Polityka Ochrony Danych Osobowych

SMART DREAM PATRYK SIARNOWSKI, ul. 3 Brygady Szczerbca 7B/9

80-041 Gdańsk, Pomorskie, NIP 583-31-24-579

Spis treści

Wstęp

Niniejsza Polityka Ochrony Danych Osobowych jest niezależną Polityką stanowiącą o zasadach przetwarzania danych osobowych w przedsiębiorstwie
SMART DREAM PATRYK SIARNOWSKI, ul. 3 Brygady Szczerbca 7B/9 80-041 Gdańsk, Pomorskie, NIP 583-31-24-579

Przedstawiony dokument stanowi akt wewnętrzny o najwyższej mocy obowiązującej w zakresie ochrony danych osobowych, a wszelkie dokumenty Spółki powinny być zgodne z niniejszą Polityką.

W przypadku jakichkolwiek wątpliwości interpretacyjnych należy je rozpatrywać łącznie z aktami wewnętrznymi o tej samej mocy obowiązującej.

Definicje

Określenie definicji	Definicja
Administrator danych osobowych **ADO**	SMART DREAM PATRYK SIARNOWSKI, ul. 3 Brygady Szczerbca 7B/9 80-041 Gdańsk, Pomorskie, NIP 583-31-24-579
Anonimizacja	Oznacza pozbawienie informacji cech Danych osobowych w taki sposób, że osoby, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować.
Dane osobowe	Informacje o zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. 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.
Dane sensytywne (tzw. wrażliwe)	Dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne, przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby fizycznej.
Dane dotyczące wyroków skazujących lub naruszeń prawa	Dane osobowe, dotyczące wyroków skazujących lub naruszeń prawa lub powiązanych środków bezpieczeństwa, o których mowa w art. 10 RODO.
Dostępność informacji	Zapewnienie dostępu do danych osobowych i związanych z nimi zasobów dla osób upoważnionych, gdy wystąpi określona potrzeba dostępu.
Organ nadzoru	Prezes Urzędu Ochrony Danych Osobowych.

Ograniczenie przetwarzania	Oznaczenie przechowywanych Danych osobowych w celu ograniczenia ich przyszłego przetwarzania.
Identyfikator użytkownika	Indywidualne, unikalne, oznaczenie Użytkownika systemu w systemach informatycznych Spółki, identyfikujące osobę upoważnioną do przetwarzania Danych osobowych w danym Systemie Informatycznym.
Inspektor Ochrony Danych	Podmiot, który może być wyznaczony przez Administratora danych osobowych w celu monitoringu zgodności działalności ADO z przepisami w zakresie ochrony danych osobowych, w tym w szczególności RODO oraz Ustawą.
Instrukcja	Instrukcja zarządzania systemem informatycznym służącym do przetwarzania Danych osobowych.
Integralność informacji	Oznacza, że informacja jest prawidłowa i kompletna, spójna i wiarygodna oraz metody przetwarzania informacji zapewniają zachowanie takiego stanu.
Odbiorca danych	Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się Dane osobowe, niezależnie od tego, czy jest stroną trzecią, z wyłączeniem organów publicznych, które mogą otrzymywać Dane osobowe w ramach konkretnego postępowania zgodnie z przepisami prawa.
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
PODO	Polityka Ochrony Danych Osobowych SMART DREAM PATRYK SIARNOWSKI, ul. 3 Brygady Szczerbca 7B/9 80-041 Gdańsk, Pomorskie, NIP 583-31-24-579

Podmiot przetwarzający lub Procesor	Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza Dane osobowe w imieniu ADO.
Poufność informacji	Oznacza, że jest ona dostępna wyłącznie osobom, które zostały upoważnione do korzystania z tych informacji.
Prawa osób, których dane dotyczą	Prawa osób, których dane dotyczą, do realizacji których zobowiązany jest Administrator, a w szczególności: - prawo dostępu do informacji, - prawo do sprostowania Danych osobowych, - prawo do usunięcia Danych osobowych *(prawo do bycia zapomnianym),* - prawo do ograniczenia przetwarzania, - prawo do przenoszenia danych, - prawo do sprzeciwu, - prawo do niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu.
Profilowanie	Dowolna forma 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.
Przetwarzanie Danych osobowych	Jakiekolwiek operacje lub zestaw operacji wykonywanych na Danych osobowych lub na zestawach Danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie 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.

Pseudonimizacja	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.
RODO lub Rozporządzenie	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem Danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)(Dz. Urz. UE L 119/1).
Strona trzecia	Osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, Administrator, Podmiot przetwarzający czy osoby, które - z upoważnienia Administratora lub Podmiotu przetwarzającego - mogą przetwarzać Dane osobowe.
System Informatyczny	Zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych.
Ustawa lub UODO	Krajowa ustawa o ochronie Danych osobowych.
Użytkownik	Osoba upoważniona do przetwarzania Danych osobowych, których SMART DREAM PATRYK SIARNOWSKI, ul. 3 Brygady Szczerbca 7B/9 80-041 Gdańsk, Pomorskie, NIP 583-31-24-579 jest Administratorem, tj. pracownicy ADO zatrudnieni w niej w ramach stosunku pracy oraz wszystkie inne osoby wykonujące na rzecz ADO czynności na podstawie umów cywilnoprawnych.

Współadministrator	Oznacza administratora danych, który wraz z ADO, jako administratorem Danych osobowych, wspólnie ustala cele i sposoby przetwarzania Danych osobowych.
Zabezpieczenie danych w Systemie Informatycznym	Wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę Danych osobowych przed ich nieuprawnionym przetwarzaniem.
Zbiór danych osobowych	Uporządkowany zestaw Danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany, czy rozproszony funkcjonalnie lub geograficznie.
Zgoda	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.

1. Cel i postanowienia ogólne

1.1 Celem PODO jest wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł przetwarzania Danych osobowych, które należy stosować, aby właściwie wykonać obowiązki jako administratora, współadministratora lub podmiotu przetwarzającego Dane osobowe, zgodnie z przepisami o ich ochronie.

1.2 Przetwarzanie Danych osobowych w ADO odbywa się w formie papierowej oraz elektronicznej przy pomocy Systemów Informatycznych.

1.3 W celu zwiększenia efektywności ochrony Danych osobowych dokonano połączenia różnych form zabezpieczeń, w sposób umożliwiający stworzenie kilku warstw ochrony. Ochrona Danych osobowych realizowana jest poprzez środki techniczne i organizacyjne, obejmujące co najmniej:

a) zabezpieczenia fizyczne,
b) szyfrowanie i pseudonimizację,
c) oprogramowanie systemowe,
d) aplikacje,
e) zarządzanie dostępem Użytkowników,
f) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

1.4 Szczegółowy opis środków technicznych i organizacyjnych, niezbędnych do zapewnienia bezpieczeństwa Danych osobowych wraz ze wskazaniem zasad ich stosowania znajduje się w *Załączniku nr 3* do niniejszej Polityki.

1.5 Zastosowane zabezpieczenia, o których mowa w punkcie 1.3 niniejszej Polityki, mają na celu zapewnienie:

a) poufności, integralności, dostępności i odporności Systemów Informatycznych i usług przetwarzania Danych osobowych, oraz
b) zdolności do szybkiego przywrócenia dostępności Danych osobowych w razie incydentu naruszającego ochronę danych osobowych.

1.6 Stosowane przez ADO zabezpieczenia uwzględniają ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do Danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez Spółkę.

1.7 Wszelkie dokumenty dotyczące przetwarzania Danych osobowych u ADO winny być zgodne z niniejszą Polityką.

1.8 PODO została opracowana zgodnie z wymogami określonymi w unijnych jak i krajowych przepisach o ochronie danych osobowych.

2. Zasady dotyczące przetwarzania Danych osobowych

Do podstawowych zasad przetwarzania danych osobowych zaliczamy:

a) zasada zgodności z prawem, rzetelności i przejrzystości;
b) zasada ograniczenia celu;
c) zasada minimalizacji danych;
d) zasada prawidłowości;
e) zasada ograniczenia przechowywania;
f) zasada integralności i poufności;
g) zasada rozliczalności.

2.1. Zasada zgodności z prawem, rzetelności i przejrzystości:

2.1.1. Dane osobowe są przetwarzane przez ADO zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.

2.1.2. Podstawę prawną przetwarzania Danych osobowych przez ADO, zgodnie z art. 6 ust. 1 RODO, stanowią:

a) zgoda osoby, której dane dotyczą;
b) wykonanie umowy zawartej z osobą, której dane dotyczą lub podjęcie działań na żądanie osoby, której dane dotyczą przed zawarciem umowy;
c) obowiązek prawny;
d) ochrona żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej, której dane są przetwarzane przez ADO;
e) interes publiczny lub sprawowanie władzy publicznej powierzonej administratorowi;
f) prawnie uzasadniony interes ADO jako administratora Danych osobowych

2.1.3. Przetwarzanie Danych sensytywnych (wrażliwych) przez ADO odbywać się może jedynie w przypadkach wyraźnie wskazanych w art. 9 RODO, w tym po spełnieniu jednego z warunków tj.:

a) zgoda osoby, której dane dotyczą;
b) ustalenie, dochodzenie i obrona roszczeń;
c) obowiązek prawny;
d) ważny interes publiczny;
e) upublicznienie przez osobę, której dane dotyczą;
f) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy;
g) do celów archiwalnych w interesie publicznym lub do celów statystycznych.

2.1.4. Przetwarzania Danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa ADO dokonuje zgodnie z wymogami art. 10 RODO.

2.1.5. Przetwarzanie Danych osobowych na podstawie prawnie uzasadnionego interesu administratora Danych osobowych, o którym mowa w punkcie 2.1.2 lit. f) niniejszej Polityki, jest realizowane przez ADO jedynie w przypadku, gdy spełnione są kumulatywnie następujące przesłanki:

a) istnieje prawnie uzasadniony interes, który jest realizowany przez ADO lub stronę trzecią,

b) przetwarzanie Danych osobowych jest niezbędne dla realizacji celu wynikającego z uzasadnionego interesu ADO lub strony trzeciej,

c) nie występują w danej sytuacji interesy lub podstawowe prawa i wolności podmiotu danych, które mają charakter nadrzędny wobec prawnie uzasadnionych interesów ADO lub strony trzeciej.

2.2. Zasada ograniczenia celu

2.2.1. Dane osobowe są zbierane przez ADO wyłącznie w konkretnych, wyraźnych i prawnie uzasadnionych celach oraz nie są przetwarzane w sposób niezgodny z tymi celami.

2.3. Zasada minimalizacji danych

2.3.1. Zbierane przez ADO Dane osobowe są adekwatne, stosowne oraz ograniczone do tego co niezbędne do celów, w których są przetwarzane. ADO wdraża odpowiednie procesy, procedury oraz postępowania kontrolne, mające na celu zapewnienie, że przetwarzanie danych osobowych spełnia niniejszą zasadę.

2.4. Zasada prawidłowości

2.4.1. ADO dokłada należytej staranności by przetwarzane Dane osobowe były prawidłowe, a w razie potrzeby niezwłocznie uaktualniane, w tym podejmuje wszelkie rozsądne działania, aby Dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania zostały niezwłocznie usunięte, zanonimizowane lub sprostowane.

2.5. Zasada ograniczenia przechowywania

2.5.1. Dane osobowe są przechowywane przez ADO w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.

2.6. Zasada integralności i poufności

2.6.1. Przetwarzanie Danych osobowych przez ADO odbywa się w sposób zapewniający odpowiednie bezpieczeństwo Danych osobowych, w tym w szczególności poprzez ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

2.7. Zasada rozliczalności

2.7.1. ADO jest odpowiedzialna za przestrzeganie wymogów RODO oraz krajowych przepisów o ochronie danych osobowych.

2.7.2. ADO może prowadzić rejestr czynności przetwarzania Danych osobowych, zaś jako podmiot przetwarzający, prowadzi rejestr kategorii czynności przetwarzania Danych osobowych.

3. Zakres stosowania

3.1. Zasady ochrony Danych osobowych, określone przez PODO, mają zastosowanie do Systemów Informatycznych, w których przetwarzane są Dane osobowe oraz do przetwarzania Danych osobowych w formie papierowej. PODO stosuje się w szczególności do:

- wszystkich istniejących, wdrażanych obecnie lub w przyszłości Systemów Informatycznych, w których przetwarzane są Dane osobowe,
- wszystkich istniejących, wdrażanych obecnie lub w przyszłości operacji przetwarzania Danych osobowych w formie papierowej,
- wszystkich lokalizacji - budynków i pomieszczeń, w których są lub będą przetwarzane Dane osobowe, definiowane w odrębnym Zarządzeniu członka Zarządu lub innej upoważnionej osoby. Lokalizacje podlegają cyklicznemu przeglądowi, nie rzadziej niż raz rocznie,
- wszystkich Użytkowników.

3.2. Do stosowania zasad ochrony Danych osobowych określonych w PODO zobowiązani są wszyscy Użytkownicy.

3.3. Użytkownicy biorący bezpośredni lub pośredni udział w procesie przetwarzania Danych osobowych są odpowiedzialni za przestrzeganie przepisów o ich ochronie ze szczególnym uwzględnieniem postanowień niniejszej Polityki.

4. Odpowiedzialność i struktura zarządzania przetwarzaniem Danych osobowych

4.1. W celu monitorowania wykonania niniejszej Polityki, ADO może powołać Inspektora Ochrony Danych, którego status oraz zadania szczegółowo reguluje art. 39 RODO.

4.1.1. ADO zapewnia, by Inspektor Ochrony Danych nie otrzymywał instrukcji dotyczących wykonywania zadań. Nie może być on odwoływany ani karany przez ADO za wypełnianie swoich zadań.

4.2. W ramach realizacji PODO wyodrębnia się następujące zadania:

4.2.1. Jednostka odpowiedzialna za administrację pomieszczeniami, odpowiedzialna jest za:

- zapewnienie, że do pomieszczeń chronionych mają dostęp wyłącznie osoby

upoważnione,

- określenie budynków, pomieszczeń lub części pomieszczeń tworzących obszar,

  w którym przetwarzane są dane.

4.2.2. Inspektor Ochrony Danych, odpowiedzialny jest za:

- doradztwo w zakresie ochrony Danych osobowych,
- prowadzenie rejestru czynności przetwarzania,
- prowadzenie rejestru kategorii przetwarzania danych,
- koordynowanie procesu odpowiedzi na wnioski podmiotów danych

4.2.3. Jednostka odpowiedzialna za zawieranie umów, odpowiedzialna jest za:

- prowadzenie rejestrów umów zawartych w imieniu ADO, w których ADO powierzyła przetwarzanie danych lub przekazała dane,
- pełnomocnicy ADO są odpowiedzialni za zgłaszanie podpisanych umów do tej jednostki umów w celu ich rejestracji.

4.2.4. Jednostka odpowiedzialna za infrastrukturę informatyczną, (w której przetwarzane są Dane osobowe), odpowiedzialna jest za:

- opracowanie procedur zarządzania infrastrukturą IT, oraz:
  - monitoring oraz zapewnianie ciągłości działania systemów informatycznych,
  - instalację i konfigurację sprzętu informatycznego,
  - konfigurację i administrację oprogramowaniem informatycznym zabezpieczającym,
  - dane chronione przed nieupoważnionym dostępem,
  - tworzenie i zarządzanie kopiami awaryjnymi danych, w tym Danych osobowych,
  - przeciwdziałanie próbom naruszenia bezpieczeństwa informacji.
  - przyznawanie ściśle określonych praw dostępu do Danych osobowych przetwarzanych w systemie,
  - prowadzenie rejestru osób dopuszczonych do systemu
  - dbanie o jakość Danych osobowych gromadzonych w systemie informatycznym,
  - określanie miejsca i czasu przetwarzania, przechowywania, tworzenia i niszczenia informacji.

4.2.6. Jednostka odpowiedzialna za komunikację marketingową, odpowiedzialna jest za zachowanie wymogów ochrony Danych osobowych w podejmowanych działaniach marketingowych.

4.3. Jeżeli w danej jednostce organizacyjnej ADO przetwarzane są Dane osobowe, kierownik tej jednostki jest odpowiedzialny za ochronę, właściwe przetwarzanie Danych osobowych oraz nadzór nad powierzeniem i przekazywaniem danych. Decyduje on, kogo dopuścić do przetwarzania danych oraz jakie czynności będą wykonywać poszczególni pracownicy w ramach przetwarzania Danych osobowych. Jest również odpowiedzialny za dopuszczenie do przetwarzania Danych osobowych wyłącznie osób, którym nadano upoważnienia, zgodnie z postanowieniami rozdziału 7 PODO.

4.4. Dostęp do Danych osobowych w ADO mają prawo mieć Użytkownicy wyłącznie w zakresie obowiązków, uprawnień i odpowiedzialności oraz w granicach nadanego im prawa dostępu.

4.5. Zarządzający jednostką organizacyjną ADO, w której zachodzą procesy przetwarzania Danych osobowych, odpowiedzialny za zadania realizowane w jednostce, jest też odpowiedzialny za przetwarzanie i ochronę Danych osobowych w ramach realizacji tych zadań, w tym za:

- określenie rodzaju uprawnień oraz urządzeń, które są niezbędne do realizacji zadań,
- określanie, które osoby i na jakich prawach mają dostęp do danych informacji.

5. Program budowania świadomości pracowników

5.1. ADO wdraża program podnoszenia świadomości pracowników w zakresie ochrony Danych osobowych. Na program ten składają się w szczególności następujące działania:

- realizacja cyklicznych kampanii informacyjnych w ADO,
- realizacja programów szkoleniowych dedykowanych dla poszczególnych grup Użytkowników,
- wprowadzenie obowiązkowych szkoleń dla nowozatrudnionych pracowników;
- cykliczna realizacja testów socjotechnicznych.
- umieszczenie w ogólnodostępnym miejscu informacji o tym jak ADO realizuje prawa podmiotów danych

5.2. Każdy pracownik, podlega przeszkoleniu z przepisów o ochronie Danych osobowych oraz zasad PODO;

5.3. Dopuszczenie pracowników do przetwarzania Danych osobowych wymaga nadania upoważnienia oraz złożenia oświadczenia o zachowaniu poufności.

6. Nadawanie upoważnienia do przetwarzania Danych osobowych

6.1. ADO nadaje upoważnienia do przetwarzania Danych osobowych.

6.2. Do przetwarzania Danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych.
6.3. Upoważnienie wydaje właściciel ADO albo upoważniona przez niego osoba.
6.4. Wzór upoważnienia stanowi Załącznik nr 1 do niniejszej Polityki.
6.5. Praca w ADO wiąże się z dostępem do przetwarzania Danych osobowych. Wszystkim pracownikom lub współpracownikom ADO nadane jest upoważnienie do przetwarzania danych. Ewidencja osób, którym nadano upoważnienie do przetwarzania Danych osobowych prowadzona jest w przez Dział Kadr lub Inspektora Ochrony Danych.
6.6. Faktyczny zakres dostępu do danych ustalany jest indywidualnie i jest zależny od zajmowanego stanowiska, zakresu obowiązków i powierzonych zadań. Decyzję o zakresie dostępu do danych osobowych podejmuje przełożony użytkownika.
6.7. Kierujący odpowiednią jednostkami przeprowadza kontrolę weryfikacji uprawnień użytkowników, której celem jest sprawdzenie czy użytkownicy nie mają nadanych nadmiarowych dostępów do Systemów informatycznych. Wynik kontroli jest raportowany do Inspektora Ochrony Danych.
6.8. Informacja o zakresie dostępu przyznanego do danego Systemu Informatycznego jest przechowywana w tym systemie. Właściciel biznesowy systemu na żądanie Inspektora Ochrony Danych przekazuje mu informacje o zakresie dostępu konkretnego użytkownika.
6.9. Użytkownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
6.10. Wszelkie przekroczenia lub jakiekolwiek próby przekroczenia przyznanych uprawnień traktowane będą, jako naruszenie podstawowych obowiązków pracowniczych lub umownych.

7. Prawa osób, których dane dotyczą

7.1. Realizacja praw podmiotów danych

7.1.1. ADO udziela osobie, której dane dotyczą, wszelkich wymaganych prawem informacji oraz prowadzi z nią wszelką komunikację dotyczącą przetwarzania Danych osobowych:
- w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie;
- jasnym i prostym językiem.

7.1.2. ADO udziela osobie, której dane dotyczą, informacji na temat przetwarzania jej Danych osobowych w formie:
- pisemnej (na przykład na formularzach, umowach, kwestionariuszach, drukach lub innych dokumentach);

- elektronicznej (na przykład droga mailową, na stronie internetowej);
- ustnej - na życzenie osoby, której dane dotyczą,

7.1.3. W przypadku zbierania Danych osobowych od osoby, której dane dotyczą obowiązek informacyjny jest spełniany podczas pozyskiwania Danych osobowych.

7.1.4. W przypadku pozyskiwania Danych osobowych w sposób inny niż od osoby, której dane dotyczą, Spółka przekazuje podmiotom danych informacje zawarte w obowiązku informacyjnym w:

- w rozsądnym terminie po pozyskaniu Danych osobowych - najpóźniej w ciągu jednego miesiąca - mając na uwadze konkretne okoliczności przetwarzania Danych osobowych,
- jeżeli Dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą, lub
- jeżeli planuje się ujawnić Dane osobowe innemu odbiorcy Danych osobowych - najpóźniej przy ich pierwszym ujawnieniu.

7.1.5. W przypadku pozyskiwania Danych osobowych w sposób inny niż od osoby, której dane dotyczą, ADO nie jest zobowiązana do podawania informacji w przypadku gdy:

- osoba, której dane dotyczą, dysponuje już tymi informacjami;
- udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku albo wymagałoby pozyskiwania informacji dodatkowych z innych źródeł zewnętrznych;
- pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega Administrator Danych osobowych, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą; lub
- Dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

7.2. Zgody podmiotów danych

7.2.1. W przypadku, gdy przewarzanie Danych osobowych odbywa się na podstawie zgody osoby, której dane dotyczą, ADO rejestruje fakt uzyskania zgody oraz treść zgody i przechowuje je w odpowiedniej formie w sposób umożliwiający jej weryfikację w dowolnym momencie.

7.2.2. ADO nie pozyskuje zgody na przetwarzanie Danych osobowych w przypadku, jeżeli dysponuje inną podstawą prawną przetwarzania Danych osobowych (brak pozyskiwania zgód nadmiarowych).

7.2.3. ADO umożliwia osobie, której dane dotyczą wycofanie zgody w dowolnym momencie w sposób równie łatwy jak jej wyrażenie, w szczególności przez ten sam kanał komunikacji. ADO informuje również osobę, której dane dotyczą, o możliwości wycofania zgody.

7.3. Tryb realizacji praw podmiotów danych

7.3.1. ADO umożliwia podmiotom danych realizację ich praw wynikających z RODO oraz przepisów krajowych o ochronie danych osobowych - dotyczy to w szczególności następujących praw:

- prawa dostępu do informacji,
- prawa do sprostowania danych
- prawa do usunięcia danych („prawo do bycia zapomnianym"),
- prawa do ograniczenia przetwarzania,
- prawa do przeniesienia danych,
- prawa do sprzeciwu wobec przetwarzania danych,
- prawa do niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu.

7.3.2. Wnioski podmiotów danych przekazywane są do właściwych jednostek odpowiadających za ich rozpatrzenie. Nadzór nad prawidłową realizacją wniosków prowadzi Inspektor Danych Osobowych (jeśli został powołany) lub osoba upoważniona przez ADO w zakresie, jakim nie są one realizowane bezpośrednio przez niego.

7.3.3. ADO udziela informacji podmiotom danych pisemnie lub w formie elektronicznej. Osoba uprawniona w imieniu ADO udziela podmiotowi danych informacji ustnie na jego żądanie jedynie w przypadku, gdy zostanie potwierdzona tożsamość osoby, której dane dotyczą.

7.3.4. Informacja w związku z żądaniem podmiotu danych udzielana jest bez zbędnej zwłoki, a w każdym razie w terminie miesiąca od otrzymania żądania. Termin, po poinformowaniu podmiotu danych o przyczynach opóźnienia, może ulec przedłużeniu o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań.

7.3.5. Wnioski związane z prawami podmiotów danych realizowane są w sposób wolny od opłat z zastrzeżeniem punktu 7.3.7. niniejszej PODO.

7.3.7. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, Spółka pobiera rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo - odmawia podjęcia działań, do których na podstawie przepisów nie

jest obowiązana.

8. Powierzenie, współadministrowanie i przekazywanie danych osobowych

8.1. Informacje ogólne

8.1.1. ADO może powierzyć przetwarzanie Danych osobowych innym podmiotom (powierzenie przetwarzania), wspólnie ustalać cele i sposoby przetwarzania z innymi podmiotami (współadministrowanie), przekazywać Dane osobowe innemu administratorowi lub innym podmiotom na podstawie właściwych przepisów lub zgody podmiotu danych. ADO może zostać również powierzone przetwarzanie Danych osobowych przez inne podmioty.

8.1.2. Rejestry umów powierzenia przetwarzania danych, umów przekazania danych oraz umów o współadministrowanie prowadzone są przez odpowiednią jednostkę.

8.1.3. Kierownik jednostki lub inna osoba planująca zawarcie umowy o powierzenie przetwarzania, przekazania danych lub o współadministrowanie, informuje o tym Inspektora Ochrony Danych (jeśli został powołany) lub osobę upoważnioną przez ADO, przedstawiając mu wyniki oceny ryzyka podmiotu, o której mowa w niniejszej Polityce. Inspektor Ochrony Danych lub osoba upoważniona przez ADO podejmuje decyzję o uczestniczeniu w negocjowaniu umowy lub o konieczności przedstawienia uzgodnionej wersji umowy do akceptacji.

8.2. Współadministrowanie

8.2.1. W przypadku, gdy dane będą przetwarzane przez ADO oraz inny podmiot, jako współadministratorów, umowa pomiędzy ADO a Współadministratorem reguluje w szczególności zakres odpowiedzialności każdego ze współadministratorów w zakresie wypełniania obowiązków wynikających z RODO, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji oraz zawierają rozstrzygnięcie, który z podmiotów dokonuje oceny skutków dla ochrony danych osobowych.

8.3. Powierzenie przetwarzania

8.3.1. Przed powierzeniem przetwarzania Danych osobowych innym podmiotom, ADO przeprowadza ocenę ryzyka Procesora w celu oszacowania, czy podmiot ten zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i innych przepisów dotyczących ochrony Danych osobowych oraz należycie

chroniło prawa osób których dane dotyczą.

8.3.2. Wzór ankiety analizującej stanowi załącznik nr 2 do niniejszej Polityki.

8.3.3. Proces oceny ryzyka oparty jest w szczególności o następujące kryteria oceny:

- rodzaj usługi świadczonej przez Procesora;
- kategorie przetwarzanych danych;
- klasyfikację przekazywanych danych pod kątem poufności;
- wolumen przekazywanych danych;
- zakres przekazywanych danych;
- zakres czynności przetwarzania;
- czy dostawca będzie miał dostęp do infrastruktury / systemów Spółki ;
- czy dostawca będzie miał dostęp do lokalizacji fizycznych Spółki.

8.3.4. Wymagania ADO w zakresie środków bezpieczeństwa przy przetwarzaniu Danych są zdefiniowane w Załączniku nr 3.

8.3.5. ADO cyklicznie przeprowadza audyt podmiotów, którym powierza przetwarzanie danych w celu zapewnienia, iż dane są przetwarzane zgodnie z umową.

8.4. Przekazywanie danych osobowych innym podmiotom

8.4.1. Dane osobowe mogą być przekazywane innym podmiotom uprawnionym do ich otrzymania na podstawie przepisów prawa. Przekazanie danych nie może naruszyć praw i wolności osób, których dane dotyczą i odbywa się wyłącznie za pośrednictwem wyznaczonej w ramach danego procesu przetwarzania jednostki organizacyjnej w ADO.

8.5. ADO jako podmiot przetwarzający

8.5.1. Właściciel biznesowy procesu, w którym ADO działa jako podmiot przetwarzający zgłasza Inspektorowi Ochrony Danych lub osobie upoważnionej przez ADO informacje dot. procesu. Zgłoszenie zawiera informacji takie jak:

- kategorie przetwarzań dokonywanych w imieniu danego administratora; gdy ma to zastosowanie,
- informację o przekazywaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwę tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 RODO akapit drugi,
- dokumentacja odpowiednich zabezpieczeń;
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

8.5.2. Inspektor Ochrony Danych lub osoba upoważniona przez ADO może żądać dodatkowych informacji w zakresie zgłaszanej czynności przetwarzania.

8.5.3. Inspektor Ochrony Danych lub osoba upoważniona przez ADO wprowadza proces do rejestru kategorii czynności przetwarzania.

8.5.4. W zakresie umów, w których ADO występuje jako podmiot przetwarzający stosuje się odpowiednio punkt 8.1.3 PODO.

8.6. Przekazywanie danych do krajów trzecich

8.6.1. W przypadku przekazywania Danych osobowych do krajów trzecich, ADO zapewnia, że odpowiednie mechanizmy prawne zostały zaprojektowane, zastosowane oraz wdrożone skutecznie, aby zapewnić, iż odbiorcy danych z krajów trzecich będą w stanie przetwarzać dane gwarantując właściwy poziom ochrony uwzględniający przepisy RODO oraz krajowe przepisy o ochronie danych osobowych.

9. Rejestr czynności przetwarzania kategorii czynności przetwarzania oraz zbiory danych osobowych

9.1. Inspektor Ochrony Danych (jeśli został powołany) lub osoba upoważniona przez ADO prowadzi rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania.

9.2. Obowiązek zgłoszenia Inspektorowi Ochrony Danych lub osobie upoważnionej przez ADO konieczności wprowadzenia czynności przetwarzania do rejestru czynności przetwarzania i rejestru kategorii czynności przetwarzania spoczywa na właścicielu biznesowym procesu przetwarzania. Informacja o konieczności zarejestrowania czynności przetwarzania może być efektem dokonanej przez właściciela biznesowego oceny skutków dla ochrony danych osobowych, o której mowa w niniejszej Polityce lub każdego innego działania uzasadniającego wprowadzenie nowej czynności przetwarzania do rejestru czynności przetwarzania lub rejestr kategorii czynności przetwarzania.

9.3. Rejestr zbioru danych osobowych prowadzony jest przez Inspektora Ochrony Danych lub osobę upoważnioną przez ADO.

9.4. Wzór rejestru stanowi *Załącznik nr 4* do niniejszej Polityki.

9.5. Wzór rejestru czynności przetwarzania i rejestru kategorii czynności przetwarzania stanowią *Załącznik nr 5* do niniejszej Polityki.

10. Wykazy

10.1. Dane osobowe są przetwarzane na obszarze wyznaczonym przez ADO w następujących lokalizacjach:

- Siedziba ADO,
- serwerownie poza budynkami siedziby ADO,

- placówki podmiotów, którym ADO powierzyła przetwarzanie Danych osobowych.

10.2. Przetwarzanie Danych osobowych za pomocą urządzeń przenośnych poza obszarem przetwarzania danych odbywa się wyłącznie za zgodą ADO.

10.3. Za wskazanie programów stosowanych do przetwarzania Danych osobowych i przypisanie ich do odpowiednich czynności przetwarzania zgodnie z rejestrem czynności przetwarzania danych odpowiada odpowiednia jednostka odpowiedzialna za administrowanie aplikacjami w infrastrukturze IT.

11. Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

11.1. Opis środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych Danych osobowych znajduje się w załączniku nr 3 do niniejszej Polityki.

12. Proces oceny skutków dla ochrony danych

12.1. ADO wdrożyła proces oceny skutków operacji przetwarzania danych dla ochrony Danych osobowych.

12.2. Proces oceny skutków dla ochrony Danych osobowych dokonywany jest przed rozpoczęciem przetwarzania, jeżeli dany rodzaj przetwarzania ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności podmiotów danych.

12.3. Jeżeli ocena wstępna nie wskazuje na wysoki poziom ryzyka naruszenia podstawowych praw lub wolności podmiotu danych dokonanie analizy o której stanowi art. 35 RODO nie jest konieczne.

12.4. ADO regularnie ocenia poziom ryzyka w prowadzonych procesach przetwarzania danych osobowych.

12.5. Inspektor Ochrony Danych (jeśli został powołany) lub osoba upoważniona przez ADO jest uczestnikiem procesu oceny ryzyka poprzez zajmowanie stanowiska w zakresie poprawności dokonania oceny i jej zgodności z przepisami o ochronie danych osobowych.

13. Naruszenie ochrony Danych osobowych i zarządzanie incydentem

13.1. Każda osoba, która stwierdzi lub poweźmie uzasadnione okolicznościami podejrzenie, że mogło dojść do naruszenia bezpieczeństwa danych osobowych, a w szczególności ich ujawnienia, zafałszowania, zniszczenia, zablokowania systemu teleinformatycznego przetwarzającego dane osobowe jest zobowiązana do powiadomienia przełożonego o zaistniałym incydencie.

13.2. Incydenty naruszeń ochrony danych osobowych procesuje Inspektor Ochrony Danych (jeśli został powołany) lub osoba upoważniona przez ADO.

13.3. W przypadku, gdy 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.

13.4. W przypadku zaistnienia naruszenia ochrony danych, Inspektor Ochrony Danych lub osoba upoważniona przez ADO dokonuje czynności zamierających do:

- rozpoznawania, zgłaszania i oceny incydentów bezpieczeństwa informacji w tym dot. ochrony danych osobowych;
- podejmowania działań w odpowiedzi na pojawiające się zagrożenia włączając w to uruchamianie działań zaradczych w celach prewencyjnych oraz w celu redukcji i eliminacji skutków;
- wyciągania wniosków z zaistniałych incydentów, organizowania działań zaradczych i udoskonalania podejścia do zarządzania incydentami bezpieczeństwa informacji;
- w razie potrzeby informuje organ nadzorczy o naruszeniu ochrony danych.

14. Pozostałe zasady przetwarzania Danych osobowych

14.1. W celu zachowania ciągłości działania ADO w przypadku zakłóceń pracy podstawowego centrum przetwarzania informacji, praca jest przejmowana przez zapasowe centrum przetwarzania informacji.

14.2. Dla każdej osoby, której dane są przetwarzane w Systemie Informatycznym system ten powinien zapewnić odnotowanie:

- daty pierwszego wprowadzenia danych, identyfikatora użytkownika wprowadzającego dane, chyba że dostęp do Systemu Informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba, źródła danych, w przypadku zbierania danych nie od osoby, której one dotyczą,
- informacji o Odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia,
- zgłoszenia żądania związanego z realizacją jej Praw przez osobę, której dane dotyczą.

Wymagania te nie dotyczą systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu, w celu udostępnienia go na piśmie.

Odnotowanie informacji, o których mowa w powyższych podpunktach, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

14.3. Za prawidłową parametryzację systemów i realizację punktów 14.1 - 14.2 odpowiedzialna jest właściwa jednostka IT administrująca systemem informatycznym.

15. Postanowienia końcowe

15.1. Polityka wchodzi w życie z dniem 25 maja 2018 r.

15.2. Inspektor Ochrony Danych (jeśli został powołany) składa nie rzadziej niż raz w roku raport ze stanu ochrony danych osobowych w ADO.

15.3. ADO dokonuje cyklicznego przeglądu Polityki pod kątem, aktualności, zupełności i zgodności z obowiązującymi przepisami o ochronie danych osobowych. Przegląd jest dokonywany raz w roku a w razie zaistnienia uzasadnionej potrzeby wynikającej ze zmieniających się przepisów lub potrzeby ADO może stanowić przyczynę dokonania ponownego przeglądu Polityki.