SUPRA BROKERS ®

POLITYKA OCHRONY DANYCH OSOBOWYCH SUPRA BROKERS S.A Z SIEDZIBĄ WE WROCŁAWIU

Wrocław, dnia 24.05.2018r.

Spis treści

I. Cel powstania dokumentu

1.1. Niniejsza Polityka ochrony danych osobowych (dalej: Polityka) została opracowana w celu wdrożenia w spółce zasad ochrony i nadzoru przetwarzania danych osobowych zgodnie z Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE oraz ustawą o ochronie danych osobowych.

1.2. Każdy pracownik oraz współpracownik spółki zobowiązany jest przed rozpoczęciem wykonywania obowiązków służbowych lub rozpoczęciem współpracy ze spółką zapoznać się z treścią niniejszej Polityki. Ponadto zobowiązany jest wykonując obowiązki służbowe lub realizując umowę cywilnoprawną przestrzegać zasad i procedur opisanych w jej treści oraz powszechnie obowiązujących przepisach prawa.

II. Sposób przechowywania, udostępniania oraz aktualizacji treści polityki

2.1. Niniejszy dokument z uwagi na konieczność jego aktualizacji oraz większą dostępność dla pracowników i współpracowników spółki prowadzony jest w formie elektronicznej. Dodatkowo w formie papierowej przechowany jest przez ADO wraz z dokumentacją dotyczącą ochrony danych osobowych.
Dokument jest regularnie aktualizowany o treści wynikające z regulacji prawnych, wytyczne dotyczące stosowania przepisów oraz zmiany zachodzące w strukturze spółki. Propozycja zmian każdorazowo zatwierdzana jest przez ADO. Raz w roku, nie później niż do końca stycznia dokonywany jest audyt treści polityki.

2.2. Dokument ten udostępniany jest pracownikom i współpracownikom spółki do zapoznania przed podjęciem zatrudnienia lub współpracy ze spółką. Dokument w wersji elektronicznej udostępniony jest także do wglądu pracowników i współpracowników w systemie Doradca.

III. Definicje

Przepisy o ochronie danych osobowych- pod tym pojęciem rozumiemy 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 oraz ustawę o ochronie danych osobowych, zatwierdzone kodeksy dobrych praktyk.
RODO- 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 z dnia 27 kwietnia 2016 r.
Administrator Danych Osobowych (dalej ADO) – należy przez to rozumieć Zarząd Supra Brokers S.A z siedzibą we Wrocławiu, Aleja Śląska 1– reprezentujący spółkę zgodnie ze sposobem reprezentacji wskazanym w Krajowym Rejestrze Sądowym.
Inspektor Ochrony Danych Osobowych (IODO) – Łukasz Czerniak, tel. 785 839 270, e-mail: l.czerniak@suprabrokers.pl.
Dane Osobowe – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą") 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;

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;

System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych

Państwo trzecie – państwo nienależące do Europejskiego Obszaru Gospodarczego

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

Użytkownik systemu informatycznego- pracownik lub współpracownik spółki, któremu nadane zostało przez ADO upoważnienie do przetwarzania danych oraz polecenie przetwarzania danych w systemach informatycznych.

Minimalizacja danych- zgodnie z tą zasadą dane musza być adekwatne, stosowne oraz ograniczone tylko do tego co jest niezbędne do realizacji przez ADO celów przetwarzania danych osobowych.

Zbiór danych - oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

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.

Naruszenie ochrony danych osobowych- oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Kodeks dobrych praktyk- zespół zasad opracowanych przez dany sektor rynku dotyczących przetwarzania danych osobowych, zatwierdzony przez organ nadzoru.

Procesor- FCG Fiscal Consulting Group Waldemar Brysz odpowiedzialny za obsługę kadrowo-księgową oraz Space One odpowiedzialny za wsparcie IT.

IV. Cele przetwarzania

4.1. Supra Brokers S.A przetwarza dane osobowe w celu realizacji zawartych z klientami umów serwisu brokerskiego oraz realizacji udzielonego pełnomocnictwa zgodnie z przepisami ustawy z dnia 22 maja 2003r. o pośrednictwie ubezpieczeniowym. W szczególności:

Czynność	Cel przetwarzania	Podstawa prawna
Obsługa klientów	realizacja umowy serwisu brokerskiego (dane kontaktowe do wyznaczonych osób)	art. 6 ust. 1b
Zatrudnienie pracowników	zatrudnienia pracownika i realizacji umowy o prace, zlecenia i wynikających z tego obowiązków	art. 6 ust. 1b i c
Rozpatrzenie poprawności	w celu rozpatrzenia poprawności decyzji	art. 6 ust.1 a

decyzji nnw	wydanej w sprawie indywidualnej (ubezpieczeniach na życie, nnw)	
Zgłoszenie szkody	w celu zgłoszenia szkody komunikacyjnej klienta	art. 6 ust. 1b
Zgłoszenie szkody	zgłoszenie szkody medycznej	art. 6 ust. 1b
Zgłoszenie szkody	zgłoszenie szkody z oc dróg	art. 6 ust. 1b
Zgłoszenie szkody	w celu zgłoszenia szkody z ubezpieczenia NNW dzieci	art. 6 ust.1 a
Ewidencjonowanie osób przebywających na terenie biura	prowadzenie listy osób odwiedzających spółkę	art. 6 ust. 1f
Zgłoszenie do ubezpieczenia zdrowotnego	w celu zgłoszenia pracownika do ubezpieczenia zdrowotnego (opieki medycznej)	art. 6 ust. 1c
Zgłoszenie do karty benefit	w celu skorzystania z karty multisport	art. 6 ust. 1c
Realizacja szkolenia u klienta	sporządzenia listy obecności na wykładzie organizowanym w siedzibie klienta	art. 6 ust. 1a
Obsługa klienta w ramach umowy	zawarcie umowy ubezpieczenia strażaków	art.6 ust.1b
Zgłoszenie osób wykonujących czynności brokerskie	zgłoszenie do KNF osób wykonujących czynności brokerskie	art. 6 ust. 1c
Działalność Klubu Supra	generowanie certyfikatu uczestnictwa w szkoleniu oraz korzystanie z bazy wiedzy Klubu Supra	art. 6 ust. 1a
Czynności związane z działalnością spółki kapitałowej	dane wspólników, członków zarządu, Rady Nadzorczej	art. 6 ust. 1c

V. Podstawy prawne przetwarzania danych

Supra Brokers S.A przetwarza dane osobowe na podstawie:
a) zgody udzielonej przez osobę fizyczną (art. 6 ust.1a RODO);
b) w celu wykonania umowy darowizny, zlecenia (art.6 ust.1b RODO);
c) wypełnienia obowiązku prawnego ciążącego na administratorze (art.6ust.1c RODO);

VI. Obowiązek informacyjny wobec osób, których dane są przetwarzane

6.1. Zgodnie z art. 13 i 14 RODO w zależności od rodzaju przetwarzania danych, w szczególności celu, podstawy prawnej, zakresu administrator informuje osobę fizyczną, od której pozyskuje bezpośrednio dane o:

a) swojej tożsamości w szczególności nazwie, adresie, danych kontaktowych,
b) danych kontaktowych Inspektora Ochrony Danych Osobowych;
c) celu przetwarzania danych osobowych,
d) podstawie prawnej przetwarzania,
e) odbiorcach danych;
f) jeżeli ma to zastosowanie informacji o prawnie uzasadnionym interesie administratora;
g) zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
h) okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

i) prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
j) prawie do cofnięcia zgody na przetwarzanie danych w dowolnym momencie;
k) prawie wniesienia skargi do organu nadzorczego;
l) 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;
m) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu;

6.2. Dodatkowo w przypadku pośredniego pozyskiwania danych osobowych administrator powinien poinformować o:

a) kategorii odnośnych danych osobowych;
b) źródle pochodzenia danych osobowych, a gdy ma to zastosowanie - czy pochodzą one ze źródeł publicznie dostępnych;

6.3. W przypadku danych osobowych pozyskanych pośrednio informacja w w/w zakresie przekazywana jest najpóźniej w ciągu miesiąca od ich pozyskania, a w przypadku gdy dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą - najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą.

6.4. Niniejszy obowiązek realizowany jest względem pracowników spółki, klientów, z którymi zawarta zostaje umowa serwisu brokerskiego, kontrahentów, klientów zgłaszających szkody do likwidacji, osób, które wspieramy w przygotowaniu odwołania od decyzji ubezpieczeniowej. Obowiązek niniejszy realizowany jest w każdym wypadku pozyskania danych poprzez przekazanie takiej osobie podczas procesu pozyskiwania danych informacji sporządzonej w formie dokumentu. Dodatkowo administrator lub pracownik administratora pozyskując dane udziela osobie fizycznej wszelkich niezbędnych wyjaśnień oraz odpowiada na wszelkie zadane mu pytania. Niniejszy dokument przekazywany jest w formie papierowej lub drogą mailową w przypadku takiej formy kontaktu.

6.5. Zawierając umowę serwisu brokerskiego lub podpisując pełnomocnictwo z nowym klientem ADO przekazuje mu informacje, o których mowa w niniejszym pkt polityki oraz zawiera z nim umowę powierzenia przetwarzania danych osobowych.

VII. Umowy powierzenia danych osobowych.

Z klientami zostały podpisane umowy powierzenia przetwarzania danych osobowych. W ich treści administratorzy danych przekazali Supra Brokers S.A polecenie do przetwarzania danych osobowych. Spółka podpisała również umowy powierzenia przetwarzania danych osobowych ze swoimi dostawcami, kontrahentami i usługodawcami.

VIII. Procedury realizacji praw osoby, której dane osobowe są przetwarzane.

8.1. *Prawo dostępu osoby fizycznej do swoich danych osobowych.*

8.1.1 Osoba fizyczna, która chce uzyskać informacje czy jej dane osobowe są przetwarzane przez spółkę, w jaki celu, na jakiej podstawie prawnej lub w jakim zakresie, składa za pośrednictwem

udostępnionego na stronie internetowej adresu mailowego lub telefonicznie na numer spółki lub adres mailowy i numer telefonu IODO wniosek o udostępnienie tych informacji.
8.1.2. ADO lub IODO powinien dokonać weryfikacji tożsamości wnioskodawcy, w szczególności gdy osoba ta nie podała informacji umożliwiających dokonanie takiej weryfikacji.
8.1.3. ADO lub w jego imieniu IODO powinien udzielić odpowiedzi na wniosek pisemnie drogą mailową na adres wnioskodawcy niezwłocznie, w każdym razie nie dłużej niż w terminie miesiąca od otrzymania żądania. W szczególnych sytuacjach termin ten może zostać przedłużony nie dłużej niż na kolejne 2 miesiące. O konieczności przedłużenia terminu ADO informuje wnioskodawcę.
8.1.4. Jeżeli wnioskodawca żąda udzielenia odpowiedzi ustnie, ADO powinien udzielić odpowiedzi w takiej formie odnotowując jednocześnie datę i formę przekazania informacji.
8.1.5. W miarę możliwości administrator powinien umożliwić wnioskodawcy zdalny dostęp do sytemu, w którym przetwarzane są jej dane tak by nie naruszyć tajemnicy handlowej, ochrony danych osobowych innych klientów oraz praw autorskich chroniących oprogramowanie. W przypadku skierowania takiego wniosku ADO podejmuje decyzje o takiej formie udostępnienia informacji.
8.1.6. Fakt zgłoszenia żądania oraz realizacji tego prawa przez ADO zostaje odnotowywany w prowadzonym przez ADO rejestrze realizacji praw osób fizycznych prowadzonego w celu realizacji uzasadnionego interesu ADO polegającego na zabezpieczaniu spółki przed roszczeniami osób fizycznych wynikających ze sposobu realizacji przysługujących im praw. W systemie Doradca tworzona jest w tym samym celu procedura.

8.2. Prawo do sprostowania danych osobowych

8.2.1. W przypadku skorzystania przez osobę fizyczną, której dane dotyczą z prawa do sprostowania i uzupełnienia, ADO zobowiązany jest do spełnienia żądań tej osoby wyłącznie w sytuacji, gdy wnioskodawca wykaże, że dane osobowe dotyczące jego osoby są nieprawidłowe lub niekompletne.
Dane nieprawidłowe – dane, które nie odpowiadają rzeczywistemu stanowi rzeczy.
Dane niekompletne – to dane prawidłowe, ale niepełne co do swojego zakresu.
8.2.2. Jeżeli osoba fizyczna wykaże, że ADO przetwarza dane nieprawidłowe lub niekompletne, ADO niezwłocznie dokonuje sprostowania bądź uzupełnienia danych osobowych.
8.2.3. ADO w sytuacji, w której dochodzi do sprostowania bądź uzupełnienia danych osobowych osoby fizycznej ma obowiązek poinformować każdego odbiorcę, któremu dane ujawniono o fakcie sprostowania bądź uzupełnienia danych osobowych. Z tego obowiązku ADO zwolniony jest wówczas, jeżeli czynność ta wymagałaby niewspółmiernie dużego wysiłku bądź byłaby niemożliwa do wykonania.
8.2.4. Jeżeli ADO nie uczyni zadość żądaniu osoby fizycznej, której dane dotyczą ma ona prawo do zwrócenia się do organu nadzorczego z wnioskiem o nakazanie ADO zadośćuczynienia żądaniu

8.3. Prawo do usunięcia danych

8.3.1.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) RODO 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.

8.3.2.. Jeżeli ADO upublicznił dane osobowe ma obowiązek usunąć te dane, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

8.3.3. Powyższe nie ma zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:

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 administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
c) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) RODO oraz i) i art. 9 ust. 3 RODO;
d) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, o ile prawdopodobne jest, że prawo do osoby do usunięcia danych, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub
e) do ustalenia, dochodzenia lub obrony roszczeń.

8.4. Prawo do ograniczenia przetwarzania danych

8.4.1. ADO jest zobowiązany do ograniczenia przetwarzania danych, jeżeli zaistnieje jedna z następujących przesłanek:

1) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych, zgodnie z art. 16 RODO; w takim przypadku ograniczenie przetwarzania następuje automatycznie, na okres pozwalający ADO sprawdzić prawidłowość tych danych;
2) osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych przetwarzanych niezgodnie z prawem (nie istnieje żadna podstawa przetwarzania danych z art. 6 albo art. 9 RODO), żądając w zamian ograniczenia ich wykorzystywania;
3) osoba, której dane dotyczą, zażąda od ADO danych zastosowania ograniczenia przetwarzania w stosunku do danych, które zgodnie z zasadą ograniczenia przechowywania danych powinny zostać usunięte, ale które są potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń przysługujących tej osobie lub wobec niej;
4) został wniesiony sprzeciw wobec przetwarzania danych osobowych zgodnie z art. 21 ust. 1 RODO; w takim przypadku ograniczenie przetwarzania następuje automatycznie, na okres pozwalający ADO stwierdzić, czy prawnie uzasadnione podstawy po stronie ADO są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą, tj. na czas potrzebny do ustalenia, czy sprzeciw jest zasadny.

8.4.2. Ograniczenie przetwarzania danych osobowych polega na konieczności ograniczenia przetwarzania danych wyłącznie do ich przechowywania. Przetwarzanie danych wykraczające poza ich przechowywanie jest możliwe wyłącznie, jeżeli zaistnieje jedna z następujących przesłanek:

1) osoba, której dane dotyczą, wyraziła na to zgodę,
2) w celu ustalenia, dochodzenia lub obrony roszczeń,
3) w celu ochrony praw innej osoby fizycznej lub prawnej,
4) z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

Przetwarzanie danych, z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego, jest uzależnione od obiektywnego istnienia jednej z tych okoliczności. Spełnienie przesłanki zgody osoby, której dane dotyczą, uzależnione jest wyłącznie od woli tejże osoby i administrator danych jest związany oświadczeniem złożonym przez tę osobę. Natomiast ustalenie, czy przetwarzanie danych miałoby następować w celu ustalenia, dochodzenia lub obrony roszczeń lub w celu ochrony praw innej osoby fizycznej lub prawnej, pozostawione jest ocenie ADO.

8.4.3. Jeżeli ADO ma zamiar uchylić ograniczenie przetwarzania danych, powinien przed tą czynnością poinformować o swoim zamiarze osobę, której dane dotyczą. To poinformowanie powinno nastąpić bez zbędnej zwłoki, nie później niż w terminie miesiąca od otrzymania żądania, aby osoba, której dane dotyczą, mogła skorzystać z innych swoich uprawnień, jeżeli uzna, że nie zgadza się z decyzją o rezygnacji z ograniczenia przetwarzania swoich danych.

8.5. Prawo do przeniesienia danych

8.5.1. Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego 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) lub art. 9 ust. 2 lit. a) lub na podstawie umowy w myśl art. 6 ust. 1 lit. b); oraz
b) przetwarzanie odbywa się w sposób zautomatyzowany.

8.5.2. 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.

8.5.3. Prawo osoby, której dane dotyczą do przeniesienia danych nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

8.5.4. Prawo osoby, której dane dotyczą do przeniesienia danych , nie może niekorzystnie wpływać na prawa i wolności innych.

8.6. Prawo do wniesienia sprzeciwu wobec przetwarzania danych

8.6.1 Osoba, której dane dotyczą może w dowolnym momencie wnieść sprzeciw wobec przetwarzania danych osobowych (w tym profilowania) na potrzeby marketingu bezpośredniego.

8.6.2. Po wpłynięciu wniosku w tej sprawie ADO jest zobowiązany do zaprzestania przetwarzania danych w wyżej wymienionych celach.

8.6.3. W szczególnych sytuacjach osoba, której dane dotyczą może wnieść sprzeciw wobec przetwarzania danych osobowych przez ADO (w tym profilowania), jeśli podstawą wykorzystania danych jest prawnie uzasadniony interes ADO lub interes publiczny. W takiej sytuacji po rozpatrzeniu wniosku osoby, której dane dotyczą ADO nie może przetwarzać danych osobowych objętych sprzeciwem na tej podstawie, chyba że wykaże, że istnieją:

a) ważne prawnie uzasadnione podstawy do przetwarzania danych, które według prawa uznaje się za nadrzędne wobec interesów, praw i wolności osoby, której dane dotyczą,

b) podstawy do ustalenia, dochodzenia lub obrony roszczeń.

IX. Inspektor Ochrony Danych Osobowych

9.1.1. Powołuje się Inspektora Ochrony Danych Osobowych dla Supra Brokers S.A. Dane kontaktowe inspektora zamieszczone są na stronie internetowej spółki oraz udostępnione klientom spółki, tak by każda osoba fizyczna mogła łatwo zrealizować swoje prawa. Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

Dane kontaktowe Inspektora Ochrony Danych Osobowych: Łukasz Czerniak
e-mail: l.czerniak@suprabrokers.pl
tel: 785 839 270

9.1.2. Do obowiązków Inspektora Ochrony Danych Osobowych określonych w art. 39 RODO należy:
a) informowanie o obowiązkach wynikających z RODO;
b) monitorowanie przestrzegania RODO;
c) konsultowanie na żądanie oceny skutków przetwarzania danych osobowych;
d) współpraca z organem nadzorczym;
e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem;

9.1.3. Inspektor wyznaczany jest na podstawie kwalifikacji zawodowych w szczególności wiedzy fachowej na temat prawa i ochrony danych osobowych. Inspektor zobowiązany jest do zachowania poufności i tajemnicy. ADO zapewnia, by IODO nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Komunikacja z inspektorem pomiędzy Zarządem spółki oraz pracownikami odbywa się osobiście oraz za pośrednictwem poczty elektronicznej.

X. Procedura nadawania i odbierania upoważnień i poleceń do przetwarzania danych osobowych.

10.1.1. Każdy nowozatrudniony pracownik lub współpracownik który wykonując obowiązki służbowe będzie przetwarzał dane osobowe otrzyma pisemne upoważnienie (załącznik nr 1 do niniejszej polityki) i polecenie upoważnienie (załącznik nr 2 do niniejszej polityki) do przetwarzania danych osobowych. Upoważnienie stanowi polecenie ADO do przetwarzania danych. Nadanie upoważnienia zostanie potwierdzone podpisem pracownika oraz ADO.

10.1.2. W przypadku wystąpienia sytuacji w wyniku której należy odwołać pracownikowi upoważnienie do przetwarzania danych w szczególności zakończenia stosunku pracy administrator odwołuje upoważnienie do przetwarzania danych.

10.1.3. ADO prowadzi i aktualizuje rejestr nadanych i odwołanych upoważnień do przetwarzania danych osobowych. W rejestrze zamieszczona jest informacja do jakich programów pracownik lub współpracownik otrzymał dostęp, data nadania i odwołania upoważnienia.

10.1.4 Nadanie haseł dostępu do programów następuje przez ADO. Pracownik lub współpracownik otrzymuje hasła dostępu co zostaje potwierdzone złożonym przez niego oświadczeniem. Po odwołaniu upoważnienia do przetwarzaniu danych ADO przeprowadza w ramach karty obiegowej procedurę zdania haseł przez pracownika lub współpracownika, co zostaje potwierdzone podpisem pracownika oraz przedstawiciela ADO.

XI. Procesy kadrowe

11.1 Rekrutacja

ADO publikuje za pośrednictwem portalu z ofertami pracy ogłoszenia o pracę. W treści ogłoszenia znajdują się zgoda na przetwarzanie danych osobowych zawartych w CV, zgoda na przetwarzanie wizerunku oraz zgoda na przetwarzanie danych w kolejnych rekrutacjach. Osoba fizyczna, która chce przesłać swoje dokumenty aplikacyjne i wziąć udział w rekrutacji powinna wyrazić zgodę na przetwarzanie danych w konkretnym procesie rekrutacyjnym. Może także wyrazić zgodę na przetwarzanie jej wizerunku i przetwarzanie danych celu skorzystania z nich w kolejnych rekrutacjach. Wszystkie zgody mają charakter dobrowolny. Zgoda na przetwarzanie danych w konkretnie wskazanym procesie rekrutacyjnym jest niezbędna do przesłania CV i umożliwienia ADO kontaktu z kandydatem do pracy. Nie wyrażenie zgody na pozostałe czynności przetwarzania nie wpływa na możliwość udziału w rekrutacji i nie będzie podstawą niekorzystnego traktowania kandydata oraz nie będzie stanowiła przyczyny uzasadniającej odmowę zatrudnienia. ADO zamieszcza w ogłoszeniu również informacje, o których mowa w art. 13 RODO.

Po zakończeniu rekrutacji przesłane CV zostaje trwale usunięte z poczty e-mail na którą zostało przesłane oraz zniszczone jeżeli zostało wydrukowane w celu przeprowadzenia rozmów. Jeżeli osoba, która brała udział w rekrutacji wyrazi zgodę na udział w kolejnych prowadzonych rekrutacjach, spółka zachowuje dokument i wykorzystuje go w kolejnej rekrutacji.

11.2. Zatrudnienie

Obsługa kadrowo-księgowa zlecona została zewnętrznemu podmiotowi FCG Fiscal Consulting Group Sp. z o. o, z którym spółka podpisała umowę powierzenia danych osobowych. Od osoby ubiegającej się o podjecie zatrudnienia oraz pracownika administrator pobiera dane niezbędne do realizacji obowiązków przewidzianych prawem, do których realizacji jest zobowiązany. W zakresie przekraczającym te obowiązki administrator przetwarza dane tylko za zgodą pracownika. Dokumentacja w wersji papierowej przekazywana jest do podmiotu przetwarzającego, który ją przechowuje i archiwizuje.

XII. Planowanie nowego działania .

12.1. *Zgłoszenie nowego działania, projektu.*

W procesie planowania rozpoczęcia realizacji nowego działania ramach działalności statutowej przez ADO, zobowiązany jest on uwzględnić ochronę danych osobowy osób fizycznych, które będzie przetwarzał w czasie ich realizacji. Wyznaczeni przez ADO pracownicy szczebla kierowniczego odpowiedzialni w związku z powierzonymi im zadaniami za opracowanie działania oraz jego prowadzenie i realizację zobowiązani są zawiadomić ADO i IODO o szczegółach realizacji nowego działania. W tym celu kierują do ADO i IODO za pomocą formularza „Zgłoszenie działania związanego z przetwarzaniem danych osobowych" taką informację. Zgłoszenie obejmuje działania, plany, w których zastosowanie znajdzie przetwarzanie danych osobowych . Formularz zgłoszenia stanowi załącznik nr 3 do niniejszej polityki.

12.2. *Ocena poziomu ryzyka pod kątem konieczności przeprowadzenia oceny skutków przetwarzania.*

ADO na podstawie informacji przekazanych przez pracownika odpowiedzialnego za opracowanie działania dokonuje oceny poziomu ryzyka naruszenia danych osobowych w celu ustalenia czy należy wykonać ocenę skutków przetwarzania danych. Ocena poziomu ryzyka przeprowadzana jest zgodnie z planem wskazanym formularzu „ Ocena poziomu ryzyka", który stanowi załącznik nr 4 do niniejszej polityki. ADO w dokonaniu tej oceny z jednoczesnym uwzględnianiem przepisów RODO.

12.2.1. Dokonując tej oceny ADO konsultuje się z IODO, który może wydać swoją opinię oraz wspomóc Administrator zobowiązany jest dokonać oceny skutków przetwarzania danych w przypadku gdy:

a) dany rodzaj przetwarzania danych osobowych ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych;
b) dokonuje systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
c) przetwarzania na dużą skalę dane wrażliwe lub dane osobowych dotyczących wyroków skazujących i naruszeń prawa;
d) w sytuacji, gdy z okoliczności nie wynika jasno czy mamy do czynienia z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych;
e) w sytuacjach wskazanych w opublikowanym i podanym do publicznej wiadomości przez organ nadzoru wykazie rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych;

12.3. *Ocena skutków przetwarzania danych*

12.3.1.Po dokonaniu analizy ryzyka pod kątem naruszenia prywatności i konieczności wykonania oceny skutków przetwarzania danych i ustaleniu, że planowane działanie wymaga jej dokonania ADO dokonuje oceny skutków przetwarzania. W procesie tym konsultuje się z IODO, który na żądanie ADO monitoruje jego wykonanie. W tym celu ADO lub na jego zlecenie IODO zakłada w systemie

Doradca procedurę zatytułowaną „Ocena skutków przetwarzania". W ramach niniejszej procedury i z zastosowaniem załączonego do niej formularza stanowiącego załącznik nr 5 do niniejszej polityki dokonuje on oceny skutków procesu przetwarzania danych osobowych.

12.3.2. Powyższy obowiązek dotyczy nowych procesów przetwarzania danych osobowych, których rozpoczęcie planuje się na dzień przypadający po 25.05.2018r. oraz procesów rozpoczętych przed dniem 25.05.2018r., jeżeli mogą one powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych lub nastąpiła zmiana ryzyk.

12.3.3. W przypadku funkcjonujących procesów przetwarzania danych osobowych, ADO raz na 2 lata dokonuje przeglądu wykonywanej oceny skutków przetwarzania danych. W przypadku zmiany ryzyka lub elementów działania dokonuje jej niezwłocznie ponownie. Przegląd ma na celu jej aktualizacje. W przypadku stwierdzenia jej dezaktualizacji w całości lub poszczególnych elementów dokonuje jej ponownie.

12.4. *Elementy oceny skutków przetwarzania danych*

12.4.1. Ocena skutków przetwarzania danych osobowych powinna zawierać co najmniej elementy wskazane w treści art. 35 ust. 7 RODO. Dokonując oceny uwzględnia się również postanowienia regulacji szczególnych takich jak kodeksy postępowania zatwierdzone przez organ nadzoru. W przypadkach szczególnych ADO może rozważyć zasięgnięcie opinii osób których dane dotyczą lub ich przedstawicieli ustawowych.

12.4.2. Dokonując analizy uwzględnia się również postanowienia umów zawartych z podmiotami, których dane będą przetwarzane. W celu uzupełnienia analizy ADO zwraca się do działu IT o wyrażenie opinii na temat form zabezpieczenia procesu przetwarzania danych w systemach informatycznych stosowanych przez ADO. Informacje z analizy IT zostaną zawarte w formularzu oceny ryzyka przetwarzania i następnie wraz z wnioskami przekazane do ADO. Opinia sporządzana jest na podstawie informacji przekazanych przez osobę dokonującą zgłoszenia nowego działania.

12.4.3. ADO po otrzymaniu informacji na temat ryzyka przetwarzania danych osobowych podejmuje decyzję czy pomimo ryzyka rozpoczyna przetwarzanie danych osobowych czy też rezygnuje. W przypadku podjęcia decyzji o rozpoczęciu przetwarzania danych osobowych zobowiązany jest zaplanować proces ochrony danych w sposób zabezpieczający dane przed jakimkolwiek naruszeniem ich bezpieczeństwa oraz zgodnie z treścią RODO.

12.5. Planowanie ochrony danych osobowych

12.5.1 Przed rozpoczęciem przetwarzania danych osobowych w ramach nowego działania ADO zobowiązany jest zaplanować ochronę ich przetwarzania. W tym celu w systemie Doradca uruchamia procedurę pod tytułem *„ Projektowanie ochrony danych osobowych*".

12.5.2. Jeżeli ocena skutków wykaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby ADO nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania ADO za pośrednictwem IODO konsultuje się z organem nadzorczym, który może skierować do ADO

specjalne zalecenia. Konsultując się z organem nadzoru administrator zobowiązany jest przedstawić informacje wskazane w art. 36 ust.3 RODO.

12.5.3. W ramach procedury dział IT informuje jakie zabezpieczenia istniejące zostaną zastosowane oraz jakie nowe rozwiązania w celu zabezpieczenia danych proponuje wprowadzić. ADO konsultuje się także z IODO.

12.5.4. Po opracowaniu propozycji projektu ochrony danych całość zostaje umieszczona w formularzu stanowiącym załącznik nr 6 po niniejszej polityki i przedstawiona ADO, który podejmuje ostateczną decyzję jakie metody i mechanizmy ochrony danych osobowych mają zostać wprowadzone. Po ostatecznej akceptacji zostają one wprowadzone jeszcze przed rozpoczęciem przetwarzania danych w związku z rozpoczęciem nowego działania, projektu biznesowego. Dopiero po ich wprowadzeniu dane osobowe mogą być przetwarzane. Wprowadzone zasady i rozwiązania ochrony danych podlegają aktualizacji przez cały okres przetwarzania danych.

XIII. Zgłaszanie incydentów naruszenia danych osobowych

W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

13.1. ADO po wystąpieniu incydentu bezpieczeństwa danych osobowych dokonuje oceny, czy incydent stanowi naruszenie ochrony danych osobowych w rozumieniu art. 4 pkt 12 RODO
13.2. Jeżeli incydent stanowi naruszenie ochrony danych osobowych – ADO dokonuje oceny, czy naruszenie to skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych, których dane dotyczą.
13.3. Przy ocenie czy naruszenie ochrony danych osobowych skutkuje naruszeniem praw i wolności, ADO bierze pod uwagę uprawnienia osób wynikające z samego RODO oraz kwestie związane z rozmiarem naruszenia (ilość danych). Dodatkowo ADO ocenia, czy osoby których dane dotyczą, będą mogły w wyniku naruszenia skutecznie wystąpić wobec ADO z roszczeniem cywilnoprawnym.
13.5. Jeżeli ryzyko naruszenia praw lub wolności osób fizycznych nie występuje lub jest małe, ADO podejmuje działania krygujące i naprawcze.
13.6. Jeżeli ryzyko naruszenia praw lub wolności osób fizycznych jest większe niż małe, ADO zgłasza naruszenie do organu nadzoru wskazanego w art. 51 RODO. Wzór zgłoszenia stanowi załącznik nr 7 do niniejszej polityki.
13.7. Jeżeli ryzyko naruszenia praw lub wolności osób fizycznych jest wysokie, ADO zgłasza naruszenie do organu nadzoru wskazanego w art. 51 RODO według schematu wskazanego w pkt 13.6. Niezależnie od zgłoszenia naruszenia organowi nadzoru, ADO bez zbędnej zwłoki, zawiadamia osób, której dane dotyczą o takim naruszeniu. Zawiadomienie jasnym i prostym językiem powinno opisywać charakter naruszenia ochrony danych osobowych oraz zwierać przynajmniej informacje i środki, zawarte w zgłoszeniu do organu nadzorczego. Zawiadomienie stanowi załącznik nr … do niniejszej polityki.
13.8. ADO dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. W tym celu prowadzi rejestr naruszeń, który stanowi załącznik nr …. do niniejszej polityki.

13.9. Przykładowe niedopuszczalne zachowania mogące prowadzić do wystąpienia incydentu.

1) Wysłanie wiadomości e-mail zawierającej dane osobowe do złego adresata;

2) Wysyłanie wiadomości e-mail zawierających dane osobowe bez zaszyfrowania.;
3) Ujawnianie adresatów wiadomości e-mail (innych adresów mailowych) przy wysyłaniu do większej liczby adresatów;
4) Zgubienie tabletu, pamięci przenośnej, telefonu, dokumentów;
5) Zapisanie haseł dostępu do konta, poczty w telefonie i trzymanie ich w miejscu ogólnodostępnym. (np. żółte karteczki);
6) Przechowywanie dokumentów z danymi osobowymi w niezamykanej szafie, pomieszczeniu.
7) Przekierowanie wiadomości e-mail do kolejnego adresata bez zgody osoby, której dane zawiera;
8) Wyrzucanie do kosza dokumentów w formie papierowej zawierających dane osobowe;
9) Zapisywanie plików na pulpicie;
10) Pozostawienie dokumentów na biurku bez ich zabezpieczenia, nieprzestrzeganie polityki czystego biurka;
11) Korzystanie z prywatnego komputera w celu wykonywania czynności służbowych;
12) Otwieranie wiadomości e-mail od nieznanych adresatów (co może powodować zainfekowanie urządzenia);
13) Pozostawienie otwartych okien, drzwi po zakończeniu pracy;
14) Pozostawianie wydruków z drukarki w ogólnodostępnym miejscu/ na korytarzu;
15) Zainstalowanie nie zatwierdzonego programu na komputer służbowy;
16) Wykorzystywanie poczty służbowej do celów prywatnych;
17) Przekazywanie haseł dostępu innym osobom;
18) Udostępnianie swojego stanowiska pracy innemu pracownikowi;
19) Ustawienie monitora w sposób, który pozwala zapoznać się z jego treściami innym osobom;
20) Zakaz używania komputera w celach prywatnych;
21) Niepoinformowanie przełożonego o incydencie naruszenia ochrony danych osobowych;

XIV. Procedura konsultacji z organem nadzoru

14.1. Jeżeli ocena skutków dla ochrony danych, o której mowa w art. 35 RODO, wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby ADO nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania ADO konsultuje się z organem nadzorczym.

14.2. Jeżeli organ nadzorczy jest zdania, że zamierzone przetwarzanie, o którym mowa powyżej, stanowiłoby naruszenie RODO – w szczególności gdy ADO niedostatecznie zidentyfikował lub zminimalizował ryzyko – organ nadzorczy w terminie do ośmiu tygodni od wpłynięcia wniosku o konsultacje udziela ADO, a gdy ma to zastosowanie także podmiotowi przetwarzającemu pisemnego zalecenia i może skorzystać z dowolnego ze swoich uprawnień, o których mowa w art. 58 RODO. Okres ten można przedłużyć o sześć tygodni ze względu na złożony charakter zamierzonego przetwarzania. Organ nadzorczy informuje ADO, a gdy ma to zastosowanie także podmiot przetwarzający, o takim przedłużeniu w terminie miesiąca od wpłynięcia wniosku o konsultacje, z podaniem przyczyn tego opóźnienia. Bieg tych terminów można zawiesić, do czasu aż organ nadzorczy uzyska wszelkie informacje, których zażądał do celów konsultacji.

14.3.Konsultując się z organem nadzorczym ADO przedstawia mu:

a) gdy ma to zastosowanie – odpowiednie obowiązki administratora, współadministratorów oraz podmiotów przetwarzających uczestniczących w przetwarzaniu, w szczególności w przypadku przetwarzania w ramach grupy przedsiębiorstw;
b) cele i sposoby zamierzonego przetwarzania;
c) środki i zabezpieczenia mające chronić prawa i wolności osób, których dane dotyczą, zgodnie z niniejszym rozporządzeniem;

d) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;
e) ocenę skutków dla ochrony danych, o której mowa w art. 35; oraz
f) wszelkie inne informacje, których żąda organ nadzorczy.

XV. Obowiązki i odpowiedzialność pracowników i współpracowników (użytkowników systemu informatycznego) za przetwarzanie danych osobowych.

15.1. Użytkownik systemu informatycznego zobowiązany jest przed przystąpieniem do wykonywania obowiązków służbowych lub podjęciem współpracy na podstawie umowy cywilnoprawnej z ADO zapoznać się z treścią niniejszej polityki oraz przepisami o ochronie danych osobowych. W czasie wykonywania pracy zobowiązany jest do aktualizacji swojej wiedzy poprzez zapoznawanie się z udostępnioną mu polityką oraz uczestnictwem w szkoleniach organizowanych przez ADO.

15.2. Do szczegółowych obowiązków użytkownika systemu informatycznego należy:
a) przetwarzanie danych osobowych zgodnie z przepisami prawa oraz niniejszą polityką;
b) zachowanie szczególnej ostrożności przy gromadzeniu danych, w szczególności mając na uwadze zasady przetwarzania danych, w tym zasadę minimalizacji danych, legalności, celowości, adekwatności oraz cel przetwarzania danych;
c) poprawnego korzystania z sytemu informatycznego;
d) niezwłocznego informowania ADO o wszelkich zauważonych nieprawidłowościach w działaniu systemu lub przy przetwarzaniu danych osobowych;
e) stosowanie polityki haseł i uwierzytelniania, utrzymywanie w ścisłej tajemnicy haseł, którymi się posługuje;
f) dokonania zmiany hasła w przypadku powzięcia podejrzenia lub stwierdzenia, że z hasłem mogły zapoznać się osoby trzecie oraz niezwłoczne zawiadomić o tym fakcie ADO,
g) w przypadku opuszczenia stanowiska pracy w celu udania się na przerwę zabezpieczenia komputera hasłem tak by osoby nieupoważnione nie mogła mieć do niego dostępu;
Po zakończeniu pracy użytkownik zobowiązany jest wylogować się z sytemu i wyłączyć komputer.

W przypadku, gdy w czasie przetwarzania danych osobowych użytkownik systemu informatycznego będzie miała problem z wykonywaniem powyżej wymienionych obowiązków zobowiązany jest niezwłocznie zawiadomić o tym dział IT w celu szybkiego rozwiązania problemu.

XVI. Informacje dotyczące ochrony i przetwarzania danych osobowych

16.1. *Obszar w którym przetwarzane są dane osobowe*
Dane osobowe przetwarzane są przez ADO w następujących budynkach, pomieszczeniach, tworzących obszar przetwarzania danych osobowych:
a) **siedziba główna** ADO , tj. ul. ul. Al. Śląska 1, 54-118 Wrocław
b) odziały ADO
- Oddział w Warszawie**,** ul. Mazura 18a, 02-830 Warszawa
- Oddział w Katowicach**,** ul. Henryka Dulęby 7, 40-833 Katowice
c) **przedstawicielstwa ADO**
- Przedstawicielstwo w Rzeszowie**,** Al. Józefa Piłsudskiego 40 lok. 14, 35-001 Rzeszów
- Przedstawicielstwo w Gdańsku, ul. Gnilna 2, 80-847 Gdańsk
- Przedstawicielstwo w Szczecinie**,** ul. Małe Błonia 31/12, 71-779 Szczecin

d) centra obliczeniowe wykorzystywane przez platformę provider.pl, zarządzane przez Procesora Danych

Obszary przetwarzania danych osobowych powierzonych przez ADO
a) FCG Fiscal Consulting Group, ul. Opolska 11-19, miejsce przetwarzania danych: ul. Opolska 11-19 Wrocław

16.2. Strefy przetwarzania

Obszary przetwarzania danych podzielone zostały na następujące strefy:
a) strefę przetwarzania danych osobowych, czyli pomieszczenia biurowe spółki w którym dane są przetwarzane przez ADO,
b) strefę specjalną, w skład której wchodzą serwerownie w których dane są przetwarzane przez ADO,
c) strefę w której są przetwarzane dane osobowe powierzone do spółki przez innego Administratora Danych Osobowych, jako procesorowi, do przetwarzania
d) strefę w której przetwarzane są dane powierzone innym podmiotom przez spółkę;

16.3. *Dostęp do obszaru przetwarzania*

Dostęp do pomieszczeń, w których przetwarzane są dane osobowe, zawarte w zbiorach administrowanych przez ADO mają: pracownicy i współpracownicy ADO, posiadający odpowiednie upoważnienie oraz polecenie do przetwarzania danych .

16.3.1. Przebywanie w tych pomieszczeniach osób niedopuszczonych/nieupoważnionych do przetwarzania danych osobowych może się odbywać tylko w obecności i pod nadzorem przedstawiciela ADO w szczególnie uzasadnionych przypadkach takich jak kontrola poprawności przetwarzania danych osobowych czy udział przedstawiciela ubezpieczyciela w otwarciu ofert w ramach procedury udzielania zamówień publicznych.

16.3.2. Drzwi wejściowe do pomieszczeń obszaru przetwarzania danych muszą pozostawać zamknięte zarówno po zakończeniu pracy przez osoby upoważnione, jak i w wypadku każdego, chociażby chwilowego, opuszczenia przez nie pomieszczenia w ciągu czasu pracy.

XVII. Procedura przydziału i zmiany haseł – polityka hasłowa

17.1. Warunkiem uzyskania dostępu do systemów jest posiadanie przez użytkownika systemu informatycznego stosownego upoważnienia oraz plecenia do przetwarzania nadanego przez ADO oraz własnego identyfikatora i hasła . Hasło do systemu Doradca i CRM nadaje każdemu nowemu użytkownikowi ADO. Dział IT zakłada natomiast indywidualne kontro użytkownika systemu komputerowego oraz konto mailowe w przypadku, gdy otrzyma taką dyspozycję od ADO.

17.2. Wprowadzona została hierarchia użytkowników systemu informatycznego związana z uprawnieniami jakie posiadają. Użytkownicy pełniący funkcje administracyjne lub zarządcze mają szerszy zakres uprawnień niż użytkownicy tych funkcji nie pełniący. ADO, przyznając upoważnienia do przetwarzania danych osobowych, stosuje zasadę przyznawania uprawnień w minimalnym zakresie, niezbędnym do wykonania czynności służbowych przez danego użytkownika.

17.3. Identyfikatory, hasła lub inne mechanizmy uwierzytelniające użytkownika przydzielane są przez ADO, który ewidencjonuje identyfikatory użytkowników mających uprawnienia dostępu do systemów związanych z przetwarzaniem danych osobowych.
Każda osoba posiada własny identyfikator (lub identyfikatory w przypadku braku możliwości korzystania z tego samego identyfikatora w różnych systemach) i ma ściśle określony zakres praw dostępu do zasobów systemów informatycznych w których przetwarzane są dane osobowe
Do identyfikatora, uprawniającego do korzystania z systemu operacyjnego komputera lub serwera, przypisane są prawa dostępu do zasobów z których korzysta przetwarzając dane osobowe.

Identyfikator użytkownika może zostać aktywowany tylko osobie, która zapoznała się przepisami dotyczącymi ochrony danych osobowych, polityką ochrony danych, obowiązującymi w Spółce instrukcjami i procedurami w zakresie przetwarzania danych osobowych oraz która podpisała zobowiązania poufności przetwarzania danych oraz stosowanych zabezpieczeń i zobowiązała się do ponoszenia odpowiedzialności z tego tytułu.

17.4. Stosowane są następujące rodzaje haseł:
a) Hasła logowania do systemu operacyjnego komputera lub serwera, na którym przetwarzane są dane osobowe
b) Hasła do wygaszacza ekranu
c) Hasła dostępu do systemów informatycznych lub aplikacji służących do przetwarzania danych osobowych
d) Hasła dostępu do baz danych

O ile to możliwe, wszystkie wyżej wymienione hasła powinny być różne.

17.5. Zasady postępowania z hasłami użytkowników (operatorów danych):
a) Hasła użytkowników (operatorów danych) muszą się składać z co najmniej 8 znaków i muszą zawierać duże i małe litery, cyfry oraz znaki specjalne. Powinny być zmieniane co 30 dni. (kategoria D – systemy przetwarzające dane osobowe),

		Kategoria
Parametr jakości hasła		D
Ilość znaków		8
Wymagane znaki wg zasady **2 z 3 wymienionych warunków**	**Duże i małe litery**	1
	Cyfry	1
	Znaki specjalne (?><{}][*&^%$#@!)	0
Ważność [dni]		30

b) Hasła nie powinny zawierać imion, nazwisk, nazw własnych ani żadnych innych popularnych lub możliwych do odgadnięcia słów,
c) Haseł nie wolno udostępniać ani dopuścić do ich ujawnienia,

d) W sytuacji możliwego naruszenia bezpieczeństwa danych osobowych lub podejrzenia ujawnienia hasła obowiązuje konieczność niezwłocznej zmiany wszystkich stosowanych przez użytkownika haseł,
e) Zarówno obecne, jak i wszystkie nieaktualne hasła objęte są ścisłą tajemnica.

Hasła administratorów do systemów i serwerów powinny spełniać wymagania wynikające z wewnętrznych polityk Procesora. Zalecane jest aby przynajmniej:

a) Hasła administratorów oraz systemowe składały z co najmniej 10 znaków i zawierały duże
i małe litery, cyfry oraz znaki specjalne. Powinny być zmieniane co 30 dni
(kategoria A – systemy i serwery o znaczeniu strategicznym),

		Kategoria
Parametr jakości hasła		*A*
Ilość znaków		*10*
Wymagane znaki wg zasady **2 z 3 wymienionych warunków**	**Duże i małe litery**	*2*
	Cyfry	*2*
	Znaki specjalne (?><{}][*&^%$#@!)	*0*
Ważność [dni]		*30*

b) Hasła nie mogą zawierać imion, nazwisk, nazw własnych ani żadnych innych popularnych lub możliwych do odgadnięcia słów,
c)Nie wolno udostępniać ani dopuścić do ujawnienia hasła,
d)Zarówno obecne, jak i wszystkie nieaktualne hasła objęte są ścisłą tajemnicą,
e) Hasła dostępu do baz danych oraz hasła administracyjne do serwerów i aplikacji wewnętrznych systemów informatycznych przetwarzających dane osobowe należy zmieniać co 30 dni, o ile nie ma ważnych przeciwskazań natury technologicznej. Hasła do pozostałych systemów powinny być zmieniane nie rzadziej niż co 3 miesiące.
Dodatkowo obowiązuje zmiana wszystkich haseł administracyjnych każdorazowo w sytuacji stwierdzenia możliwego naruszenia bezpieczeństwa systemów informatycznych lub danych osobowych, podejrzenia ujawnienia któregoś z haseł lub odejścia z zespołu administratora,
f) Dostęp do kopii aktualnych haseł administracyjnych (do kont, serwerów, systemów, aplikacji oraz baz danych) maja tylko uprawnione przez ADO osoby.

W przypadku cofnięcia operatorowi danych prawa do przetwarzania danych osobowych (np. w związku ze zmianą zakresu obowiązków lub stanowiska, rozwiązaniem umowy o pracę lub zakończeniem współpracy) obowiązują następujące zasady:

g) Zobowiązania do nierozpowszechniania i niewykorzystywania poufnych informacji zdobytych w trakcie wykonywania powierzonych prac zachowują ważność także po cofnięciu uprawnień,
h) Operator musi zwrócić wszelkie dokumenty i inne materiały dotyczące zbiorów i baz danych osobowych, przetwarzanych danych osobowych lub stosowanych zabezpieczeń,
i) Z chwilą cofnięcia uprawnienia do przetwarzania danych osobowych wszystkie identyfikatory wykorzystywane przez operatora danych zostają, we współpracy z ADO, zablokowane i wyrejestrowane z systemów, a wszystkie hasła z nimi powiązane tracą ważność,
j) Identyfikatory są przechowywane i nie są przydzielane żadnemu innemu operatorowi danych.

XVIII. Procedury rozpoczęcia, zakończenia pracy i obsługi komputera.

18.1. Stanowiska stacjonarne

18.1.1 Każdorazowo przy rozpoczęciu pracy użytkownik systemu informatycznego ma obowiązek podać hasło startowe komputera, a następnie zalogować sie do systemu informatycznego (system operacyjny lub aplikacja) w którym przetwarzane są dane osobowe.
18.1.2. Użytkownik systemu informatycznego rozpoczynając pracę zobowiązany jest dopilnować, czy załadowało sie programowanie antywirusowe monitorujące komputer, jeśli takowe jest dostępne.
18.1.3. Wszelkie zauważone okoliczności wskazujące na możliwość naruszenia bezpieczeństwa danych osobowych muszą zostać bezzwłocznie zgłoszone do ADO.
18.1.4. Po każdorazowym odejściu od stanowiska użytkownik zobowiązany jest dokonywać blokady ekranu. Blokada włącza się automatycznie po maks. 10 minutach bezczynności.
18.1.5. Wyłączenie wygaszacza ekranu wymaga podania hasła operatora danych lub administratora komputera na którym wygaszacz został uruchomiony.
18.1.6. Po zakończeniu pracy operator danych oraz administrator jest zobowiązany wylogować się z aplikacji/systemu, wyłączy komputer oraz zabezpieczyć komputer przed dostępem do danych przez osoby nieuprawnione.

18.2. Komputery przenośne wykorzystywane przetwarzania danych osobowych

18.2.1. Osoba użytkująca komputer przenośny, służący do przetwarzania danych osobowych, zobowiązana jest zachować szczególną ostrożność podczas transportu oraz używania komputera poza siedzibą ADO, w celu zapobieżenia dostępowi do zgromadzonych i przetwarzanych na nim danych przez osoby nieupoważnione, a w szczególności:
a. Nie zezwalać na korzystanie komputera osobom nie posiadającym upoważnienia do przetwarzania danych osobowych wydanego przez ADO. Dotyczy to również osób bliskich i domowników.
b. Przewozić lub przenosić komputer z zachowaniem koniecznych wymogów bezpieczeństwa, w szczególny sposób chroniąc go przed utratą
c. W przypadku zgubienia lub kradzieży komputera użytkownik zobowiązany jest niezwłocznie powiadomić o tym fakcie ADO.
18.2.2. Użytkownik przenośnego komputera nie może korzystać z publicznych sieci dostępu do Internetu.

XIX. Usługi świadczone przez Procesora w zakresie administracji pocztą elektroniczną- załącznik nr 9 do niniejszej polityki.

XX. Tworzenie kopi zapasowych (backup) i ich usuwanie

20.1. Kopie awaryjne powinny być wykonywane regularnie i zgodnie z przyjętym harmonogramem przez upoważnionego administratora systemu lub inna upoważniona osobę. Po sporządzeniu powinno się sprawdzić wykonaną kopię pod kątem jej prawidłowości i możliwości odtworzenia danych.
20.2. Kopie awaryjne są okresowo sprawdzane pod kątem przydatności do odtworzenia danych w przypadku awarii systemu.
20.3. Przechowuje się kopie zapasowe baz danych osobowych według poniższej specyfikacji:
a) Backup online baz danych - synchronizacja baz danych w trybie master-slave,
b) Backup dzienny baz danych - przechowywany w oddzielnych lokalizacjach,

c) Backup miesięczny baz danych - pełny, według stanu bieżącego, kasowany po ustalonym okresie od daty wykonania.
20.4. Kopie danych opisane w punkcie 20.2 przechowywane są na dyskach lokalnych lub macierzach serwerów wykonujących backup lub magazynujących dane.
20.5. Serwery i repozytoria danych znajdują się w strefach przetwarzania danych osobowych.
20.6. W przypadku konieczności oddania dysku lub innego nośnika danych osobowych do serwisu, ADO lub inna upoważniona osoba pod jego nadzorem, wymazuje zawartość nośnika tak, by nie dało sie jej potem odzyskać. Jeśli skasowanie danych jest niemożliwe lub nie daje pewności usunięcia, nośnik taki powinien być zniszczony, a nie serwisowany.
20.7. W uzasadnionych przypadkach (np. wysoka cena nośnika który powinien być, zgodnie z pkt. 20.5, zniszczony) istnieje możliwość wykonania naprawy nośnika danych na którym znajdują się nieusunięte dane osobowe, ale czynność taka musi odbywać pod nadzorem ADO, Procesora lub na mocy osobnego porozumienia z wykonującym serwis. Porozumienie takie musi zawierać zapisy związane z ochroną danych osobowych przetwarzanych przez Administratora Danych. Jeśli to możliwe powinna to być „Umowa powierzenia przetwarzania danych osobowych", zapewniająca ochronę danych, o których mowa w art. 28 RODO.
20.8. Wszelkie nośniki, w tym uszkodzone dyski twarde przechowywane są w zamkniętym sejfie, do którego dostęp mają tylko wyznaczone przez ADO osoby.

XXI. Metody i częstotliwość sprawdzania obecności niebezpiecznego oprogramowania na stanowiskach oraz sposoby ich usuwania.

21.1.Wszystkie komputery i stacje robocze, na których użytkownicy systemu informatycznego przetwarzają dane osobowe wyposażone są w aktualizowane automatycznie, oprogramowanie antywirusowe sprawdzające aktywnie funkcjonowanie systemów operacyjnych, przetwarzanych plików danych oraz podłączanych nośników danych, w celu wykrycia obecności lub identyfikacji podatności na działanie „złośliwego oprogramowania (malware)".
21.2. W przypadku wykrycia nieprawidłowości w zakresie opisanym w punkcie 1, należy niezwłocznie powiadomić ADO oraz podjąć niezbędne działania mające na celu weryfikację zidentyfikowanych nieprawidłowości oraz, jeśli potwierdzono zagrożenie dla przetwarzanych danych osobowych, przywrócenie bezpieczeństwa komputera lub stacji roboczej.

XXII. Metody i częstotliwość aktualizacji i instalacji oprogramowania systemowego na stanowiskach.

22.1. Na wszystkich komputerach i stacjach roboczych, na których operatorzy danych przetwarzają dane osobowe, obowiązują następujące zasady:
a) System operacyjny instaluje i konfiguruje osoba upoważniona przez ADO,
b) Urządzenia, które w trakcie udostępnienia i aplikowania poprawek nie były włączone powinny zostać zaktualizowane po uruchomieniu i restartowane po zakończeniu procesu.
c) Operatorzy danych nie są upoważnieni do samodzielnego instalowania na swoich stanowiskach aplikacje i oprogramowania użytkowego.
d) Aktualizacja aplikacji i oprogramowania użytkowego odbywa się w trybie automatycznym lub manualnym, pod nadzorem osoby upoważnionej przez ADO.
22.2. Z wyjątkiem uzasadnionym przypadków, potwierdzonych decyzją ADO, operatorzy danych nie posiadają uprawnień administracyjnych do swoich komputerów lub stacji roboczych.
22.3. W przypadku wykrycia nieprawidłowości w zakresie opisanym w punktach poprzedzających, należy niezwłocznie powiadomić ADO oraz podjąć niezbędne działania mające na celu weryfikację

zidentyfikowanych nieprawidłowości oraz, jeśli potwierdzono zagrożenie dla przetwarzanych danych osobowych, przywrócenie bezpieczeństwa komputera lub stacji roboczej.

XXIII. Metody i częstotliwość sprawdzania obecności niebezpiecznego oprogramowania na serwerach oraz sposoby ich usuwania.

23.1.Serwery baz danych oraz inne serwery, na których dane osobowe są przetwarzane, powinny być sprawdzane pod kątem oryginalności i poprawności systemu plików za pomocą odpowiedniego oprogramowania kontrolnego, w celu wykrycia ewentualnych różnic w zainstalowanym oprogramowaniu i plikach na nośnikach danych oraz dla identyfikacji „złośliwego oprogramowania (malware)".
23.2. Na serwerach, na których jest to możliwe i uzasadnione, zalecane jest zainstalowanie, na bieżąco aktualizowanych, autonomicznych skanerów antywirusowych i wykrywających oprogramowanie złośliwe.
W przypadku wykrycia nieprawidłowości w zakresie opisanym powyżej, należy niezwłocznie powiadomić ADO oraz podjąć niezbędne działania mające na celu weryfikację zidentyfikowanych zmian oraz, jeśli potwierdzono zagrożenie dla przetwarzanych danych osobowych, przywrócenie bezpieczeństwa systemu.

XXIV. Zabezpieczenie serwerów

Serwer znajduje się w siedzibie głównej ADO w specjalnie wydzielonym do tego pomieszczeniu. Dostęp do pomieszczenia mają wyznaczone przez ADO osoby. Serwer przechowywany jest w specjalnych zamykanych szafach. Regularnie dokonuje się Backup serwera.

XXV. Metody i częstotliwość aktualizacji i instalacji oprogramowania systemowego oraz aplikacji i oprogramowania użytkowego na serwerach.

25.1. Na wszystkich serwerach baz danych oraz innych serwerach, na których dane osobowe są przetwarzane, obowiązują następujące zasady:
a) System operacyjny i niezbędne aplikacje (w tym bazodanowe) instaluje i konfiguruje odpowiednio przeszkolony personel Procesora,
b) Aktualizacja systemu operacyjnego odbywa się pod Procesora.
Wskazane jest aby decyzję o instalacji nowych poprawek systemowych każdorazowo podejmował upoważniony administrator systemu, ale dopuszczalna jest również aktualizacja automatyczna.
c) Aktualizacja aplikacji i oprogramowania użytkowego odbywa się w trybie automatycznym lub manualnym, pod nadzorem Procesora.
25.2. Dostęp administracyjny do serwerów przetwarzających dane osobowe posiadają upoważnieni pracownicy Procesora (na podstawie Umowy) oraz, po uzyskaniu zgody ADO, inne osoby którym uprawnienia są niezbędne do wykonywania przydzielonych im przez ADO obowiązków związanych przetwarzaniem danych osobowych.
Procesor odpowiedzialny jest za prowadzenie nadzoru nad zgodnością i aktualnością zainstalowanego oprogramowania z przyjętymi zasadami.
W przypadku wykrycia nieprawidłowości w zakresie opisanym w punktach poprzedzających, należy niezwłocznie powiadomić ADO oraz podjąć niezbędne działania mające na celu weryfikację

zidentyfikowanych nieprawidłowości oraz, jeśli potwierdzono zagrożenie dla przetwarzanych danych osobowych, przywrócenie bezpieczeństwa serwerów.

XXVI. Sposób dokonywania przeglądów i konserwacji systemów przetwarzania danych osobowych.

26.1. Operacje związane z dokonywaniem przeglądów i konserwacji systemów przetwarzających dane osobowe wykonywane są pod nadzorem ADO.
ADO wyznaczył osobę upoważnioną do dokonywania przynajmniej raz w miesiącu, pod nadzorem, całościowego przeglądu i konserwacji systemów, wykorzystywanych w Spółce nośników informacji i zbiorów danych osobowych. W przypadku wykrycia nieprawidłowości w działaniu systemów, związanych z naruszeniem mechanizmów ochrony, niezwłocznie podejmowane są działania określone w Instrukcji postępowania w przypadku naruszenia ochrony danych osobowych.

XXVII.Sposoby postępowania w zakresie komunikacji w sieci komputerowej

27.1. Dane osobowe przetwarzane przez serwery powinny być przesyłane za pośrednictwem sieci komputerowych w postaci zaszyfrowanej lub przy użyciu transmisji kodowanej.
27.2.Dostęp do sieci wewnętrznych (biurowej) i wszystkich urządzeń je obsługujących mają jedynie uprawnione osoby posiadające Upoważnienie nadane przez ADO.
27.3. Bazy danych w których przetwarzane są dane osobowe powinny być skonfigurowana tak, by pozwalać na połączenia tylko z wcześniej określonych komputerów. Wszelkie inne próby dostępu muszą zostać zalogowane i sprawdzone przez Procesora. W przypadku stwierdzenia prób połączenia z nieuprawnionego komputera należy niezwłocznie podjąć czynności wyjaśniające oraz powiadomić ADO.

XXVIII. Zabezpieczenie zasilania systemów przetwarzających dane osobowe.

28.1 Serwery i urządzenia uczestniczące w przetwarzaniu danych osobowych, w szczególności te na których zainstalowane są bazy danych osobowych lub funkcjonują repozytoria danych, muszą być podłączone do awaryjnych źródeł zasilania (UPS) lub posiadać własne, niezależne źródła zasilania, pozwalających na ich awaryjną pracę przez okres czasu wystarczający do pełnego, automatycznego zamknięcia systemu, gwarantującego zachowanie integralności danych osobowych.
28.2 O ile to możliwe urządzenia opisane w punkcie poprzedzającym powinny być podłączone do dwóch niezależnych, gwarantowanych źródeł zasilania.
28.3 Nadzór nad funkcjonowaniem systemu zasilania urządzeń sprawuje ADO w zakresie sprzętu biurowego, serwerów oraz Procesor w stosunku do platformy provider.pl.

XXIX.Rejestracja i monitoring dostępu do systemów przetwarzania danych osobowych

Każdorazowy dostęp do baz danych osobowych oraz serwerów, na których przetwarzane są dane osobowe jest odnotowywany w logach/rejestrach. System rejestracji w pełni pozwala na identyfikację tożsamości operatora danych, aplikacji lub administratora, który w danym czasie uzyskał dostęp do systemów przetwarzających dane osobowe i/lub dokonał operacji na danych. ADO, a na jego zlecenie Procesor, lub osoba przez nich wyznaczona, zobowiązani są do bieżącego monitorowania logów. Wszelkie próby nieuprawnionego dostępu muszą być zgłaszane ADO zgodnie z Instrukcją postępowania w przypadku naruszenia ochrony danych osobowych. Kopie zapasowe logów/rejestrów są tworzone automatycznie i są przechowywane.

XXX. Tryb postępowania w przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego

30.1.W przypadku stwierdzenia naruszenia ochrony danych osobowych, a w szczególności, gdy:

a) osoba nieuprawniona uzyskała dostęp do danych;

b) techniczne zabezpieczenia zbioru kopii roboczych lub awaryjnych, a także alarmy zarejestrowały naruszenie systemu ochrony, lub zamknięcia drzwi lub sejfów zostały uszkodzone, zniszczone lub usunięte (na podstawie informacji od administratorów systemu informatycznego lub powzięcia informacji od osób trzecich);

c) ujawniono jakiekolwiek nieprawidłowości w działaniu któregokolwiek z elementów systemu, które mogą mieć wpływ na poprawność przetwarzania danych osobowych z zbiorze;

osoby zatrudnione przy przetwarzaniu danych (operatorzy danych) zobowiązane są do bezzwłocznego zawiadomienia ADO lub upoważnionej przez ADO osoby oraz IODO podjęcia wszelkich prawnie dozwolonych działań niezbędnych w danym momencie dla zapobieżenia dalszym naruszeniom bezpieczeństwa danych.

30.2. Zasady określone w pkt. 1 należy stosować odpowiednio w wypadku stwierdzenia powstania niebezpieczeństwa naruszenia zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych.

30.3. ADO lub upoważniona przez ADO oraz IODO osoba ustala przyczynę naruszenia bezpieczeństwa danych i określa, samodzielnie lub wspólnie z powołanym przez siebie specjalistą (np. administratorem systemu informatycznego), czy jest to wynik próby naruszenia zabezpieczeń.

30.4. Pracownik działu IT lub osoba wyznaczona przez zewnętrzną firmę IT na wniosek ADO ub upoważnionej przez ADO osoby, kopie plików danych i plików systemowych, które mogą zawierać informacje istotne dla wyjaśnienia sprawy, przeprowadza przegląd praw dostępu i rejestrów systemu. W szczególnych przypadkach blokuje dostęp do danych osobowych aż do chwili usunięcia bezpośredniej przyczyny naruszenia ich bezpieczeństwa. W zależności od rodzaju stwierdzonego naruszenia ADO lub upoważniona przez ADO osoba podejmuje decyzje mające na celu usunięcie naruszenia i uniemożliwienie ponownego wystąpienia takiego przypadku w przyszłości.

XXI. Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności przetwarzania danych

Celem zabezpieczenia danych osobowych przed dostępem osób nieupoważnionych wprowadza się odpowiednie rozwiązania techniczne i organizacyjne opisane poniżej.

31.1. Opis najważniejszych zastosowanych środków technicznych i organizacyjnych

a) został wyznaczony Inspektor Ochrony Danych Osobowych monitoruje przestrzeganie przepisów RODO,
b) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez ADO;
c) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych,
d) została opracowana i wdrożona Polityka ochrony danych osobowych, która reguluje zasady przetwarzania danych osobowych w spółce;
e) ADO przeprowadza szkolenia okresowe pracowników;
f) ADO stosuje ochronę fizyczną, kontrolę dostępu do pomieszczeń;
g) dostęp zdalny do danych osobowych jest zarządzany centralnie;

31.2. *Dokumenty w formie papierowej*

Dokumenty papierowe przechowywane są w zamkniętych szafach znajdujących się w pomieszczeniach biurowych. Szafy są zabezpieczone zamkami mechanicznymi z kluczem. Dokumenty papierowe, zawierające dane osobowe, po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów. Obowiązuje polityka czystego biurka wszystkie dokumenty zawierające dane osobowe powinny zostać schowane przez pracownika do szafy tak by nie miał do nich dostępu inny pracownik lub osoba trzecia.

Dokumenty archiwalne przechowywane są w zamkniętym pomieszczeniu specjalnie do tego przeznaczonym, które otwierane jest na kartę dostępu. Dostęp do pomieszczenia mają tylko pracownicy sekretariatu i zarząd.

31.3. Oprogramowanie i sprzęt komputerowy

W systemach przechowywania i przetwarzania danych Zastosowano macierze dyskowe w celu ochrony danych osobowych przed skutkami awarii pojedynczych zasobów pamięci dyskowych.
Zastosowano oprogramowanie i rozwiązania chroniące komputery oraz serwery przed szkodliwym oprogramowaniem kategorii malware (robaki, wirusy, konie trojańskie, rootkity itp.).Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych komponentach zbiorów danych osobowych.
Wdrożono mechanizmy umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych. Dostęp do baz danych zawierających dane osobowe wymaga uwierzytelnienia, użytkowników i aplikacji, z wykorzystaniem identyfikatora oraz hasła. Zastosowano mechanizmy wymuszające okresową zmianę haseł dostępu do systemów. Zastosowano kryptograficzne środki ochrony danych osobowych. Zainstalowano wygaszacze ekranów na komputerach i stacjach roboczych, na których przetwarzane są dane osobowe. Zastosowano mechanizm automatycznej blokady dostępu do konsoli systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz polityką ochrony danych. Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.
Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich oraz informacji o ich zabezpieczeniu, w tajemnicy. Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane. Kopie zapasowe zbiorów danych osobowych przechowywane są w innych pomieszczeniach niż to, w którym znajdują się serwery, na których dane osobowe przetwarzane są na bieżąco.

Załączniki:

Załącznik nr 1 Upoważnienie do przetwarzania danych
Załącznik nr 2 Polecenie do przetwarzania danych
Załącznik nr 3 Formularz zgłoszenia działania związanego z przetwarzaniem danych osobowych.
Załącznik nr 4 Formularz Oceny poziomu ryzyka.
Załącznik nr 5 Formularz Oceny skutków przetwarzania danych osobowych.
Załącznik nr 6 Formularz projektowania ochrony danych osobowych.
Załącznik nr 7 Wzór zgłoszenia incydentu naruszenia danych
Załącznik nr 8 Wzór powiadomienia osoby której dane dotyczą o incydencie
Załącznik nr 9 Oświadczenie pracownika o zapoznaniu się z polityką
Załącznik nr 10 Polityka ładu i porządku na stanowisku pracy