POLITYKA BEZPIECZEŃSTWAW ZAKRESIE OCHRONY DANYCH OSOBOWYCH

CIS Sp. z o.o. z siedzibą w Pogwizdowie

Spis treści

INFORMACJE OGÓLNE

Niniejszy dokument Polityki Bezpieczeństwa w zakresie ochrony danych osobowych w CIS Spółka z ograniczoną odpowiedzialnością (dalej „Polityka Bezpieczeństwa") został opracowany przez Administratora Danych Osobowych, w celu zapewnienia zgodności przetwarzania danych osobowych z obowiązującymi przepisami prawa.

Polityka Bezpieczeństwa wraz z Instrukcją Zarządzania Systemem Informatycznym oraz dokumentami w nich wskazanym stanowi dokumentację przetwarzania danych osobowych w rozumieniu § 1 pkt 1rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024 z późn. zm.). Potrzeba opracowania Polityki Bezpieczeństwa wynika z przepisów § 3 i 4 w/w Rozporządzenia.

Dokument zwraca uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.
Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym.

Polityka Bezpieczeństwa wskazuje sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych i jest w szczególności przeznaczony dla osób pracujących przy przetwarzaniu danych osobowych. Opisuje zasady i procedury przetwarzania danych osobowych oraz zabezpieczania przed dostępem osób nieuprawnionych. Polityka bezpieczeństwa odnosi się całościowo do problemu zabezpieczania danych osobowych, zarówno zabezpieczania danych przetwarzanych tradycyjnie jak i przetwarzanych w systemach informatycznych.

CEL PRZYGOTOWANIA POLITYKI BEZPIECZEŃSTWA

Podstawowym celem przygotowania i wdrożenia Polityki Bezpieczeństwa jest zapewnienie zgodności działania z ustawą obowiązującymi przepisami prawa, a w szczególności z:

a) ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. nr 101, poz. 926 z późn. zm.),

b) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r., Nr 100, poz. 1024 z późn. zm.).

Przez powyższe należy rozumieć w szczególności realizację w niniejszym dokumencie wymogu opisania sposobu przetwarzania danych osobowych oraz środków technicznych i organizacyjnychzapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

Zadaniem Polityki Bezpieczeństwa jest także określenie podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz wymagań w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych.

ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ BEZPECZEŃSTWA:

Zgodnie z par. 3 rozporządzenia na politykę bezpieczeństwa składają się następujące informacje:

1. wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w których przetwarzane są dane osobowe,
2. wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych osobowych,
3. opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,
4. sposób przepływu danych pomiędzy poszczególnymi systemami,
5. określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

DEFINICJE

Ilekroć w niniejszym dokumencie jest mowa o:

1. **Polityce bezpieczeństwa**,– należy przez to rozumieć „Politykę bezpieczeństwa w zakresie ochrony danych osobowych w CIS Sp. z o.o. (zwaną dalej „CIS").
2. **Danych osobowych** – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

3. **Osobie możliwej do zidentyfikowania** – należy przez to rozumieć osobę, 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.
4. **Zbiorze danych osobowych** – należy przez to rozumieć każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
5. **Administratorze Danych** („**AD**") – osoba, która decyduje o celach i środkach przetwarzania danych osobowych.
6. **Administratorze Bezpieczeństwa Informacji** („**ABI**") – należy przez to rozumieć osobę wyznaczoną przez Administratora Danych do nadzorowania przestrzegania zasad ochrony danych osobowych oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych.
7. **Osobie upoważnionej** – należy przez to rozumieć osobę posiadającą pisemne upoważnienie do przetwarzania danych osobowych nadane przez AD lub ABI w imieniu AD.
8. **Przetwarzaniu danych** – należy przez to rozumieć jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
9. **Systemie informatycznym** – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych.
10. **Systemie tradycyjnym** – należy przez to rozumieć zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze.
11. **Zabezpieczeniu danych w systemie informatycznym** – należy przez to rozumieć wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
12. **Usuwaniu danych** – należy przez to rozumieć zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
13. **Zgodzie osoby, której dane dotyczą** – należy przez to rozumieć oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli innej treści.
14. **Odbiorcy danych** – należy przez to rozumieć każdego, komu udostępnia się dane osobowe, z wyłączeniem:

a) osoby, której dane dotyczą,
b) osoby upoważnionej do przetwarzania danych,
c) przedstawiciela, o którym mowa w art. 31a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst pierwotny: Dz. U. z 1997 r. Nr 133, poz. 883; tekst jednolity: Dz. U. z 2002 r., Nr 101, poz. 926),
d) podmiotu, o którym mowa w art. 31 ww. Ustawy,
e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

15. **Użytkowniku systemu informatycznego** – należy przez to rozumieć upoważnionego przez Administratora Danych, wyznaczonego do przetwarzania danych osobowych w systemie informatycznym pracownika, który odbył stosowne szkolenie w zakresie ochrony tych danych.
16. **Instrukcji** – należy przez to rozumieć „Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych.
17. **Rozporządzeniu** – rozumie się przez to rozporządzenie ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024 z późn. zm.), zwane dalej „Rozporządzeniem".
18. **Ustawie**– rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), zwaną dalej „Ustawą".

ADMINISTRATOR DANYCH OSOBOWYCH

Za bezpieczeństwo danych osobowych przetwarzanych w systemach przetwarzania danych osobowych odpowiada Administrator Danych Osobowych (ADO). Administrator Danych Osobowych obowiązany jest zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Administrator Danych Osobowych wyznacza Administratora Bezpieczeństwa Informacji (ABI), nadzorującego przestrzeganie zasad ochrony. Imienne upoważnienie udzielane jest w formie pisemnej do niniejszego dokumentu.

Administrator Danych Osobowych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych. Prowadzi również ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać:

1) Imię, nazwisko i stanowisko osoby upoważnionej,
2) Datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych.

Upoważnienie do przetwarzania danych osobowych wydawane jest na piśmie przez Administrator Danych Osobowych.

ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

Administrator Bezpieczeństwa Informacji wykonuje wszystkie prace niezbędne do efektywnego i bezpiecznego zarządzania systemami informatycznymi oraz tradycyjnymi.

Administrator Bezpieczeństwa Informacji może zostać wyznaczony przez Administratora Danych Osobowych. Administrator Danych upoważnia Administrator Bezpieczeństwa Informacji do przetwarzania wszystkich zbiorów danych osobowych zaewidencjonowanych w „Rejestrze zbiorów danych osobowych. Upoważnienie ma formę pisemną. Administrator Danych może w każdym czasie odwołać upoważnienie. Odwołanie ma formę pisemną.

Administrator Bezpieczeństwa Informacji realizuje zadania w zakresie ochrony danych osobowych, a w szczególności w zakresie:

a) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach danych,
b) sprawowania kontroli nad wprowadzaniem i udostępnianiem danych osobowych,
c) podejmowania stosownych działań zgodnie z niniejszą „Polityką bezpieczeństwa" w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym lub każdym innym,
d) niezwłocznego informowania Administratora Danych o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
e) nadzoru i kontroli – wraz z Administratorem Systemu Informatycznego (ASI) – systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.

POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

Administrator danych osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi w drodze umowy zawartej na piśmie.

Umowa o powierzenie przetwarzania danych osobowych określa zakres i cel przetwarzania powierzonych danych osobowych.

Podmiot, z którym zawarto umowę w zakresie przetwarzania danych osobowych jest obowiązany przed rozpoczęciem przetwarzania danych osobowych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39 Ustawy, oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a Ustawy. W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak Administrator Danych.

Przetwarzanie danych osobowych w zakresie i celu niezgodnym z zawartą umową jest zabronione. Odpowiedzialność za przestrzeganie przepisów Ustawy spoczywa na Administratorze Danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę za przetwarzanie danych niezgodnie z umową.

Administrator Danych czuwa nad prawidłowym wykonaniem umowy o powierzenie przetwarzania danych.

Umowa o powierzenie przetwarzania danych osobowych musi być zgodna z aktualną Polityką Bezpieczeństwa.

WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

Siedziba Spółki CIS mieści się pod adresem: Pogwizdów 155, 37-126 Medynia Głogowska;

Cały teren Spółki CIS jest ogrodzony. Ogrodzenie wykonane jest ze słupków stalowych wmurowanych w grunt i z siatki stalowej o wysokości 1,50 m. Wjazd do obiektu realizowany jest przez bramę główną zlokalizowaną obok portierni głównej. Do celów prowadzenia akcji ratowniczych ogrodzenie posiada bramy pożarowe usytuowane od strony wschodniej. Brama główna wyposażona jest w szlaban, który obsługiwany jest przez Portiera (ochroniarz z firmy SED-HUT). Każdy gość zakładu musi uzyskać przepustkę, podając: Imię (imiona) i Nazwisko, nr rejestracyjny pojazdu. Przedsiębiorstwo Usługowe „SED-HUT" Sp. z o.o. prowadzi całodobową bezpośrednią ochronę fizyczną. Służba ochrony realizowana jest przez jednego pracownika na zmianie. Uniemożliwia to wtargnięcie na teren obiektu osób postronnych.

Teren wyposażony jest w monitoring, system sygnalizacji pożaru (wizualny i dźwiękowy), instalację odgromową.

Dane przetwarzane są w dwukondygnacyjnym (bez podpiwniczenia) budynku biurowym. Przeznaczony on jest dla kierownictwa i administracji zakładu. Składa

się z pomieszczeń biurowych, sanitarnych, laboratorium, magazynu artykułów BPH i środków czystości oraz kotłowni gazowej. Obiekt posiada system alarmowy podłączony do Centrum Monitorowania P.W. „Karabela" Sp. z o.o. przy pomocy nadajnika radiowego. Drzwi wejściowe zamykane na klucz, który znajduje się na portierni. Budynek mogą otworzyć osoby posiadające hasło dostępu po czym klucz zwracany jest na portiernię.

Parter budynku przeznaczony jest do obsługi kontrahentów zakładu. Piętro przeznaczone jest głównie dla kadry zarządzającej zakładem oraz pomieszczeń pomocniczych, w tym archiwum i sekretariat zakładu.

Na strefę przetwarzania składa się: dział sprzedaży, biuro I (parter), biuro II (parter), biuro III (parter), biuro I (piętro), biuro II (piętro), biuro III (piętro), sekretariat. Dodatkowo wyznaczona jest strefa specjalna na którą składa się archiwum (piętro) oraz serwerownia (parter). Wszystkie pomieszczenia zamykane są na klucz. Do wyżej wymienionych miejsc dostęp mają osoby wykonujące w nich swoje obowiązki służbowe. Wszystkie klucze przechowywane są w pomieszczeniu sekretariatu w stalowej skrzynce zamykanej kluczem do której dostęp mają osoby zatrudnione w Sekretariacie. Skrzynka znajduje się w szafie zwykłej, zamykanej kluczem.

WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM ICH STRUKTURY ORAZ PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA DANYCH

W CIS przetwarza się następujące dane osobowe:

1. Udziałowców,
2. Członków Zarządu,
3. Pracowników,
4. Współpracowników,
5. Osób ubiegających się o zatrudnienie,
6. Rejestr korespondencji,
7. Klientów CIS Pianka,
8. Potencjalnych Klientów CIS Deweloper,
9. Klientów CIS Deweloper,
10. Dostawców.

Dane osobowe są gromadzone, przechowywane i przetwarzane w formie papierowej i elektronicznej. Przechowanie w formie papierowej ma postać list, formularzy lub innych dokumentów przechowywanych w segregatorach i teczkach umiejscowionych w drewnianych zamykanych szafach. W zakresie systemy

informatycznego dane przetwarzane są jako pliki pakietu Microsoft Office i przechowywane na dyskach twardych oraz sewerach. Ponadto CIS korzysta z programów księgowych, kadrowych i płacowych takich jak R2 Płatnik, Płatnik (ZUS), PL 21, FK21, HURT 21.

Dane osobowe Udziałowców CIS przetwarzane są w formie papierowej oraz elektronicznej i obejmują następujący zakres:

a) imię i nazwisko,
b) adres zamieszkania,
c) numer i serię dowodu osobistego,
d) numer telefonu oraz adres poczty elektronicznej,
e) liczbę oraz wartość udziałów,
f) numer PESEL
g) nazwę banku i numer rachunku bankowego.

Dane osobowe członków zarządu CIS przetwarzane są w formie papierowej oraz elektronicznej i obejmują następujący zakres:

a) imię i nazwisko,
b) adres zamieszkania,
c) numer i serię dowodu osobistego,
d) numer telefonu oraz adres poczty elektronicznej,
e) funkcja w zarządzie,
f) numer PESEL
g) nazwę banku i numer rachunku bankowego.

Dane osobowe pracowników CIS przetwarzane są w formie papierowej oraz elektronicznej i obejmują następujący zakres:

a) imię i nazwisko,
b) adres zamieszkania,
c) numer i serię dowodu osobistego,
d) numer PESEL,
e) numer telefonu oraz adres poczty elektronicznej,
f) imiona rodziców,
g) data urodzenia,
h) wykształcenie,
i) przebieg dotychczasowego zatrudnienia
j) nazwę banku i numer rachunku bankowego,
k) obywatelstwo,
l) dodatkowe uprawnienia,
m) stan rodzinny,
n) stosunek do powszechnego obowiązku obrony,
o) kary dyscyplinarne.

Dane osobowe współpracowników współpracujących z CIS przetwarzane są w formie papierowej oraz elektronicznej i obejmują następujący zakres:

a) imię i nazwisko,
b) adres zamieszkania,
c) serię i numer dowodu osobistego,
d) numer ewidencyjny PESEL i/lub NIP,
e) ramy graniczne obowiązywania umowy cywilnoprawnej,
f) kompetencje zawodowe,
g) doświadczenie zawodowe,
h) dane kontaktowe (telefon stacjonarny i/lub komórkowy, adres poczty elektronicznej),
i) nazwę banku i numer rachunku bankowego.

Dane osobowe osób ubiegających się o zatrudnienie przetwarzane są w formie papierowej oraz elektronicznej i obejmują następujący zakres:

a) imię i nazwisko,
b) adres zamieszkania,
c) obywatelstwo,
d) wykształcenie,
e) przebieg dotychczasowego zatrudnienia,
f) wizerunek – zdjęcie,
g) dane kontaktowe (telefon stacjonarny i/lub komórkowy, adres poczty elektronicznej).

Dane osobowe zawarte w rejestrze korespondencji przetwarzane są w formie papierowej oraz elektronicznej i obejmują następujący zakres:

a) imię i nazwisko,
b) adres korespondencyjny.

Dane osobowe Klientów CIS w zakresie handlu piankami poliuretanowymi przetwarzane są w formie papierowej i elektronicznej i obejmują następujący zakres:

a) imię i nazwisko,
b) adres korespondencyjny,
c) numer NIP,
d) nr telefonu, adres e – mail,
e) nazwa banku i numer rachunku bankowego

Dane osobowe Klientów CIS w zakresie potencjalnych klientów w zakresie działalności na rynku nieruchomości przetwarzane są w formie papierowej i elektronicznej i obejmują następujący zakres:

a) imię i nazwisko,
b) adres e – mail, numer telefonu.

Dane osobowe Klientów CIS w zakresie klientów zawierających z CIS umowy mające na celu nabycie nieruchomości przetwarzane są w formie papierowej i elektronicznej i obejmują następujący zakres:

a) imię i nazwisko,
b) adres zamieszkania,
c) seria i numer dowodu osobistego,
d) numer ewidencji PESEL,
e) adres e-mail,
f) numer telefonu,
g) obywatelstwo,
h) imiona rodziców,
i) stan rodzinny.

Dane osobowe kierowców wjeżdżających na teren CIS przetwarzane są w formie papierowej i elektronicznej i obejmują następujący zakres:

a) imię i nazwisko,
b) nr rejestracyjny pojazdu,
c) nr dowodu osobistego,
d) numer telefonu.

SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY SYSTEMAMI

CIS posiada nie własnego systemu informatycznego służącego do przetwarzania danych osobowych. Dane osobowe przetwarzane są przy pomocy wyspecjalizowanych programów zakupionych na zasadach licencji w zakresie księgowości, kadr i płac oraz edytora tekstu MS Word, jak również arkusza kalkulacyjnego MS Excel.

Pomiędzy systemami informatycznymi służącymi do przetwarzania danych występują następujące przepływy danych osobowych.

Z systemu kadrowego do systemu płacowego (przepływ jednostronny).

Z systemu płacowego do systemu księgowego – listy płac – przepływ jednostronny.

Z systemu sprzedażowego do systemu księgowego – przepływ jednostronny.

Przelewy bankowe i międzybankowe realizowane są przy użyciu teletransmisji.

OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI DANYCH OSOBOWYCH

A) Środki techniczne

Do zastosowanych przez ADO w organizacji środków technicznych służących zapewnieniu poufności, integralności i rozliczalności przy przetwarzaniu danych osobowych należy w przypadku zewnętrznych (obcych) systemów informatycznych dla potrzeb bieżącego użytkowania i przesyłania danych stosowane są zabezpieczenia podmiotów, którym przekazywane są dane:

a) „Płatnik" (program ZUS) –organizacja posiada certyfikowany publiczny klucz dostępu do tego programu wydany na czas określony,
b) Przelewy bankowe i międzybankowe – CIS używa witryn zabezpieczonych protokołem bezpieczeństwa oraz metod uwierzytelniających użytkownika.

Dostęp do danych osobowych przetwarzanych w systemach informatycznych jest chroniony poprzez zastosowanie loginów i haseł uniemożliwiających nieuprawnione korzystanie osobom nieupoważnionym.
W CIS stosuje się oprogramowanie antywirusowe na wszystkich urządzeniach oraz jako filtr poczty elektronicznej.
Elektroniczne przetwarzanie danych osobowych odbywa się na komputerach stacjonarnych i przenośnych.

B) Środki organizacyjne

Do zastosowania przez Administratora Danych i osoby przez niego upoważnione środków organizacyjnych służących zapewnieniu poufności, integralności i rozliczalności przy przetwarzaniu danych osobowych należy:

1. opracowanie i wdrożenie Polityki bezpieczeństwa w zakresie ochrony danych osobowych,
2. opracowanie i wdrożenie „Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych",
3. wyznaczenie przez Administratora Danych (ADO) Administratora Bezpieczeństwa Informacji (ABI) i nadanie mu upoważnienia do przetwarzania danych osobowych,
4. nadanie przez ADO, bądź jeżeli go wyznaczono ABI osobom upoważnionym upoważnień do przetwarzania danych osobowych oraz dopuszczenie wyłącznie tych osób do przetwarzania danych,
5. prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
6. zaznajomienie osób upoważnionych przy przetwarzaniu danych osobowych z przepisami dotyczącymi ochrony danych osobowych oraz ich przeszkolenie w zakresie zabezpieczeń systemu informatycznego,

7. sprawowanie przez ABI kontroli i nadzoru nad procesem wprowadzania danych osobowych do zbioru oraz ich udostępniania,

Osoby upoważnione do przetwarzania danych osobowych obowiązane zostały do zachowania ich w tajemnicy.

Monitory komputerów, na których przetwarzane są dane osobowe ustawione zostały w sposób uniemożliwiający wgląd osobom postronnym.

Dla potrzeb ochrony danych osobowych przetwarzanych w formie papierowej stosuje się zabezpieczenia polegające na przechowywaniu:

- dokumentacji bieżącej –w szafach zamykanych a zamki w obszarach przetwarzania danych osobowych

- dokumentacji archiwalnej – w specjalnie do tego celu przeznaczonym pomieszczeniu.

OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

Podział zagrożeń:

1. zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu) – ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu – ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
2. zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania) – może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
3. zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia naruszenia poufności danych – zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy.

Zagrożenia te możemy podzielić na:
a) nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
b) nieuprawniony dostęp do systemu z jego wnętrza,
c) nieuprawniony przekaz danych,
d) pogorszenie jakości sprzętu i oprogramowania,
e) bezpośrednie zagrożenie materialnych składników systemu.

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zasad bezpieczeństwa:

1. **Przełamanie zabezpieczeń tradycyjnych** – zerwane plomby na drzwiach, szafach, segregatorach,
2. **sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu**, jak np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.;
3. **niewłaściweparametry środowiska**, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych;
4. **awaria sprzętu lub oprogramowania**, które wyraźnie wskazują na umyślne działanie
   w kierunku naruszenia ochrony danych lub wręcz sabotaż;
5. **pojawienie się odpowiedniego komunikatu alarmowego** od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;
6. **pogorszenie jakości danych w systemie lub inne odstępstwo od stanu oczekiwanego** wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;
7. **naruszenie lub próba naruszenia** integralności systemu lub bazy danych w tym systemie;
8. stwierdzona **próba modyfikacji lub modyfikacja danych lub zmiana** w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
9. **niedopuszczalna manipulacja** danymi osobowymi w systemie;
10. **ujawnienie osobom nieupoważnionym** danych osobowych lub objętych tajemnicą procedury ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń;
11. **nieprzypadkowe odstępstwaod zasad bezpieczeństwa pracyw systemie lub sieci komputerowej** wskazujące na przełamanie lub zaniechanie ochrony danych osobowych – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu itp.;
12. **istnienie nieautoryzowanych kont dostępu** do danych lub tzw. „bocznej furtki" itp.;
13. **podmiana lub zniszczenie nośników z danymi osobowymi** bez odpowiedniego upoważnienia, jak również skasowanie lub skopiowanie w sposób niedozwolony danych osobowych;
14. **rażące naruszenie dyscypliny pracy** w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych itp.).

ZABEZPIECZENIE DANYCH OSOBOWYCH

Administrator Danych Osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych i na nośnikach tradycyjnych, a w szczególności do:

a) zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym,
b) zapobiegania kradzieży danych,
c) zapobiegania przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

Do zastosowanych środków technicznych należy:

a) przetwarzanie danych osobowych w wydzielonych, odpowiednio zabezpieczonych i przystosowanych do tego pomieszczeniach;
b) zabezpieczenie wejścia do pomieszczeń, o których mowa w pkt a;
c) wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji i nośników danych.

Do zastosowanych środków organizacyjnych należą następujące zasady:

a) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych przed jej przystąpieniem do pracy przy przetwarzaniu danych osobowych;
b) przeszkolenie osób, o których mowa w pkt a, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych;
c) kontrolowanie otwierania i zamykania pomieszczeń, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę i niepozostawianiu pomieszczenia w czasie pracy bez nadzoru.

Niezależnie od niniejszych zasad, w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie, przy czym dokumenty te nie mogą być sprzeczne z regulacjami okrcślonymi w „Polityce bezpieczeństwa".

ADO bezpośrednio bądź za pośrednictwem ABI sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.

POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

W przypadku stwierdzenia :

a) naruszenia zabezpieczeń systemu informatycznego,
b) naruszenia technicznego stanu urządzeń,
c) naruszenia zawartości zbioru danych osobowych,
d) ujawnienia metody pracy lub sposobu działania programu,
e) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
f) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.)

<u>każda osoba zatrudniona przy przetwarzaniu danych osobowych jest zobowiązana niezwłocznie powiadomić o tym fakcie ABI.</u>

W razie niemożliwości zawiadomienia ABI lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego.

Do czasu przybycia na miejsce naruszenia danych osobowych ABI lub upoważnionej przez niego osoby, należy:

a) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia – o ile istnieje taka możliwość – a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców naruszenia danych osobowych;
b) udokumentować wstępnie zaistniałe naruszenie;
c) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ABI lub osoby przez niego upoważnionej.

Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, ABI lub osoba przez niego upoważniona:

a) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania, mając na uwadze ewentualne zagrożenia dla prawidłowości pracy organizacji;
b) może żądać dokładnej relacji z zaistniałego naruszenia lub ujawnienia ochrony danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem;
c) rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu lub ujawnieniu ochrony danych osobowych ADO;
d) nawiązuje bezpośredni kontakt – jeżeli zachodzi taka potrzeba – ze specjalistami spoza organizacji.

Po wyczerpaniu niezbędnych środków doraźnych związanych z zaistniałym naruszeniem/ujawnieniem ochrony danych osobowych, ABI zasięga niezbędnych opinii i proponuje postępowanie naprawcze, w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

ABI dokumentuje zaistniały przypadek naruszenia lub ujawnienia ochrony danych osobowych oraz sporządza raport, który powinien zawierać w szczególności:

a) wskazanie osoby powiadamiającej oraz innych osób zaangażowanych lub odpytywanych w związku z naruszeniem lub ujawnieniem ochrony danych osobowych;
b) określenie czasu i miejsca: naruszenia/ujawnienia i powiadomienia o tym fakcie;
c) określenie okoliczności towarzyszących i rodzaju naruszenia/ujawnienia;
d) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania;
e) wstępną ocenę przyczyn wystąpienia naruszenia/ujawnienia;
f) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

ABI niezwłocznie przekazuje raport ADO.

Zaistniałe naruszenie/ujawnienie ochrony danych osobowych może stać się przedmiotem szczegółowej analizy prowadzonej przez ADO i ABI.

Analiza, o której mowa powyżej, powinna zawierać:
a) wszechstronną ocenę zaistniałego naruszenia/ujawnienia ochrony danych osobowych;
b) wskazanie odpowiedzialnych;
c) wnioski co do ewentualnych przedsięwzięć: proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom/ujawnieniom w przyszłości.

UDOSTĘPNIANIE DANYCH OSOBOWYCH

Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych przetwarzanych, a zwłaszcza prawo do:

1. uzyskania wyczerpującej informacji, czy taki zbiór istnieje oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy;
2. uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze;
3. uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące oraz podania w powszechnie zrozumiałej formie treści tych danych;
4. uzyskania informacji o źródle danych, z którego pochodzą dane jej dotyczące, chyba że administrator danych jest zobowiązany do zachowania w tym zakresie tajemnicy państwowej, służbowej lub zawodowej;
5. uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane;

6. żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r., Nr 101, poz. 926) albo są już zbędne do realizacji celu, dla którego zostały zebrane.

Dane osobowe udostępnia się na pisemny, umotywowany wniosek. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie. Udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

POSTANOWIENIA KOŃCOWE

Polityka bezpieczeństwa jest dokumentem wewnętrznym, zawiera dane, których ujawnienie mogłoby spowodować utratę danych chronionych w związku z czym nie może być udostępniana osobom nieupoważnionym w żadnej formie.

Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszym dokumencie.

Każda osoba mającą dostęp do danych osobowych z upoważnienia Administratora Danych, została zapoznana z Polityką Bezpieczeństwa i zobowiązana do jej przestrzegania w zakresie wynikającym z przydzielonych zadań. Dotyczy to w szczególności pracowników zatrudnionych przez Administratora Danych. Osoby o których mowa, złożyły na piśmie oświadczenie o zapoznaniu się z treścią Polityki Bezpieczeństwa oraz zobowiązały się do stosowania zawartych w niej postanowień.

Ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych zobowiązany jest prowadzić ABI.

Wdrożenie „Polityki bezpieczeństwa" odbywa się przez:
1) zapoznanie osób upoważnionych z treścią „Polityki bezpieczeństwa",
2) szkolenia z zakresu ochrony danych osobowych.

Polityka Bezpieczeństwa obowiązuje od dnia podjęcia uchwały przez Zarząd.