POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

W

RAZ, DWA, TRZY RYTMIKA ANNA SZEWCZYK

Spis treści

I. Informacje ogólne oraz wnioski z analizy ryzyka.

1. Głównym celem wprowadzenia Polityki Bezpieczeństwa jest zapewnienie zgodności działania firmy **RAZ, DWA, TRZY RYTMIKA ANNA SZEWCZYK, Nowe Racibory, ul. Zielona 30, 05-555 Tarczyn** jako Administratora Danych Osobowych z przepisami prawa regulującymi kwestię administrowania i przetwarzania danych osobowych. Niniejsza Polityka Bezpieczeństwa opisuje w szczególności zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem.

2. **Sporządzenie Polityki bezpieczeństwa jako fundamentalnego dokumentu wynika z obowiązku rozliczalności z wdrożenia stosownych metod organizacyjnych i technicznych oraz wdrożenia stosownych polityk ochrony danych zgodnie z treścią Artykułu 24 ust. 2, Artykułu 39 ust. 5 oraz motywu 49 i 78 preambuły 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**: *Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych. Aby móc wykazać przestrzeganie niniejszego rozporządzenia, administrator powinien przyjąć wewnętrzne polityki i wdrożyć środki, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych.*

3. Dokument Polityki Bezpieczeństwa został opracowany w oparciu o wytyczne zawarte w następujących aktach prawnych:

   - Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (**dalej u.o.d.o**),
   - Rozporządzeniu 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 (**dalej RODO**)
   - Rozporządzeniu Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (**dalej ePrivacy**)

4. Obszarem przetwarzania danych osobowych przez **Administratora** jest każda jednostka organizacyjna firmy.

5. Użyte w niniejszej Polityce Bezpieczeństwa Przetwarzania Danych Osobowych określenia zostały wyjaśnione w Rozdziale II “Definicje”.

6. Ochrona danych osobowych realizowana jest poprzez stosowanie zabezpieczeń w postaci środków organizacyjnych, środków ochrony fizycznej oraz środków technicznych.

7. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w **firmie Administratora** rozumiane jest jako zapewnienie ich poufności, integralności, dostępności i odporności systemów i usług przetwarzania na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych. W ramach realizowanej przez administratora Polityki Bezpieczeństwa Przetwarzania Danych Osobowych sporządzono stosowną, wymaganą RODO Analizę Ryzyka.

8. Zastosowane zabezpieczenia mają służyć osiągnięciu poniższych celów:
   1) Poufność danych – zapewnienie, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom,
   2) Integralność danych – zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
   3) Dostępność danych – zapewnienie osiągalności danych i możliwości ich wykorzystania na żądanie , w założonym czasie, przez autoryzowany podmiot,
   4) Rozliczalność danych – zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
   5) Autentyczność danych – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana,
   6) Integralność (odporności) systemów i usług przetwarzania – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;

   7) Zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

9. Administrator przetwarza dane osobowe w następujących celach:

   - przetwarzanie jest niezbędne do wykonania umowy tj. Administrator sprzedaje utwory muzyczne oraz inne produkty i usługi za pośrednictwem sklepu internetowego. Przetwarzanie ma podstawę prawną w postaci zawartej z klientami umowy – Artykuł 6 ust. 1 lit b) RODO,
   - przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze – jak wynika z art. 86 § 1 Ordynacji podatkowej podatnicy zobowiązani do prowadzenia ksiąg podatkowych przechowują je oraz związane z ich prowadzeniem dokumenty do czasu upływu okresu przedawnienia zobowiązania podatkowego tj. 5 lat. Przechowywanie danych pracowników wynika natomiast z prawa regulującego kwestie nawiązywania stosunków pracy. Zgodnie z rozporządzeniem Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika (Dz. U. 1996.62.286) po ustaniu zatrudnienia pracodawca ma obowiązek przechowywania dokumentacji pracowniczej (akt osobowych) przez 50 lat, licząc od dnia zakończenia pracy a od 1 stycznia 2019 r. okres ten w odniesieniu do osób zatrudnionych od 1 stycznia 1999 r. , zostanie skrócony do 10 lat. Przetwarzanie jest realizowane w związku z prawnie usprawiedliwionym interesem Administratora, o którym mowa w Artykule 6 ust. 1 lit. f) RODO,
   - dane przetwarzane przez przedsiębiorstwo w pozostałych przypadkach są prawnie usprawiedliwione i służą zabezpieczeniu pozostałych interesów administratora m.in. w zakresie dochodzenia roszczeń

oraz wypełnienia pozostałych obowiązków narzuconych przez ustawodawcę (Artykuł 6 ust. 1 lit. f) RODO).

Administrator może wykorzystywać dane w celach marketingowych, w związku z czym Administrator przetwarza dane osobowe na podstawie zgody osób, których dane dotyczą (Artykuł 6 ust. 1 lit. a) RODO).

10. **Wnioski z analizy ryzyka:**

Administrator prowadzi działalność gospodarczą związaną ze sprzedażą utworów muzycznych oraz innych produktów i usług, co stanowi główny przedmiot działalności firmy. Ze względu na charakter prowadzonej działalności, firma na moment sporządzenia Polityki Bezpieczeństwa Przetwarzania Danych Osobowych oraz dokonania **analizy ryzyka** jest zwolniona z obowiązku przygotowania Oceny Skutków, o której mowa w Artykule 35 RODO.

W podmiocie o nazwie: **RAZ, DWA, TRZY RYTMIKA ANNA SZEWCZYK, Nowe Racibory, ul. Zielona 30, 05-555 Tarczyn** po przeprowadzeniu analizy poufności , integralności i rozliczalności systemów przetwarzania pod kątem zagrożeń i ryzyka, wartość i poziom ryzyka przedstawia się następująco:

Ryzyko ogólne wynosi: **31,2 / 100.**

Powyższa wartość ryzyka określa **Średnie** ryzyko utraty bezpieczeństwa danych osobowych.

Administrator stale podnosi wiedzę oraz umiejętności w celu wyeliminowania ryzyka, poprzez stałe prace nad zmniejszeniem prawdopodobieństwa zdarzenia oraz minimalizowania skali oddziaływania w przypadku ich wystąpienia.

II. Definicje

1. Przez użyte w Polityce Bezpieczeństwa Przetwarzania Danych Osobowych określenia należy rozumieć:

1) Polityka Bezpieczeństwa– rozumie się przez to Politykę Bezpieczeństwa Przetwarzania Danych Osobowych w **firmie Administratora** wraz z załącznikami.

2) Administrator Danych Osobowych (ADO) / Firma **–** Administratorem Danych Osobowych w rozumieniu niniejszej Polityki Bezpieczeństwa jest **RAZ, DWA, TRZY RYTMIKA ANNA SZEWCZYK, Nowe Racibory, ul. Zielona 30, 05-555 Tarczyn**

3) Biuro – Biuro Administratora Danych Osobowych;

4) Ustawa/U.o.d.o. – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;

5) RODO - Rozporządzeniu 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 [rozporządzenie ogólne o ochronie danych]

6) ePrivacy - Rozporządzeniu Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE

7) Dane osobowe– informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną , ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

8) Zbiór danych osobowych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

9) Baza danych osobowych – zbiór uporządkowanych powiązanych ze sobą tematycznie zapisanych np. w pamięci wewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze – rekordów lub obiektów, w których są zapisywane dane osobowe;

10) Usuwanie danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację , która nie pozwoli na ustalenie tożsamości osoby, której dotyczą.

11) Przetwarzanie danych- oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie ,organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie ,pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie ,rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie ,ograniczanie, usuwanie lub niszczenie;

12) Użytkownik - rozumie się przez to osobę wyznaczoną i upoważnioną przez Administratora danych do przetwarzania danych osobowych, przeszkoloną w zakresie ochrony tych danych.

13) Stacja robocza – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.

14) Podmiot Przetwarzający/Procesor - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu osoby fizycznej lub prawnej, organu publicznego, jednostki lub innego podmiotu, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

15) Profilowanie - oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych , które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

16) Współadministrator - podmiot wspólnie ustalający cele i sposoby przetwarzania.

17) Informacje Poufne - wszelkie ustne lub pisemne informacje, dokumenty, materiały czy procedury uzyskane od Strony, która udostępniła Informacje Poufne (Udostępniający) stronie, która je otrzymała (Odbiorca), w tym informacji, materiałów, procedur lub dokumentów dotyczących

Udostępniającego, kontrahentów, klientów, współpracowników, jak również wszelkich innych Informacji Poufnych nieujawnionych wcześniej publicznie przez Udostępniającego. Informacje Poufne obejmują w szczególności: dane osobowe (w rozumieniu RODO) oraz informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16.04.1993 r. o zwalczaniu nieuczciwej konkurencji.

18) System przetwarzania - należy przez to rozumieć metodologię przetwarzania danych osobowych przez administratora bez względu na formę (przetwarzanie manualne lub za pośrednictwem systemu informatycznego).

19) Koordynator Do Spraw Ochrony Danych Osobowych – w przypadku braku konieczności powoływania Inspektora Ochrony Danych Osobowych, powołana stosownym zarządzeniem przez Administratora osoba fizyczna (pracownik lub członek zarządu) odpowiedzialna za przestrzeganie Polityki Bezpieczeństwa Ochrony Danych Osobowych w firmie Administratora.

III. Cel i zakres Polityki

1. Ustawa o ochronie danych osobowych oraz RODO nakładają na Administratora Danych obowiązek stosowania odpowiednich środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych oraz zabezpieczenie ich między innymi przed udostępnieniem osobom nieupoważnionym, przetwarzaniem z naruszeniem ustawy, a także zmianą, utratą , uszkodzeniem lub zniszczeniem. Celem niniejszej Polityki Bezpieczeństwa Przetwarzania Danych osobowych jest opracowanie optymalnych i zgodnych z wymogami prawa zasad przetwarzania danych, których zbieranie i przetwarzanie jest niezbędne dla bieżącej działalności Administratora.

2. Polityka Bezpieczeństwa Przetwarzania Danych Osobowych została sporządzona z poszanowaniem treści stosownych umów powierzenia przetwarzania danych osobowych.

3. W firmie przetwarzane są przede wszystkim dane osobowe klientów oraz pracowników. Firma dopuszcza możliwość przetwarzania danych osób współpracujących z firmą na podstawie umów cywilnoprawnych. Firma przetwarza dane w wyłącznie prawnie usprawiedliwiony sposób.

4. Dane osobowe we wskazanych powyżej zbiorach danych są przetwarzane w postaci tradycyjnej (papierowej) oraz elektronicznej.

5. Politykę Bezpieczeństwa stosuje się przede wszystkim do:

   1) Wszystkich informacji dotyczących danych pracowników ADO oraz osób współpracujących z ADO na podstawie umów cywilnoprawnych, w tym danych osobowych i treści zawieranych umów.

   2) Wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji.

   3) Wszystkich informacji dotyczących danych klientów zainteresowanych usługami firmy.

   4) Informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych.

   5) Rejestru osób dopuszczonych do przetwarzania danych osobowych.

   6) Rejestru podmiotów przetwarzających.

   7) Wszystkich informacji przekazywanych przez klientów.

8) Innych dokumentów zawierających dane osobowe.

6. Zakres ochrony danych osobowych określony w Polityce Bezpieczeństwa ma zastosowanie również do:

   1) Wszystkich wdrażanych w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie.

   2) Wszystkich lokalizacji - pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie.

   3) Wszystkich osób świadczących pracę bądź usługi cywilnoprawne na rzecz Administratora Danych Osobowych, które uzyskały upoważnienie do przetwarzania danych osobowych.

7. Do stosowania zasad określonych w Polityce Bezpieczeństwa zobowiązani są wszyscy Użytkownicy danych, w tym w szczególności pracownicy ADO, zleceniobiorcy, podmioty przetwarzające oraz wszelkie inne osoby bądź firmy mające dostęp do informacji podlegających ochronie.

IV. Obowiązki i odpowiedzialność

1. Do najważniejszych obowiązków Administratora Danych (lub, jeżeli został powołany – Koordynatora Do Spraw Ochrony Danych Osobowych) należy:

   1) Organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami U.o.d.o., RODO oraz innych przepisów regulujących zasady bezpieczeństwa i ochrony danych osobowych;

   2) Zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki Bezpieczeństwa;

   3) Stosowanie się do wszelkich postanowień Polityki Bezpieczeństwa.

   4) Wydawanie i anulowanie upoważnień do przetwarzania danych osobowych;

   5) Przeprowadzanie szkoleń użytkowników przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe;

   6) Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;

   7) Prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych;

   8) Nadzór nad bezpieczeństwem danych osobowych;

   9) Kontrola działań pracowników pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych;

   10) Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych;

   11) Bieżący monitoring wszystkich baz danych oraz lokalizacji, w których przetwarzane są dane osobowe;

   10) Przeciwdziałanie próbom naruszenia bezpieczeństwa informacji;

   11) Zmiana lub usprawnianie procedur bezpieczeństwa i standardów zabezpieczeń;

   12) Prowadzenie profilaktyki antywirusowej.

13) Administrator dba o to aby przetwarzane dane osobowe były prawidłowe i w razie potrzeby uaktualniane; podejmuje wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.

14) ADO przestrzega postanowień umów powierzenia zawartych z m.in. biurami rachunkowymi czy firmami hostingowymi.

15) ADO zapewnia, aby dostęp do Danych Osobowych posiadały jedynie osoby, których rola w procesie wykonywania przez ADO Umowy z klientem wymaga dostępu do takich danych.

16) ADO zapewnia odpowiednią identyfikację i wyraźne oznaczenia wszystkich dokumentów lub nośników danych zawierających Dane Osobowe.

17) W przypadku zbierania danych osobowych od osoby, której one dotyczą, w wypadkach gdy zmieni się cel przetwarzania tych danych lub gdy osoba, której dane dotyczą wyrazi chęć uzyskania tych informacji, ADO zobowiązany jest do przesłania tej osobie informacji wymienionych w **Obowiązku Informacyjnym.**

2. Do najważniejszych obowiązków osób upoważnionych do przetwarzania danych osobowych należy:

1) Znajomość, zrozumienie i stosowanie w możliwie największym zakresie wszelkich dostępnych środków ochrony danych osobowych oraz uniemożliwienie osobom nieuprawnionym dostępu do swojej stacji roboczej;

2) Przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa oraz przyjętymi regulacjami;

3) Postępowania zgodnie z ustalonymi regulacjami wewnętrznymi dotyczącymi przetwarzania danych osobowych;

4) Zachowania w tajemnicy danych osobowych, do których uzyskały dostęp oraz informacji o sposobach ich zabezpieczenia;

5) Ochrony danych osobowych oraz systemów przetwarzania przed nieuprawnionym dostępem , ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;

6) Informowania Administratora Danych Osobowych o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe;

7) Zapoznanie się z Polityką Bezpieczeństwa przetwarzania danych osobowych wraz z załącznikami;

V. Zarządzanie ochroną danych osobowych

1. Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba przetwarzająca te dane w zakresie zgodnym z upoważnieniem oraz rolą sprawowaną w procesie przetwarzania danych.
2. Dostęp do danych osobowych powinien być przyznawany zgodnie z zasadą wiedzy koniecznej tj. Nie udostępnianiem tych danych, do których dostęp nie jest konieczny aby zrealizować zadanie.
3. Każda z osób mająca styczność z danymi osobowymi jest zobowiązana do ochrony danych osobowych oraz przetwarzania ich w granicach udzielonego jej upoważnienia.
4. Należy zapewnić poufność, integralność i rozliczalność przetwarzanych danych osobowych.
5. Należy stosować adekwatny do zmieniających się warunków i technologii poziom bezpieczeństwa przetwarzania danych osobowych.
6. Dane osobowe powinny być chronione przed nieuprawnionym dostępem i modyfikacją.
7. Dane osobowe należy przetwarzać wyłącznie za pomocą autoryzowanych urządzeń służbowych.
8. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie. Upoważnienia wydawane są indywidualnie przez Administratora Danych Osobowych.

VI. Szkolenia użytkowników

1. Każdy użytkownik przed dopuszczeniem do pracy winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach tradycyjnych (papierowych).
2. Za przeprowadzenie szkolenia odpowiada Administrator Danych Osobowych lub Koordynator Do Spraw Ochrony Danych.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz Polityką Bezpieczeństwa służącą do przetwarzania danych osobowych. Po zaznajomieniu się z powyższymi regulacjami, użytkownik, przed dopuszczeniem do przetwarzania danych, powinien zobowiązać się do ich przestrzegania.

VII. Upoważnienie do przetwarzania danych osobowych

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie.
2. Upoważnienia są wydawane indywidualnie przed rozpoczęciem przetwarzania danych osobowych przez Administratora Danych Osobowych.
3. Upoważnienie może być w każdym czasie odwołane przez Administratora Danych Osobowych. Oświadczenie o odwołaniu upoważnienia do przetwarzania danych osobowych powinno być sporządzone na piśmie. Upoważnienie do przetwarzania danych osobowych wygasa z chwilą ustania przesłanki będącej podstawą wydania upoważnienia, w tym w szczególności wygaśnięcia stosunku pracy lub umowy cywilnoprawnej łączącej Użytkownika z Administratorem Danych Osobowych.

VIII. Udostępnianie danych osobowych

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

IX. Dokonanie obowiązku informacyjnego

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

   a) Pełnej nazwie ADO i adresie siedziby;

   b) Celu zbierania danych, a w szczególności o znanych w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych;

   c) Prawie dostępu do swoich danych oraz ich poprawiania;

   d) Dobrowolności lub obowiązku podania danych - jeżeli taki obowiązek istnieje, o jego podstawie prawnej;

   e) Gdy ma to zastosowanie, dane Inspektora ochrony danych osobowych – **na moment sporządzenia Polityki Bezpieczeństwa Przetwarzania Danych Osobowych powołanie Inspektora Ochrony Danych Osobowych nie jest wymagane.**

   f) okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, o kryteriach ustalania tego okresu;

   g) informacji o prawie do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

   h) informacji o prawie wniesienia skargi do organu nadzorczego;

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

   j) jeżeli dotyczy: informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, istotnych informacji o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Ponadto:

1. Administrator bez zbędnej zwłoki, a w każdym razie w terminie miesiąca od otrzymania żądania, udziela osobie, której dane dotyczą powyższych informacji.
2. Jeżeli występuje przedłużenie terminu do spełnienia żądań osoby, której dane dotyczą, może to wystąpić jedynie z uwagi na skomplikowany charakter żądania lub liczbę żądań. Czas udzielenia informacji jednak nie może być dłuższy niż dalsze dwa miesiące.
3. Jeżeli administrator nie podejmuje działań w związku z żądaniem osoby której dane dotyczą, niezwłocznie lecz nie później niż w terminie miesiąca od otrzymania żądania informuje o:
   a) powodach niepodjęcia działań;
   b) możliwości wniesienia skargi do organu nadzorczego;
   c) skorzystania z ochrony prawnej przed sądem.
4. Jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby składającej żądanie, żąda dodatkowych informacji niezbędnych do potwierdzenia tożsamości.

Informacje wynikające z obowiązku informacyjnego, w przypadku zbierania danych osobowych nie od osoby, której dotyczą podawane są:

a) w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych;

b) 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 – najpóźniej przy ich pierwszym ujawnieniu.

X. Przetwarzanie danych osobowych. Wymagania bezpieczeństwa.

1. Dane osobowe mogą być przetwarzane wyłącznie w obszarze przetwarzania danych osobowych, na które składają się pomieszczenia biurowe w siedzibie ADO z wyjątkiem sytuacji udostępnienia danych osobowych lub powierzenia przetwarzania danych osobowych.
2. Dane osobowe w siedzibie ADO przetwarzane są przy zastosowaniu zabezpieczeń zapewniających ich ochronę w postaci środków organizacyjnych, technicznych i środków ochrony fizycznej.
3. Dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych stosuje się następujące środki:
   A. Środki organizacyjne i zalecenia:
      - wdrożenie Polityki Bezpieczeństwa wraz z załącznikami;
      - udzielanie upoważnień przez Administratora poprzedzone szkoleniem z zakresu przepisów i zasad ochrony danych osobowych;
      - zadbanie aby wszyscy pracownicy ADO wyznaczeni do korzystania ze sprzętu, lub systemu, lub aplikacji mają obowiązek podpisać stosowne indywidualne oświadczenia potwierdzające zobowiązanie do przestrzegania zasad ochrony danych osobowych określonych w umowach powierzenia
      - prowadzenie ewidencji osób uprawnionych do przetwarzania danych osobowych,

- stosowanie procedury postępowania w sytuacji naruszenia ochrony danych osobowych zgodnie z niniejszą Polityką Bezpieczeństwa
- dbanie aby pomieszczenia były zamykane na klucz,
- dbanie aby szafki na dokumenty były zamykane na klucz z zamkiem o adekwatnej do ryzyka trwałości i liczbie zastawek;
- stosowanie niszczarek rozrywających służących do utylizacji niepotrzebnych dokumentów;
- wyposażenie biurek w kuwetki uniemożliwiające wgląd w dokumentację poddaną bieżącej obróbce przez pracowników, jeżeli osoby te znajdują się w pomieszczeniu wyznaczonym do przetwarzania danych osobowych;
- zadbanie aby wszystkie dokumenty firmy w wersji papierowej zawierające dane osobowe przechowywane były w szafce zamykanej na klucz, w pomieszczeniu zamykanym na klucz po zakończeniu pracy;
- przy podpisywaniu umów z klientami unikanie kserowania, kopiowania ich dowodów osobistych jeżeli nie jest to konieczne do zawarcia umowy;
- prowadzenie utylizacji niepotrzebnych dokumentów zawierających dane osobowe;
- rozstawienie biurek pracowników w taki sposób, aby uniemożliwić wgląd przez osoby nieuprawnione;
- ustanowienie haseł na telefonach służbowych;
- przy wszystkich stanowiskach komputerowych utworzenie dedykowanych kont użytkowników zabezpieczonych hasłem w tym konto „Administrator" tylko w określonych celach administracyjnych;
- na komputerach firmowych uruchomienie wygaszaczy ekranu z opcją domyślną dotyczącą czasu uruchomienia;
- wdrożenie polityki nieinstalowania nieoryginalnego oprogramowania lub nieznanego pochodzenia;
- uregulowanie przetwarzania danych przez podmioty przetwarzające (biura rachunkowe, firmy serwisujące sprzęt IT itp.);
- utworzenie dedykowanych, pracowniczych kont email;

B. Środki techniczne:
- zbiory danych osobowych przetwarzane są wyłącznie na autoryzowanym sprzęcie służbowym;
- stacje robocze wyposażone są w indywidualną ochronę antywirusową;
- dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
- stosowanie bezpieczników oraz baterii UPS,
- okresowa kontrola stanu bezpieczników
- weryfikacja stanu technicznego sprzętu,
- serwery IT i inne urządzenia infrastruktury informatycznej muszą znajdować się w wyznaczonych pomieszczeniach komputerowych z kontrolą środowiska. Dodatkowo musi funkcjonować fizyczna kontrola dostępu, a dzienniki dostępu do obszarów chronionych muszą być monitorowane.
- aktualizacje zabezpieczeń (poprawki) są stosowane do systemów/urządzeń przechowujących lub przetwarzających dane,
- czynności administracyjne są rejestrowane i przeglądane okresowo, co najmniej raz na kwartał.

- dostęp do środowisk niekomercyjnych wymaga użycia unikalnych identyfikatorów i haseł a dzienniki systemowe do tych środowisk są przeglądane okresowo.
- dostęp do systemów przetwarzania jest formalnie monitorowany i regularnie poddawany przeglądowi w celu ustalenia, czy prawa dostępu są odpowiednie (przeglądy dokonywane, co najmniej raz w roku).

C. Środki ochrony fizycznej:

- Pomieszczenia, w których znajdują się zbiory danych osobowych, są zamykane na klucz, a dostęp do nich odbywa się wyłącznie w obecności pracowników firmy;
- Drzwi zwykłe (niewzmacniane, nie przeciwpożarowe) do pomieszczeń, w których przetwarzane są dane osobowe znajdują się wewnątrz budynku w strefie ograniczonego dostępu;
- Zbiór danych osobowych w formie papierowej przechowywany jest (w zależniości od charakteru danych osobowych) we wzmacnianej szafce zamykanej na klucz;
- Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej niemetalowej szafie;
- Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek rozrywających;

XI. Postępowanie w sytuacji naruszenia bezpieczeństwa danych osobowych

1. Każdy użytkownik w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest o tym poinformować Administratora Danych.

2. Do typowych zagrożeń bezpieczeństwa danych osobowych, określonych na podstawie Analizy Ryzyka, ze względu na utratę poufności mogą należeć:

   a) nieuprawniony dostęp do pomieszczenia, w którym przetwarzane są dane osobowe;

   b) ujawnienie haseł dostępu do stanowiska komputerowego, na którym przetwarzane są dane osobowe;

   c) nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik;

   d) utrata nośnika zawierającego dane osobowe;

   e) nieuprawnione wyniesienie danych osobowych zawartych na nośniku elektronicznym;

   f) udostępnianie danych osobowych osobom nieupoważnionym;

   g) wejście w posiadanie danych osobowych przez osobę nieuprawnioną;

   h) pokonanie zabezpieczeń fizycznych lub programowych;

   i) niekontrolowana obecność osób nieuprawnionych w obszarze przetwarzania danych osobowych;

   j) niedyskrecja osób uprawnionych do przetwarzania danych osobowych;

   k) nieuprawnione kopiowanie danych na nośniki informacji (CD, DVD, pendrive, itp.);

l) niekontrolowane wynoszenie poza obszar przetwarzania danych osobowych nośników informacji i komputerów przenośnych;

m) naprawy i konserwacje systemów lub sieci teleinformatycznej służących do przetwarzania danych osobowych przez osoby nieuprawnione do przetwarzania danych osobowych;

n) podsłuch lub podgląd danych osobowych;

o) zagubienie dokumentów lub utrata przetwarzanych informacji.

3. Do typowych zagrożeń bezpieczeństwa danych osobowych, określonych na podstawie Analizy Ryzyka, ze względu na utratę integralności mogą należeć:

a) nielegalny dostęp do danych osobowych, w tym do stanowiska komputerowego;

b) błędy, pomyłki;

c) brak mechanizmów uniemożliwiających skasowanie lub zmianę logów przez administratora lub innego użytkownika;

d) wadliwe działanie systemu operacyjnego;

e) brak w wykorzystywanych aplikacjach mechanizmów zapewniających integralność danych.

f) uszkodzenie, celowe lub przypadkowe systemu operacyjnego lub urządzeń sieciowych;

g) celowe lub przypadkowe uszkodzenie, zniszczenie lub nieuprawniona modyfikacja danych,

h) działanie złośliwego oprogramowania (wirusy);

i) pożar, zalanie, ekstremalna temperatura, itp.;

4. Do typowych zagrożeń bezpieczeństwa danych osobowych, określonych na podstawie Analizy Ryzyka, ze względu na utratę rozliczalności mogą należeć:

a) brak kontroli nad dokumentami wykonywanymi na stanowisku komputerowym w zakresie ich kopiowania i drukowania;

b) wprowadzenie zmian w treści dokumentu zawierającego dane osobowe;

c) błędy oprogramowania lub sprzętu;

d) nieprzydzielenie użytkownikom indywidualnych identyfikatorów;

e) niewłaściwa administracja systemem informatycznym;

f) niewłaściwa konfiguracja systemu informatycznego;

g) zniszczenie lub sfałszowanie logów systemowych;

h) brak rejestracji udostępnienia danych osobowych;

i) podszywanie się pod innego użytkownika.

5. W przypadku stwierdzenia wystąpienia zagrożenia, Administrator Danych prowadzi postępowanie wyjaśniające w toku którego:

1) Ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki;

2) Inicjuje ewentualne działania dyscyplinarne;

3) Rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości;

4) Dokumentuje prowadzone postępowania.

6. W przypadku stwierdzenia incydentu (naruszenia), Administrator Danych prowadzi postępowanie wyjaśniające, w toku którego:

1) Ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały;

2) Zabezpiecza ewentualne dowody;

3) Ustala osoby odpowiedzialne za naruszenie;

4) Podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody);

5) Inicjuje działania dyscyplinarne;

6) Wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości;

XII. Zgodność

Niniejsza Polityka powinna być aktualizowana wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi w firmie ADO które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.

XIII. Postanowienia końcowe

1. Administrator Danych ma obowiązek zapoznać z treścią Polityki każdego użytkownika.

2. Wszystkie regulacje określone w Polityce dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.

3. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce.

4. Wobec osoby, która w przypadku naruszenia lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.

5. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z ustawą oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

6. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy, RODO oraz ePrivacy.