POLITYKA BEZPIECZEŃSTWA

PRZETWARZANIA DANYCH OSOBOWYCH

W PODHALAŃSKIWEJ LOKALNEJ GRUPIE DZIAŁANIA

Podstawa prawna opracowania:

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, zwane w skrócie rozporządzeniem RODO

Zatwierdzono, Biały Dunajec, dnia 04.10.2018 r.

DEFINICJE

Określenia i skróty użyte w niniejszej Polityce Bezpieczeństwa i w art. 4 RODO:

1. **Administrator** – tu Podhalańska Lokalna Grupa Działania oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;
2. **Baza danych osobowych** - zbiór uporządkowanych powiązanych ze sobą tematycznie zapisanych danych. Baza danych jest złożona z elementów o określonej strukturze-rekordów lub obiektów, w których są zapisane dane osobowe.
3. **Dane dotyczące zdrowia** - oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;
4. **Dane genetyczne** - oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;
5. **Dane osobowe (dane)** - oznaczają 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;
6. **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.
7. **Nośnik komputerowy (wymienny)** – nośnik służący do zapisu i przechowywania informacji np. CD, dyskietki, dyski twarde;
8. **Odbiorca** - 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;
9. **Ograniczenie przetwarzania** - oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
10. **Organ nadzorczy** - oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51.
11. **Organ nadzorczy, którego sprawa dotyczy** - oznacza organ nadzorczy, którego dotyczy przetwarzanie danych osobowych, ponieważ:
    a) administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną na terytorium państwa członkowskiego tego organu nadzorczego;

b) przetwarzanie znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, mające miejsce zamieszkania w państwie członkowskim tego organu nadzorczego; lub

c) wniesiono do niego skargę;.

12. **Polityka** – rozumie się przez to Politykę bezpieczeństwa ochrony danych osobowych.
13. **Prawnie uzasadniony interes administratora danych osobowych** – na podstawie art. 23 ust. 1 ustawy o ochronie danych osobowych istnieje możliwość przetwarzania danych osobowych, gdy „jest to niezbędne do wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą". Ustawa wskazuje także w art. 23 ust. 4, że może być to: marketing bezpośredni własnych produktów lub usług administratora danych, dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej.
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. **Przedsiębiorca** - oznacza osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą.
16. **Przetwarzanie** - oznacza 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;
17. **Pseudonimizacja** – oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Grupa Robocza – będąca niezależnym, europejskim organem doradczym w sprawie ochrony danych osobowych wystosowała opinie, które wymienia metody pseudonimizacji, z których korzysta się najczęściej. Wśród nich jest między innymi: szyfrowanie kluczem tajnym, tokenizacja i skracanie wybranych wartości, tak aby odczytanie ich faktycznego znaczenia stało się niemożliwe.
18. **Rozporządzenie** – rozumie się przez to 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
19. **System informatyczny (system)** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
20. **Ustawa** – rozumie się przez to Ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 poz. 1182 i 1662)
21. **Usuwanie danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację , która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
22. **Użytkownik** - pracownik posiadający uprawnienia do pracy w systemie informatycznym zgodnie ze swoim zakresem obowiązków.

23. **Wrażliwe dane osobowe** – szczególna kategoria danych osobowych. Należą do nich informacje dotyczące: pochodzenia rasowego lub etnicznego, poglądów politycznych, przekonań religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, stanu zdrowia, kody genetycznego, nałogów, życia seksualnego, skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.
24. **Zabezpieczenie systemu informatycznego** – należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą.
25. **Zbiór danych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie
26. **Zgoda osoby, której dane dotyczą** - oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

ARTYKUŁ I. INTENCJE, CELE, ZAKRES I WYJAŚNIENIE POLITYKI BEZPIECZEŃSTWA

1.

Realizując postanowienia 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 wprowadza się zestaw reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej pozwalający na zapewnienie odpowiedniej ochrony danych osobowych

2.

Celem Polityki Bezpieczeństwa jest zapewnienie ochrony danych osobowych przed wszelakiego rodzaju zagrożeniami, tak wewnętrznymi, jak i zewnętrznymi, świadomymi lub nieświadomymi.

3.

Jako integralną część niniejszej polityki opracowano i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwaną dalej **„Instrukcją zarządzania systemami informatycznymi".** Określa ona sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem zapewnienia ich bezpieczeństwa.

4.

Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez samych użytkowników.

Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

1. **Poufność i integralność danych** rozumianą jako właściwość zapewniającą, że dane będą przetwarzane w sposób zapewniający ich odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, a także zapewniające, że dane te nie będą ujawnione osobom nieuprawnionym,
2. **Rozliczalność danych** rozumianą jako takie postępowanie, aby możliwe było wykazanie przestrzegania przepisów RODO
3. **Dostępność danych** – tj. iż dane są dostępne na żądanie upoważnionego podmiotu lub Upoważnionej osoby,
4. **Integralność systemu** rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

ARTYKUŁ II. OSOBY ODPOWIEDZIALNE ZA BEZPIECZEŃSTWO DANYCH OSOBOWYCH I ICH OBOWIĄZKI

1

1. Osobami odpowiedzialnymi za bieżącą realizację Polityki Bezpieczeństwa i zarządzanie bezpieczeństwem danych osobowych u Administratora są:

   A/ ABI i ASI – o ile zostali wyznaczeni przez Administratora

   B/ Użytkownicy.

2. Osoby będące Użytkownikami wyznaczane są przez Administratora. Administrator może scedować to uprawnienie na ABI lub inną osobę.
3. Administrator może upoważnić inne osoby (Pracowników) do wykonywania określonych czynności znajdujących się w zakresie zadań Administratora.
4. Do przetwarzania danych osobowych mogą zostać dopuszczone wyłącznie osoby **upoważnione przez administratora na piśmie i deklarujące zapoznanie się z zasadami niniejszej Polityki Bezpieczeństwa oraz Instrukcji przetwarzania danych w systemach informatycznych**, ich zrozumienie i stosowanie jak również osoby upoważnione na podstawie odrębnych umów – podmioty zewnętrzne. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien zapoznać się z obowiązującymi u Administratora zasadami w zakresie przetwarzania danych osobowych zgodnie z upoważnieniem.
5. Każdy Pracownik jest zobowiązany do niezwłocznego raportowania Administratorowi dostrzeżonych zagrożeń lub naruszeń bezpieczeństwa danych osobowych i stosowania się do przepisów dotyczących ochrony danych osobowych jak również do Polityki Bezpieczeństwa i innych podanych mu do wiadomości regulacji wewnętrznych dotyczących bezpieczeństwa informacji.

2

Użytkownicy zobowiązani są do:

a) dołożenia szczególnej staranności przy przetwarzaniu danych osobowych oraz stosowania się do wszystkich zasad przetwarzania danych osobowych określonych zgodnie z RODO, Polityką Bezpieczeństwa i innymi standardami w zakresie zapewnienia bezpieczeństwa danych osobowych przekazanych przez Administratora, tak aby w pełni zachować poufność, integralność oraz rozliczalność danych osobowych,
b) przetwarzania danych osobowych wyłącznie w zakresie otrzymanego Upoważnienia,
c) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczania,
d) zaznajamiania się z obowiązkami w zakresie przetwarzania danych osobowych zgodnie z RODO, Polityką Bezpieczeństwa i innymi standardami w zakresie zapewnienia bezpieczeństwa danych osobowych przekazanymi przez Administratora przed podjęciem czynności z zakresu przetwarzania danych osobowych oraz bieżącej aktualizacji swojej wiedzy w tym zakresie,

3

Naruszanie przez osoby odpowiedzialne za bezpieczeństwo danych osobowych zasad przetwarzania danych osobowych lub zapewnienia ich bezpieczeństwa traktowane jest przez

Administratora jako ciężkie naruszenie podstawowych obowiązków pracowniczych przez taką osobę z wszystkimi wynikającymi stąd konsekwencjami, z rozwiązaniem stosunku pracy włącznie.

4.

OBOWIĄZKIEM ADMINISTRATORA JEST ZAPEWNIENIE BEZPIECZNEGO PRZETWARZANIA DANYCH OSOBOWYCH TAKŻE PRZEZ PODMIOTY ZEWNĘTRZNE, GDY CEL I ZAKRES TEGO PRZETWARZANIA OKREŚLA ADMINISTRATOR.

1. Administrator udostępnia dane osobowe będące w jego obszarze fizycznym podmiotom zewnętrznym w oparciu o **umowę poufności.**
    a. Podmiot zewnętrzny zobowiązany jest do zachowania poufności udostępnionych danych i przetwarzania ich zgodnie z celem umowy.
2. Administrator powierza dane osobowe do przetwarzania w formie usługi zewnętrznej podmiotom zewnętrznym w oparciu o **umowę powierzenia przetwarzania danych**.
    a. Podmiot zewnętrzny zobowiązany jest do przetwarzania danych zgodnie z zakresem i celem określonym w umowie powierzenia przetwarzania danych osobowych

ARTYKUŁ III. WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ – OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator prowadzi **Rejestr czynności przetwarzania** zgodnie z art. 30 rozporządzenia RODO
2. Administrator określił w odrębnym dokumencie **Zakres i kategorie przetwarzanych danych osobowych poszczególnych zbiorów.**
3. Administrator prowadzi **rejestr budynków, pomieszczeń lub części pomieszczeń stanowiących obszar przetwarzania poszczególnych zbiorów danych osobowych**.
4. Zabrania się tworzenia zbiorów danych osobowych, a także gromadzenia danych osobowych w zbiorach lub poza zbiorami, zwłaszcza w Systemie, w zakresie niezwiązanym z prowadzoną przez Administratora działalnością lub w zakresie, jaki wykracza poza dozwolony zakres.
5. Organizacyjne środki ochrony obszaru przetwarzania danych osobowych obejmują w szczególności:

a) lokalizację obszaru przetwarzania danych osobowych w pomieszczeniach o ograniczonym i kontrolowanym dostępie;
b) dopuszczenie do pomieszczeń stanowiących obszar przetwarzania danych osobowych wyłącznie osoby upoważnione,
c) dopuszczenie do pomieszczeń stanowiących obszar przetwarzania danych osobowych osób postronnych lub Pracowników Administratora nie będących Użytkownikami wyłącznie w obecności i pod kontrolą Użytkowników;
d) dopuszczenie do przetwarzania danych osobowych wyłącznie osób posiadających upoważnienie wydane przez Administratora;
e) prowadzenie ewidencji udzielonych upoważnień do przetwarzania danych osobowych;
f) zapoznanie Użytkowników z zasadami przetwarzania danych osobowych oraz ochroną danych osobowych, w tym zabezpieczeń Systemu;
g) zapoznanie Pracowników z zasadami ochrony przetwarzania danych osobowych;

a) odebranie stosownych zobowiązań od użytkowników i podmiotów zewnętrznych, tj.: zobowiązania do zachowania w tajemnicy danych i sposobów ich zabezpieczenia oraz

oświadczenia o zapoznaniu z treścią przepisów określających zasady postępowania przy przetwarzaniu danych osobowych, a także z dokumentacją opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ich ochronę w tym ograniczenia wobec pracowników i członków organu decyzyjnego wskazane w procedurach oceny i wyboru operacji.

6. Techniczne środki ochrony obejmują w szczególności:

a) zabezpieczenie pomieszczeń, w których przetwarzane są zbiory danych osobowych przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.
b) nałożenie na członków organu decyzyjnego którym udostępniane będą internetowo wnioski beneficjentów celem ich oceny, obowiązku dbania o dostęp do własnego konta aby niedopuścić do udostępnienia danych osobom nieupoważnionym.
c) wprowadzenie zakazu wykorzystywania sprzętu, oprogramowania i zasobów sieci Administratora do zadań, które nie są związane z działalnością Administratora,
d) regularne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych;
e) zastosowanie ochrony zasilania (urządzenia UPS, bezpieczniki przepięciowe itp.).
f) przechowywanie kopii zapasowych/archiwalnych zbioru danych osobowych w zamkniętej szafie ognioodpornej bądź w odrębnym zamykanym na klucz pomieszczeniu do którego nie mają wstępu osoby nieupoważnione.
g) wprowadzeniu zasady niezwłocznego usuwania danych osobowych po ustaniu ich użyteczności;
h) Podczas obsługi Klienta monitory powinny być ustawione tak, aby uniemożliwić podgląd osobom postronnym, a dokumenty zawierające dany osobowe osoby innej, niż interesant nie mogą znajdować się w zasięgu wzroku interesanta
i) Pomieszczenia w których przechowywane są nośniki zawierające dane osobowe (np. akta podręczne, akta osobowe, umowy z osobami fizycznymi, systemy informatyczne, serwerownie) nie są dostępne dla interesantów i osób postronnych. W pomieszczeniach w których przechowywane są nośniki zawierające dane osobowe obowiązuje zakaz używania urządzeń rejestrujących obraz lub dźwięk, c. Pomieszczenia w których przechowywane są nośniki zawierające dane osobowe są poza godzinami pracy zamykane na klucz. d. Pomieszczenia w których przechowywane są nośniki zawierające dane osobowe nie mogą pozostawać otwarte bez dozoru,
j) Inne Czynności określone w instrukcji zarządzania systemami informatycznymi zapewniające bezpieczeństwo przetwarzanych danych w formie elektronicznej.

ARTYKUŁ IV. ZABEZPIECZENIE DOKUMENTÓW I WYDRUKÓW

1. Za bezpieczeństwo dokumentów i wydruków odpowiedzialne są osoby je przetwarzające oraz kierownicy właściwych jednostek lub komórek organizacyjnych, a w szczególności odpowiadają za:
    a. Zamykanie dokumentów na klucz w szafach, biurkach, sejfach podczas nieobecności w pomieszczeniach lub po zakończeniu pracy **(tzw. Polityka czystego biurka).**
    b. Niszczenie dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania.
    c. Nie pozostawianie wydruków i ksero na urządzeniach lub w ich okolicy bez nadzoru.

ARTYKUŁ V. ZABEZPIECZENIE DANYCH PRZETWARZANYCH DROGĄ ELEKTRONICZNĄ W SYSTEMACH INFORMATYCZNYCH, TELEKOMUNIKACYJNYCH, NA NOŚNIKACH DANYCH

1. Zasady w zakresie zapewnienia bezpieczeństwa przetwarzania danych drogą elektroniczną określa załącznik nr 5 do regulaminu biura tj. **Instrukcja Zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Podhalańskiej LGD**

ARTYKUŁ VI. INSTRUKCJA POSTEPOWANIA W SYTUACJI NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. Celem instrukcji jest określenie sposobu postępowania gdy:
   a) Stwierdzono naruszenie zabezpieczeń danych osobowych.
   b) W przypadku danych przetwarzanych w formie tradycyjnej stan pomieszczeń, szaf, okien, drzwi, dokumentów lub inne zaobserwowane symptomy mogą wskazywać na naruszenie bezpieczeństwa danych osobowych.
   c) W przypadku danych przetwarzanych w formie elektronicznej stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu, jakość komunikacji lub inne zaobserwowane symptomy mogą wskazywać na naruszenie bezpieczeństwa danych osobowych.
2. Instrukcja określa zasady postępowania wszystkich osób zatrudnionych przy przetwarzaniu danych osobowych w przypadku naruszenia bezpieczeństwa tych danych, zgodne z „Tabelą form naruszeń bezpieczeństwa danych osobowych".

3. Naruszeniem zabezpieczenia danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia lub usunięcia, a w szczególności:
   a) nieautoryzowany dostęp do danych,
   b) nieautoryzowane modyfikacje lub zniszczenie danych,
   c) udostępnienie danych nieautoryzowanym podmiotom,
   d) nielegalne ujawnienie danych,
   e) pozyskiwanie danych z nielegalnych źródeł.
4. W przypadku stwierdzenia naruszenia zabezpieczeń lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych w jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie zgłosić ten fakt bezpośredniemu przełożonemu a następnie postępować stosownie do podjętej przez niego decyzji.
5. Zgłoszenie naruszenia zabezpieczeń danych osobowych powinno zawierać:
   a) opisanie symptomów naruszenia zabezpieczeń danych osobowych,
   b) określenie sytuacji i czasu w jakim stwierdzono naruszenie zabezpieczeń danych osobowych,
   c) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia,
   d) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.
6. Administrator danych lub inna upoważniona przez niego osoba podejmuje wszelkie działania mające na celu:
   a) minimalizację negatywnych skutków zdarzenia,
   b) wyjaśnienie okoliczności zdarzenia,
   c) zabezpieczenie dowodów zdarzenia,
   d) umożliwienie dalszego bezpiecznego przetwarzania danych.

7. W celu realizacji zadań wynikających z niniejszej instrukcji Administrator danych lub inna upoważniona przez niego osoba ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, a w szczególności:
   a) żądania wyjaśnień od pracowników,
   b) korzystania z pomocy konsultantów,
   c) nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.
8. Polecenia Inspektora ochrony danych lub innej upoważnionej przez niego osoby wydawane w celu realizacji zadań wynikających z niniejszej instrukcji są priorytetowe i winny być wykonywane przed innymi poleceniami, zapewniając ochronę danych osobowych.
9. Odmowa udzielenia wyjaśnień lub współpracy z Inspektorem ochrony danych lub inną upoważnioną przez niego osobą traktowana będzie jako naruszenie obowiązków pracowniczych.
10. Inspektor ochrony danych po zażegnaniu sytuacji naruszającej bezpieczeństwo danych osobowych opracowuje raport końcowy, w którym przedstawia przyczyny i skutki zdarzenia oraz wnioski, w tym kadrowe, ograniczające możliwość wystąpienia zdarzenia w przyszłości.
11. Nieprzestrzeganie zasad postępowania określonych w niniejszej instrukcji stanowi naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej określonej w Kodeksie Pracy.
12. W związku z RODO opracowano nowe procedury reagowania na incydenty:

    a) **Procedura postępowania w przypadku naruszenia ochrony danych osobowych**
    b) **Rejestr działań zapobiegawczych i korygujących wraz z planem i harmonogramem kontroli mechanizmów ochrony danych osobowych i bezpieczeństwa informacji prawem chronionych**
    c) **Rejestr naruszeń ochrony danych osobowych**
    d) **Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu**

ARTYKUŁ VII. KONTROLA SYSTEMU OCHRONY DANYCH OSOBOWYCH

1.

a) Celem procedury jest uporządkowanie i przedstawienie czynności związanych z: kontrolą stanu bezpieczeństwa danych osobowych.
b) Procedura obejmuje wszystkie procesy organizacji, gdzie przestrzeganie zasad ochrony danych osobowych jest wymagane.
c) Do kontroli stanu ochrony danych osobowych upoważniony jest ABI, wyznaczeni kontrolerzy wewnętrzni lub ADO.
d) Kontroli podlegają: systemy informatyczne przetwarzające dane osobowe, zabezpieczenia fizyczne, zabezpieczenia organizacyjne, bezpieczeństwo osobowe oraz zgodność stanu faktycznego z wymaganiami ustawy i aktów wykonawczych.
e) Inspektor ochrony danych przygotowuje plan kontroli uwzględniając zakres oraz potrzebne zasoby fizyczne, czasowe i osobowe. Kontrola powinna odbyć się co najmniej raz w roku.
f) Kontrola przeprowadzana jest na podstawie **listy kontrolnej.**
g) Po dokonanej kontroli osoba ją przeprowadzająca przygotowuje i przekazuje **raport pokontrolny** kierownikowi kontrolowanej jednostki lub komórki organizacyjnej oraz Administratorowi Danych Osobowych. Na jego podstawie IOD inicjuje działania korygujące lub zapobiegawcze.

ARTYKUŁ VIII. UDOSTĘPNIANIE DANYCH

1.

a) Dane osobowe mogą być udostępniane wyłącznie podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa oraz osobom, których dotyczą.
b) Udostępnianie danych osobowych może nastąpić wyłącznie za zgodą Administratora Danych Osobowych.
c) Informacje zawierające dane osobowe powinny być przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru listem poleconym za pokwitowaniem odbioru lub innym bezpiecznym sposobem, określonym wymogiem prawnym lub umową.
d) Udostępniając dane osobowe, należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

ARTYKUŁ IX. OBOWIĄZEK INFORMACYJNY

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, w wypadkach przewidzianych Ustawą należy poinformować tę osobę o:

1) Pełnej nazwie firmy i adresie siedziby;
2) Celu zbierania danych, a w szczególności o znanych w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych;
3) Prawie dostępu do swoich danych oraz ich poprawiania;
4) Dobrowolności lub obowiązku podania danych - jeżeli taki obowiązek istnieje, o jego podstawie prawnej;

ARTYKUŁ X. KLAUZULE ZGODY

1. Art. 7 pkt 5 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (UODO) dotyczący oświadczenia woli, został zastąpiony przez:

- **art. 4 pkt 11 RODO**, który definiuje:
  dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych
- **art. 7 ust. 1 RODO**, który definiuje:
  Jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.
- **art. 7 ust. 2 RODO**, który definiuje:
  Jeżeli osoba, której dane dotyczą, wyrażą zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie niniejszego rozporządzenia nie jest wiążąca.
- **art. 7 ust. 3 RODO**, który definiuje:
  Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. 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. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.
- **art. 7 ust. 4 RODO**, który definiuje:

Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.

- **motyw 32 preambuły, który definiuje:**
  Zgoda powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwolenie osoby, których dane dotyczą, na przetwarzanie dotyczących jej danych osobowych i która ma na przykład formę pisemnego (w tym elektronicznego) lub ustnego oświadczenia. Może to polegać na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej, na wyborze ustawień technicznych do korzystania z usług społeczeństwa informacyjnego lub też na innym oświadczeniu bądź zachowaniu, które w danym kontekście jasno wskazuje, że osoba, której dane dotyczą, zaakceptowała proponowane przetwarzanie jej danych osobowych. Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie powinny zatem oznaczać zgody. Zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele. Jeżeli osoba, której dane dotyczą, ma wyrazić zgodę w odpowiedzi na elektroniczne zapytanie, zapytanie takie musi być jasne, zwięzłe i nie zakłócać niepotrzebnie korzystania z usługi, której dotyczy.
- **motyw 42 preambuły, który definiuje:**
  Aby wyrażenie zgody było świadome, osoba, której dane dotyczą, powinna znać przynajmniej tożsamość administratora oraz zamierzone cele przetwarzania danych osobowych. Wyrażenia zgody nie należy uznawać za dobrowolne, jeżeli osoba, której dane dotyczą, nie ma rzeczywistego lub wolnego wyboru oraz nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji. W szczególności w przypadku pisemnego oświadczenia składanego w innej sprawie powinny istnieć gwarancje, że osoba, której dane dotyczą, jest świadoma wyrażenia zgody oraz jej zakresu.
- **motyw 43 preambuły, który definiuje:**
  Aby zapewnić dobrowolność, zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w szczególnej sytuacji, w której istnieje wyraźny brak równowagi między osobą, której dane dotyczą, a administratorem, w szczególności gdy administrator jest organem publicznym i dlatego jest mało prawdopodobne, by w tej konkretnej sytuacji zgodę wyrażono dobrowolnie we wszystkich przypadkach. Zgody nie uważa się za dobrowolną, jeżeli nie można jej wyrazić z osobna na różne operacje przetwarzania danych osobowych, mimo że w danym przypadku byłoby to stosowne, lub jeżeli od zgody uzależnione jest wykonanie umowy – w tym świadczenie usługi – mimo że do jej wykonania zgoda nie jest niezbędna.

ARTYKUŁ XI. POSTANOWIENIA KOŃCOWE

1. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.
2. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.
3. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia 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, można wszcząć postępowanie dyscyplinarne.

4. Kara dyscyplinarna, orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby zgodnie z Rozporządzeniem 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. oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
5. W sprawach nieuregulowanych w niniejszej Polityce bezpieczeństwa mają zastosowanie przepisy 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.
6. Niniejsza Polityka Bezpieczeństwa została zatwierdzona przez Administratora i podana do wiadomości u Administratora osobom odpowiedzialnym za realizację zadań związanych z ochroną danych osobowych w dniu 04.10.2018 r. i została wdrożona z dniem 04.10.2018 r.
7. Niniejsza Polityka Bezpieczeństwa zastępuje wszelkie poprzednio obowiązujące u Administratora regulacje dotyczące ochrony danych osobowych.
8. Polityka Bezpieczeństwa winna być na bieżąco weryfikowana i dostosowywana do aktualnego stanu faktycznego i prawnego związanego z ochroną przetwarzania danych osobowych u Administratora.