zapewnia osobom przetwarzającym dane osobowe u Przedsiębiorcy szkolenia wstępne i okresowe z zakresu ochrony danych osobowych oraz zagrożeń związanych z ich przetwarzaniem, ze szczególnym uwzględnieniem przetwarzania danych w infrastrukturze Informatycznej.

4) Do obowiązków Administratora Danych Osobowych należy:

    a. zapewnianie przestrzegania przepisów o ochronie danych osobowych,
    b. wdrożenie niezbędnych procedur dotyczących zasad przetwarzania danych osobowych u Przedsiębiorcy,
    c. zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
    d. prowadzenie rejestru incydentów, analizy przypadków pod kątem konieczności dokonania ewentualnego zgłoszenia do organu nadzorczego,
    e. kontrola przestrzegania przepisów o ochronie danych osobowych,
    f. kontrola zgodności gromadzenia i przetwarzania danych osobowych u Przedsiębiorcy,
    g. opracowanie i aktualizowanie dokumentacji, w tym prowadzenie rejestru czynności przetwarzania danych osobowych, ewidencji osób i podmiotów upoważnionych do przetwarzania danych osobowych u Przedsiębiorcy oraz nadzorowania przestrzegania zasad w niej określonych,
    h. regularna kontrola stosowanych środków i metod zabezpieczenia gromadzonych u Przedsiębiorcy informacji,
    i. nadzór nad udostępnianiem danych osobowych innym podmiotom, weryfikacja wniosków o udostępnienie danych osobowych Przedsiębiorcy

5) Ponadto Administrator Danych Osobowych ma obowiązek dbania o to aby przetwarzanie odbywało się zgodnie z RODO i aby móc to skutecznie wykazać. W tym celu, ma on wdrażać odpowiednie i skuteczne środki techniczne i organizacyjne, które regularnie poddawane są aktualizacji i w razie potrzeby konserwacji.

Obowiązki i kompetencje Pracowników

1) Pracownik jest zobowiązany do przestrzegania przepisów prawa oraz niniejszej Polityki jak i przetwarzania danych zgodnie ze swoimi uprawnieniami i upoważnieniem.

2) Do obowiązków każdej osoby upoważnionej do przetwarzania danych osobowych należy przede wszystkim dochowanie należytej staranności w celu ochrony danych, ponadto do obowiązków każdej osoby należy w szczególności:

    a. postępowania zgodnie z ustalonymi regulacjami wewnętrznymi,
    b. zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia,
    c. informowania ADO za pośrednictwem przełożonego lub bezpośrednio, o wszelkich podejrzeniach lub zauważonych naruszeniach oraz słabościach infrastruktury informatycznej przetwarzających dane osobowe.

Dopuszczenie osób do przetwarzania danych osobowych, upoważnienia i ich ewidencja

1) Przed dopuszczeniem pracownika Przedsiębiorcy do wykonywania zadań związanych z przetwarzaniem danych osobowych ADO:
    a. zapoznaje pracownika z przepisami dotyczącymi ochrony danych osobowych i uregulowaniami wewnętrznymi obowiązującymi w tym zakresie u Przedsiębiorcy,
    b. odbiera od pracownika podpisane zobowiązanie do zachowania danych osobowych i sposobów ich zabezpieczania w tajemnicy, przetwarzania danych osobowych zgodnie z obowiązującymi przepisami oraz oświadczenie o znajomości wewnętrznej dokumentacji z zakresu ochrony danych osobowych,
    c. nadaje pracownikowi upoważnienie do przetwarzania danych osobowych.

2) Oświadczenia i upoważnienia, o których mowa w ust. 1 powyżej, przechowuje się w aktach osobowych pracownika.

Procedura wydawania upoważnień

1) Upoważnienia wydaje ADO. Upoważnienia te zawierają imię i nazwisko oraz stanowisko pracownika.

2) Upoważnienia, obowiązują do czasu ustania zatrudnienia lub obowiązków związanych z przetwarzaniem danych osobowych, chyba, że w treści upoważnienia zaznaczono inaczej.

3) Zapewnia się, aby u Przedsiębiorcy była prowadzona ewidencja osób upoważnionych do przetwarzania danych osobowych.

4) Każde nadanie, pozbawienie i inna zmiana uprawnień dla pracownika powinno być odnotowane w prowadzonej ewidencji.

Obowiązek informacyjny

W związku z obowiązkiem informacyjnym jaki ciąży na administratorze została przygotowana klauzula informacyjna zgodnie z art. 13 RODO. Dokument ten powinien być dostępny dla klientów, pracowników i wszystkich pozostałych osób, których dane są przetwarzane. Przepisy prawa nie wskazują konkretnie sposobu udostępnienia klauzuli. Zwyczajowo przyjmuje się, że klauzula powinna wisieć w widocznym dla wizytujących Przedsiębiorcę miejscu lub być udostępniana na żądanie, by osoby zainteresowane mogły zasięgnąć informacji o przetwarzaniu danych u Przedsiębiorcy.

Obszar przetwarzania danych osobowych

1) Dane osobowe mogą być przetwarzane wyłącznie w obszarach przetwarzania w których Przedsiębiorca prowadzi swoją działalność. Przedsiębiorca prowadzi działalność w praktyce przy ul. Lęborska 9 lok. 7, (92-713) w Łodzi. Do pomieszczeń, w których przetwarzane są dane osobowe dostęp jest ograniczony dla osób posiadających upoważnienie do przetwarzania danych osobowych u Przedsiębiorcy.

2) Dostęp do gabinetu Przedsiębiorcy ograniczony jest przez zamykane drzwi na klucz, monitoringiem na terenie budynku, bramą ograniczającą wjazd samochodem i domofonem.

Sposób zbierania danych

1) Zbieranie danych osobowych u Przedsiębiorcy jest dozwolone po wypełnieniu jednej z przesłanek zawartych w art. 6 ust. 1 oraz art. 9 ust. 2 RODO.
2) Wszelkie dane przetwarzane u Przedsiębiorców są zbierane w celu wykonania usług psychoterapeutycznych, zatrudnienia pracowników oraz w celu wypełnienia wymogów prawnych spoczywających na Przedsiębiorcy.
3) Dane są zbierane jedynie po wypełnieniu przesłanek pozwalających na przetwarzanie danych osobowych.
4) Zbieranie danych u Przedsiębiorcy dokonywane jest przez następujące czynności:
    a. umówienie wizyty;
    b. przeprowadzenie wizyty;
    c. zatrudnianie pracowników;
    d. wypełnianie obowiązków prawnych ciążących na Przedsiębiorcy.

Identyfikacja zagrożeń

1) Przypadki zakwalifikowane, jako naruszenie lub uzasadnienie podejrzenia naruszenia bezpieczeństwa infrastruktury informatycznej, podlegające monitorowaniu, są nimi w szczególności:
    a. sytuacje losowe (np. pożar, zalanie, itp.),
    b. niewłaściwe środowisko użytkowania (np. nadmierna wilgotność),
    c. uszkodzenie sprzętu lub oprogramowania wskazujące na umyślne działanie ukierunkowane na naruszenie ochrony danych, niewłaściwe działanie serwisu,
    d. odstępstwo od stanu oczekiwanego wskazujące na zakłócenia infrastruktury lub inną nadzwyczajną i niepożądaną modyfikację w infrastrukturze informatycznej,
    e. wystąpienie naruszenia lub próba naruszenia integralności infrastrukturze informatycznej,
    f. wystąpienie niedopuszczalnej zmiany danych osobowych w infrastrukturze informatycznej,
    g. ujawnienie osobom trzecim danych osobowych,
    h. nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych np. skasowanie lub skopiowanie danych w niedozwolony sposób, rażące naruszenie dyscypliny pracy w zakresie procedur bezpieczeństwa informacji (np. opuszczenie stanowiska bez wcześniejszego wylogowania pozostawienie danych osobowych w kserokopiarce)

2) Analizy ryzyka, związanego z wystąpieniem oraz wagą ewentualnego zaistniałego incydentu dokonuje okresowo ADO.

Środki bezpieczeństwa

1) W zakresie środków bezpieczeństwa organizacyjnych I fizycznych stosuje się m.in.:

    a) osoby upoważnione do przetwarzania danych zostały przeszkolone i zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz zobowiązane do zachowania danych w tajemnicy;
    b) wszystkie pomieszczenia po zakończeniu pracy są zamykane na klucz, te przechowywane są w specjalnie do tego wyznaczonym miejscu;
    c) jedynie osoby posiadające stosowne upoważnienie posiadają klucze wejściowe do gabinetu, wyłącznie te osoby są uprawnione do otwierania i zamykania pomieszczeń, gdzie przetwarzane są dane osobowe;
    d) wszystkie drzwi wejściowe są zabezpieczone zamkiem;
    e) dane osobowe w formie papierowej i elektronicznej przechowywane są w ściśle określonych pomieszczeniach lub częściach pomieszczeń do których dostęp mają jedynie osoby upoważnione;
    f) ochronę obszaru przetwarzania danych osobowych zapewnia się poprzez odpowiednie fizyczne zabezpieczenia, w szczególności zapewnienie solidnej konstrukcji ścian zewnętrznych pomieszczeń oraz odpowiednie zabezpieczenie drzwi zewnętrznych przed nieautoryzowanym dostępem za pomocą mechanizmów zabezpieczeń;

g) dostęp osób trzecich jest możliwy jedynie pod nadzorem osoby upoważnionej, szafy z dokumentacją są stalowe;
h) dane w postaci papierowej zawierające dane osobowe zabezpiecza się przed dostępem osób nieupoważnionych w zamykanych szafach, znajdujących się w specjalnie wydzielonych strefach, do których nie mają dostępu osoby trzecie.
i) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone, ekrany komputerów, ustawione są w sposób uniemożliwiający wgląd w ekrany osobom nieupoważnionym, pracownicy zobowiązani są stosować politykę czystego biurka i ekranu, opuszczając stanowisko pracy, dokumenty zawierające dane osobowe powinny zostać schowane, a ekrany komputerów zablokowane. Wydruki powinny być niezwłocznie usuwane z drukarki, a robocze, błędne lub zdezaktualizowane powinny być niezwłocznie niszczone.

2) W zakresie zabezpieczenia sprzętowego i infrastruktury informatycznej i telekomunikacyjnej u Przedsiębiorcy stosuje się m.in. takie środki jak:

a) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora Użytkownika oraz hasła zmienianego raz na 90 dni, hasła składają się z min. 8 znaków w tym jedna cyfra,
b) każdy komputer został wyposażony w program antywirusowy i system Firewall,
c) podłączenie urządzeń komputerowych dokonywane jest przez osobę wyznaczoną przez ADO,
d) zastosowanie mają automatyczne wygaszacze ekranu, przy czym każdy Użytkownik zobowiązany jest do blokowania nieużywanego komputera,
e) cyklicznie wykonywane są kopie zapasowe, wyznaczono osoby odpowiedzialne za zabezpieczenie danych w wypadku wystąpienia incydentu lub zdarzenia losowego, które mogłoby zakłócić zasady ciągłości przetwarzania danych.

Postępowanie w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych

1. Przed przystąpieniem do pracy pracownicy Przedsiębiorcy zobowiązani są dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy. Wszelkie naruszenie lub podejrzenie naruszenia ochrony danych są zgłaszane ADO.

2. Za okoliczności, które uznaje się za naruszenie lub podejrzenie naruszenia ochrony danych mogą być uznane w szczególności:

a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, infrastruktury informatycznej lub dokumentacji,
b. nieprzestrzeganie zasad ochrony danych osobowych,
c. zdarzenia losowe (np. pożar, zalanie wodą, utrata zasilania) i awarie,
d. umyślne incydenty (np. włamanie do komputera, kradzież sprzętu),
e. nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których dane osobowe się znajdują,
f. niezamierzoną zmianę lub utratę danych zapisanych na kopiach zapasowych,

g. udostępnienie osobom nieupoważnionym danych osobowych lub ich części;
h. inny stan infrastruktury informatycznej lub pomieszczeń, niż pozostawiony przez Użytkownika po zakończeniu pracy;
i. utrata nośników danych, czyli zagubienie lub kradzież sprzętu informatycznego lub nośników zewnętrznych zawierających dane osobowe;
j. pozostawianie osób postronnych bez nadzoru w miejscach, gdzie dane osobowe są przetwarzane i łatwo dostępne;
k. przekazywanie danych osobowych podczas rozmowy telefonicznej, bez weryfikacji czy rozmówca jest osobą uprawnioną do uzyskania takich informacji;
l. wyrzucanie podręcznych notatek lub dokumentów zawierających dane osobowe do zwykłych koszy na śmieci, bez użycia niszczarki.

3. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych osoba stwierdzająca naruszenie zobowiązana jest:

   a. powstrzymać się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów bądź innych dowodów naruszenia;
   b. zabezpieczyć elementy infrastruktury informatycznej lub dokumentację, przede wszystkim poprzez uniemożliwienie dostępu do nich osobom nieupoważnionym;
   c. podjąć stosowne do zaistniałej sytuacji i niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych
   d. bezzwłocznie powiadomić o naruszeniu ADO i wykonywać ich polecenia.

4. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych ADO:

   a. ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki;
   b. ocenia zastałą sytuację;
   c. wysłuchuje relacji osoby, która dokonała powiadomienia o incydencie,
   d. podejmuje decyzje o toku dalszego postępowania,
   e. dokumentuje prowadzone postępowanie,
   f. dokonuje oceny ryzyka ewentualnego naruszenia,
   g. wykonuje analizę incydentu, mającą na celu eliminację ich wystąpienia w przyszłości,
   h. każdy incydent jest ewidencjonowany przez ADO.

5. W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej u Przedsiębiorcy dyscypliny pracy, ADO wyjaśnia wszystkie okoliczności incydentu i podejmuje stosowne działania wobec osób, które dopuściły się wskazanego naruszenia.

Powierzanie przetwarzania danych osobowych

Powierzenie przetwarzania danych osobowych następuje w sytuacji kiedy Administrator Danych Osobowych, zleca innemu podmiotowi wykonanie zadań, w trakcie realizacji których podmiot ten

będzie miał dostęp do danych i będzie przeprowadzał na nich jakiekolwiek operacje, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w infrastrukturze informatycznej. Podmiot, któremu powierzono przetwarzanie danych osobowych, może przetwarzać te dane wyłącznie w imieniu i za zgodą wyrażoną w umowie powierzenia przetwarzania danych Przedsiębiorcy, który pozostaje administratorem tych danych osobowych.

Zasady bezpieczeństwa podczas przekazywania danych osobowych

1) Podczas przekazywania informacji lub dokumentów zawierających dane osobowe, pracownicy Przedsiębiorcy zobowiązani są stosować następujące zasady bezpieczeństwa:

   a. stosowanie technik kryptograficznych podczas przesyłania danych publicznymi sieciami telekomunikacyjnymi;
   b. zapewnienie ochrony przesyłanych danych osobowych przed przechwyceniem, skopiowaniem, modyfikacją, zniszczeniem poprzez zastosowanie odpowiednich środków technicznych I organizacyjnych oraz należytej staranności;
   c. upewnienie się przed ustnym przekazaniem danych osobowych, czy rozmówca jest osobą upoważnioną do uzyskania określonych danych osobowych;
   d. zachowanie szczególnej ostrożności w trakcie rozmów telefonicznych, aby uniknąć podsłuchania danych osobowych przez osoby nieupoważnione;
   e. nie pozostawianie wiadomości zawierających dane osobowe w automatycznych sekretarkach.

Instrukcja Zarządzania Infrastrukturą Informatyczną służącą do przetwarzania danych osobowych

1) Instrukcja Zarządzania Infrastrukturą Informatyczną służącą do przetwarzania danych osobowych u Przedsiębiorcy, zwana dalej „Instrukcją", określa zasady postępowania osób upoważnionych podczas przetwarzania danych osobowych w infrastrukturze informatycznej i jest integralną częścią „Polityki Ochrony Danych Osobowych".

2) Na niniejszą Instrukcję składają się:

   a. procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w infrastrukturze informatycznej oraz wskazanie osób odpowiedzialnych za te czynności;
   b. stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;

c. procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników infrastruktury IT;
d. procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
e. opis sposobów, miejsca i okresu przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych,
f. opis sposobów zabezpieczania infrastruktury informatycznej przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do infrastruktury informatycznej;
h. procedury wykonywania przeglądów i konserwacji infrastruktury IT oraz nośników informacji służących do przetwarzania danych.

3) Podstawowym celem zabezpieczeń infrastruktury informatycznej służącej do przetwarzania danych osobowych jest zapewnienie jej jak najwyższego poziomu bezpieczeństwa.

4) Nomenklatura użyta w niniejszej Instrukcji jest zdefiniowana w Polityce Ochrony Danych Osobowych dla Przedsiębiorcy.

Obowiązki i kompetencje osób zaangażowanych w przetwarzanie danych osobowych w infrastrukturze informatycznej

1. Do obowiązków osoby wyznaczonej do administrowania infrastrukturą IT w zakresie ochrony danych osobowych należy w szczególności:

   a. zapewnienie ochrony danych osobowych przetwarzanych w infrastrukturze IT;
   b. przestrzeganie opracowanych dla infrastruktury IT procedur operacyjnych i bezpieczeństwa;
   c. kontrola przepływu informacji pomiędzy stacją roboczą a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej;
   d. utrzymanie infrastruktury IT w należytej sprawności technicznej;
   e. regularne tworzenie kopii zapasowych danych osobowych i sprawdzanie poprawności tych kopii zapasowych;
   f. wykonywanie lub nadzór nad wykonywaniem okresowych przeglądów i konserwacji infrastruktury IT oraz elektronicznych nośników informacji, na których zapisane są dane osobowe.

2. Do obowiązków wszystkich użytkowników infrastruktury IT należy w szczególności:

   a. przestrzeganie zasad opisanych w niniejszej Instrukcji i Polityce;
   b. uniemożliwienie dostępu danych osobowych przetwarzanych w infrastrukturze IT osobom nieupoważnionym;
   c. informowanie ADO o wszelkich naruszeniach, podejrzeniach naruszenia i nieprawidłowościach w sposobie przetwarzania i ochrony danych osobowych w infrastrukturze IT;

3. Podejmowanie współpracy przy ustaleniu przyczyn naruszenia ochrony danych osobowych oraz usuwania skutków naruszeń, w tym zapobieganie ich ponownemu wystąpieniu.

Nadawanie, zmiana i cofnięcie uprawnień do przetwarzania danych osobowych w infrastrukturze informatycznej

1) Każdy Użytkownik infrastruktury IT przetwarzający dane osobowe u Przedsiębiorcy, przed pierwszym zalogowaniem i przystąpieniem do przetwarzania danych osobowych na stacji roboczej, zobowiązany jest zapoznać się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa, Polityką oraz niniejszą Instrukcją.

2) Użytkownicy, przed dopuszczeniem do obsługi infrastruktury IT zostają przeszkoleni w zakresie obsługi sprzętu informatycznego oraz oprogramowania.

3) Pierwsze zalogowanie Użytkownika w infrastrukturze IT i nadanie odpowiednich uprawnień do infrastruktury IT musi być poprzedzone złożeniem przez użytkownika oświadczenia o zachowaniu w tajemnicy danych osobowych i zobowiązaniu do przetwarzania danych osobowych zgodnie z przepisami oraz uzyskaniem upoważnienia.

4) Użytkownik otrzymuje tymczasowe hasło dostępowe, które następnie zmienia na hasło składające się z 8 znaków, zawierające wielkie i małe litery oraz cyfry lub znaki specjalne.

5) Procedurę nadawania uprawnień do przetwarzania danych osobowych w infrastrukturze IT stosuje się odpowiednio w przypadku zmiany i odbierania uprawnień.

6) W przypadku rozwiązania umowy z użytkownikiem lub utraty przez niego upoważnienia do przetwarzania danych osobowych, użytkownik jest natychmiast wyrejestrowywany z infrastruktury IT oraz unieważnienia się jego hasła.

Stosowane metody i środki uwierzytelniania w infrastrukturze IT

1) W infrastrukturze IT stosuje się uwierzytelnienie przez każdorazowe podanie indywidualnego hasła.

2) Wszystkie hasła dostępowe do sprzętów informatycznych, sieci, poczty elektronicznej, muszą być zmieniane nie rzadziej niż co 90 dni. Hasło musi się składać z co najmniej z 8 znaków, zawierać litery i co najmniej jedną cyfrę. Hasła nie mogą być takie same jak identyfikator użytkownika.

3) Hasła dostępu do infrastruktury IT stanowią tajemnicę służbową, znaną wyłącznie użytkownikowi i osobie wyznaczonej do administracji infrastrukturą IT.

4) Użytkownicy są odpowiedzialni za wszelkie działania w infrastrukturze IT prowadzone z użyciem ich identyfikatora i hasła.

5) ADO nadaje hasło dostępu do aplikacji dla nowego użytkownika albo dla użytkownika, który zapomniał swojego ostatniego hasła.

6) Użytkownik niezwłocznie po pierwszym prawidłowym zalogowaniu się do infrastruktury IT zmienia hasło podane przez osobę wyznaczoną do administracji infrastruktury IT.

7) Zasady kontroli dostępów dotyczą wszystkich komputerów stacjonarnych, laptopów, urządzeń mobilnych, zdalnych użytkowników, sieci na których przetwarza się dane osobowe.

Wymagania dotyczące sprzętu i oprogramowania

1) U Przedsiębiorcy stosuje się automatyczne wygaszacze ekranów.

2) Programy zainstalowane na sprzęcie informatycznym muszą być użytkowane z zachowaniem praw autorskich i posiadać aktualne licencje.

3) Przed zainstalowaniem nowego oprogramowania upoważniona osoba, zobowiązana jest sprawdzić jego działanie pod kątem bezpieczeństwa całej infrastruktury IT.

4) Sieć teleinformatyczna wykorzystywana do przetwarzania danych osobowych powinna mieć zapewnione prawidłowe zasilanie energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu informatycznego.

5) Infrastruktura techniczna związana z siecią teleinformatyczną i jej zasilaniem (rozdzielnie elektryczne, skrzynki z bezpiecznikami) powinna być zabezpieczona przed dostępem osób nieupoważnionych.

6) Gniazda zasilania sieci teleinformatycznej powinny być odpowiednio oznakowane, zabezpieczone przed włączeniem do nich innych odbiorników.

Bezpieczna eksploatacja infrastruktury informatycznej

1) Z serwisu służbowej poczty elektronicznej i Internetu mogą korzystać jedynie pracownicy Przedsiębiorcy.

2) Do komputera nie można podłączać modemów lub innych urządzeń umożliwiających dostęp do Internetu niepochodzących z zaopatrzenia Przedsiębiorcy.

3) Bezpieczna eksploatacja infrastruktury informatycznej zostaje zapewniona poprzez przestrzeganie następujących zasad:

   a) użytkownikom zabrania się umożliwiania stronom trzecim uzyskiwania nieupoważnionego dostępu do infrastruktury IT;
   b) użytkownikom nie wolno korzystać z infrastruktura IT dla celów innych niż związane z wykonywaniem obowiązków służbowych.

6) Przedsiębiorca może zlecić osobie wyznaczonej do administracji infrastrukturą IT zastosowanie środków blokujących dostęp do wszystkich lub określonych stron www Użytkownikom.

Zalecenia dotyczące wymagań sprzętowych przetwarzających dane osobowe

1) Przynajmniej raz w roku infrastruktura IT jest skanowana pod kątem nieautoryzowanego oprogramowania.

2) Infrastruktura IT stosowana u Przedsiębiorcy posiada włączone aktualizacje automatyczne, zgodne z zaleceniami producenta.

Przetwarzanie i udostępnianie danych osobowych

1) W przypadku przekazywania danych osobowych należy je zabezpieczyć w sposób zapewniający poufność, integralność i rozliczalność tych danych, w szczególności poprzez:

   a) ograniczenie dostępu do danych osobowych hasłem zabezpieczającym;
   b) stosowanie metod kryptograficznych;
   c) stosowanie odpowiednich zabezpieczeń fizycznych i organizacyjnych.

2) Nieuzasadnione kopiowanie danych przez użytkowników jest zabronione.

Opis zabezpieczeń infrastruktury informatycznej przeciw oprogramowaniu wirusowemu, tworzenia kopii zapasowych, wykorzystaniu pamięci przenośnej, sposobu przesyłania danych

1) W celu zabezpieczenia infrastruktury IT Przedsiębiorcy przed działalnością szkodliwego oprogramowania zainstalowane zostało oprogramowanie antywirusowe wyposażone w aktualną bazą sygnatur wirusów, które skanują na bieżąco infrastrukturę IT. Użytkownicy podłączając jakiekolwiek nośniki lub też importując dane w inny sposób są zobowiązani do ich przeskanowania. Osoba wyznaczona przez ADO na bieżąco aktualizuje oprogramowanie antywirusowe i sprawdza jej funkcjonowanie. Pliki z nieznanych źródeł powinny być bezzwłocznie usunięte.

2) Kopie zapasowe wykonywane są cyklicznie przez wyznaczoną osobę. ADO sprawuje nadzór nad procesem oraz weryfikuje poprawność kopii. Kopie zapasowych są przechowywane w wyznaczonym do tego miejscu, zaś dostęp do nich mają wyłącznie ADO i osoby upoważnione. Kopie zapasowe, które uległy uszkodzeniu zostają natychmiast zniszczone.

3) Wykorzystanie urządzeń pamięci przenośnej jest dozwolone wyłącznie dla upoważnionych użytkowników. Po wykorzystaniu danych osobowych należy je

niezwłocznie usunąć z nośnika elektronicznego. Do przenoszenia danych służyć mogą jedynie nośniki należące do Przedsiębiorcy.

4) Przesyłanie danych osobowych drogą teletransmisji powinno odbywać się wyłącznie przy wykorzystaniu zabezpieczeń chroniących przed nieuprawnionym dostępem.

5) Adres e-mail przypisany do Użytkownika jest własnością ADO i powinien być używany wyłącznie do celów służbowych. Niedozwolone są używanie poczty elektronicznej do celów prywatnych i korzystanie z poczty innego Użytkownika. Zabronione jest wysyłanie danych osobowych droga mailowa bez odpowiedniego zabezpieczenia.

6) W przypadku konieczności dostępu do informacji znajdujących się na kontach użytkowników w przypadku zerwania wszelkich stosunków prawnych z Przedsiębiorcą bądź urlopu pracownika dopuszcza się możliwość przekierowania przychodzącej korespondencji elektronicznej na adres skrzynki poczty elektronicznej przełożonego lub innego pracownika.

7) Przedsiębiorca zastrzega sobie prawo do dokonywania przeglądu zawartości kont Użytkownika oraz danych przesyłanych lub przechowywanych przez Użytkownika w infrastrukturze IT. Decyzję o dokonaniu przeglądu może podjąć tylko Administrator Danych Osobowych. O każdym dokonaniu przeglądu zawartości kont Użytkownik jest informowany. Sprawdzenie musi odbywać się z zachowaniem obowiązującego prawa, w tym prawa do prywatności oraz poszanowania dóbr osobistych. Monitoring poczty elektronicznej i Internetu udostępnionego przez Przedsiębiorcę może być wykonywany tylko w uzasadnionych przypadkach, z zachowaniem gwarancji wynikających z obowiązujących przepisów prawa i przepisów wewnętrznych oraz może być podjęty i wykonywany wyłącznie na podstawie decyzji ADO.

8) Dostęp zdalny do danych jest możliwy jedynie na podstawie obowiązującej umowy powierzenia przetwarzania danych i dla osoby posiadającej upoważnienie do przetwarzania danych osobowych. Zabezpieczenia dostępu zdalnego do danych osobowych powinny zapewniać ich integralność, poufność i rozliczalność oraz ochronę kryptograficzną.

Zasady wykonywania przeglądów i konserwacji infrastruktura informatycznej oraz nośników służących do przetwarzania danych osobowych

1) Za prawidłowość przeprowadzenia przeglądów, konserwację i dokumentowanie zmian w infrastrukturze informatycznej odpowiada ADO. Procedury te wykonywane są przez osobę wyznaczoną do administracji infrastrukturą IT.

2) Przeprowadzany jest przegląd programów i narzędzi programowych w przypadku wykonania zmian w sprzęcie informatycznym spowodowanych koniecznością naprawy, konserwacji lub modyfikacji.

3) Konserwację oprogramowania przeprowadza się po zgłoszeniu przez użytkownika potrzeby wprowadzenia zmian pozwalających utrzymać funkcjonalność infrastruktury informatycznej.

4) Przeglądy, naprawy i konserwacje infrastruktury IT, które będą przeprowadzane w miejscu użytkowania infrastruktury IT przez osoby trzecie, wymagają obecności osoby wyznaczonej do administracji infrastruktury IT lub innej osoby wyznaczonej przez ADO.

5) W przypadku gdy konieczne jest dokonanie przeglądu, naprawy lub konserwacji sprzętu informatycznego poza miejscem jego użytkowania, z urządzenia (o ile jest to możliwe) należy wymontować element, na którym zapisane są dane osobowe. W przeciwnym wypadku należy zawrzeć z podmiotem dokonujący naprawy umowę powierzenia przetwarzania danych.

6) Przegląd programów i narzędzi programowych powinien być przeprowadzany przez osobę wyznaczoną do administracji infrastruktury IT.

7) Raz do roku osoba wyznaczona powinna przeprowadzać weryfikację całej infrastruktury informatycznej pod kątem spełnienia wymogów bezpieczeństwa.

8) Sprzęt komputerowy i nośniki (płyty cd, dyski, pamięci przenośne itd.), które mają ulec zniszczeniu, a zawierają dane osobowe, powinny być uprzednio pozbawione zapisu tych danych.

Incydenty bezpieczeństwa z zakresu IT

1) Za incydentem związany z bezpieczeństwem danych osobowych należy uznać każde pojedyncze zdarzenie lub serię niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działania infrastruktury lub zagrażają bezpieczeństwu danych osobowych.

2) Do incydentów bezpieczeństwa w infrastrukturze informatycznej zaliczamy między innymi:

   a) nieuprawniony dostęp lub próbę dostępu do infrastruktury,
   b) nieuprawnione naruszenie lub próbę naruszenia poufności, integralności i rozliczalności danych i infrastruktury,
   c) niezamierzona zmiana lub utrata danych zapisanych na kopiach zapasowych,
   d) nieuprawniony dostęp do danych osobowych,
   e) niewłaściwe zaadresowanie wiadomości poczty elektronicznej,
   f) niewykorzystywanie opcji „kopii ukrytej”, czyli nieukrywanie poszczególnych odbiorców wiadomości (poza głównym) podczas wysyłki do wielu adresatów,
   g) utrata nośników danych, czyli zagubienie lub kradzież telefonu, laptopa, pamięci przenośnej z danymi osobowymi,
   h) udostępnienie danych lub hasła nieuprawnionej osobie,
   i) niewłaściwe zabezpieczenie danych umożliwiające dostęp do nich osobom nieupoważnionym.

3) W przypadku stwierdzenia incydentu bezpieczeństwa, każdy Użytkownik infrastruktury zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie ADO.

Rejestr Czynności

W związku z obowiązkiem prowadzenia Rejestru Czynności Przetwarzania Danych Osobowych wynikającym z art. 30 ust. 1 RODO, który spoczywa na Administratorze, dokument taki został przygotowany i wdrożony.

Postanowienia końcowe

1) Niniejsza Polityka i dokumenty z nią powiązane podlegają cyklicznemu przeglądowi i aktualizacji, dokonywanym przez ADO. Przeglądy doraźne są przeprowadzane w razie konieczności, w szczególności przy każdej zmianie stanu faktycznego lub prawnego dotyczącego przetwarzania danych osobowych, zmian organizacyjnych u Przedsiębiorcy oraz gdy jest to niezbędne w wyniku zmian wprowadzonych na skutek zaistniałych incydentów bezpieczeństwa lub wyników audytów wewnętrznych i zewnętrznych.

2) Administrator Danych Osobowych uprawniony jest do cyklicznej weryfikacji i aktualizacji ewidencji zbiorów danych osobowych i wykorzystywania do przetwarzania danych osobowych infrastruktury informatycznej.

3) Wszyscy Pracownicy Przedsiębiorcy zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszych Polityce i Instrukcji.