POLITYKA OCHRONY DANYCH OSOBOWYCH

w przedsiębiorstwie

THETA Consulting Sp. z o.o.

SPIS TREŚCI

1. **CEL POLITYKI**
2. **DOKUMENTY POWIĄZANE**
3. **ZAKRES STOSOWANIA**
4. **BEZPIECZEŃSTWO PRZETWARZANIA DANYCH OSOBOWYCH**
5. **DEFINICJE**
6. **ODPOWIEDZIALNOŚĆ**
   - 6.1 Administrator Danych
   - 6.2 Administrator Systemu Informatycznego
   - 6.3 Osoby upoważnione do przetwarzania danych
7. **ZARZĄDZANIE OCHRONĄ DANYCH OSOBOWYCH**
   - 7.1 Podstawowe zasady
   - 7.2 Procedury postępowania z danymi osobowymi
   - 7.3 Upoważnienie do przetwarzania danych osobowych
   - 7.4 Ewidencja osób upoważnionych
   - 7.5 Zachowanie danych osobowych w tajemnicy
   - 7.6 Zgodność
8. **ZARZĄDZANIE USŁUGAMI ZEWNĘTRZNYMI**
   - 8.1 Bezpieczeństwo usług zewnętrznych
   - 8.2 Powierzanie przetwarzania danych osobowych
   - 8.3 Udostępnianie danych osobowych
9. **BEZPIECZEŃSTWO FIZYCZNE OBSZARÓW PRZETWARZANIA** .
   - 9.1 Obszar przetwarzania
   - 9.2 Bezpieczeństwo środowiskowe
   - 9.3 Bezpieczeństwo urządzeń
   - 9.4 Fizyczna kontrola dostępu
10. **OCHRONA DANYCH OSOBOWYCH W FAZIE PROJEKTOWANIA ORAZ DOMYŚLNA OCHRONA DANYCH**
11. **ZARZĄDZANIE INCYDENTAMI I ZGŁOSZENIA NARUSZEŃ OCHRONY DANYCH OSOBOWYCH**
    - 11.1 Monitorowanie incydentów
    - 11.2 Zgłaszanie naruszeń ochrony danych osobowych
12. **PRAWA I ŻĄDANIA OSÓB FIZYCZNYCH, KTÓRYCH DANE DOTYCZĄ**
13. **POSTANOWIENIA KOŃCOWE**

1. CEL POLITYKI

Niniejszy dokument określa zasady bezpieczeństwa przetwarzania danych osobowych jakie powinny być przestrzegane i stosowane w THETA Consulting Sp. z o.o., przez pracowników i współpracowników, którzy przetwarzają dane osobowe.

Stosowanie zasad określonych w niniejszym dokumencie ma na celu zapewnienie prawidłowej ochrony danych osobowych przetwarzanych przez THETA Consulting Sp. z o.o. rozumianej jako ochronę danych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem 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.

2. DOKUMENTY POWIĄZANE

Integralną częścią niniejszej polityki jest instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w THETA Consulting Sp. z o.o. oraz procedury uszczegóławiające ochronę danych osobowych.

3. ZAKRES STOSOWANIA

Politykę stosuje się do danych osobowych przetwarzanych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany, danych osobowych stanowiących część zbiorów danych lub mających stanowić część zbioru, tj. do danych przetwarzanych w systemie informatycznym, zapisanych na zewnętrznych nośnikach informacji, w wersji papierowej oraz do informacji dotyczących bezpieczeństwa przetwarzania danych osobowych, w szczególności dotyczących wdrożonych zabezpieczeń technicznych i organizacyjnych.

W zakresie podmiotowym Polityka obowiązuje wszystkich pracowników i współpracowników THETA Consulting Sp. z o.o.

4. BEZPIECZEŃSTWO PRZETWARZANIA DANYCH OSOBOWYCH

Przez bezpieczeństwo przetwarzania danych osobowych rozumie się zapewnienie:

poufności — właściwości zapewniającej, że dane nie są udostępniane i ujawniane nieupoważnionym osobom, podmiotom lub procesom;

integralności — właściwości zapewniającej że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

dostępności — właściwości zapewniającej, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne;

odporności — właściwości zapewniającej zdolność systemów do prawidłowego funkcjonowania.

Ponadto zapewnienie zdolności do szybkiego przywracania dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

5. DEFINICJE

RODO — rozporządzenie ogólne — 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.

Administrator danych – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych tj. **THETA Consulting Sp. z o.o.** reprezentowana przez Aleksandrę Gendek (dalej jako **ADO**).

Dane osobowe – oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). Osobą możliwą do zidentyfikowania jest osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Przetwarzanie danych osobowych – oznacza operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Zbiór danych osobowych – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

Zbiór nieinformatyczny – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest zdecentralizowany czy rozproszony funkcjonalnie, prowadzony poza systemem informatycznym, w szczególności w formie papierowej np. kartoteki, skorowidza, księgi, wykazu lub innego zbioru ewidencyjnego.

Osoba upoważniona – osoba posiadająca formalne upoważnienie wydane przez Administratora Danych Osobowych (ADO), przetwarzająca dane osobowe wyłącznie na polecenie administratora.

Współadministrator – co najmniej dwóch administratorów wspólnie ustalających cele i sposoby przetwarzania danych osobowych.

Podmiot przetwarzający – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora (np. usługodawca IT, biuro księgowe, dostawca usługi Enova czy innego systemu informatycznego).

Podmiot podprzetwarzający – podmiot który przetwarzana dane osobowe na zlecenie podmiotu przetwarzającego.

Odbiorca danych – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią; organy

publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców. Przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.

Osoba, podmiot danych – oznacza osobę, której dane dotyczą.

Administrator Systemu Informatycznego (ASI) – osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna za sprawne działanie systemu informatycznego, a w szczególności za bezpieczeństwo systemów informatycznych służących do przetwarzania danych osobowych.

Udostępnienie – przekazanie innemu Administratorowi danych osobowych do realizacji własnych celów np. Bank Polski, Poczta Polska.

Powierzenie – zlecenie podmiotowi wykonania operacji lub zestawu operacji na przekazanych danych osobowych, na podstawie pisemnej umowy określającej m.in. charakter i cel przetwarzania.

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

Polityka – oznacza niniejszą politykę ochrony danych osobowych.

Procedura – oznacza sposób postępowania w określonych sytuacjach i jest uszczegółowieniem zasad ochrony danych osobowych spisanych w polityce.

Postępowanie z ryzykiem – proces wyboru i wdrażania środków sterowania ryzykiem mających na celu zminimalizowanie poziomu ryzyka.

Raport – rozumie się przez to przygotowanie przez system informatyczny zestawienia zakresu i treści przetwarzanych danych.

Ryzyko – niepewność osiągnięcia zamierzonych celów.

System informatyczny administratora danych – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych. W systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych.

Szacowanie ryzyka – proces identyfikowania, analizowania i oceniania ryzyka.

Teczka ODO – zbiór dokumentów, instrukcji, regulaminów, załączników opisujących sposób przetwarzania i ochrony danych, składający się na politykę ochrony danych osobowych, gromadzonych i nadzorowanych przez Inspektora Ochrony Danych.

6. ODPOWIEDZIALNOŚĆ

6.1. Administrator Danych

Do obowiązków Administratora Danych należy zapewnienie bezpieczeństwa przetwarzania danych osobowych, uświadomienie osobom upoważnionym do przetwarzania danych problematyki oraz wymagań rozporządzenia ogólnego – RODO.

Administrator danych w szczególności:

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

2. W przypadku zamiaru rozpoczęcia przetwarzania danych osobowych w nowym procesie przeprowadza się ocenę skutków dla ochrony danych w stosunku do tego procesu. Ponadto w każdym przypadku tworzenia nowego produktu lub usługi uwzględnia prawa osób których dane dotyczą, na każdym kluczowym etapie jego projektowania i wdrażania.

6.2. Administrator Systemu Informatycznego

Do obowiązków Administratora Systemu Informatycznego należy bieżąca ocena ryzyka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych, identyfikacja podatności na zagrożenia bezpieczeństwa przetwarzania danych osobowych oraz bezpieczne zarządzanie tymi systemami. Administrator Systemu Informatycznego podlega bezpośrednio pod Administratora Danych Osobowych.

Do obowiązków **ASI** należy również:

1. Aktualizowanie dokumentacji opisującej środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, w tym opracowanie procedury zapewniającej zachowanie ciągłości pracy systemów na wypadek zaistnienia incydentu;
2. Weryfikacja zdarzeń systemowych;
3. Kontrola przepływu informacji pomiędzy systemem informatycznym, a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej a systemem informatycznym;
4. Zarządzanie kontrolą dostępu do systemów informatycznych: nadzorowanie pracy serwerów, konfiguracja komputerów, instalowanie oprogramowania;
5. Monitorowanie incydentów związanych z bezpieczeństwem przetwarzania danych osobowych: weryfikacja zdarzeń systemowych; nadzorowanie, wykrywanie i eliminowanie nieprawidłowości, a w przypadku zaistnienia incydentu odnotowanie go w rejestrze incydentów;
6. Zarządzanie kontami użytkowników: dodawanie, edycja danych i kasowanie kont użytkowników;
7. Wdrażanie mechanizmów bezpieczeństwa systemu informatycznego, w tym przetwarzania danych osobowych;

8. Regularne tworzenie kopii zapasowych zasobów danych osobowych i programów służących do ich przetwarzania oraz okresowe sprawdzanie poprawności wykonania kopii zapasowych;
9. Asystowanie i współpraca ze specjalistami zewnętrznymi: przy pracach instalacyjnych, naprawczych i konfiguracyjnych;
10. Niezwłoczne zgłaszanie do ADO wszelkich stwierdzonych nieprawidłowości lub naruszeń przestrzegania Instrukcji Zarządzania Systemem Informatycznym.

6.3. Osoby upoważnione do przetwarzania danych

Do obowiązków osób upoważnionych do przetwarzania danych osobowych należy:

1. Zachowanie w tajemnicy danych osobowych, do których przetwarzania zostały upoważnione i których przetwarzane zostało im polecone.
2. Zachowanie w tajemnicy sposobów zabezpieczenia danych osobowych.
3. Zapewnienie bezpieczeństwa przetwarzania danych osobowych poprzez ich ochronę przed zniszczeniem, utraceniem, nieuzasadnioną modyfikacją, nieuprawnionym ujawnieniem nieuprawnionym dostępem do danych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
4. Nieprzetwarzanie danych osobowych, do których przetwarzania zostały upoważnione i których przetwarzane zostało im polecone, w innym celu niż objęte poleceniem.
5. Zachowanie tajemnicy również po upływie czasu trwania polecenia, w tym ustania stosunku pracy.
6. Informowanie Administratora Danych o wszelkich naruszeniach, podejrzeniach naruszenia i nieprawidłowościach w sposobie przetwarzania i ochrony danych osobowych.
7. Współpraca przy ustaleniu przyczyn naruszenia ochrony danych osobowych oraz usuwania skutków tych naruszeń, w tym zapobieganie ich ewentualnemu ponownemu wystąpieniu.

7. ZARZĄDZANIE OCHRONĄ DANYCH OSOBOWYCH

7.1. Podstawowe zasady

Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba przetwarzająca te dane w zakresie zgodnym z obowiązkami służbowymi oraz rolą sprawowaną w procesie przetwarzania danych.

Każda z osób mająca styczność z danymi osobowymi jest zobowiązana do ochrony danych osobowych oraz przetwarzania ich w granicach udzielonego jej upoważnienia.

Ponadto każda osoba przetwarzająca dane osobowe jest zobowiązana do przestrzegania poniższych zasad:

- ✓ zgodność z prawem – przetwarzanie w oparciu o podstawę prawną i zgodnie z prawem;
- ✓ rzetelność – rzetelnie i uczciwie;
- ✓ przejrzystość – w sposób przejrzysty dla osoby, której dane dotyczą;
- ✓ ograniczonego celu – w konkretnych celach i nie "na zapas";

- ✓ minimalizacji danych – nie więcej niż potrzeba;
- ✓ prawidłowość – z dbałością o prawidłowość danych;
- ✓ ograniczenie przechowywania – nie dłużej niż potrzeba;
- ✓ integralność i poufność – zapewniając odpowiednie bezpieczeństwo danych.

7.2. Procedury postępowania z danymi osobowymi

Dostęp do danych osobowych powinien być przyznawany zgodnie z zasadą wiedzy koniecznej, niezbędnej do wypełnienia obowiązków służbowych na zajmowanym stanowisku pracy oraz zgodnie z poleceniami Administratora Danych.

Dane osobowe powinny być chronione przed nieuprawnionym dostępem, modyfikacją oraz utratą, uszkodzeniem lub zniszczeniem.

Dane osobowe należy przetwarzać wyłącznie za pomocą autoryzowanych urządzeń służbowych.

7.3. Upoważnienie do przetwarzania danych osobowych

Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane na podstawie art. 29 i art. 32 ust. 4 RODO – ogólnego rozporządzenia o ochronie danych oraz przepisów krajowych uszczegółowiających zasady postępowania podczas nadawania upoważnień.

Upoważnienia wydawane są indywidualnie przed rozpoczęciem przetwarzania danych osobowych, po uprzednim przeszkoleniu osoby upoważnianej z podstawowych zasad dotyczących ochrony danych osobowych, wynikających z przepisów prawnych i przyjętych w przedsiębiorstwie środków technicznych i organizacyjnych.

7.4. Ewidencja osób upoważnionych

1. Ewidencja osób upoważnionych do przetwarzania danych osobowych jest prowadzona przez Administratora Danych Osobowych lub osobę do tego upoważnioną i zawiera w szczególności:
   - ✓ imię i nazwisko osoby upoważnionej do przetwarzania danych osobowych;
   - ✓ datę nadania i ustania upoważnienia do przetwarzania danych osobowych;

2. Zmiany dotyczące użytkownika, takie jak: zmiana imienia lub nazwiska lub zmiana zakresu upoważnienia podlegają niezwłocznemu odnotowaniu w ewidencji.

3. Zmiany dotyczące użytkownika, takie jak: rozwiązanie umowy, utrata upoważnienia do przetwarzania danych osobowych lub zmiana zakresu obowiązków służbowych skutkująca ustaniem upoważnienia powodują wyrejestrowanie użytkownika przez Administratora Systemu Informatycznego w trybie natychmiastowym, zablokowanie identyfikatora i unieważnienie hasła tego użytkownika oraz odnotowania informacji w ewidencji.

4. ADO przy współpracy z ASI odpowiada za nadzór nad osobami, które utraciły uprawnienia do dostępu do danych osobowych oraz za zablokowanie im dostępu do systemu informatycznego poprzez zablokowanie identyfikatora i wyrejestrowanie z ewidencji osób upoważnionych.

5. Identyfikator, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi.

7.5. Zachowanie danych osobowych w tajemnicy

Osoby, które zostały upoważnione do przetwarzania danych osobowych są zobowiązane do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których uzyskały dostęp w trakcie zatrudnienia, również po ustaniu zatrudnienia.

7.6. Zgodność

Niniejsza Polityka jest aktualizowana adekwatnie do zmieniających się przepisów o ochronie danych osobowych oraz zmian faktycznych mających miejsce w THETA Consulting Sp. z o.o.

Polityka podlega okresowemu przeglądowi, który ma na celu stwierdzenie, czy postanowienia Polityki odpowiadają aktualnej i planowanej działalności THETA Consulting Sp. z o.o. oraz stanowi prawnemu, aktualnemu w momencie dokonywania przeglądu.

Zmiany niniejszej Polityki wymagają przeglądu innych dokumentów dotyczących ochrony danych osobowych obowiązujących w THETA Consulting Sp. z o.o.

8. ZARZĄDZANIE USŁUGAMI ZEWNĘTRZNYMI

8.1. Bezpieczeństwo usług zewnętrznych

Należy zapewnić, aby usługi zewnętrzne były prowadzone zgodnie z wymaganiami bezpieczeństwa przetwarzania danych osobowych wynikających z ogólnego rozporządzenia o ochronie danych – RODO.

8.2. Powierzanie przetwarzania danych osobowych

THETA korzysta wyłącznie z usług podmiotów zewnętrznych (podmiotów przetwarzających) zapewniających wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych spełniających wymagania rozporządzenia RODO i chroniących prawa osób, których dane dotyczą.

Powierzenie przetwarzania danych odbywa się na podstawie umowy lub innego instrumentu prawnego, wiążąc podmiot przetwarzający i THETA, określając co najmniej przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

Powierzenie przetwarzania danych osobowych nie oznacza zwolnienia ADO z odpowiedzialności za zgodne z prawem przetwarzanie powierzonych danych.

8.3. Udostępnianie danych osobowych

Dane osobowe mogą być udostępniane wyłącznie odbiorcom uprawnionym do ich otrzymania na mocy przepisów prawa lub na podstawie umowy powierzenia oraz osobom, których dane dotyczą.

Udostępnianie danych osobowych może nastąpić wyłącznie za wiedzą i zgodą Administratora Danych Osobowych.

Podmiot występujący o udostępnienie informacji powinien wskazać podstawę prawną upoważniającą go do otrzymania tych danych albo uzasadnioną potrzebę żądania ich udostępnienia. Tylko w takiej sytuacji można dokonać oceny, czy w określonym przypadku udostępnienie danych jest prawnie dopuszczalne i czy nie będzie ono stanowić naruszenia zasad ochrony informacji.

Informacje zawierające dane osobowe powinny być przekazywane w formie umożliwiającej potwierdzenie odebrania informacji np.: listem poleconym za pokwitowaniem odbioru lub innym bezpiecznym sposobem, określonym wymogiem prawnym lub umową.

Udostępniając dane osobowe na podstawie umów powierzenia i przepisów prawnych należy odnotowywać informacje o udostępnieniu bezpośrednio w Rejestrze czynności przetwarzania.

Przetwarzanie, w tym udostępnianie danych osobowych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą oraz następuje w celu badań naukowych, dydaktycznych, historycznych oraz statystycznych.

9. BEZPIECZEŃSTWO FIZYCZNE OBSZARÓW PRZETWARZANIA

9.1. Obszar przetwarzania

Dane osobowe przetwarzane są w obszarach przetwarzania danych osobowych, na które składają się pomieszczenia biurowe oraz budynki, gdzie THETA Consulting Sp. z o.o. prowadzi działalność. Do takich pomieszczeń, zalicza się w szczególności:

- ✓ pomieszczenia biurowe, w których zlokalizowane są stacje robocze lub serwery służące do przetwarzania danych osobowych;
- ✓ pomieszczenia, w których przechowuje się dokumenty źródłowe oraz wydruki z systemu informatycznego zawierające dane osobowe;
- ✓ pomieszczenia, w których przechowywane są sprawne i uszkodzone urządzenia, elektroniczne nośniki informacji oraz kopie zapasowe zawierające dane osobowe;
- ✓ pomieszczenia biurowe w których przechowywane są dokumenty archiwalne.

9.2. Bezpieczeństwo środowiskowe

Lokalizację i umiejscowienie danych osobowych należy starannie dobierać z uwzględnieniem wymaganych aspektów bezpieczeństwa przetwarzania danych osobowych. W szczególności należy rozważyć aspekty dotyczące:

- ✓ zasilania energią elektryczną;
- ✓ klimatyzacji oraz wentylacji;
- ✓ wykrywania oraz ochrony przed pożarem i powodzią;
- ✓ fizycznej kontroli dostępu.

Pomieszczenia wchodzące w skład obszaru przetwarzania danych osobowych należy wyposażyć w odpowiednie środki ochrony fizycznej i organizacyjnej chroniące przed nieautoryzowanym lub nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami pracy.

Kopie zapasowe zawierające dane osobowe należy przechowywać w drugiej fizycznej lokalizacji w bezpiecznej odległości od lokalizacji podstawowej.

9.3. Bezpieczeństwo urządzeń

Urządzenia służące do przetwarzania danych osobowych należy przechowywać w bezpieczny i nadzorowany sposób.

Urządzenia mobilne takie jak np. komputery przenośne lub urządzenia PDA (Personal Digital Asisstant) nie powinny być pozostawiane bez opieki ponadto system i komputer przenośny powinien być zabezpieczony odpowiednim hasłem.

9.4. Fizyczna kontrola dostępu

Należy wdrożyć procedury eksploatacyjne w celu ochrony danych osobowych oraz dokumentacji systemowej przed nieautoryzowanym lub nieuprawnionym ujawnieniem, modyfikacją, usunięciem i zniszczeniem.
Należy wdrożyć politykę czystego biurka i czystego ekranu w celu redukcji ryzyka nieautoryzowanego i nieuprawnionego dostępu lub uszkodzenia danych osobowych.
Przyznawanie dostępu gościom należy wykonywać wyłącznie w określonych i autoryzowanych celach. Monitory należy ustawić w taki sposób aby uniemożliwiać podgląd wyświetlanych danych osobowych przez osoby nieuprawnione.

W przypadku korzystania z usług zewnętrznych podmiotów oferujących zbieranie i niszczenie papierów, urządzeń lub nośników zwierających dane osobowe, należy wybrać wykonawcę z odpowiednimi zabezpieczeniami i doświadczeniem.

10. OCHRONA DANYCH OSOBOWYCH W FAZIE PROJEKTOWANIA ORAZ DOMYŚLNA OCHRONA DANYCH

Za ochronę danych w fazie tworzenia nowych projektów oraz domyślną ochronę danych odpowiada Administrator Danych. Na wczesnym etapie projektowania operacji przetwarzania danych należy wdrożyć środki techniczne i organizacyjne zapewniające od samego początku ochronę prywatności i bezpieczeństwo danych osobowych. Należy domyślnie zapewnić jak najwyższy poziom prywatności przetwarzanych danych poprzez zastosowanie m.in.

- ✓ minimalizacji zakresu przetwarzania danych osobowych,
- ✓ jak najszybszej pseudonimizacji danych osobowych,
- ✓ przejrzystości co do funkcji i przetwarzania danych osobowych,
- ✓ umożliwienie osobie, której dane dotyczą, monitorowania przetwarzania danych.

11. ZARZĄDZANIE INCYDENTAMI I ZGŁASZANIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH

11.1. Monitorowanie incydentów

Incydenty związane z bezpieczeństwem przetwarzania danych osobowych powinny być wykrywane, rejestrowane i monitorowane w celu ich zidentyfikowania i zapobiegania wystąpieniu w przyszłości.

Zdarzenia systemowe powinny być przechowywane jako materiał dowodowy zaistniałych incydentów związanych z bezpieczeństwem przetwarzania danych osobowych.

Osoby upoważnione do przetwarzania danych osobowych powinny znać i przestrzegać zasady zgłaszania naruszeń związanych z bezpieczeństwem przetwarzania danych osobowych, w tym rodzaje naruszeń podlegające zgłoszeniu do ADO.

Zdarzenie wraz z działaniami korygującymi rejestrowane są w rejestrze naruszeń oraz działań korygujących i zapobiegawczych.

11.2. Zgłaszanie naruszenia ochrony danych osobowych

Zaistniałe zdarzenia związane z naruszeniem lub podejrzeniem naruszenia bezpieczeństwa przetwarzania danych osobowych takie jak np. utrata integralności, niedostępność, awarie, uszkodzenia, ostrzeżenia i alarmy bezpieczeństwa systemów informatycznych, urządzeń teleinformatycznych oraz danych powinny być niezwłocznie zgłaszane do Administratora Danych Osobowych.

ADO weryfikuje uzyskane informacje pod kątem skutków związanych z naruszeniem praw i wolności osób fizycznych i postępuje zgodnie z przyjętą procedurą postępowania w przypadku wystąpienia naruszeń.

12. PRAWA I ŻĄDANIA OSÓB FIZYCZNYCH, KTÓRYCH DANE DOTYCZĄ

Każdej osobie, której dane osobowe są przetwarzane przysługuje prawo do kontroli przetwarzania jej danych osobowych, a w szczególności prawo do:

1. Uzyskania wyczerpującej informacji, czy jej dane osobowe są przetwarzane oraz do otrzymania informacji o pełnej nazwie i adresie siedziby Administratora Danych.
2. Uzyskania informacji o celu, zakresie i sposobie przetwarzania danych osobowych.
3. Uzyskania informacji, do kiedy są przetwarzane jej dane osobowe, oraz podania w powszechnie zrozumiałej formie treści tych danych.
4. Uzyskania informacji o źródle, z którego pochodzą dane osobowe jej dotyczące.
5. Uzyskania informacji o sposobie udostępniania danych osobowych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym te dane osobowe są udostępniane.
6. Żądania dostępu do danych osobowych, ich sprostowania, usunięcia, czasowego lub stałego ograniczenia przetwarzania danych, przenoszenia danych do innego administratora, wniesienia sprzeciwu wobec przetwarzania oraz niepodlegania decyzjom opartym wyłącznie na profilowaniu.

13. POSTANOWIENIA KOŃCOWE

Polityka wraz z dokumentami powiązanymi jest dokumentem wewnętrznym zawierającym opis środków technicznych i organizacyjnych.

W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie aktualnie obowiązujące przepisy prawa w zakresie ochrony danych osobowych, szczególnie RODO.

Użytkownicy zobowiązani są do bezwzględnego stosowania postanowień zawartych w niniejszej Polityce.
W wypadku odrębnych od zawartych w niniejszej Polityce uregulowań występujących w innych procedurach obowiązujących u Administratora Danych, użytkownicy mają obowiązek stosowania unormowań dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.