POLITYKA BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

DLA FIRMY: Rondo Fitness Club Sp. z o.o.,

Prowadzącą działalność pod nazwa Rondo Fitness Club

w Piasecznie przy ul. Wojska Polskiego 30

Piaseczno, wrzesień 2018 r.

WPROWADZENIE

Zarząd spółki „Rondo Fitness Club Sp. z o.o." (dalej „ADO") świadomy wagi problemów związanych z ochroną danych osobowych, w tym w szczególności praw osób fizycznych przekazujących (pełna nazwa przedsiębiorstwa) swoje dane osobowe, w celu ich właściwej i skutecznej ochrony, postanawia:

- realizować działania niezbędne dla ochrony praw i usprawiedliwionych interesów (pełna nazwa przedsiębiorstwa) związanych z ochroną danych osobowych,

- stale podnosić świadomości oraz kwalifikację osób przetwarzających dane osobowe u ADO, w zakresie problematyki bezpieczeństwa danych osobowych,

- podejmować w niezbędnym zakresie współpracę z instytucjami powołanymi do ochrony danych osobowych.

ADO przetwarza dane osobowe w związku z prowadzeniem działalności gospodarczej.

ADO świadomy zagrożeń związanych z przetwarzaniem przez niego danych osobowych – w tym, w szczególności z zagrożeń wynikających z dynamicznego rozwoju metod i technik przetwarzania tych danych w systemach informatycznych oraz sieciach telekomunikacyjnych - na bieżąco doskonali i rozwija nowoczesne metody przetwarzania danych, w tym danych osobowych, doskonali i rozwija organizacyjne, techniczne oraz informatyczne środki ochrony danych osobowych przetwarzanych zarówno metodami tradycyjnymi jak i elektronicznie tak, aby skutecznie zapobiegać zagrożeniom, w szczególności zabezpieczać dane przed ich udostępnieniem osobom nieupoważnionym, przetwarzaniem z naruszeniem prawa, zmianą, utratą, uszkodzeniem lub zniszczeniem. W tym celu ADO wdraża i stosuje odpowiednie zabezpieczenia uwzględniające skalę, zakres oraz rodzaj przetwarzanych danych osobowych.

Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, ADO wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z przepisami Ogólnego Rozporządzenia o Ochronie Danych Osobowych z dnia 27 kwietnia 2016 r. (dalej „RODO"). Niniejsza Polityka Bezpieczeństwa jest tego wyrazem.

I. Osoby wyznaczone do realizacji polityki ochrony danych osobowych

ADO wyznacza osoby odpowiedzialne za realizację polityki bezpieczeństwa w zakresie ochrony danych osobowych w swoim przedsiębiorstwie, w tym również na terenie poszczególnych jednostek organizacyjnych (jeśli takowe będą funkcjonować). Bezpośrednią kontrolę na przestrzeganiem zasad ochrony danych osobowych u ADO sprawuje zarząd. Pomimo braku obowiązku wyznaczenia przez ADO Inspektora Ochrony Danych, ADO może zdecydować o powołaniu takiej osoby.

II. Obszary przetwarzania danych osobowych oraz rodzaj przetwarzanych danych osobowych

Przetwarzanie danych osobowych przez ADO może odbywać się w następujący sposób:

1) w formie papierowej na obszarze prowadzonej działalności gospodarczej, w szafach zamykanych na klucz z dostępem tylko dla osób upoważnionych przez ADO;
2) w formie elektronicznej za pośrednictwem urządzeń umieszczonych w miejscu prowadzenia działalności gospodarczej, zabezpieczonych kontrolą dostępu i za pomocą systemów teleinformatycznych.

ADO przetwarza następujące rodzaje danych osobowych:

1) Dane personalne i kontaktowe (imiona, nazwiska, daty urodzenia, numery telefonów komórkowych, adresy poczty elektronicznej etc.);
2) Dane fizyczne (waga, wzrost, wiek, płeć etc.);
3) Dane dotyczące zdrowia (informacje o przebytych zabiegach, dolegliwościach zdrowotnych, przyjmowane leki, tętno, ilość wody w organizmie, zawartość tłuszczu w organizmie etc.);
4) Dane dotyczące aktywności osób w klubach (ilość wizyt, ilość i rodzaj nabytych towarów bądź dodatkowych usług);
5) Dane dotyczące umowy i jej realizacji (rodzaj wykupionej usługi, długość obowiązywania umowy, warunki i sposób płatności, numer rachunku bankowego lub karty płatniczej).

Powyższe dane odnoszą się do danych osobowych klientów korzystających z usług ADO. Poza tymi osobami ADO może przetwarzać dane personalne, kontaktowe oraz inne dane wynikające z przepisów prawa, osób przez niego zatrudnianych lub podmiotów współpracujących.

Szczegółowe informacje dotyczące rodzaju przetwarzanych danych osobowych zostały umieszczone w Rejestrze Przetwarzania Danych Osobowych.

III. Wykonywanie przez ADO obowiązków związanych z prawami osób których dane są przetwarzane

ADO świadomy praw osób których dane dotyczą, umożliwia im w granicach przewidzianych przez RODO realizację następujących praw:

1) Prawo do informacji.

ADO wypełnia obowiązek informacyjny poprzez bieżące informowanie osób, których dane przetwarza, o wszelkich kwestiach związanych z przetwarzaniem danych osobowych tych osób; nadto obowiązek ten jest realizowany poprzez przekazywanie każdorazowej osobie udzielającej swoich danych osobowych pisemnych klauzul informacyjnych.

ADO bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z jej żądaniem. W razie potrzeby ADO może wskazany powyżej termin przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania ADO informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

Jeżeli ADO 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 nie podjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

ADO wypełnia swój obowiązek informacyjny wobec osób, których dane dotyczą bez pobierania jakichkolwiek opłat z zastrzeżeniem, iż jeżeli żądania osoby, której dane dotyczą są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, ADO może:

a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo

b) odmówić podjęcia działań w związku z żądaniem.

Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na ADO.

Jeżeli ADO ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie dotyczące jej danych osobowych, powinien zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą. W tym celu ADO może wprowadzić wybraną przez siebie formę identyfikacji osoby, która domaga się udzielenia informacji o danych osobowych, w taki sposób, aby ograniczyć udzielanie informacji osobom nieuprawnionym i zapewnić odpowiednią ochronę przed wyciekiem danych. Żądanie dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą powinno odbywać się w szczególności w wypadku, gdy udzielenie informacji obejmujących dane osobowe ma miejsce z wykorzystaniem form komunikacji na odległość (telefon, poczta elektroniczna). Przekazywanie danych osobowych w plikach, za pośrednictwem poczty elektronicznej powinno być w miarę możliwości szyfrowane, w sposób uniemożliwiający dostęp do tych danych osobom nieuprawnionym.

Na żądanie osoby której dane dotyczą ADO dostarcza tej osobie, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, ADO może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.

2. <u>Prawo do sprostowania, usuwania oraz ograniczenia przetwarzania danych osobowych.</u>

Osoba, której dane dotyczą, ma prawo żądania od ADO niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

Osoba, której dane dotyczą, ma prawo żądania od ADO niezwłocznego usunięcia dotyczących jej danych osobowych, a ADO ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

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

b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO i nie ma innej podstawy prawnej przetwarzania;

c) osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 RODO wobec przetwarzania;

d) dane osobowe były przetwarzane niezgodnie z prawem;

e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega ADO;

f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 RODO.

Jeżeli ADO upublicznił dane osobowe, a ma obowiązek usunąć te dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe lub podmioty który powierzył te dane osobowe do przetwarzania, że osoba, której dane dotyczą, żąda, by podmioty te usunęły wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje. W przypadku, gdy ADO posiada odpowiednie narzędzia techniczne, z uwagi na zależności i powiazania z Milon Care GmbH związane z kompleksowym świadczeniem usług na rzecz swoich klientów, ADO samodzielnie usuwa dane z systemu MilonCare, które zostały umieszczone przez niego w tym systemie. ADO informuje osobę której dane dotyczą, na jej żądanie, o każdorazowym usunięciu jej danych osobowych, w sposób wyraźny w formie pisemnej lub elektronicznej. Sposób usuwania danych z systemów informatycznych w których są przetwarzane odbywa się zgodnie z procedurą i funkcjonalnościami danego systemu. Usuwanie danych osobowych powinno mieć charakter definitywny, uniemożliwiający ich następcze odtworzenie.

Prawo żądania usunięcia danych osobowych nie ma zastosowania i nie może być skutecznie wykonane, w zakresie w jakim przetwarzanie jest niezbędne, w szczególności:

a) do korzystania z prawa do wolności wypowiedzi i informacji;

b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega ADO, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej ADO;

c) do ustalenia, dochodzenia lub obrony roszczeń.

Osoba, której dane dotyczą, ma prawo żądania od ADO ograniczenia przetwarzania w następujących przypadkach:

a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający ADO sprawdzić prawidłowość tych danych;

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

c) ADO nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;

d) osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie ADO są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

Jeżeli przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub jej państwa członkowskiego.

Przed uchyleniem ograniczenia przetwarzania ADO informuje o tym osobę, której dane dotyczą, która żądała ograniczenia przetwarzania jej danych osobowych.

ADO informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. ADO informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

3. Prawo do przenoszalności danych.

Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego (przy użyciu komputera) dane osobowe jej dotyczące, które dostarczyła ADO, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony ADO, któremu dostarczono te dane osobowe, jeżeli:

a) przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a) RODO lub art. 9 ust. 2 lit. a) RODO lub na podstawie umowy w myśl art. 6 ust. 1 lit. b) RODO; oraz

b) przetwarzanie odbywa się w sposób zautomatyzowany.

Wykonując prawo do przenoszenia danych osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez ADO bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

4. Prawo do sprzeciwu.

Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f) RODO, tj. przetwarzania jej danych osobowych m.in. w celach marketingu bezpośredniego lub w celach dochodzenia roszczeń, w tym profilowania na podstawie tych przepisów.

ADO nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim. Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.

IV. Powierzanie przetwarzania danych osobowych na rzecz podmiotów trzecich (procesorów)

W związku z realizacją usług na rzecz swoich klientów ADO będzie powierzać do przetwarzania dane osobowe na rzecz podmiotów trzecich (procesorów).

Przetwarzanie powierzonych danych osobowych odbywa się na podstawie stosownych umów zawieranych pomiędzy ADO, a procesorem, zgodnych z wymaganiami określonymi w RODO.

ADO korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

V. Zgłaszanie naruszeń oraz prowadzenie rejestru naruszeń

W przypadku naruszenia ochrony danych osobowych, ADO bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je właściwemu organowi nadzorczemu tj. Prezesowi Urzędu Ochrony Danych Osobowych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

Zgłoszenie, o którym mowa powyżej musi co najmniej:

a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;

d) opisywać środki zastosowane lub proponowane przez ADO w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, ADO udziela ich sukcesywnie bez zbędnej zwłoki.

ADO dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze poprzez prowadzenie Rejestru Naruszeń Danych Osobowych.

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

Zawiadomienie, o którym mowa powyżej, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej:

a) imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

b) opis możliwych konsekwencji naruszenia ochrony danych osobowych;

c) opis środków zastosowanych lub proponowanych przez ADO w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Zawiadomienie, osób których dane osobowe zostały naruszone nie jest wymagane, w następujących przypadkach:

a) ADO wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

b) ADO zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,

c) wymagałoby ono niewspółmiernie dużego wysiłku.

W takim przypadku ADO wydaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

VI. Nadawanie uprawnień do przetwarzania danych

ADO zapewnia kontrolę nad dostępem do przetwarzania danych osobowych, która w szczególności realizowana jest poprzez ewidencjonowanie osób przetwarzających dane osobowe oraz wdrożenie procedur udzielania dostępu do tych danych.

Uprawnienia do przetwarzania danych osobowych nadawane są przez właściciela przedsiębiorstwa, organ zarządzający albo osobę upoważnioną w imieniu takiej osoby lub podmiotu do tych czynności. Nadawanie uprawnień może również przysługiwać inspektorowi ochrony danych osobowych, o ile osoba taka zostanie powołana przez ADO. Uprawnienia dotyczą zarówno danych osobowych gromadzonych w systemie informatycznym, jak również w tradycyjnych rejestrach papierowych.

ADO lub wyznaczony do tego podmiot lub osoba, prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych, zawierający imię i nazwisko oraz identyfikator (login) osoby upoważnionej, datę nadania i ustania oraz zakres uprawnień do danych osobowych.

Uprawnienia, do przetwarzania danych osobowych nadawane są przed przystąpieniem osoby do pracy na danych osobowych oraz odbierane są w przypadku naruszenia ochrony

danych osobowych przez tą osobę, ustania stosunku pracy lub rozwiązania albo wygaśnięcia umowy cywilnoprawnej tej osoby z ADO.

Osoby, które otrzymują upoważnienie (Użytkownicy) zobowiązane są zapoznać się z niniejszą Polityką Bezpieczeństwa Danych Osobowych obowiązującą w przedsiębiorstwie ADO oraz złożyć oświadczenie o zobowiązaniu się do ich przestrzegania.

Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia.

Nadawanie uprawnień do przetwarzania danych osobowych w systemie informatycznym następuje poprzez przekazanie indywidualnych loginów oraz haseł na rzecz osób upoważnianych do przetwarzania danych osobowych.

VII. Zasady Użytkownika upoważnionego do przetwarzania danych osobowych w przedsiębiorstwie ADO

Mając na uwadze zagwarantowanie wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych oraz zagwarantowania Użytkownikom pełnej rozliczalności wykonywanych przez nich operacji w systemie informatycznym, wszyscy Użytkownicy przy uwierzytelnianiu do systemów informatycznych powinni stosować się do poniższych zasad:

a) Użytkownik systemu powinien posiadać unikalny identyfikator (login) do swojego osobistego i wyłącznego użytku,
b) Hasła dostępu do systemów informatycznych stanowią tajemnicę służbową,
c) Użytkownik ponosi pełną odpowiedzialność za utrzymanie poufności hasła oraz jego przechowywanie,
d) Hasła nie mogą być ujawniane lub przekazywane komukolwiek, za wyjątkiem lub wyraźną zgodą Administratora Danych Osobowych;
e) Użytkownik nie powinien przechowywać haseł w widocznych miejscach, nie powinien umieszczać haseł w żadnych automatycznych procesach logowania (skryptach, makrach lub pod klawiszami funkcyjnymi),
f) Użytkownicy są odpowiedzialni za wszelkie działania w systemach informatycznych prowadzone z użyciem ich identyfikatora i hasła,
g) Użytkownik ma obowiązek zmieniać hasło nadane po raz pierwszy przez Administratora Danych Osobowych, nie rzadziej niż raz na kwartał;
h) Hasła nie mogą być takie same jak identyfikator użytkownika oraz nie mogą być zapisywane w systemach w postaci jawnej,
i) Udostępnienie hasła osobie postronnej należy traktować jak poważny incydent naruszenia ochrony danych osobowych;
j) Użytkownik powinien dokonywać tylko takich operacji na danych osobowych w systemach informatycznych, jakie wymagane są do celów związanych z prawidłowym świadczeniem usług na rzecz klientów lub ich wyraźnym żądaniem;
k) Użytkownikowi nie wolno dokonywać na danych czynności mogących zagrozić ich integralności lub wyciekowi, w szczególności użytkownikowi nie wolno powielać, kopiować, transferować danych poza system informatyczny; powyższe nie dotyczy czynności dozwolonych przepisami prawa w tym przesyłania danych do podmiotów na rzecz których dane osobowe zostały powierzone do przetwarzania lub generowania danych na żądanie klienta i przesyłania ich do wskazanych przez niego podmiotów (w ramach prawa do przenoszalności danych osobowych).

l) Korzystanie z systemów informatycznych powinno odbywać się w sposób uniemożliwiający dostęp lub podgląd danych przez osoby nieupoważnione i winno być zakończone poprzez każdorazowe wylogowanie się z systemu przez upoważnionego Użytkownika.

VIII. Bezpieczna eksploatacja systemów informatycznych

Bezpieczna eksploatacja systemów informatycznych przetwarzających dane osobowe, zostaje zapewniona poprzez przestrzeganie następujących zasad:

a) Użytkownikom zabrania się bez zgody ADO, wprowadzania zmian do oprogramowania, sprzętu informatycznego poprzez jego samodzielne konfigurowanie i wyposażanie;
b) Użytkownikom zabrania się, umożliwiania stronom trzecim uzyskiwania nieupoważnionego dostępu do systemów informatycznych;
c) Użytkownikom nie wolno samodzielnie instalować nowego lub aktualizować już zainstalowanego oprogramowania, chyba że uzyskali na to wyraźną zgodę od ADO;
d) Użytkownikom nie wolno korzystać z systemów informatycznych dla celów innych niż związane z wykonywaniem obowiązków służbowych,
e) Użytkownikom nie wolno korzystać z prywatnego sprzętu informatycznego, w tym oprogramowania oraz nośników pamięci,
f) Użytkownikom nie wolno podejmować prób testowania, modyfikacji i naruszenia zabezpieczeń systemów informatycznych lub jakichkolwiek działań noszących takie znamiona,
g) Nieautoryzowane podłączenie własnego lub należącego do osoby trzeciej urządzenia teleinformatycznego do systemu informatycznego jest zabronione,
h) Użytkownicy przed dopuszczeniem do obsługi systemu informatycznego, w którym przetwarzane są dane osobowe, powinni podlegać przeszkoleniu w zakresie obsługi sprzętu informatycznego, oprogramowania systemowego oraz oprogramowania do obsługi aplikacji, którą będą wykorzystywali.

IX. Kopie zapasowe

Kopie zapasowe zbiorów danych osobowych przetwarzanych w systemach informatycznych, programach lub narzędziach programowych służących do ich przetwarzania powinny być wykonywane na bieżąco przez ADO lub przez podmioty dostarczające usługi korzystania z takich systemów tj. procesorów.

Kopie zapasowe powinny być tworzone na nośnikach magnetycznych, odpowiednio opisanych, oznakowanych i ewidencjonowanych a każdy proces wykonywania kopii zapasowej powinien być dokumentowany.

Kopie zapasowe należy opisywać w sposób umożliwiający szybką i jednoznaczną identyfikację zawartych w nich danych.

Tworzenie, przechowywanie i likwidację kopii zapasowych powinny regulować szczegółowe instrukcje operacyjne dla poszczególnych systemów informatycznych. W tym zakresie ADO zobowiązuje się zapewnić stosowne wykonywanie kopii zapasowych danych osobowych przetwarzanych w systemach informatycznych dostarczanych przez procesorów.

Kopie zapasowe, które uległy uszkodzeniu powinny podlegać natychmiastowemu zniszczeniu. Niszczenia kopii zapasowych, na nośnikach magnetycznych dokonuje ADO

lub inna upoważniona przez niego osoba. Proces niszczenia kopi zapasowych powinien odbywać się komisyjnie i powinien być dokumentowany.

X. Ochrona systemów informatycznych przed działaniem szkodliwego oprogramowania

Na każdej stacji roboczej w sieci oraz serwerze przetwarzającym dane osobowe powinno być zainstalowane oprogramowanie antywirusowe skanujące na bieżąco system informatyczny.

ADO jest zobowiązany wymóc na podmiotach na rzecz których, dochodzi do powierzenia przetwarzania danych osobowych z wykorzystaniem ich systemów informatycznych, posiadanie i aktualizowane programów antywirusowych zabezpieczających ich systemy informatyczne lub serwery na których przetwarzane są dane osobowe.

XI. Zasady postępowania z komputerami przenośnymi

Osoba używająca komputera przenośnego lub innego urządzenia zawierającego dane osobowe zobowiązana jest zachować szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych.

Osoba ta w szczególności powinna:

a) stosować ochronę kryptograficzną wobec danych osobowych przetwarzanych na komputerze przenośnym,
b) zabezpieczyć dostęp do komputera na poziomie systemu operacyjnego - identyfikator i hasło,
c) nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych,
d) nie wykorzystywać komputera przenośnego do przetwarzania danych osobowych w obszarach użyteczności publicznej,
e) zachować szczególną ostrożność przy podłączaniu do sieci publicznych poza obszarem przetwarzania danych osobowych. W przypadku podłączania komputera przenośnego do sieci publicznej poza siecią ADO należy zastosować firewall zainstalowany bezpośrednio na tym komputerze oraz system antywirusowy,
f) Użytkownik powinien zachować wyjątkową ostrożność podczas korzystania z zasobów sieci publicznej.

Za wszelkie działania wykonywane na komputerze przenośnym odpowiada jego formalny użytkownik.

XII. Retencja danych osobowych

ADO przechowuje dane osobowe przez okres:

1) całkowitego korzystania przez osobę udzielającą danych z usług ADO, a w przypadku ich zaprzestania i braku ostatecznego zawarcia umowy z ADO, przez okres miesiąca od ostatniego dnia w którym możliwe było skorzystanie przez osobę udzielającą danych z usług ADO;

2) realizacji oraz całkowitego rozliczenia umowy zawartej z ADO, w tym wygaśnięcia roszczeń z jej tytułu, nie dłużej jednak niż przez czas przedawnienia roszczeń obu stron z tytułu zawartej umowy wyznaczonych przepisami prawa;
3) do czasu odwołania zgody przez osobę udzielającą danych osobowych, co do których zgoda ta została uprzednio udzielona, np. w zakresie wysyłania treści marketingowych drogą elektroniczną;
4) trwania usprawiedliwionego celu po stronie ADO;
5) wyznaczony przez przepisy prawa, obligujące ADO do przechowywanie tych danych.

Każdorazowe usunięcie (baz, zbiorów, pojedynczych rekordów) danych zarówno po upływie czasu w jakim można było je przetwarzać, jak i na żądanie osób których dane dotyczą, powinno zostać odnotowane w sposób umożliwiający następcze uzyskanie informacji o:

- czasie usunięcia tych danych,

- rodzaju i ilości danych

- osobie która dokonała usunięcia danych.

W przypadku likwidacji elektronicznych nośników informacji, należy dokonać wcześniej skutecznego usunięcia danych z tych nośników. W przypadku gdy usunięcie danych nie jest możliwe, należy uszkodzić nośniki w sposób uniemożliwiający odczyt tych danych. Przed przekazaniem elektronicznego nośnika informacji osobie nieuprawnionej, należy usunąć z nośnika dane osobowe.