Polityka Bezpieczeństwa Danych Osobowych

w

Ogólnopolskim Towarzystwie Ochrony Ptaków

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH ORAZ INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

W związku z wejściem w życie 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 (RODO) i jego obowiązywaniem od 25 maja 2018 r., **stowarzyszenie Ogólnopolskie Towarzystwo Ochrony Ptaków** pragnąc wykazać zgodność z przepisami ochrony danych osobowych przyjmuje niniejszy dokument.

Celem Polityki Bezpieczeństwa Danych Osobowych jest określenie kierunków działań oraz wsparcia dla zapewnienia bezpieczeństwa przetwarzania zbiorów danych osobowych zarządzanych przez Administratora danych dla wykazania zgodności z wymogami RODO oraz innymi regulacjami prawnymi i wewnętrznymi wytycznymi dotyczącymi przetwarzania danych osobowych.

ROZDZIAŁ I - POJĘCIA I DEFINICJE

§1

1) **Administrator Danych Osobowych (Administrator, ADO, organizacja)** – Ogólnopolskie Towarzystwo Ochrony Ptaków z siedzibą w Markach przy ul. Odrowąża 24, Marki 05-270, posiadające nr KRS: 0000015808, NIP: 9570553373, REGON: 190524320, numer kontaktowy: +48 22 761 82 05; adres e-mail: biuro@otop.org.pl;
2) **Dane osobowe** – oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
3) **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym Administratora;
4) **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;
5) **Strona trzecia** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które z upoważnienia administratora lub podmiotu przetwarzającego mogą przetwarzać dane osobowe;
6) **Osoba upoważniona do przetwarzania danych osobowych (Osoba upoważniona)** – osoba, która została upoważniona do przetwarzania danych osobowych przez Administratora;
7) **Poufność danych** – rozumie się jako właściwość zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym osobą i podmiotom;
8) **Dostępność danych** – rozumie się jako właściwość zapewniającą, że upoważnieni Użytkownicy mają dostęp do informacji w każdej sytuacji, kiedy jest to niezbędne do realizacji ich zadań;
9) **Integralność danych** – rozumie się jako właściwość zapewniającą, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

10) **Postać elektroniczna danych** – dane przechowywane za pomocą środków elektronicznych w formie zapisów w pamięci ulotnej i/lub stałej, przetwarzane za pomocą Systemu Informatycznego;
11) **Postać tradycyjna danych** – dane w formie papierowej, przetwarzane za pomocą tradycyjnych metod składowania (np. w segregatorach, teczkach, kuwetach biurowych, na pułkach);
12) **Podmiot Przetwarzający (Przetwarzający, Procesor)** – osoba fizyczna lub prawna, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;
13) **Przetwarzanie** – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
14) **Profilowanie** – oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
15) **Rozliczalność** – rozumie się jako właściwość zapewniająca, że działania podmiotu (osoby) mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi (tej osobie);
16) **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;
17) **System informatyczny Administratora Danych (system informatyczny)** – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych, telefony komórkowe, systemy e-mail lub inne, gdzie przetwarzane są dane osobowe w formie elektronicznej;
18) **Użytkownik** – osoba upoważniona do dostępu i przetwarzania danych osobowych, której nadano identyfikator Użytkownika i przyznano hasło do systemów informatycznych;
19) **Zbiór danych** – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
20) **Polityka Bezpieczeństwa Danych Osobowych (Polityka, Polityka Bezpieczeństwa, PBDO, IZSI)** – niniejszy dokument określający nadrzędne zasady ochrony danych osobowych u Administratora wraz z załącznikami i dokumentami stworzonymi na ich podstawie.
21) **Osoba związana z organizacją** – podmiot danych osobowych, dla którego organizacja jest Administratorem danych osobowych w rozumieniu RODO. Może nim być w szczególności pracownik, współpracownik, kontrahent, pracownicy kontrahenta, klient, darczyńca, osoby kontaktujące się przez kanały elektroniczne lub w sposób tradycyjny.

ROZDZIAŁ II – POLITYKA BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

Cele i zasady funkcjonowania polityki bezpieczeństwa

§2

Niniejsza Polityka zapewnia:

1) Spójność z wyznaczonymi zadaniami oraz pełną integrację z podstawowymi procedurami zdefiniowanymi u Administratora;
2) Skuteczne działania w odniesieniu do zagrożeń poufności, integralności i dostępności danych osobowych, realizację zadań Administratora w taki sposób, aby podnieść jakość i wiarygodność Ogólnopolskiego Towarzystwa Ochrony Ptaków oraz aby zapewnić rozliczalność przetwarzania danych osobowych i bezpieczeństwo ich praw;
3) Ochronę danych osobowych tworzonych, przetwarzanych, przechowywanych i przesyłanych nie tylko za pomocą systemów informatycznych, ale również i w sposób tradycyjny;
4) Zgodność z materialnym zakresem stosowania RODO, co oznacza, że ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowanych oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.

§3

Celem Polityki Bezpieczeństwa Danych Osobowych oraz jej załączników i dokumentów wewnętrznych stosowanych przez Administratora jest wskazanie działań, jakie należy podejmować oraz ustanowienie zasad, jakie należy stosować, aby prawidłowo były realizowane obowiązki Administratora Danych Osobowych w zakresie zabezpieczenia udostępnionych oraz powierzonych mu danych osobowych.

§4

1. Realizując niniejszą Politykę, Administrator przyjmuje następujące zasady w zakresie:

a) **Poufności** – dane nie są udostępniane lub ujawniane podmiotom bądź osobom nieupoważnionym;
b) **Integralności** – dane nie zostają zmienione lub zniszczone w sposób nie autoryzowany;
c) **Dostępności** – istnieje możliwość wykorzystania danych na żądanie, w założonym czasie, przez autoryzowany podmiot;
d) **Rozliczalności** – możliwość jednoznacznego przypisania działań dotyczących danych poszczególnym osobom;
e) **Autentyczności** – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana;
f) **Niezawodności** – zamierzone zachowania i skutki są spójne;

- przyjmując jako naczelne zasady działania:

a) ***Privacy by design*** (zasada prywatności w fazie projektowania) polegającą na wdrożeniu odpowiednich środków technicznych i organizacyjnych w celu skutecznej realizacji zasad ochrony danych osobowych, tak by spełnić wymogi zawarte w tym paragrafie, przy określaniu nowego sposobu przetwarzania, a także w trakcie trwania tego przetwarzania oraz
b) ***Privacy by default*** (zasada prywatności w ustawieniach domyślnych) polegającą na wdrożeniu odpowiednich środków technicznych i organizacyjnych, aby domyślnie przetwarzane były wyłącznie dane osobowe niezbędne do osiągnięcia celu ich przetwarzania.

2. Administrator przetwarza dane:

- **a)** zgodnie z prawem, rzetelnie i w sposób przejrzysty (zasada zgodności z prawem, rzetelności, przejrzystości),
- **b)** w sprecyzowanych, wyraźnie i prawnie uzasadnionych celach (zasada ograniczenia celu),
- **c)** tylko w takim zakresie, jaki jest niezbędny dla osiągnięcia celu ich zbierania (zasada minimalizacji danych),
- **d)** w formie aktualnej, umożliwiającej identyfikację osoby, przez czas niezbędny dla realizacji celu ich zbierania, a w razie potrzeby są uaktualniane, aby dane nieprawidłowe zostały usunięte lub sprostowane (zasada prawidłowości danych),
- **e)** w formie umożliwiającej identyfikację osoby, której dane dotyczą przez ograniczony okres, nie dłuższy, niż jest to niezbędne do celów, w których dane są przetwarzane (zasada ograniczenia przechowywania),
- **f)** w sposób zapewniający odpowiednie bezpieczeństwo przed ich nieuprawnioną zmianą czy zniszczeniem (zasada integralności i poufności),
- **g)** w sposób umożliwiający wykazanie przestrzegania tych zasad (zasada rozliczalności).

§5

Polityka Bezpieczeństwa Danych Osobowych ma na celu zredukowanie, a ostatecznie wyeliminowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, tj.:

1) naruszeń danych osobowych rozumianych jako prywatne dobro powierzone;
2) naruszeń przepisów prawa oraz innych regulacji;
3) utraty lub obniżenia reputacji podmiotów, których dane dotyczą;
4) strat finansowych ADO ponoszonych w wyniku nałożonych kar;
5) zakłóceń organizacji pracy spowodowanych nieprawidłowym działaniem systemów,

a w szczególności niedoprowadzenia u osób związanych z organizacją do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, jeżeli nieuprawnione przetwarzanie mogłoby skutkować:

1) dyskryminacją,
2) kradzieżą tożsamości lub oszustwem dotyczącym tożsamości,
3) stratą finansową,
4) naruszeniem dobrego imienia,
5) naruszeniem poufności danych osobowych,
6) nieuprawnionym odwróceniem pseudonimizacji lub
7) wszelką inną znaczną szkodą gospodarczą lub społeczną;

jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi.

Kompetencje i odpowiedzialność w zarządzaniu bezpieczeństwem danych osobowych

§6

1. **Administrator Danych Osobowych** realizuje zadania w zakresie ochrony danych osobowych, w tym upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków, w tym zwłaszcza:
   - **a)** wprowadza właściwe procedury i zabezpieczenia zapewniające bezpieczeństwo przetwarzanych danych osobowych oraz monitoruje ich przestrzeganie,

b) informuje pracowników na temat obowiązujących przepisów, zasad i wewnętrznych procedur ochrony danych osobowych, w tym zapoznaje ich z zapisami niniejszej Polityki

c) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych,

d) sprawdza aktualność polityk, zasad i procedur ochrony danych osobowych, a w szczególności aktualizuje na bieżąco Rejestr Czynności Przetwarzania, Rejestr Kategorii Czynności Przetwarzania, Ewidencję zbiorów danych osobowych oraz Rejestr naruszeń.

e) jeżeli uzna za zasadne lub wymagają tego przepisy prawa, ponownie przeprowadza określenie i szacowanie ryzyka.

2. Administrator Danych Osobowych realizuje również zadania w zakresie **zarządzania i bieżącego nadzoru nad systemem informatycznym**, w tym zwłaszcza:

a) zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora,

b) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,

c) zarządza uprawnieniami i jeżeli wynika taka konieczność, udziela dostęp poszczególnym Użytkownikom (poprzez identyfikatory, hasła) do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta Użytkowników,

d) podejmuje działania zapewniające integralność danych w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego;

e) sprawuje nadzór nad wykonywaniem napraw, konserwacją, uaktualnianiem oraz likwidacją urządzeń komputerowych i systemów informatycznych, na których zapisane są dane osobowe i nad wykonywaniem kopii zapasowych.

Wykaz osób upoważnionych do przetwarzania danych osobowych

§7

ADO prowadzi i na bieżąco aktualizuje wykaz osób upoważnionych do gromadzenia i przetwarzania danych osobowych, który powinien zawierać następujące dane:

1) nazwisko i imię osoby upoważnionej,

2) identyfikator osoby upoważnionej w systemie informatycznym (jeśli dotyczy),

3) stanowisko,

4) wskazanie zbiorów danych osobowych, do którego osoba upoważniona ma prawo dostępu,

5) zakres uprawnień danej osoby w zakresie przetwarzania danych osobowych,

6) datę przyznania uprawnień,

7) termin wygaśnięcia uprawnień,

8) zobowiązanie do zachowanie poufności,

9) oświadczenie o zapoznaniu się z niniejszą Polityką i zobowiązanie do jej przestrzegania.

Rejestr czynności przetwarzania

§8

1. ADO prowadzi rejestr czynności przetwarzania danych osobowych. W rejestrze tym zamieszcza się w szczególności wszystkie następujące informacje:
   - **a)** imię i nazwisko lub nazwę oraz dane kontaktowe ADO
   - **b)** cele przetwarzania
   - **c)** opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
   - **d)** kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych (o ile dotyczy)
   - **e)** jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
   - **f)** jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa danych.
2. Rejestr czynności przetwarzania obejmuje zarówno zbiory danych przetwarzanych w wersji elektronicznej jak i zbiory danych przechowywane w wersji papierowej.

Powierzenie danych podmiotom zewnętrznym

§9

1. Powierzenie danych przetwarzanych przez ADO może nastąpić w drodze pisemnej umowy, w której osoba przyjmująca dane zobowiązuje się do przestrzegania obowiązujących przepisów ustawy o ochronie danych osobowych oraz zasad wynikających z RODO. Umowa powinna zawierać informacje wynikające z art. 28 RODO.
2. ADO zawiera umowy powierzenia bądź dba o wprowadzenie odpowiednich klauzul odnoszących się do zapewnienia bezpieczeństwa danych osobowych w ramach powierzenia, z umowami określającymi współpracę ze wszystkimi podmiotami zewnętrznymi, którym zleca przetwarzanie danych.

ROZDZIAŁ III - BEZPIECZEŃSTWO W PRZETWARZANIU DANYCH OSOBOWYCH

Pomieszczenia tworzące obszar, w którym przetwarzane są dane osobowe

§10

1. Pomieszczeniami tworzącymi obszar, w którym znajdują się przetwarzane dane osobowe są pomieszczenia, w których znajdują się zbiory danych w formie kartotek, rejestrów, segregatorów, czyli danych papierowych oraz systemy informatyczne, w których są przetwarzane dane osobowe.
2. Przebywanie w pomieszczeniach znajdujących się wewnątrz obszaru, o którym mowa w ust. 1, osób nieuprawnionych do dostępu do danych osobowych, powinno być zorganizowane w sposób uniemożliwiający zapoznanie się tym osobom z przetwarzanymi przez ADO danymi osobowymi.
3. Meble oraz inne schowki, w których przechowywane są dane osobowe powinny być zamykane i chronione przed dostępem do nich osób nieupoważnionych do przetwarzania danych osobowych.
4. W przypadku zamykanych na klucz szaf, schowków i pomieszczeń, w których przechowywane są dane osobowe, ADO prowadzi rejestr kluczy, w tym osób posiadających upoważnienia do systemów informatycznych, a dokumenty z danymi udostępniane są wyłącznie osobom upoważnionym przez ADO, w tym podmiotom przetwarzającym.

§11

Każda osoba zatrudniona u Administratora (niezależnie od formy zatrudnienia), bądź pomioty, których Administrator upoważnił do przetwarzania danych osobowych, są zobowiązane do przestrzegania następujących zasad ogólnych dotyczących bezpieczeństwa ochrony danych osobowych:

1) dbanie o poufność, dostępność i zachowanie integralności przetwarzanych danych osobowych,

2) przetwarzanie danych osobowych wyłącznie w czasie i w zakresie ustalonym indywidualnie przez ADO w upoważnieniu lub w umowie powierzenia oraz wyłącznie w celu wykonywania nałożonych na nią obowiązków, w tym praw wynikających z przepisów prawnych,

3) zachowanie w poufności danych osobowych oraz przestrzeganie procedur ich bezpiecznego przetwarzania. Przestrzeganie zasady poufności danych osobowych obowiązuje przez cały okres zatrudnienia lub wykonywania zlecenia bądź umowy powierzenia na rzecz ADO, a także po ustaniu współpracy zgodnie z właściwymi regulacjami ustawowymi lub umownymi,

4) dopuszczenie do przetwarzania danych osoby/podmioty znające przepisy w zakresie ochrony danych oraz postanowienia niniejszej Polityki służące do przetwarzania danych osobowych,

5) stosowanie określonych przez ADO procedur i wytycznych mających na celu przetwarzanie danych osobowych zgodnie z obowiązującym prawem oraz realizacje praw podmiotów danych,

6) niedopuszczenie osób nieuprawnionych do elektronicznych/papierowych nośników danych w których znajdują się dane osobowe podmiotów, z którymi współpracuje ADO, a w razie stwierdzenia takiego nieuprawnionego dostępu, niezwłoczne informowanie ADO,

7) korzystanie z systemu informatycznego w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników oraz stosowanie higieny hasła,

8) zabezpieczenie danych na wszystkich rodzajach nośników, z których osoba/podmiot korzysta, przed ich udostępnianiem osobom nieupoważnionym (np. przy pomocy szyfrowania, hasła).

Zabezpieczenia zbiorów danych w wersji papierowej oraz innych nośników danych

§12

1. Gwarancją zapewnienia bezpieczeństwa systemu informatycznego oraz przetwarzanych i przechowywanych danych osobowych jest zapewnienie **bezpieczeństwa fizycznego, organizacyjnego i technicznego**.

2. Zabezpieczenia danych osobowych, w tym zabezpieczenia systemów informatycznych (fizyczne, organizacyjne, techniczne) stanowią prawnie chronioną tajemnicę przedsiębiorstwa, której pracownicy bądź osoby współpracujące są zobowiązani zachować w tajemnicy w trakcie trwania stosunku prawnego oraz po jego zakończeniu.

3. Ochronę gromadzonych zbiorów danych stanowią:
- **a)** antywłamaniowe drzwi na podwójny klucz do biura Administratora,
- **b)** zamykane szafy z danymi osobowymi,
- **c)** przyznawanie upoważnień dostępu do przetwarzania danych, w tym w systemach informatycznych,
- **d)** zapoznanie upoważnionych osób z zasadami ochrony danych,
- **e)** ustawienie monitorów w sposób uniemożliwiający osobom nieupoważnionym dostępu do danych osobowych wyświetlanych na nich,

f) przydzielanie haseł dostępu do systemu informatycznego i indywidualnych kont,
g) systematyczna zmiana haseł dostępu do systemu informatycznego i indywidualnych kont,
h) posiadanie kopii danych,
i) wprowadzona zasada czystego biurka,
j) wprowadzona polityka kluczy,
k) współpraca z agencją ochrony (jeżeli dotyczy),
l) zabezpieczenie systemu informatycznego programami antywirusowymi niedopuszczającymi do zainfekowania szkodliwym oprogramowaniem m. in. typu ransomware,
m) zakaz wynoszenia danych na niezaszyfrowanych pamięciach przenośnych poza obszar przetwarzania, a dane zgrane na pamięci przenośne nie powinny być dłużej na nich przechowywane niż jest to konieczne,
n) szkolenia z ochrony danych/inny sposób uświadamiania pracowników/współpracowników,
o) instrukcje oraz wytyczne wewnętrzne OTOP opracowywane na bieżąco,
p) wprowadzona procedura monitoringu wizyjnego (jeżeli dotyczy).

4. Należy chronić dokumenty papierowe jak i nośniki magnetyczne i optyczne (płyty, pendrive itp.) zawierające dane osobowe przed ich fizycznym uszkodzeniem lub zniszczeniem, co uniemożliwiałoby odczytanie lub odzyskanie informacji w nich zawartych.

5. Dokumenty papierowe oraz nośniki magnetyczne i optyczne zawierające dane osobowe muszą być chronione przed zagrożeniami ze strony otoczenia, kradzieżą lub niewłaściwym używaniem (ogień, wyciek wody, kradzież itp.). Opuszczając stanowisko pracy należy sprawdzić, czy są one zamknięte w odpowiednich szafach oraz innych zabezpieczonych schowkach. Klucze do zamykanych szaf oraz schowków, gdzie przechowywane są dane, nie mogą być pozostawiane w drzwiach lub w innym miejscu ogólnie dostępnym dla osób nieupoważnionych.

6. Zabrania się przekazywania lub udostępniania dokumentów papierowych lub innych nośników zawierających dane osobowe osobom nieuprawnionym.

7. Zabrania się kopiowania jakichkolwiek danych osobowych zawartych na dokumentach papierowych lub innych nośnikach bez zgody ADO lub osoby przez niego upoważnionej.

8. Usunięcie lub wyniesienie poza siedzibę podmiotu dokumentu papierowego lub innego nośnika zawierającego dane osobowe wymaga zgody ADO lub upoważnionej przez niego osoby.

9. Utrata, kradzież lub uzyskanie dostępu przez osobę nieuprawnioną do dokumentów papierowych lub innych nośników zawierających dane osobowe powinna być niezwłocznie zgłoszona ADO.

10. Każdy dokument papierowy zawierający dane osobowe który nie podlega archiwizacji, należy zniszczyć w sposób trwały, uniemożliwiający odczytanie danych osobowych. W przypadku innych nośników, zapisane dane, które nie podlegają archiwizacji należy usunąć w sposób uniemożliwiający ich odczytanie.

11. Komputer przeznaczony do naprawy może być pozbawiony dysku twardego przed naprawą lub może zostać naprawiony pod nadzorem ADO lub osoby przez niego upoważnionej, jeżeli czynności nie dotyczą kwestii hardware'u.

ROZDZIAŁ IV - INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Nadawanie i rejestrowanie uprawnień do przetwarzania danych w systemie informatycznym

§13

1. Najwyższe uprawnienia w systemie informatycznym posiada Administrator Danych osobowych.
2. ADO odpowiada za tworzenie, modyfikację i nadawanie uprawnień dla kont Użytkowników.
3. ADO jest osobą uprawnioną do instalowania i usuwania oprogramowania systemowego i narzędziowego.

§14

Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie ADO do przetwarzania danych osobowych.

§15

Osoby dopuszczone do przetwarzania danych osobowych zobowiązane są do zachowania tajemnicy w zakresie tych danych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu stosunku pracy lub innej formy zatrudnienia.

Zabezpieczenie danych w systemie informatycznym

§16

1. O wyborze, instalacji i odinstalowywaniu oprogramowania i aplikacji decyduje wyłącznie ADO w porozumieniu z głównym informatykiem, jeżeli taki został wyznaczony.
2. ADO stosuje oprogramowanie legalne i posiadające ważną licencję Użytkownika.
3. Oprogramowanie albo bazy danych wykorzystywane do przetwarzania danych muszą posiadać własny system zabezpieczeń oraz dostęp chroniony hasłem.
4. Hasła do systemu stacji roboczych na których przetwarzane są dane osobowe mają długość przynajmniej 12 znaków (duże i małe litery oraz cyfry lub znaki specjalne – co najmniej 3 z podanych 4 kategorii) i okres ważności nie dłużej niż kwartał. Hasło nie może być zapisywane lub przechowywane w miejscu dostępnym dla osób nieuprawnionych, powinno być przechowywane w pamięci.
5. W przypadku utracenia hasła Użytkownik ma obowiązek skontaktować się z ADO celem uzyskania nowego hasła.

§17

Osobom korzystającym z systemu informatycznego, w którym przetwarzane są dane osobowe, zabrania się:

1) ujawniania loginu i hasła innym osobom,
2) przechowywania haseł w sposób umożliwiający zapoznania się z nimi przez innych,
3) udostępniania stanowisk informatycznych wraz z danymi osobowymi osobom nieuprawnionym,
4) udostępniania osobom nieuprawnionym programów komputerowych zainstalowanych w systemie, a służących do przetwarzania danych osobowych,
5) używania oprogramowania w innym zakresie niż pozwala na to umowa licencyjna,
6) rozpowszechniania danych osobowych w sposób elektroniczny lub tradycyjny (drukując dane),
7) kopiowania danych na niezaszyfrowane przenośne pamięci, kopiowania na inne systemy celem wynoszenia ich poza siedzibę podmiotu,
8) samowolnego instalowania i używania jakichkolwiek programów komputerowych, szczególnie pirackich, oraz niestosowania aktualnego oprogramowania antywirusowego,

9) używania nośników danych udostępnionych przez osoby postronne,
10) rozpowszechniania danych, w tym przesyłania dokumentów, zdjęć dla publicznej wiadomości,
11) otwierania załączników oraz linków/odnośników do stron internetowych przesłanych pocztą elektroniczną od nieznanych i „niezaufanych" nadawców, a także w przypadku niespodziewanej wiadomości. Za każdym razem należy sprawdzić dane nadawcy oraz język, którym się posługuje, czy nie jest podejrzany.

Zasady bezpieczeństwa podczas pracy w systemie informatycznym
Procedura rozpoczęcia, zawieszenia i zakończenia pracy systemu informatycznego

§18

Przed przystąpieniem do pracy w systemie informatycznym należy:

1) sprawdzić stanowisko pracy, czy nie zostało zmodyfikowane (np. przez podłączenie nowego urządzenia do niego), włączyć komputer,
2) dokonać uwierzytelnienia zgodnie z monitem systemu operacyjnego komputera,
3) bezwzględnie należy zapewnić zachowanie poufności podczas wprowadzania hasła,
4) po uruchomieniu systemu operacyjnego można rozpocząć pracę na programie Użytkowym,
5) w razie problemów związanych z uruchamianiem systemu lub uwierzytelnianiem, lub stwierdzeniem fizycznej ingerencji w przetwarzane dane, osoby upoważnione do pracy na systemie informatycznym mają obowiązek skontaktować się z ADO.

§19

1. Podczas dokonywania czynności związanych z operacjami na danych osobowych Administrator zapewnia odpowiednie środki bezpieczeństwa, aby osoby nieuprawnione nie miały do nich dostępu.
2. Podczas nawet chwilowego opuszczenia stanowiska pracy należy zablokować możliwość wglądu do przetwarzanych danych przez osoby trzecie poprzez wylogowanie Użytkownika z aplikacji /systemu operacyjnego/ lub blokadę uniemożliwiającą dostęp – wygaszacz ekranu z hasłem.
3. Odchodząc na dłużej należy wylogować się z systemu informatycznego oraz mieć ustawione automatyczne wylogowywanie.

§20

W celu zakończenia pracy w systemie informatycznym należy wylogować się z systemu informatycznego lub zamknąć system operacyjny. Należy również odczekać do poprawnego zakończenia procesu wylogowania lub zamknięcia systemu operacyjnego. W razie problemów z systemem operacyjnym osoby upoważnione do pracy na systemie informatycznym mają obowiązek skontaktować się z ADO lub bezpośrednio przełożonym.

ROZDZIAŁ V – PROCEDURA ZBIERANIA I PRZETWARZANIA DANYCH OSOBOWYCH ORAZ OBOWIĄZEK INFORMACYJNY

Procedura zbierania danych osobowych

§21

1. ADO gromadzi niezbędne dane osobowe osób związanych z organizacją zgłaszających się do niego bezpośrednio lub pośrednio w określonych celach różnymi kanałami komunikacyjnymi. Proces zbierania danych odbywa się w sposób zapewniających ich wiarygodność, poufność oraz bezpieczeństwo.
2. ADO oraz inne upoważnione przez niego osoby, zobowiązane są do zweryfikowania tożsamości każdej osoby przed udzieleniem odpowiedzi na żądania związane z przetwarzaniem danych osobowych tj. dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych.
3. Weryfikacji tożsamości celem realizacji żądań wynikających z art. 15-21 RODO, dokonuje się poprzez kontrolę okazanego dokumentu potwierdzającego tożsamość zawierającego co najmniej zdjęcie, imię i nazwisko oraz PESEL lub w przypadku jego braku inny dokument jednoznacznie identyfikujący daną osobę. Dokumentem potwierdzającym tożsamość jest w szczególności: dowód osobisty, prawo jazdy, paszport, podlegający okazaniu nie stanowi procesu przetwarzania danych osobowych podlegającego pod RODO.
4. W przypadku gdy weryfikacja tożsamości realizowana jest w sposób inny niż osobiście (np. na odległość lub przy użyciu środków komunikacji elektronicznej) lub w sytuacji powzięcia przez osobę weryfikującą wątpliwości co do tożsamości osoby, ADO lub upoważniona osoba może żądać dodatkowych informacji lub podjęcia przez osobę zgłaszającą żądanie dodatkowych działań niezbędnych do potwierdzenia tożsamości tej osoby, takich jak np. podania dodatkowych danych osobowych w celu ich porównania z posiadanymi przez ADO.
5. Wszelką komunikację z podmiotem danych w zakresie realizacji jego praw wynikających z RODO należy podejmować po ustaleniu jego tożsamości na zasadach określonych wyżej, chyba że ADO wprowadził szczegółową wewnętrzną regulację.
6. Komunikacja z podmiotem danych w zakresie realizacji jego praw jest wolna od opłat. Nie oznacza to jednak, że wszystko jest wolne od opłat, mogą one być uzasadnione szczególnymi przepisami prawa, albo uzasadnione na podstawie art. 12 ust. 5 RODO, na co wskazuje regulacja z §34.

Legalność przetwarzanych danych osobowych

§22

1. Jeżeli Administrator Danych Osobowych nie przetwarza danych osobowych bezpośrednio:
   - **a)** na podstawie przepisów prawa polskiego,
   - **b)** na podstawie przepisów prawa UE,
   - **c)** na podstawie uzasadnionego interesu,
   - **d)** w ramach wykonywania umowy,
   - **e)** w celu ochrony żywotnych interesów,
   - **f)** lub wykonując zadanie realizowane w interesie publicznym,

   to podstawą przetwarzania tych danych jest zgoda uzyskana od właściciela danych.
2. Zgoda wyrażana jest samodzielnie, świadomie i dobrowolnie na podstawie oświadczenia w formie tradycyjnej lub elektronicznej. Formuła zgody jest przedstawiona przejrzyście i przystępnie dla każdej osoby fizycznej odpowiednio do jej wieku. Każda zgoda zawiera ponadto, zakres i cel przetwarzania danych.

3. Osoba udzielająca zgodę ma prawo ją wycofać w każdym momencie. Wycofanie zgody powinno następować w równie prosty sposób, jak jej wyrażenie. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę.
4. Zakazane jest przetwarzanie danych osobowych szczególnej kategorii, o których mowa w art. 9 ust. 1 RODO, chyba że spełniono przynajmniej jedną przesłankę wynikającą z art. 9 ust. 2 RODO.
5. W procesie uzyskiwania danych osobowych ADO wypełnia swój obowiązek informacyjny rzetelnie, przestrzegając art. 13 oraz art. 14 RODO.

Upoważnienie do przetwarzania danych osobowych

§23

1. Administrator nadaje upoważnienia i dostęp do przetwarzania danych osobowych wyłącznie tym osobom, które zapoznały się z zasadami bezpieczeństwa i ochrony danych osobowych, a także zobowiązały się do ich przestrzegania.
2. Dostęp do danych osobowych realizowany jest wyłącznie na podstawie ważnych upoważnień, dokładnie precyzujących zakres danych, czynności i cel ich przetwarzania.
3. Administrator prowadzi ewidencję i monitoring upoważnień w sposób ciągły. Usuwane są z systemów informatycznych konta Użytkowników, którzy przestali być upoważnieni do przetwarzania danych.
4. Upoważnienia wydawane są w formie pisemnej, w tym mogą być elektronicznie, osobiście przez ADO lub wyznaczonego pełnomocnika.

Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą

§24

1. Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, ADO przekazuje następujące informacje:
   - **a)** swoją tożsamość i dane kontaktowe,
   - **b)** dane kontaktowe Inspektora Ochrony Danych – jeżeli dotyczy ADO,
   - **c)** cele przetwarzania danych osobowych;
   - **d)** jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) – prawnie uzasadnione interesy realizowane przez ADO lub przez stronę trzecią;
   - **e)** informację o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
   - **f)** informacje o zamiarze przekazania danych osobowych do państwa trzeciego – jeżeli dotyczy ADO;
   - **g)** okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
   - **h)** informacje o prawie do żądania od ADO dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

i) informację o prawie wniesienia skargi do organu nadzorczego;

j) informację czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;

k) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu,

l) jeżeli przetwarzanie opiera się na zgodzie – informację o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przewarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

2. Obowiązek informacyjny może być zrealizowany w szczególności poprzez:

a) udostępnienie klauzuli informacyjnej na tablicy informacyjnej w biurze ADO oraz na stronie internetowej,

b) zamieszczenie klauzuli informacyjnej w oddziałach terenowych,

c) umieszczenie klauzul informacyjnych w przekazywanych dokumentach papierowych (np. umowa o świadczenie usług) oraz elektronicznych,

d) umieszczenie odpowiedniej informacji w umowach (np. zawieranych z pracownikami),

e) umieszczenie klauzul informacyjnych na stronach społecznościowych ADO,

f) zamieszczenie odnośnika w stopce mailowej do klauzuli znajdującej się na stronie internetowej.

3. W przypadku pozyskania danych osobowych w sposób inny niż wskazany w ust. 1, Administrator przekazuje wszystkie informacje z ust. 1 (oprócz ust. 1 lit. j) i dodatkowo ADO informuje o:

a) źródle pozyskania danych,

b) kategorii odnośnych danych osobowych tj. typ i rodzaj danych (np. dane kontaktowe)

ROZDZIAŁ VI – INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA DANYCH OSOBOWYCH

Opis zdarzeń naruszających ochronę danych osobowych

§25

1. Sytuacje określane jako zagrożenia dla przetwarzanych przez ADO danych osobowych można podzielić na:

a) **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.

b) **Zagrożenia losowe wewnętrzne** (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania, pogorszenie jakości sprzętu i oprogramowania, nieprawidłowości w zakresie zabezpieczenia fizycznego miejsc przechowywania i przetwarzania danych osobowych) - może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.

c) **Zagrożenia zamierzone** - świadome i celowe działania powodujące naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości

pracy), zagrożenia te możemy podzielić na: - nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), - nieuprawniony dostęp do systemu z jego wnętrza, - nieuprawnione przekazanie danych, - bezpośrednie zagrożenie materialnych składników systemu (np. kradzież sprzętu).

2. Dla wszystkich zidentyfikowanych typów zagrożeń ADO przeprowadza analizę ryzyka, określa możliwe skutki takich zdarzeń oraz działania minimalizujące ryzyko ich wystąpienia.

Opis zdarzenia naruszającego ochronę danych osobowych

§26

O naruszeniu ochrony danych osobowych mogą świadczyć w szczególności następujące symptomy:

1) zniszczenie lub stwierdzenie nieuprawnionego dostępu do sprzętu lub pomieszczeń, w których przechowywane są dane osobowe,

2) ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych osobowych, w szczególności do pomieszczenia, gdzie znajduje się sprzęt komputerowy służący do przechowywania danych oraz do pomieszczeń, w których przechowywane są zbiory danych w wersjach papierowych,

3) brak możliwości uruchomienia lub przez Użytkownika aplikacji/oprogramowania pozwalającej na dostęp do danych osobowych, lub zalogowania się do tej aplikacji,

4) ograniczone, w stosunku do normalnej sytuacji, uprawnienia Użytkownika aplikacji (np. brak możliwości wykonywania pewnych operacji normalnie dostępnych Użytkownikowi) lub uprawnienia poszerzone w stosunku do normalnej sytuacji,

5) wygląd aplikacji inny niż normalnie,

6) inny zakres danych niż normalnie dostępny dla Użytkownika dużo więcej lub dużo mniej danych,

7) znaczne spowolnienie działania systemu informatycznego,

8) pojawienie się niestandardowych komunikatów generowanych przez system informatyczny,

9) zagubienie, kradzież lub zniszczenie sprzętu, nośnika danych osobowych, albo dokumentów w formie papierowych, zawierających dane osobowe,

10) informacja z systemu antywirusowego o zainfekowaniu systemu informatycznego wirusami,

11) fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu informatycznego przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań albo zaistnienia siły wyższej,

12) podejrzenie nieautoryzowanej modyfikacji przetwarzanych danych osobowych.

Procedura postępowania w sytuacji naruszenia ochrony danych osobowych

§27

1. Każda osoba biorąca udział w przetwarzaniu danych osobowych jest odpowiedzialna za bezpieczeństwo tych danych.

2. Każda osoba, która zauważyła zdarzenie mogące być przyczyną naruszenia ochrony danych osobowych lub mogących spowodować naruszenie bezpieczeństwa danych, zobowiązana jest do natychmiastowego poinformowania ADO.

§28

1. Informacja o pojawieniu się zagrożenia lub wystąpieniu zagrożenia bezpieczeństwa danych osobowych przekazywana jest niezwłocznie - osobiście, telefonicznie lub pocztą elektroniczną do Administratora Danych Osobowych.
2. Informacja, o której mowa w pkt. 1 powinna zawierać imię i nazwisko osoby zgłaszającej oraz zauważone symptomy zagrożenia.

§29

1. Do czasu interwencji ADO, zgłaszający:
   a) niezwłocznie podejmuje czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnia w działaniu również ustalenie przyczyn lub sprawców,
   b) zabezpiecza dostęp do miejsca lub urządzenia przez osoby trzecie,
   c) jeżeli ma to miejsce w przestrzeni informatycznej wstrzymywana jest praca urządzeniu elektronicznym na którym zaistniało naruszenie ochrony,
   d) nie zmienia położenia przedmiotów, które pozwalają stwierdzić naruszenie ochrony lub odtworzyć jej okoliczności,
   e) podejmuje, stosownie do zaistniałej sytuacji, inne niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych,
   f) podejmuje inne działania stosownie do objawów i komunikatów towarzyszących naruszeniu,
   g) powinien wstępnie udokumentować zaistniałe naruszenie.
2. Dokonywanie zmian w miejscu naruszenia ochrony jest dopuszczalne, jeżeli zachodzi konieczność ratowania osób lub mienia albo zapobieżenia grożącemu niebezpieczeństwu.

§30

ADO lub osoba upoważniona, niezwłocznie po uzyskaniu sygnału o naruszeniu bezpieczeństwa danych osobowych, powinien:

1) zapoznać się z zaistniałą sytuacją i dokonać wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy,

2) przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej,

3) dokonać oględzin pomieszczeń, szaf i schowków, w których doszło do naruszenia bezpieczeństwa danych osobowych lub ewentualnie systemów informatycznych,

4) jeżeli dotyczy to systemów informatycznych, należy wylogować Użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych,

5) jeżeli dotyczy to systemów informatycznych, należy dokonać zmiany hasła Użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania,

6) podjąć działania w celu usunięcia skutków incydentu,

7) udokumentować wszelkie informacje związane z danym zdarzeniem, zgodnie z wewnętrznymi dokumentami,

8) dokonać analizy, zgodnie z wewnętrznymi dokumentami, czy jest zobowiązany do zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu lub zawiadomić o naruszeniu podmiot danych (odpowiednio zgodnie z §31 oraz §32).

§31

Po wykonaniu czynności, o których mowa wyżej, ADO niezwłocznie podejmuje działania w celu:

1) wyjaśnienia zdarzenia w szczególności czy w wyniku incydentu miało miejsce naruszenie bezpieczeństwa danych osobowych,

2) wyjaśnienia przyczyn naruszenia bezpieczeństwa danych osobowych i zebranie ewentualnych dowodów w szczególności, gdy zdarzenie było związane z celowym działaniem pracowników bądź osób trzecich spoza organizacji,

3) usunięcia skutków incydentu i przywrócenia prawidłowego przebiegu procesu przetwarzania danych osobowych.

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

§32

1. W przypadku naruszenia ochrony danych osobowych, ADO bez zbędnej zwłoki i nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je właściwemu organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

2. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je ADO, zgodnie z dokumentami wewnętrznymi.

3. Jeżeli naruszenie ochrony danych osobowych podlega zgłoszeniu do organu nadzorczego, ADO zgłasza takie naruszenie zgodnie ze wzorem udostępnionym przez Urząd Ochrony Danych Osobowych.

4. Jeżeli – i w zakresie, w jakim – informacji z ust. 3 nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.

Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

§33

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

2. Zawiadomienie o naruszeniu powinno jasnym i prostym językiem opisywać charakter naruszenia ochrony danych osobowych, zgodnie z dokumentami wewnętrznymi, oraz zawierać co najmniej:

a) imię i nazwisko oraz dane kontaktowe inspektora ochrony danych, bądź osoby kontaktowej,

b) opis możliwych konsekwencji naruszenia ochrony danych osobowych

c) opis środków zastosowanych lub proponowanych przez ADO w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

3. Zawiadomienie nie jest wymagane, w następujących przypadkach:

a) ADO wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

b) ADO zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,

c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

ROZDZIAŁ VII - UDOSTĘPNIANIE DANYCH OSOBOWYCH

Prawo dostępu, sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania.

§34

Każda osoba fizyczna, której dane przetwarzane są u Administratora, ma prawo zwrócić się z wnioskiem o udzielenie informacji związanych z przetwarzaniem danych osobowych. Sprawy związane z udzielaniem informacji w tym zakresie prowadzi ADO, udzielając informacji o zawartości zbioru danych na piśmie bądź elektronicznie w sposób odpowiednio zabezpieczony – zgodnie z drogą wpłynięcia wniosku od podmiotu danych.

§35

1. W przypadku żądań podmiotu danych, podejmowanych w związku z przetwarzaniem danych osobowych tj. dostępu do danych osobowych jego dotyczących, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych, które można uznać za ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ciągły i nieuzasadniony charakter, ADO może pobrać dodatkową opłatę. Przy ustaleniu wysokości opłaty uwzględnia się administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań. Opłata może mieć charakter zryczałtowany i może być ustalona w formie dostępnego cennika.

2. Za ewidentnie nieuzasadnione lub nadmierne żądania pomiotów danych, które uzasadniają pobranie opłaty dodatkowej bądź odmowę podjęcia działań uznaje się w szczególności skierowane:

a) żądania o informacje częściej niż raz na 3 miesiące, jeżeli zakres danych przetwarzanych przez ADO bądź inne okoliczności związane z przetwarzaniem nie ulegały zmianie od czasu złożenia poprzedniego żądania;

b) żądania o informacje dzielone sztucznie na kilka lub kilkanaście żądań;

c) żądanie szczególnego, niestandardowego formatu odpowiedzi;

d) żądanie udzielenia odpowiedzi w języku innym niż polski.

3. Za ewidentnie nieuzasadnione lub nadmierne żądania osoby, które uzasadniają odmowę ich zrealizowania uznaje się w szczególności:
   a) żądanie informacji, których przekazanie spowodowałyby nieuprawnione ujawnienie tajemnicy organizacji lub danych osobowych osób związanych z organizacją, lub innej tajemnicy prawnie chronionej;
   b) żądanie informacji, których udzielenie wymagałoby nadmierne zaangażowanie ADO lub jego pracowników, w sposób utrudniający jego bieżące funkcjonowanie.

4. ADO zobowiązany jest do każdorazowego uzasadnienia i podania do wiadomości osoby zgłaszającej żądanie przyczyny pobrania dodatkowej opłaty lub odmowy podjęcia działań poprzez wskazanie, dlaczego w jego ocenie żądania są ewidentnie nieuzasadnionych lub nadmiernych.

§36

1. Udostępnienie danych przetwarzanych przez ADO, może nastąpić na pisemny wniosek, zawierający m.in. następujące elementy:
   a) adresata wniosku, umożliwiające jednoznaczne stwierdzenie, że chodzi o Administratora,
   b) dane wnioskodawcy, umożliwiające jego identyfikację,
   c) wskazanie dyspozycji, zgodnie z RODO,
   d) zakres informacji.

2. Wniosek o udostępnienie danych może być również skierowany drogą elektroniczną, w sposób umożliwiający potwierdzenie tożsamości wnioskodawcy.

3. Bez potwierdzenia tożsamości wnioskodawcy ADO nie spełnia żądania osoby nieznanej, o czym informuje.

Prawo dostępu do danych

§37

1. Osoby związane z organizacją, których dane osobowe są przetwarzane przez Administratora mają prawo dostępu do swoich danych.

2. W przypadku, w którym osoba związana z organizacją jednoznacznie powołuje się na prawo dostępu do danych osobowych, o którym mowa w art. 15 RODO, w zależności od zakresu wskazanego w żądaniu, jest uprawniony do:
   a) uzyskania od ADO potwierdzenia czy ADO przetwarza jego dane osobowe, a jeżeli ma to miejsce;
   b) uzyskania dostępu do tych danych oraz informacji odnośnie:
      i. celów przetwarzania,
      ii. kategorii odnośnych danych osobowych,
      iii. informacji o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione,
      iv. w miarę możliwości - planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
      v. informacje o prawie do żądania od ADO sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania,
      vi. informacje o prawie wniesienia skargi do organu nadzorczego,

vii. jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle,

viii. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o ile jest podejmowane,

ix. jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, związanych z przekazaniem.

c) uzyskania od ADO kopii danych osobowych podlegających przetwarzaniu.

3. Przed udostępnieniem osobie zainteresowanej żądanych informacji, w szczególności zaś przed udzieleniem dostępu do danych osobowych lub wydaniu kopii danych osobowych, w tym elektronicznie, ADO weryfikuje tożsamość tej osoby.

4. Nieodpłatnemu udostępnieniu podlega pierwsza kopia przetwarzanych danych. ADO może jednak pobierać opłatę od kolejnych kopii, o czym mowa w §34, chyba że przepis prawa stanowi inaczej.

5. W przypadku przekazania kopii danych w postaci elektronicznej, można w szczególności przesłać te dane na adres e-mail wskazany we wniosku a lub inny powszechnie stosowany sposób transmisji elektronicznej. W przypadku niewskazania adresu e-mail lub innego sposobu transmisji elektronicznej ADO zwraca się do wnioskodawcy o wskazanie adresu e-mail lub innego powszechnie stosowanego sposobu transmisji elektronicznej informując jednocześnie o najczęstszych zagrożeniach związanych z transmisją elektroniczną. W razie, gdy wnioskodawca kontaktuje się za pośrednictwem poczty elektronicznej z prośbą o przesłanie dokumentacji, korzystając z adresu, którego nie wskazał podczas rejestracji, przesłanie tej dokumentacji możliwe jest wyłącznie po weryfikacji jego tożsamości i poprawności adresu (np. poprzez wykonanie telefonu).

Prawo do sprostowania danych

§38

Osoba, której dane dotyczą, ma prawo żądania od ADO niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

Prawo do usunięcia danych („prawo do bycia zapomnianym")

§39

1. Osoba, której dane dotyczą, ma prawo żądania od ADO niezwłocznego usunięcia dotyczących jej danych osobowych, a ADO ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi w szczególności jedna z następujących okoliczności:

a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;

c) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania.

d) dane osobowe były przetwarzane niezgodnie z prawem;
e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego, któremu podlega ADO.

2. Dane osobowe nie są usuwane w zakresie, w jakim przetwarzanie jest niezbędne w szczególności:
a) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa, któremu podlega ADO, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej ADO;
b) do ustalenia, dochodzenia lub obrony roszczeń.

Prawo do ograniczenia przetwarzania

§40

1. Osoba, której dane dotyczą, ma prawo żądania od ADO ograniczenia przetwarzania w szczególności, w następujących przypadkach:
a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający ADO sprawdzić prawidłowość tych danych,
b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
c) ADO nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń
d) osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie ADO są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

2. Jeżeli na mocy ust. 1 przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.

3. Przed uchyleniem ograniczenia przetwarzania ADO informuje o tym osobę, której dane dotyczą, która żądała ograniczenia na mocy ust. 1.

Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania

§41

Administrator Danych Osobowych informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał zgodnie z powyższymi zasadami, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

Prawo do przenoszenia danych

§42

Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła ADO, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony Administratora, któremu dostarczono te dane osobowe, jeżeli:

a) przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy oraz

b) przetwarzanie odbywa się w sposób zautomatyzowany.

Prawo do sprzeciwu wobec przetwarzania danych osobowych

§43

1. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych. ADO nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.
2. Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim. W takim przypadku, danych tych nie wolno już dalej przetwarzać do takich celów.

Terminy odpowiedzi

§44

1. W przypadku wpłynięcia wniosku od osoby, której dane są przetwarzane, odnośnie dostępu do danych, realizacji prawa do sprostowania i usunięcia danych, prawa do ograniczenia przetwarzania, prawa do przenoszenia danych lub prawa do złożenia sprzeciwu na przetwarzanie danych, ADO udziela odpowiedzi w terminie miesiąca od otrzymania tego żądania.
2. ADO może wydłużyć czas odpowiedzi o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania ADO informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia.
3. Jeżeli ADO nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

ROZDZIAŁ VIII – POSTANOWIENIA KOŃCOWE

§45

1. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia, nie wywiązała się z obowiązków określonych niniejszą Polityką, nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, ADO może wszcząć postępowanie dyscyplinarne i/lub dochodzić odpowiedzialności na ścieżce cywilnej bądź karnej.
2. ADO prowadzi ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych.
3. Wszelkie załączniki do Polityki Bezpieczeństwa Informacji i Instrukcji Zarządzania Systemem Informatycznym stanowią jej integralną część.

§46

W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustaw szczególnych, RODO oraz umowy zawarte z podmiotami przetwarzającymi dane.