POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

Biuro Rachunkowe

M. Wachowicz, A. Ziółkowski s.c.

WARSZAWA DNIA 25 MAJA 2018 R.

Spis treści:

Rozdział 1

Postanowienia ogólne

§ 1

Ilekroć w Polityce, używa się poniższych sformułowań i skrótów, rozumie się przez to:

a) **rozporządzeniu** – 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 (ogólne rozporządzenie o ochronie danych);
b) **przepisami krajowymi** – rozumie się przez to przepisy rangi ustawowej oraz akty wykonawcze do nich regulujące ochronę danych osobowych w porządku krajowym;
c) **administratorze danych** – Marek Wachowicz, Andrzej Ziółkowski prowadzący działalność gospodarczą w formie spółki cywilnej pod firmą Biuro Rachunkowego M. Wachowicz, A Ziółkowski s.c.;
d) **danych osobowych** – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
e) **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
f) **zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
g) **przetwarzaniu danych** – jakiekolwiek operacje wykonywane na danych osobowych takie jak: zbieranie, opracowywanie, utrwalanie, zmienianie, przechowywanie, analizowanie, raportowanie, aktualizowanie, udostępnianie lub usuwanie danych osobowych, w tym także w wykonywanych w systemach informatycznych;
h) **usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
i) **zgodzie osoby, której dane dotyczą** – oznacza to 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;
j) **odbiorcy danych** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.;
k) **zabezpieczenie danych** – należy przez to rozumieć środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych;
l) **ograniczeniu przetwarzania** – należy przez to rozumieć oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
m) **pseudonimizacji** – oznacza to 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;
n) **podmiocie przetwarzającym** – oznacza to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora danych osobowych;
o) **naruszeniu ochrony danych osobowych** – oznacza to 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;

p) **użytkownik** – osoba zatrudniona u administratora danych osobowych na podstawie stosunku pracy lub osoba związana z administratorem danych osobowych stosunkiem zobowiązaniowym;
q) **osoba upoważniona do przetwarzania danych osobowych** – użytkownik, który otrzymał upoważnienie do przetwarzania danych;
r) **naruszenie zabezpieczenia systemu informatycznego** – jakiekolwiek naruszenie bezpieczeństwa, niezawodności, integralności lub poufności systemu;
s) **rejestr czynności przetwarzania** – rejestr prowadzony przez administratora danych osobowych zawierający m.in.:
   1) imię i nazwisko lub nazwę oraz dane kontaktowe administratora;
   2) cele przetwarzania danych osobowych;
   3) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
   4) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione;
   5) planowany terminy usunięcia poszczególnych kategorii danych.

§2

W celu ochrony danych osobowych zostały zrealizowane następujące wymogi:

a) przeprowadzono ocenę skutków dla ochrony danych oraz analizy ryzyka w stosunku do zasobów biorących udział w poszczególnych procesach zgodnie z załącznikiem nr 1 do niniejszej Polityki,
b) do przetwarzania danych zostały dopuszczone wyłącznie osoby upoważnione przez administratora danych, Wzór listy osób upoważnionych do przetwarzania danych osobowych oraz wzór upoważnienia do przetwarzania danych stanowią załącznika nr 2 i nr 3 do niniejszej Polityki;
c) zawarto umowę powierzenia przetwarzania danych zgodnie z załącznikiem nr 4;
d) przygotowano Wzór klauzul informacyjnych oraz zgód na przetwarzanie danych osobowych, stanowiących załącznik nr 5 do niniejszej Polityki;
e) została opracowana i wdrożona niniejsza Politykę.

§3

Dane osobowe przetwarzane przez administratora danych objęte są ochroną i poufnością. Ich przetwarzanie następuje wyłącznie na zasadach określonych przepisami rozporządzenia, przepisami krajowymi oraz niniejszą Polityką.

Rozdział 2
Administrator Danych

§4

1. Administrator danych nadzoruje wykonywanie Polityki, w szczególności sprawuje nadzór nad doborem i realizacją środków ochrony danych osobowych oraz realizacją czynności dotyczących przetwarzania danych przez użytkowników.
2. Administrator danych realizuje wszelkie obowiązki nałożone na niego przepisy rozporządzenia, przepisy krajowe oraz Politykę.
3. Administrator danych zapewnia osobom fizycznym, których dane osobowe są przetwarzane realizację uprawnień gwarantowanych im przez przepisy rozporządzenia, przepisy krajowe.
4. Każda osoba, której dane osobowe dotyczą ma prawo do kontroli przetwarzania danych osobowych, w zakresie określonym przepisami rozporządzenia, przepisami krajowymi, w

szczególności do realizacji prawa dostępu do danych osobowych, prawa do ich sprostowania i ich usunięcia jak i również do przenoszenia danych osobowych oraz do sprzeciwu wobec przetwarzania danych.

5. W każdym przypadku pobierania danych bezpośrednio od osoby, której dane dotyczą, administrator danych informuje osobę, której dane dotyczą, zgodnie z załącznikiem nr 5
6. Administrator danych prowadzi rejestr czynności przetwarzania, którego wzór stanowi załącznik nr 6 do niniejszej polityki.

§5

1. Administrator danych może powierzyć podmiotom zewnętrznym, na podstawie umowy zawartej na piśmie, przetwarzanie danych.
2. Podmiot zewnętrzny może przetwarzać dane osobowe wyłącznie w zakresie i celu niezbędnym do realizacji postanowień właściwej umowy bazowej.
3. Podmiot zewnętrzny, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć równoważne, co administrator danych środki zabezpieczające dane osobowe.

§6

1. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.
2. Administratora danych sprawuje kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo oraz komu są przekazywane.
3. Administratora danych prowadzi pisemną listy osób upoważnionych do przetwarzania danych osobowych oraz nadaje upoważnienia w zakresie przetwarzania danych.

Rozdział 3
Zasady postępowania przez Użytkownika z danymi osobowymi

§7

Osoby, które zostały upoważnione do przetwarzania danych lub odebrano im upoważnienie, zachowują przez cały czas w tajemnicy dane osobowe, do których uzyskały dostęp oraz sposoby ich zabezpieczenia.

§ 8

1. Środki do przetwarzania danych osobowych wykorzystywane u administratora danych są przeznaczone wyłącznie do wykonywania zadań służbowych.
2. Zabrania się podłączania do sieci teleinformatycznej jakichkolwiek urządzeń nieposiadających autoryzacji.
3. Użytkownicy mogą korzystać ze stacji roboczych wyłącznie na stanowiskach im przydzielonych. Korzystanie z innego stanowiska komputerowego dopuszczalne jest jedynie za zgodą i na polecenie administratora danych.
4. Użytkowników obowiązuje zakaz testowania lub podejmowania prób poznania metod zabezpieczenia systemów teleinformatycznych.
5. Użytkownicy nie mogą samodzielnie dokonywać jakiejkolwiek zmiany konfiguracji systemu teleinformatycznego.

§ 9

1. Przydzielanie uprawnień do korzystania z systemów teleinformatycznych realizowane jest w oparciu o następujące zasady:
   a) „minimalnych przywilejów" – każdy użytkownik posiada prawa dostępu do zasobów ograniczone wyłącznie do tych, które są niezbędne do wykonywania powierzonych mu obowiązków,

b) „wiedzy koniecznej” – użytkownicy posiadają wiedzę o zasobach ograniczoną wyłącznie do zagadnień, które są niezbędne do realizacji powierzonych im zadań,
c) „domniemanej odmowy” – wszystkie działania, które nie są jawnie dozwolone są zabronione.

2. Każdy użytkownik otrzymuje prawa dostępu wyłącznie w zakresie niezbędnym do realizowania powierzonych zadań na danym stanowisku pracy.
3. Prawa dostępu są przydzielone po nadaniu użytkownikowi identyfikatora i hasła dostępu lub innych danych uwierzytelniających użytkownika.
4. W przypadku dłuższej nieobecności na stanowisku pracy użytkownik obowiązany jest zakończyć aktywne sesje i wylogować się. Ponadto, użytkownik każdorazowo w przypadku oddalenia się od stacji roboczej obowiązany jest zablokować system.
5. Na użytkowniku spoczywa obowiązek zabezpieczenia opracowywanych bądź tworzonych przez siebie danych przed utratą. Również wszelkie dane źródłowe, na których użytkownik wykonuje operacje, winny być zabezpieczone przed utratą i nieautoryzowanym użyciem bądź modyfikacją.
6. Niedopuszczalne jest umieszczanie przez Użytkownika plików danych niezwiązanych z wykonywanymi obowiązkami służbowymi.
7. Zabronione jest:
   a) umożliwianie dostępu do systemów teleinformatycznych osobom nieupoważnionym,
   b) dokonywanie prób sprawdzania, testowania i omijania zabezpieczeń systemów teleinformatycznych wewnętrznych jak również zewnętrznych;
   c) udzielanie informacji o zasadach ochrony systemów teleinformatycznych u administratora danych, w tym o identyfikatorach używanych w tych systemach;
   d) samowolne modyfikowanie ustawień związanych z bezpieczeństwem w systemach teleinformatycznych;
   e) świadome niszczenie danych mających znaczenie archiwalne gromadzonych w systemach teleinformatycznych;
   f) świadome wprowadzanie błędnych danych do systemów teleinformatycznych;
   g) udostępnianie danych osobom nieupoważnionym.

§ 10

1. Wszyscy użytkownicy mają dostęp do wewnętrznej poczty elektronicznej.
2. Poczta elektroniczna służy wyłącznie do celów służbowych. Korespondencja realizowana drogą elektroniczną z wykorzystaniem systemów teleinformatycznych podlega rejestrowaniu i może być monitorowana. Informacje przesyłane za pośrednictwem sieci (w tym do i z Internetu) nie stanowią własności prywatnej użytkownika.
3. Użytkownicy obowiązani są do okresowego porządkowania i usuwania wiadomości zbędnych z folderów programu pocztowego tak, aby nie dopuścić do jego zablokowania z powodu przekroczenia dopuszczalnej pojemności skrzynki.
4. Zabronione jest:
   a) rozsyłanie z komputerów oraz przyznanych użytkownikom kont poczty wiadomości, których treść nie jest związana z wykonywaną pracą;
   b) wykorzystywanie systemu poczty elektronicznej do działań mogących zaszkodzi wizerunkowi administratorowi danych;
   c) odbieranie przesyłek z nieznanych źródeł;
   d) otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.;
   e) przesyłanie pocztą elektroniczną plików wykonywalnych typu: bat, com, exe, plików multimedialnych oraz plików graficznych;
   f) ukrywanie lub dokonywanie zmian tożsamości nadawcy,

g) czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika;
h) odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki oraz na inne formy wymiany danych określanych spamem;
i) posługiwanie się adresem służbowym e-mail w celu rejestrowania się na stronach handlowych, informacyjnych, chat'ach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy;
j) wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej niż wynikającej z potrzeb administratora danych lub do poszukiwania dodatkowego zatrudnienia.

§ 11

1. Hasła użytkowników lub inne dane uwierzytelniające podlegają szczególnej ochronie.
2. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła i jego przechowywanie.
3. Zabronione jest:
   a) zapisywanie haseł w sposób jawny i umieszczania ich w miejscach dostępnych dla innych osób;
   b) używanie tych samych haseł w różnych systemach operacyjnych i aplikacjach;
   c) udostępnianie haseł innym użytkownikom;
   d) przeprowadzanie prób łamania haseł.

§ 12

1. Użytkownicy nie mogą instalować oraz uruchamiać żadnych aplikacji, które nie zostały wcześniej formalnie dopuszczone do użytkowania.
2. Użytkownikowi nie wolno:
   a) uruchamiać jakiegokolwiek innego oprogramowania niż to, które zostało mu przydzielone na danej stacji roboczej,
   b) pobierać z sieci, kopiować, przechowywać lub rozprowadzać oprogramowania, utworów muzycznych i wideo oraz innych plików, których używanie może powodować naruszenie praw do własności intelektualnej,
   c) samodzielnie usuwać oprogramowania, którego używa.
3. Każdy plik znajdujący się:
   a) na wymiennym nośniku komputerowym,
   b) otrzymany za pomocą poczty elektronicznej lub pobrany z Internetu, podlega sprawdzeniu za pomocą oprogramowania antywirusowego zainstalowanego na komputerze przypisanym do użytkownika.
4. Użytkownik ponosi finansowe i prawne konsekwencje posiadania nielegalnego oprogramowania w przypisanym mu komputerze.

§ 13

1. Każdy użytkownik zobowiązany jest do przestrzegania zakazu prowadzenia rozmów, podczas których może dochodzić do wymiany danych osobowych, jeśli rozmowy te odbywają się w miejscach publicznych, otwartych pomieszczeniach biurowych lub takich, które nie gwarantują zachowania poufności rozmów.
2. Drukarki nie mogą być pozostawione bez kontroli, jeśli są wykorzystywane (lub wkrótce będą) do drukowania dokumentów zawierających dane osobowe.

§ 14

1. Palenie, jedzenie oraz picie na stanowiskach komputerowych oraz w pomieszczeniach, w których znajdują się środki przetwarzania informacji (pomieszczenia serwerowni i węzłów teletechnicznych) jest zabronione.
2. W celu ograniczenia ryzyka nieuprawnionego dostępu, utraty lub uszkodzenia informacji w czasie godzin pracy i poza nimi użytkownik jest zobowiązany:
   a) przechowywać dokumenty papierowe i wymienne nośniki komputerowe w odpowiednio zabezpieczonych meblach biurowych,
      nie pozostawiać komputerów bez nadzoru w stanie aktywnej sesji dostępu do sieci,
   b) po zakończeniu pracy wylogować się z systemu i wyłączyć komputer,
   c) niedopuszczalne jest zakończenie pracy bez wykonania pełnej i poprawnej procedury zamknięcia lub przez wyłączenie napięcia zasilającego,
   d) po zakończeniu pracy uporządkować swoje stanowisko pracy, uniemożliwiając dostęp osób nieupoważnionych do dokumentów (w szczególności zawierających dane osobowe),
   e) przestrzegać zasady niepozostawiania otwartych i niezabezpieczonych drzwi i/lub okien podczas nieobecności w pomieszczeniu,
   f) używać wygaszaczy ekranu zabezpieczonych hasłem,
   g) zabezpieczać nieużywany w danym momencie komputer przed nieupoważnionym dostępem, włączając blokadę systemową; ponowny dostęp do komputera następuje po podaniu hasła,
   h) ustawiać monitory komputerów w taki sposób, żeby uniemożliwić osobom nieupoważnionym wgląd w zawartość ekranu,
   i) niszczyć niepotrzebne nośniki papierowe w niszczarkach, jak np. dokumenty błędnie wydrukowane, powielone kopie itp.

§ 15

1. Nieprzestrzeganie zasad określonych Polityce przez użytkownika stanowi naruszenie podstawowych obowiązków pracowniczych i podlega odpowiedzialności dyscyplinarnej.
2. W szczególności umyślne działanie może zostać zakwalifikowane jako ciężkie naruszenie obowiązków pracowniczych.

Rozdział 4

Środki organizacyjne i techniczne zabezpieczające dostęp do danych

§ 16

Wydzielenie części pomieszczenia, w której przetwarza się dane osobowe jest w szczególności dokonane poprzez odpowiednie ustawienie mebli biurowych uniemożliwiające niekontrolowany dostęp osób niepowołanych do określonych danych osobowych przetwarzanych w danym pomieszczeniu.

Rozdział 5

DPIA (Data Protection Impact Assessment) oraz analizy ryzyka i plan postępowania z ryzykiem

§ 17

1. DPIA jest przeprowadzana przy każdorazowej istotnej zmianie procesu przetwarzania danych osobowych, np. zmiana dostawcy usług, zmiana sposobu przetwarzania danych, wymiana zasobów biorących udział w procesie.
2. Administrator danych w przypadku zamiaru rozpoczęcia przetwarzania danych osobowych w nowym procesie przeprowadza DPIA w stosunku do tego procesu.

3. W każdym przypadku tworzenia nowego produktu lub usług administrator danych uwzględnia prawa osób, których dane dotyczą, na każdym kluczowym etapie jego projektowania i wdrażania.

§ 18

1. Analiza ryzyka jest przeprowadzana przy każdorazowej istotnej zmianie procesu przetwarzania danych i stanowi podstawę do aktualizacji sposobu postępowania z ryzykiem.
2. Na podstawie wyników przeprowadzonej analizy ryzyka, administrator danych samodzielnie wdraża sposoby postępowania z ryzykiem.
3. Każdorazowo administrator danych wybiera sposób postępowania z ryzykiem i określa, które ryzyka i w jakiej kolejności będą rozpatrywane jako pierwsze.

Rozdział 6
Postępowanie w przypadku naruszenia ochrony danych

§19

1. Przed przystąpieniem do pracy użytkownik obowiązany jest sprawdzić stację roboczą (komputer) i stanowisko pracy ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie lub próbę naruszenia bezpieczeństwa danych osobowych.
2. Do przypadków mogących świadczyć lub świadczących o naruszenia bezpieczeństwa danych osobowych, niewłaściwym funkcjonowaniu oprogramowania lub słabości systemu teleinformatycznego zalicza się:
   a) nieautoryzowany dostęp do danych;
   b) naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych;
   c) w pomieszczeniach (np. wyłamane lub zacinające się zamki, naruszone plomby, nie domykające się bądź wybite okna, itp.);
   d) utratę usługi, urządzenia lub funkcjonalności;
   e) udostępnienie danych osobowych osobom nieupoważnionym;
   f) pozyskiwanie oprogramowania z nielegalnych źródeł;
   g) pojawianie się nietypowych komunikatów na ekranie;
   h) niemożność zalogowania się do systemu teleinformatycznego;
   i) spowolnienie pracy oprogramowania;
   j) niestabilna praca systemu teleinformatycznego;
   k) ponowny start lub zawieszanie się komputera;
   l) ograniczenie funkcjonalności oprogramowania;
3. Za naruszenie zasad ochrony danych osobowych uważa się w szczególności;
   a) nieupoważniony dostęp, modyfikację, kopiowanie, udostępnienie lub zniszczenie/usunięcie danych osobowych, zarówno w systemie teleinformatycznym, jak i na nośnikach papierowych i elektronicznych;
   b) udostępnianie danych osobowych nieuprawnionym podmiotom;
   c) stworzenie niezabezpieczonego kanału dystrybucji danych osobowych;
   d) nielegalne bądź nieświadome ujawnienie danych osobowych;
   e) pozyskiwanie danych osobowych z nielegalnych źródeł;
   f) przetwarzanie danych osobowych niezgodne z uprawnionym celem i zakresem;
   g) niepodjęcie działań zmierzających do eliminacji wirusów komputerowych lub innych programów zagrażających integralności systemu teleinformatycznego;
   h) ujawnienie indywidualnych haseł dostępu do danych osobowych w systemie;
   i) przesyłanie danych osobowych przez Internet bez zabezpieczenia,
   j) przesyłanie dokumentów papierowych i nośników elektronicznych z danych osobowych bez zabezpieczenia;

k) wykonanie nieuprawnionych kopii danych osobowych;
l) kradzież nośników zawierających dane osobowe lub oprogramowanie;
m) kradzież sprzętu służącego do przetwarzania danych osobowych;
n) dopuszczenie do przetwarzania danych osobowych pracowników bez odpowiednich upoważnień;
o) inne sytuacje wskazujące lub potwierdzające naruszenie bezpieczeństwa danych osobowych u administratora danych.

4. W przypadku zauważenia zdarzenia mogącego świadczyć lub świadczącego o naruszeniu bezpieczeństwa, niewłaściwym funkcjonowaniu oprogramowania, błędów lub awarii systemu użytkownik:
   a) zabezpiecza dostęp do miejsca lub urządzenia w sposób umożliwiający odtworzenie okoliczności naruszenia bezpieczeństwa lub niewłaściwego funkcjonowania oprogramowania;
   b) wstrzymuje pracę na stacji roboczej i odseparowuje komputer od sieci.

§ 20.

1. W każdym przypadku naruszenia ochrony danych osobowych administrator danych weryfikuje, czy naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
2. Administrator danych w przypadku stwierdzenia, że naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, zawiadamia niezwłocznie organ nadzorczy, jednak nie później niż w ciągu 72 godz. od identyfikacji naruszenia.
3. Administrator danych zawiadamia osoby, których dane dotyczą, w przypadku wystąpienia wobec nich naruszeń skutkujących ryzykiem naruszenia ich praw lub wolności, chyba że zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka wystąpienia ww. naruszenia.
4. Administrator danych dokumentuje naruszenia, które skutkują naruszeniem praw i wolności osób fizycznych

Rozdział 7
Realizacji praw osób

§ 21

1. Każdy przypadek zgłoszenia przez osobę, której dane dotyczą, woli skorzystania z praw przewidzianych w rozporządzeniu administrator danych rozpatruje indywidualnie.
2. Administrator danych niezwłocznie realizuje następujące prawa osób, których dane dotyczą:
   a) prawo dostępu do danych,
   b) prawo do sprostowania danych,
   c) prawo do usunięcia danych,
   d) prawo do przenoszenia danych,
   e) prawo do sprzeciwu wobec przetwarzania danych,
   f) prawo do niepodlegania decyzjom oparty wyłącznie na profilowaniu.
3. W przypadku realizacji prawa do sprostowania, usunięcia i ograniczenia przetwarzania danych administrator danych niezwłocznie informuje odbiorców danych, którym udostępnił on przedmiotowe dane, chyba że jest to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.
4. Administrator danych odmawia realizacji praw osób, których dane dotyczą, jeżeli możliwość taka wynika z przepisów rozporządzenia, jednak każda odmowa realizacji praw osób, których dane dotyczą, wymaga uzasadnienia z podaniem podstawy prawnej wynikającej z rozporządzenia.

Rozdział 8

Postanowienia końcowe

§ 22

1. Polityka jest dokumentem wewnętrznym administratora danych stanowiącym tajemnicę przedsiębiorstwa i i objętym obowiązkiem zachowania w tajemnicy przez wszystkie osoby, którym zostanie ujawniona.
2. Wszelkie zasady opisane w niniejszym dokumencie są przestrzegane przez osoby upoważnione do przetwarzania danych osobowych ze szczególnym uwzględnieniem dobra osób, których dane te dotyczą.
3. Dokument niniejszy obowiązuje od dnia jego zatwierdzenia przez administratora danych.
4. Integralną część Polityki stanowią załączniki od 1 do 6.