Polityka bezpieczeństwa danych osobowych

Rotomat sp. z o.o. z siedzibą we Wrocławiu

PODSTAWA PRAWNA

art. 24 ust. 2 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 (Dz. Urz. UE L. z 2016r. nr 119)

I. Postanowienia wstępne

§ 1

Niniejszą Politykę ochrony danych osobowych (zwaną dalej: „Polityką") sporządzono stosownie do 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 (Dz. Urz. UE L. z 2016r. nr 119; zwanym dalej: RODO).

§ 2

Zadaniem niniejszej Polityki jest zagwarantowanie adekwatnej oraz zgodnej z powszechnie obowiązującymi przepisami prawa metody przetwarzania danych osobowych, w tym zabezpieczenie ochrony danych osobowych przed wszelkiego rodzaju zagrożeniami, w tym niezgodnym z prawem przetwarzaniem oraz przypadkowym zniszczeniem, uszkodzeniem lub utratą danych osobowych, poprzez zapewnienie odpowiednich środków organizacyjnych i technicznych.

§ 3

Użyte w niniejszej Polityce określenia oznaczają:

a. Administrator (zwany również Spółką) - należy przez to rozumieć spółkę Rotomat sp. z o.o. z/s we Wrocławiu, ul. Stabłowicka 134, 54-062 Wrocław,

b. RODO – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L. z 2016r. nr 119);

c. dane osobowe lub dane – 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: numer identyfikacyjny, imię i nazwisko, , dane o lokalizacji, identyfikator internetowy itd.;

d. wrażliwe dane osobowe – dane osobowe uzewnętrzniające pochodzenie rasowe lub etniczne, przekonania religijne lub światopoglądowe, poglądy polityczne, dane biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczących zdrowia, seksualności lub orientacji seksualnej danej osoby oraz przetwarzania danych genetycznych, przynależność do związków zawodowych, , a także dane osobowe dotyczące wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa;

d. dane osobowe dzieci –dane osobowe osób poniżej szesnastego roku życia;

e. przetwarzanie –operacja lub zestaw operacji wykonywanych na danych osobowych lub 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;

f. ograniczenie przetwarzania – oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

g. profilowanie –dowolna 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;

h. 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;

i. zbiór danych – należy przez to rozumieć uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

j. podmiot przetwarzający –osoba fizyczną lub prawna, organ publiczny, jednostka lub inny podmiot, któremu Administrator Danych Osobowych powierzył przetwarzanie danych osobowych;

k. Inspektor lub IOD –Inspektor Ochrony Danych powołany przez Administratora Danych Osobowych do nadzorowania przestrzegania zasad ochrony danych osobowych określonych na podstawie niniejszej Polityki oraz w zakresie wynikającym z powszechnie obowiązujących przepisów o ochronie danych osobowych;

l. odbiorca –osobę fizyczną lub prawną, organ publiczny, jednostka 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 uznawane za odbiorców;

ł. pracownik –każda osoba zatrudniona przez Administratora na podstawie umowy o pracę, powołania, wyboru, mianowania lub spółdzielczej umowy o pracę, a także osobę wykonującą pracę na innej podstawie niż stosunek pracy, doktoranta, studenta, ucznia, praktykanta, stażystę, wolontariusza niebędących pracownikami, jak również osobę fizyczną prowadzącą jednoosobową działalność gospodarczą, współpracującą z pracodawcą;

m. system informatyczny –zespół urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych w ramach prowadzonej przez Administratora działalności gospodarczej;

n. system tradycyjny –zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji /wyposażenia/środków trwałych w celu przetwarzania danych osobowych w formie papierowej;

o. administrator systemu informatycznego - osoba lub osoby, upoważnione przez administratora do administrowania i zarządzania systemami informatycznymi,

p. identyfikator pracownika (login) –ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,

r. hasło –ciąg co najmniej ośmiu znaków literowych, cyfrowych lub innych, przypisany do identyfikatora pracownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

s. Polityka – należy przez to rozumieć niniejszą Politykę ochrony danych osobowych.

II. Zasady ochrony danych osobowych – postanowienia ogólne

§ 4

Niniejsza Polityka statuuje reguły ochrony danych osobowych obowiązujące u Administratora. Polityka obejmuje odwołania do wzorów dokumentów konkretyzujących jej postanowienia w zakresie procedur lub instrukcji dot. poszczególnych sfer z zakresu ochrony danych osobowych.

§ 5

1. Administrator przetwarza dane osobowe przestrzegając następujących zasad:

   a. w oparciu o podstawę prawną i zgodnie z prawem (**legalizm**);

   b. uczciwie i rzetelnie i (**rzetelność);**

   c. w sposób przejrzysty dla osoby, której dane dotyczą (**transparentność**);

   d. w wyraźnie i konkretnie określonym celu (**minimalizacja**);

e. w ilości nie większej oraz w okresie nie dłuższym niż jest to niezbędne do celów, w których dane te są przetwarzane (**adekwatność i czasowość**);

f. z dbałością o prawidłowość danych (**prawidłowość**);

e. z zapewnieniem odpowiedniego bezpieczeństwa danych (bezpieczeństwo);

g. z zapewnieniem integralności danych (integralność).

2. Administrator przetwarza dane osobowe w sposób zapobiegający dostępowi do danych osobom nieupoważnionym oraz modyfikację danych osobowych lub ich zniszczenie w sposób nieautoryzowany.

3. Administrator identyfikuje, sprawuje kontrolę i minimalizuje, a w miarę możliwości eliminuje zagrożenia bezpieczeństwa, w zakresie systemów tradycyjnych oraz informatycznych służących do przetwarzania danych osobowych.

4. Administrator umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.

III. Zakres zastosowania. Zadania Administratora oraz Inspektora Danych Osobowych

§ 6

1. Niniejsza Polityka ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych w związku z działalnością Administratora prowadzoną na terytorium Unii Europejskiej, niezależnie od tego, czy przetwarzanie odbywa się na terytorium Unii Europejskiej.

2. Polityka w szczególności znajduje zastosowanie do:

a. danych osobowych przetwarzanych w systemach tradycyjnych,

b. danych osobowych przetwarzanych w systemach informatycznych,

c. informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,

d. rejestru osób dopuszczonych do przetwarzania danych osobowych,

e. innych dokumentów zawierających dane osobowe.

§ 7

Administratorem danych jest Rotomat sp. z o.o. z/s we Wrocławiu przy ul. Stabłowickiej 134.

§ 8

1. Odpowiedzialny za wdrożenie i kontrolowanie przestrzegania niniejszej Polityki w imieniu Administratora jest jego Zarząd, a w ramach Zarządu: Prezes Zarządu, któremu powierzono nadzór nad obszarem ochrony danych osobowych albo osoba pisemnie wyznaczona przez Zarząd.

2. W razie powołania, Inspektor Ochrony Danych odpowiada za nadzór i monitorowanie przestrzegania niniejszej Polityki.

3. Za stosowanie i realizację niniejszej Polityki odpowiedzialny jest Administrator, w szczególności komórki organizacyjne przetwarzające dane osobowe w znacznej ilości, a ponadto pozostałe komórki organizacyjne oraz wszyscy pracownicy Administratora.

§ 9

1. Do obowiązków Administratora należą w szczególności :

a. zagwarantowanie bezpieczeństwa i ochrony przetwarzania danych osobowych zgodnie z wymogami powszechnie obowiązujących przepisów prawa,

b. zapewnienie przetwarzania danych zgodnie z postanowieniami niniejszej Polityki oraz Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych,

c. udzielanie i odwoływanie upoważnień do przetwarzania danych osobowych,

d. prowadzenie rejestru czynności przetwarzania danych osobowych oraz rejestru osób upoważnionych do przetwarzania danych osobowych,

e. prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych i zgłoszenie faktu naruszenia organowi nadzorczemu oraz zawiadomienie o tym osobę, której dane dotyczą,

f. nadzór nad bezpieczeństwem danych osobowych,

g. przeprowadzanie corocznych audytów systemu ochrony danych osobowych zastosowanego u Administratora oraz aktualizacja środków organizacyjnych, technicznych oraz mechanicznych wykorzystywanym w jego ramach;

h. przeprowadzanie szkoleń pracowników;

i. współpraca z organem nadzorczym.

2. Przed dopuszczeniem do pracy z systemem informatycznym lub systemem tradycyjnym zawierającym dane osobowe, Administrator udziela pracownikom, upoważnienia do przetwarzania danych osobowych.

3. W razie potrzeby Administrator może udzielić upoważnienia do przetwarzania danych osobowych osobie niebędącej pracownikiem, przed dopuszczeniem do pracy z systemem informatycznym lub systemem tradycyjnym zawierającym dane osobowe.

4. Administrator może w każdym czasie, w formie pisemnej, odwołać udzielone upoważnienie do przetwarzania danych osobowych.

§ 10

1. Administrator może ustanowić Inspektora Ochrony Danych.

2. Inspektor ochrony danych jest powoływany z uwzględnieniem kwalifikacji zawodowych, a w szczególności wiedzy specjalistycznej w zakresie powszechnie obowiązujących przepisów prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności wypełnienia zadań, o których mowa w ust. 4.

3. Inspektor ochrony danych może być pracownikiem Administratora lub podmiotu przetwarzającego.

4. Do zadań Inspektora Ochrony Danych należy przede wszystkim:

a. informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na podstawie powszechnie obowiązujących przepisów o ochronie danych osobowych i wydawanie zaleceń w tej materii;

b. kontrolowanie przestrzegania obowiązujących powszechnie przepisów prawa w zakresie ochrony danych osobowych oraz regulacji wewnętrznych przyjętych przez Administratora, w tym podziału obowiązków, działań zwiększających świadomość, szkoleń personelu uczestniczącego w operacjach przetwarzania oraz powiązanych z tym audytów;

c. udzielanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;

d. współpraca z organem nadzorczym;

e. w stosownych przypadkach prowadzenie konsultacji z organem nadzorczym.

5. Inspektor ochrony danych realizuje w/w zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

6. Powołanie oraz odwołanie Inspektora Ochrony Danych wymaga zachowania formy pisemnej.

§ 11

1. Administrator może powierzyć przetwarzanie danych osobowych w systemach informatycznych administratorowi systemu informatycznego. Jeżeli administrator systemu informatycznego nie zostanie powołany, jego zadania wykonuje Administrator.

2. Powołanie oraz odwołanie administratora systemu informatycznego wymaga zachowania formy pisemnej.

3. Zakres obowiązków administratora systemu informatycznego reguluje Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.

IV. Opis działalności Administratora, obszary przetwarzania danych osobowych oraz zbiory danych osobowych

§ 12

1. Administrator prowadzi działalność gospodarczą m.in. w zakresie zarządzania i realizacji projektów budowlanych (organizacja ruchu tymczasowego i docelowego, elementy bezpieczeństwa ruchu drogowego i mała architektura, bariery i osłony energochłonne, sygnalizacja świetlna i oświetlenie, urządzenia ochrony środowiska) oraz w zakresie całorocznego utrzymania infrastruktury drogowej. W związku z prowadzoną działalnością Administrator przetwarza dane osobowe.

2. Dane osobowe przetwarzane są zarówno w formie elektronicznej jak i papierowej.

§ 13

1. Dane osobowe w formie papierowej przetwarzane są na terenie siedziby Administratora.

2. Dane osobowe w formie elektronicznej mogą być przetwarzane za pomocą komputerów, komputerów przenośnych, zewnętrznych dysków twardych, innych zewnętrznych elektronicznych nośników danych, telefonów oraz innych urządzeń. Mając to na uwadze dane osobowe w formie elektronicznej mogą być przetwarzane w dowolnym miejscu. Ponadto, dane osobowe mogą być przetwarzane w ramach systemów informatycznych, do których Administrator uzyskuje dostęp on-line, a systemy te nie są zainstalowane na komputerach wykorzystywanych przez Administratora.

3. Administrator może powierzyć przetwarzanie danych osobowych podmiotom trzecim na podstawie umowy powierzenia przetwarzania danych osobowych. W związku z powyższym, do przetwarzania danych osobowych może dochodzić również w innych lokalizacjach. W zakresie czynności przetwarzania dokonywanych przez podmiot przetwarzający lub podmioty przez niego upoważnione, podmiot przetwarzający oraz podmioty przez niego upoważnione zobowiązały się do stosowania odpowiednich środków ochrony danych osobowych wymaganych przez powszechnie obowiązujące przepisy.

5. W siedzibie Administratora oraz na urządzeniach wykorzystywanych do przetwarzania danych osobowych zostały wdrożone odpowiednie środki ochrony danych osobowych.

§ 14

1. Administrator dokonuje czynności przetwarzania w ramach następujących zbiorów:

1) zbiór „Umowy”

2) zbiór „Oferty handlowe”

3) zbiór „Dokumenty rozliczeniowe”,

4) zbiór „Pracownicy”,

5) zbiór „Osoby biorące udział w procesach rekrutacyjnych”

6) zbiór „Korespondencja”,

7) zbiór „Książka teleadresowa”,

8) zbiór „Media społecznościowe”,

9) zbiór „Osoby upoważnione”.

2. Szczegółowy zakres przetwarzania danych osobowych w ramach poszczególnych zbiorów określa Rejestr czynności przetwarzania danych osobowych.

3. Administrator dołożył należytej staranności w celu zidentyfikowania wszelkich procesów przetwarzania danych osobowych zachodzących w ramach jego struktury, wyodrębniając jednocześnie zbiory danych osobowych, w ramach których dane są przetwarzane. Dane osobowe mogą być jednak przetwarzane incydentalnie również poza zbiorami wskazanymi w ust. 1, w szczególności w sytuacji korzystanie przez pracowników z oprogramowania biurowego Microsoft Office.

V. System ochrony danych osobowych

§ 15

1. Administrator dokonuje inwentaryzacji przetwarzanych danych osobowych rozumianej jako identyfikację zasobów danych osobowych, klas danych, identyfikacji sposobów wykorzystania danych, w tym:

a. przypadków przetwarzania danych osobowych,

b. przypadków przetwarzania wrażliwych danych osobowych,

c. przypadków przetwarzania danych osób, których Spółka nie identyfikuje;

d. przypadków przetwarzania danych dzieci;

e. profilowania;

f. współadministrowania danymi.

2. Administrator identyfikuje przypadki, w których przetwarza lub może przetwarzać wrażliwe dane osobowe oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania danych wrażliwych. W przypadku zidentyfikowania przypadków przetwarzania danych wrażliwych, Administrator postępuje zgodnie z zasadami wynikającymi z powszechnie obowiązującymi przepisami prawa, w szczególności dokonuje zgodnie z zasadami określonymi w art. 9 oraz art. 10 RODO.

§ 16

1. Administrator prowadzi Rejestr Przetwarzania Danych Osobowych.

2. Rejestr stanowi formę dokumentowania czynności przetwarzania danych, w którym inwentaryzuje dane osobowe oraz monitoruje sposób przetwarzania danych osobowych.

3. Administrator zamieszcza w Rejestrze swoją nazwę i dane kontaktowe oraz nazwy i dane kontaktowe wszelkich współadministratorów, a także gdy zostali powołani - przedstawiciela administratora oraz Inspektora ochrony danych;

4. Dla każdej czynności przetwarzania danych, którą Administrator uznał za odrębną dla potrzeb Rejestru, Administrator odnotowuje co najmniej:

a. nazwę czynności,

b. cel przetwarzania,

c. opis kategorii osób,

d. opis kategorii danych osobowych,

e. opis kategorii odbiorców, którym dane osobowe zostały lub zostaną ujawnione,

f. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,

g. jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

6. Administrator prowadzi Rejestr w formie pisemnej oraz w formie elektronicznej.

7. Administrator może powierzyć prowadzenie Rejestru Inspektorowi Ochrony Danych, jeżeli został powołany.

§ 17

1. Spółka weryfikuje podstawy prawne przetwarzania danych i odnotowuje je w Rejestrze, a ponadto:

a. utrzymuje system zarządzania zgodami na przetwarzanie danych,

b. identyfikuje i szczegółowo uzasadnia przypadki, gdy Spółka przetwarza dane na podstawie prawnie uzasadnionego interesu Spółki.

2. Administrator stosuje metody zarządzania zgodami umożliwiające weryfikację posiadania zgody osoby, której dane dotyczą na przetwarzanie jej danych w konkretnym celu oraz odnotowanie faktu odmowy zgody, cofnięcia zgody i czynności o podobnym charakterze, w szczególności wyrażenia sprzeciwu lub ograniczenia przetwarzania danych. Administrator może w tym celu prowadzić ewidencję udzielonych zgód na przetwarzanie danych osobowych.

3. Kierownik w spółce Administratora ma obowiązek znać podstawę prawną czynności przetwarzania danych osobowych dokonywanych w ramach kierowanej przez niego jednostki. Jeżeli podstawę przetwarzania danych stanowi uzasadniony interes Spółki, kierownik komórki organizacyjnej ma obowiązek znać konkretny interes Spółki.

§ 18

1. Administrator spełnia obowiązki informacyjne wobec osób, których dane dotyczą oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania.

2. Administrator przekazuje informacje i prowadzi komunikacje z osobami, których dane dotyczą w sposób przejrzysty, zwięzły i zrozumiały.

3. Administrator zapewnia osobom, których dane osobowe przetwarza korzystanie z ich praw poprzez różne działania, w tym zamieszczenie na stronie internetowej Spółki informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich w Spółce, wymaganiach dotyczących identyfikacji oraz metodach kontaktu ze Spółką w tym celu.

4. Administrator informuje osobę o przetwarzaniu jej danych osobowych przy pozyskiwaniu danych od tej osoby.

5. W przypadku pozyskania danych niebezpośrednio od osoby, której dane dotyczą Administrator informuje osobę o przetwarzaniu jej danych w rozsądnym terminie, nie później niż w terminie miesiąca od pozyskania danych osobowych. Jeżeli dane osobowe będą podlegały przetwarzaniu w komunikacji z osobą, której dane dotyczą – Administrator informuje o tym najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą.

6. Administrator informuje w miarę możliwości osobę, której dane dotyczą o przetwarzaniu danych niezidentyfikowanych. Spółka informuje w szczególności o objęciu siedziby Spółki oraz jednostek jej podległych monitoringiem wizyjnym poprzez zamieszczenie tablicy informacyjnej.

7. Administrator informuje osobę, której dane dotyczą o planowanej zmianie celu przetwarzania danych.

8. Administrator informuje osobę, która wystąpiła z żądaniem ograniczenia przetwarzania danych o planowanym uchyleniu ograniczenia przetwarzania danych przed uchyleniem wyżej wskazanego ograniczenia.

9. Administrator informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych, chyba że poinformowanie odbiorców będzie wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe.

10. Administrator informuje osobę, której dane dotyczą o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.

11. Administrator zawiadamia niezwłocznie osobę, której dane dotyczą o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

12. Administrator wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.

13. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach - elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.

14. Administrator dokumentuje realizację obowiązków informacyjnych oraz zawiadomień.

§ 19

1. Na żądanie osoby, której dane dotyczą Administrator informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania, a także udziela osobie dostępu do danych jej dotyczących.

2. Uprawnienie do uzyskania dostępu do danych może być realizowane przez wydanie kopii danych. Kopii danych wydanych w wykonaniu prawa dostępu do danych nie poczytuje się za pierwszą nieodpłatną kopię danych zgodnie z zasadami uiszczania opłat za kopie danych.

3. Administrator informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.

§ 20

1. Dostęp do danych osobowych przetwarzanych przez Administratora zabezpiecza się poprzez wykonywanie kopii bezpieczeństwa zbiorów danych.

2. Kopie bezpieczeństwa danych osobowych mogą być wykonywane w formie papierowej lub w formie elektronicznej. Jeżeli kopie bezpieczeństwa danych osobowych zostały wykonane w formie elektronicznej nie sporządza się kopii bezpieczeństwa w formie papierowej.

3. Szczegółowy tryb postępowania w zakresie tworzenia oraz przechowywania kopii bezpieczeństwa w formie elektronicznej reguluje Instrukcja zarządzania systemem informatycznym.

4. Za sporządzanie kopii bezpieczeństwa danych odpowiedzialny jest pracownik dokonujący czynności przetwarzania danych osobowych

5. Kopie bezpieczeństwa powinny być wykonywane codziennie po zakończonym dniu pracy ze zbiorem danych, chyba że danego dnia nie dokonano jakichkolwiek zmian w zbiorze danych.

6. Administrator sprawuje kontrolę nad prawidłowością wykonanych kopii bezpieczeństwa.

7. Administrator przechowuje kopie bezpieczeństwa danych przez okres wyszczególniony dla danej czynności w Rejestrze czynności przetwarzania danych lub do momentu zgłoszenia przez osobę, której dane dotyczą żądania usunięcia danych.

§ 21

1. Na żądanie osoby, której dane dotyczą Administrator dokonuje sprostowania danych, jeżeli są nieprawidłowe.

2. W przypadku sprostowania danych Administrator informuje osobę, której dane dotyczą o odbiorcach danych, na żądanie tej osoby.

§ 22

1. Na żądanie osoby, której dane dotyczą Administrator dokonuje uzupełnienia niekompletnych danych, uwzględniając cel przetwarzania danych. W celu uzupełnienia danych Administrator może zwrócić się do osoby, która wystąpiła z żądaniem o przedstawienie dodatkowego oświadczenia.

2. Administrator ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie danych byłoby niezgodne z celami przetwarzania danych.

§ 23

1. Na żądanie osoby, której dane dotyczą Administrator usuwa dane, gdy:

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

   b. zgoda na ich przetwarzanie została cofnięta i brak jest innej podstawy prawnej przetwarzania,

   c. osoba, której dane dotyczą wniosła skuteczny sprzeciw wobec przetwarzania danych,

   d. dane osobowe były przetwarzane niezgodnie z prawem,

   e. dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego, któremu podlega administrator;

   f. żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.

2. Przed zadośćuczynieniem żądaniu, o którym mowa w ust. 1 Administrator weryfikuje, czy nie zachodzą wyjątki określone w art. 17 ust. 3 RODO, w szczególności, czy przetwarzanie danych jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń.

3. Jeżeli dane podlegające usunięciu zostały upublicznione przez Administratora, Administrator podejmie rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, o potrzebie usunięcia danych i dostępu do nich.

4. W przypadku usunięcia danych Administrator informuje osobę, której dane dotyczą o odbiorcach danych, na żądanie tej osoby.

§ 24

1. Na żądanie osoby, której dane dotyczą Administrator dokonuje ograniczenia przetwarzania danych, gdy:

a. osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,

b. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,

c. Administrator nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,

d. osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Administratora zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

2. Jeżeli na mocy ust. 1 przetwarzanie zostało ograniczone, dane osobowe mogą być przetwarzane wyłącznie za zgodą osoby, której dane dotyczą, w celu ustalenia, dochodzenia lub obrony roszczeń, w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego. Powyższe nie znajduje zastosowania do przechowywania danych osobowych.

3. W przypadku ograniczenia przetwarzania danych Spółka informuje osobę, której dane dotyczą o odbiorcach danych, na żądanie tej osoby.

§ 25

1. Na żądanie osoby, której dane dotyczą Administrator wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu administratorowi, dane dotyczące tej osoby:

a. przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej,

b. przetwarzane w sposób zautomatyzowany.

2. Wykonując prawo do przenoszenia danych, o którym mowa w ust. 1, osoba, której dane dotyczą ma prawo żądania, by dane osobowe zostały przesłane przez Administratora bezpośrednio innemu administratorowi, jeśli jest to technicznie możliwe.

3. Żądanie przeniesienia danych osobowych przysługuje osobie, której dane dotyczą niezależnie od prawa do żądania usunięcia przekazanych danych osobowych, o których mowa wyżej.

§ 26

1. Jeżeli osoba, której dane dotyczą zgłosi uzasadniony jej szczególną sytuacją sprzeciw wobec przetwarzania jej danych osobowych, a dane przetwarzane są przez Administratora w oparciu o uzasadniony interes Administratora lub o powierzone Administratorowi zadanie w interesie publicznym, Administrator uwzględni sprzeciw, jeżeli po stronie Administratora ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

2. Jeżeli osoba, której dane dotyczą zgłosi sprzeciw względem przetwarzania jej danych przez Spółkę na potrzeby marketingu bezpośredniego, w tym profilowania Administrator uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

3. Sprzeciw, o którym mowa w ust. 1 oraz w ust. 2 może zostać zgłoszony w dowolnym momencie.

§ 27

W przypadku podejmowania przez Administratora decyzji wywołujących skutki prawne lub inaczej istotnie wpływające na osobę w sposób automatyczny, w tym profilowaniu, Administrator zapewnia możliwość zakwestionowania powyższej decyzji, w szczególności poprzez żądanie podjęcia decyzji w sposób niezautomatyzowany (przez człowieka), chyba że taka automatyczna decyzja:

a. jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Administratorem,

b. jest wprost dozwolona przepisami prawa,

c. opiera się o wyraźną zgodę odwołującej osoby.

§ 28

1. Administrator udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z zgłoszonym żądaniem niezwłocznie, najpóźniej w terminie miesiąca od otrzymania żądania.

2. Termin wskazany w ust. 1 może zostać przedłużony o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania Administrator informuje osobę, której dane dotyczą o przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie w formie elektronicznej, Administrator w miarę możliwości przekazuje informacje również w formie elektronicznej, chyba że osoba, której dane dotyczą, zażąda innej formy.

4. Jeżeli administrator 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.

5. Administrator informuje osobę, której dane dotyczą, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.

§ 29

Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, Administrator może pobrać opłatę w wysokości administracyjnych kosztów udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań albo odmówić podjęcia działań w związku z żądaniem.

§ 30

Realizując prawa osób, których dane dotyczą, Administrator zapewnia należyta ochronę praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób, Administrator może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone działania, łącznie z odmową zadośćuczynienia żądaniu.

§ 31

Administrator podejmuje działania mające na celu minimalizację przetwarzania danych, uwzględniając adekwatność danych do celów przetwarzania (ilości danych i zakresu przetwarzania), dostęp do danych oraz czas przechowywania danych.

§ 32

1. Administrator dokonał weryfikacji zakresu pozyskanych danych, zakresu ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia zasad ochrony danych osobowych wynikających z Ogólnego Rozporządzenia o Ochronie Danych.

2. Administrator dokonuje audytu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz w roku.

3. Administrator przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (privacy by design).

§ 33

1. Administrator stosuje procedury kontroli okresu przetwarzania danych osobowych, w szczególności dokonuje weryfikacji dalszej przydatności danych zgodnie z terminami wskazanymi w rejestrze czynności przetwarzania danych.

2. Administrator usuwa z wykorzystywanego systemu informatycznego oraz systemu tradycyjnego dane, których przydatność ustała w związku z upływem czasu.

3. Dane, o których mowa w ust. 2 nie mogą znajdować się w kopiach bezpieczeństwa danych osobowych. Procedury tworzenia i wykorzystania kopii bezpieczeństwa uwzględniają wymagania kontroli dalszej przydatności danych zgodnie z terminami wskazanymi w rejestrze czynności przetwarzania danych oraz wymogi związane z usuwaniem danych na żądanie osoby, której dane dotyczą.

§ 34

1. Administrator zapewnia stopień bezpieczeństwa danych osobowych odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych.

2. W celu zapewnienia adekwatnych środków bezpieczeństwa danych osobowych Administrator:

a. podejmuje działania w celu zapewnienia odpowiedniego stanu wiedzy o bezpieczeństwie informacji oraz cyberbezpieczeństwie - samodzielnie lub ze wsparciem podmiotów wyspecjalizowanych,

b. kategoryzuje dane oraz czynności przetwarzania z uwzględnieniem ryzyka, które przedstawiają;

c. przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii.

d. ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania, w szczególności ustala przydatność środków takich jak pseudonimizacja, szyfrowanie danych osobowych, środki zapewnienia ciągłości działania i zapobiegania skutkom awarii oraz innych zdarzeń losowych, to jest zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich oraz inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania.

3. Administrator może w szczególności wdrożyć pseudonimizację danych osobowych poprzez zastosowanie szyfrowania kluczem tajnym, tokenizacji lub skracania.

§ 35

1. Administrator stosuje ograniczenia dostępu do danych osobowych o charakterze, fizycznym, organizacyjnym i technicznym.

2. Fizyczną ochronę danych osobowych i ich przetwarzania realizuje się przez:

1) przetwarzanie danych osobowych w ściśle określonych miejscach do tego przeznaczonych;

2) zabezpieczenie dostępu do wszelkiego rodzaju pomieszczeń, w których przetwarzane są dane osobowe poprzez zastosowanie wysokiej jakości zamków drzwiowych, do których klucze posiadają tylko upoważnione osoby;

3) zamykanie pomieszczeń, w których przetwarzane są dane osobowe na czas nieobecności osób upoważnionych do przetwarzania danych;

4) zabezpieczenie wszelkich możliwych dróg dostępu do pomieszczeń, w tym również okien;

5) zabezpieczenie pomieszczeń, w których przetwarzane są dane osobowe przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy;

6) wyposażenie pomieszczeń w sprzęty oraz meble biurowe dające gwarancję bezpieczeństwa dokumentacji (szafy, biurka zamykane na klucz);

7) przechowywanie kopii bezpieczeństwa danych osobowych w innym pomieszczeniu niż to, w którym dokonuje się bieżących czynności przetwarzania danych;

8) zapewnienie odpowiedniej organizacji stanowisk pracy osobom, które przetwarzają dane osobowe;

9) przechowywanie danych osobowe w teczkach i segregatorach wykonanych z nieprzezroczystych materiałów,;

10) oznaczenie teczek oraz segregatorów, w których przechowywane są dane osobowe w sposób utrudniający identyfikację ich zawartości osobom nieupoważnionym.

3. Organizacyjną ochronę danych i ich przetwarzania realizuje się przez:

1) wdrożenie i stosowanie niniejszej Polityki ochrony danych osobowych,

2) wdrożenie i stosowanie Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych,

3) dopuszczenie do przetwarzania danych osobowych wyłącznie osób posiadających upoważnienia udzielone przez Administratora,

4) zapoznanie każdego pracownika z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem do pracy przy ich przetwarzaniu oraz w zakresie zabezpieczeń systemu informatycznego,

5) odebranie od pracowników upoważnionych do przetwarzania danych oświadczeń o zachowaniu poufności przetwarzanych danych.

4. Techniczną ochronę danych i ich przetwarzania realizuje się poprzez:

1) zastosowanie oprogramowania typu Firewall do ochrony dostępu do sieci komputerowej,

2) zastosowanie środków ochrony przed szkodliwym oprogramowaniem,

3) zastosowanie uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła przy starcie systemu operacyjnego komputera,

4) zastosowanie uwierzytelnienia z wykorzystaniem identyfikatora pracownika oraz hasła przy dostępie do programu, aplikacji lub innego narzędzia programowego, przy użyciu którego przetwarzane są dane osobowe, jeżeli jest to technicznie możliwe,

5) zastosowanie środków pozwalających na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych,

6) zastosowanie wygaszaczy ekranów na stanowiskach, na których przetwarzane są dane osobowe,

7) zastosowanie środków uniemożliwiających wykonywanie nieautoryzowanych kopii danych osobowych.

§ 36

1. Każdy pracownik przed dopuszczeniem do pracy z systemem informatycznym lub systemem tradycyjnym przetwarzającym dane osobowe powinien odbyć szkolenie w zakresie ochrony danych osobowych.

2. Zakres szkolenia powinien obejmować zaznajomienie pracownika z powszechnie obowiązującymi przepisami prawa w zakresie ochrony danych osobowych oraz z regulacjami wewnętrznymi obowiązującymi u Administratora.

3. Każdy pracownik, który przetwarza dane osobowe powinien potwierdzić na piśmie fakt zapoznania się z powszechnie obowiązującymi przepisami prawa w zakresie ochrony danych osobowych oraz z regulacjami wewnętrznymi obowiązującymi u Administratora.

§ 37

1. Przetwarzać dane osobowe może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych udzielone przez Administratora, o którym mowa w § 9 ust. 2 niniejszej Polityki.

2. Upoważnioną do przetwarzania danych może być tylko osoba, która uczestniczyła uprzednio w szkoleniu z zakresu ochrony danych osobowych.

3. Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana przestrzegać następujących zasad:

1) może przetwarzać dane osobowe zgodnie z zakresem opisanym w upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków. Ustanie stosunku pracy powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych;

2) musi zachować tajemnicę danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji;

4) stosuje określone przez Administratora procedury oraz wytyczne mające na celu zgodne z prawem, w tym zwłaszcza adekwatne i celowe, przetwarzanie danych;

5) zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym.

4. Administrator utrzymuje system zarządzania upoważnieniami do przetwarzania danych osobowych, pozwalający na rejestrację i weryfikację, czy dana osoba została upoważniona do przetwarzania danych osobowych. Administrator może w tym celu prowadzić rejestr osób upoważnionych do przetwarzania danych osobowych.

§ 38

1. Każdy pracownik przetwarzający dane osobowe zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są pracownikowi niezbędne w danym momencie pracy do wykonania bieżących zadań.

2. Po zakończonej pracy pracownik przetwarzający dane osobowe zobowiązany jest odłożyć wszystkie dokumenty oraz, jeżeli ma to zastosowanie, komputer przenośny wykorzystywany do przetwarzania danych do szafy zamykanej na klucz.

3. Każdy pracownik przetwarzający dane osobowe zobowiązany jest do niszczenia zbędnych dokumentów w taki sposób, aby nie było możliwe odtworzenie zawartych w nich informacji.

§ 39

1. Spółka dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych przed rozpoczęciem przetwarzania w przypadkach, gdy dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych,

2. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem Administrator może przeprowadzić pojedynczą ocenę.

3. Dokonując oceny skutków dla ochrony danych, Administrator konsultuje się z Inspektorem Ochrony Danych, jeżeli został on powołany.

VI. Podmioty przetwarzające

§ 40

1. Administrator dokonuje weryfikacji podmiotów przetwarzających dane na jego rzecz w celu zapewnienia, by podmioty przetwarzające dawały wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na Administratorze.

2. Podmiot przetwarzający nie może korzystać z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody Administratora.

3. W przypadku wyrażenia przez Administratora ogólnej pisemnej zgody podmiot przetwarzający informuje Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających. Administratorowi przysługuje prawo sprzeciwu wobec planowanych zmian.

4. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy powierzenia przetwarzania danych osobowych. Wzór umowy stanowi załącznik do niniejszej Polityki.

VII. Zawiadamianie o naruszeniu ochrony danych osobowych

§ 41

1. Za naruszeniem ochrony danych osobowych w rozumieniu niniejszej Polityki należy rozumieć każde zdarzenie, powodujące zagrożenie bezpieczeństwa danych osobowych, w szczególności:

1) prowadzące do utraty integralności danych,

2) zagrażające poufności danych,

3) zagrażające rozliczalności danych.

2. Za naruszenie ochrony danych osobowych uznaje się w szczególności przypadki, gdy:

1) stwierdzono naruszenie obowiązujących przepisów wewnętrznych,

2) stwierdzono naruszenie powszechnie obowiązujących przepisów prawa,

3) stwierdzono naruszenie zabezpieczeń fizycznych.

§ 42

1. Każde naruszenie ochrony danych osobowych powinno być niezwłocznie zgłaszane Administratorowi. Postepowanie w przedmiocie stwierdzonego naruszenia ochrony danych

osobowych przy korzystaniu z systemów informatycznych reguluje Instrukcja zarządzania systemami informatycznymi.

2. W razie stwierdzenia naruszenia ochrony danych osobowych Administrator powinien niezwłocznie:

1) wysłuchać relacji zawiadamiającego, jak również każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem, w celu oceny zaistniałej sytuacji;

2) utrwalić wszelkie informacje i okoliczności związane z danym zdarzeniem, a w szczególności: dokładny czas uzyskania informacji uzasadniającej podejrzenie naruszenia ochrony danych osobowych albo samodzielnego wykrycia tego faktu, dane osoby zgłaszającej oraz stan zabezpieczeń;

3) podjąć niezwłocznie wszelkie działania zmierzające do odzyskania utraconych danych albo zabezpieczenia danych przed utratą;

4) podjąć niezwłocznie wszelkie działania zmierzające do ustalenia przyczyn zdarzenia, jak i okoliczności sprzyjających naruszeniu;

5) podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby nieuprawnionej do danych osobowych, zminimalizować szkody i zabezpieczyć przed usunięciem ślady naruszenia ochrony danych osobowych.

3. W przypadku stwierdzenia naruszenia ochrony danych osobowych, Administrator w miarę możliwości niezwłocznie, nie później jednak 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.

4. Do zgłoszenia naruszenia ochrony danych osobowych przekazanego organowi nadzorczemu po upływie 72 godzin Administrator dołącza wyjaśnienie przyczyn opóźnienia.

5. Zgłoszenie, o którym mowa w ust. 1 powinno zawierać co najmniej:

a. opis charakteru naruszenia ochrony danych osobowych,

b. jeśli jest to możliwe, kategorie i przybliżoną liczbę osób, których dane dotyczą,

c. jeśli jest to możliwe, kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

d. imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych lub oznaczenie innego punktu kontaktowego;

e. opis możliwych konsekwencji naruszenia ochrony danych osobowych;

f. opis środków zaradczych zastosowanych lub proponowanych przez Administratora, a w stosownych przypadkach – środków w celu zminimalizowania negatywnych skutków naruszenia ochrony danych osobowych.

5. Jeżeli Administrator nie jest w stanie udzielić wszystkich informacji, o których mowa w ust. 3 w tym samym czasie, może ich udzielać sukcesywnie bez zbędnej zwłoki.

6. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

VIII. Postanowienia końcowe

§ 43

Niniejsza Polityka jest udostępniana pracownikom upoważnionym do przetwarzania danych osobowych w taki sposób, aby mogli się zapoznać z jej treścią.

§ 44

W sprawach nieuregulowanych niniejszą Polityką, zastosowanie znajdują powszechnie obowiązujące przepisy w zakresie ochrony danych osobowych, w szczególności Ogólne Rozporządzenia o Ochronie Danych.

§ 45

Niniejszą Politykę wprowadza się na czas nieokreślony.

§ 46

Polityka może być zmieniona lub uzupełniona w takim samym trybie, w jakim została ustanowiona lub przez wprowadzenie nowej polityki.

§ 47

Polityka wchodzi w życie z dniem podpisania.

Wrocław, dnia ……2018r.

Prezes Zarządu