Polityka bezpieczeństwa przetwarzania danych osobowych AMBusiness Sp. z o.o.

Metryka dokumentu

Wersja dokumentu	1.0
Liczba stron	**21**

Lista modyfikacji i historii dokumentu

Wersja dokumentu	Data wersji	Informacja o zmianach i statusie	Osoba dokonująca modyfikacji
1.0	17.04.2024	Utworzenie dokumentu, do akceptacji	Maciej Chwaliński, specjalista@osobowedane.pl

Przyjęcie do stosowania

Imię i nazwisko, stanowisko	Data
Adam Walas - Prezes Zarządu	

Spis treści

1)Wprowadzenie....5
2)Deklaracja Administratora Danych Osobowych 6
3)Definicje....8
4)Administrator Danych Osobowych 8
5)Dane osobowe....8
6)Zbiór danych osobowych 8
7)Przetwarzanie danych osobowych....8
8)Rozporządzenie lub RODO....8
9)Polityka Bezpieczeństwa 8
10)UODO....8
11)System informatyczny 8
12)Pracownik, Personel....9
13)Użytkownik....9
14)Hasło....9
15)Identyfikator użytkownika lub login....9
16)Dane wrażliwe....9
17)Integralność danych....9
18)Rozliczalność danych....9
19)Poufność danych....9
20)Strona trzecia 9
21)Profilowanie....9
22)Pseudonimizacja....10
23)Podmiot przetwarzający lub procesor....10
24)Odbiorca....10
25)Zgoda 10
26)Naruszenie ochrony danych osobowych....10
27)Zasady przetwarzania danych osobowych....11
28)Podstawowe zasady....11
29)Obowiązki związane z dopuszczeniem do danych osobowych....13
30)Powierzanie danych osobowych innym firmom i podmiotom (folder nr 7 Procesorzy (powierzenie danych)....15
31)Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie...15
32)Obowiązki ADO i Personelu....16
33)Obowiązki Pracowników i Personelu....20

34)Rejestrowanie naruszeń w ochronie danych osobowych i informowanie osoby, której dane dotyczą o naruszeniu (folder nr 5 Zarządzanie naruszeniami)....20
35)Realizacja praw podmiotów danych....21
2.1 Prawo do sprostowania danych....22
2.2 Prawo do usunięcia danych („prawo do bycia zapomnianym”)....22
2.3 Procedura usunięcia danych osobowych....22
2.4 Prawo do ograniczenia przetwarzania....23
2.5 Prawo do przenoszenia danych....23
36)Wykaz budynków i pomieszczeń tworzących obszar przetwarzania danych osobowych....23
37)Obszar przetwarzania danych osobowych....23
38)Środki techniczne i organizacyjnych niezbędne dla ochrony przetwarzanych danych....23
1)Środki organizacyjne....23
39)Środki ochrony fizycznej....25
40)Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej....25
41)Środki ochrony w ramach narzędzi programowych i baz danych....25

1) Wprowadzenie

Niniejszy dokument wchodzi w skład dokumentacji przewarzania danych osobowych w firmie AMBusiness Sp. z o.o.

Celem Polityki bezpieczeństwa jest wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie wykonać obowiązki Administratora danych osobowych w zakresie zabezpieczenia danych osobowych.

Niniejsza polityka, wraz z pozostałymi dokumentami wchodzącymi w skład dokumentacji ochrony danych, opisuje sposoby przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę danych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczające dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem, zniszczeniem lub innym zagrożeniem powodującym naruszenie praw i wolności osoby, której dane dotyczą.

Podstawą do wdrożenia powyższych zasad jest Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.

Polityka Bezpieczeństwa zostaje zatwierdzona i przyjęta do stosowania:

Pruszków	Adam Walas - Prezes Zarządu
Miejscowość i data	Administrator danych osobowych

2) Deklaracja Administratora Danych Osobowych

Jako Administrator Danych Osobowych jestem świadomy wagi problemów związanych z ochroną prawa do prywatności, w tym w szczególności prawa osób fizycznych do właściwej i skutecznej ochrony ich danych przetwarzanych przez Administratora, deklaruję zamiar podejmowania wszystkich działań niezbędnych dla ochrony praw i usprawiedliwionych interesów jednostki związanych z bezpieczeństwem danych osobowych.

Jako Administrator Danych Osobowych jestem świadomy zagrożeń związanych z przetwarzaniem danych osobowych. Będę stale doskonalić i rozwijać organizacyjne, techniczne oraz informatyczne środki ochrony danych osobowych przetwarzanych zarówno metodami tradycyjnymi jak i elektronicznie, tak, aby skutecznie zapobiegać zagrożeniom:

- *związanym z infekcjami wirusów, koni trojańskich i innego złośliwego oprogramowania,*
- *związanym z dostępem do stron internetowych, na których zainstalowane są skrypty pozwalające wykradać zasoby komputera,*
- *związanym z możliwością niekontrolowanego kopiowania danych na zewnętrzne, przenośne nośniki,*
- *związanym z możliwością podsłuchiwania sieci, dzięki któremu można zdobyć hasła i skopiować objęte ochroną dane,*
- *związanym z lekceważeniem zasad ochrony danych polegającym na pozostawianiu pomieszczenia lub stanowiska pracy bez ich należytego zabezpieczenia,*
- *związanym z brakiem świadomości niebezpieczeństwa dopuszczania osób postronnych do swojego stanowiska pracy,*
- *związanym z działaniami mającymi na celu zaburzenie poufności, integralności, dostępności i odporności systemów i usług przetwarzania.*
- *związanym z kradzieżą sprzętu lub nośników z danymi, które zazwyczaj są niezabezpieczone,*
- *związanym z przekazywaniem sprzętu z danymi do serwisu,*

i innym zagrożeniom mogącym wystąpić w przyszłości w związku z rozwojem techniki metod przetwarzania danych.

Adam Walas - Prezes Zarządu

Administrator danych osobowych

3) Definicje

W niniejszym dokumencie przyjmuje się następujące definicje:

4) Administrator Danych Osobowych

AMBusiness Sp. z o.o. zwana dalej ADO lub Administratorem. „Administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

5) Dane osobowe

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

6) Zbiór danych osobowych

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

7) Przetwarzanie danych osobowych

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.

8) Rozporządzenie lub 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 (ogólne rozporządzenie o ochronie danych).

9) Polityka Bezpieczeństwa

Niniejsza Polityka Bezpieczeństwa obejmująca zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych w organizacji ADO.

10) UODO

Urząd Ochrony Danych Osobowych.

11) System informatyczny

Zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

12) Pracownik, Personel

Osoby zatrudnione na podstawie stosunku pracy, umów cywilnoprawnych (umowa o dzieło, umowa zlecenia) przez przedsiębiorcę, wykonujące działalność osobiście, jak również osoby odbywające praktyki, stażyści, osoby skierowane do pracy w ramach umów z agencjami pracy tymczasowej wykonujące prace związane z przetwarzaniem danych osobowych u ADO.

13) Użytkownik

Każda osoba w organizacji ADO posiadająca dostęp i korzystająca z narzędzi umożliwiających przetwarzanie danych osobowych na podstawie nadanego upoważnienia i na polecenie ADO.

14) Hasło

Ciąg znaków literowych, cyfrowych lub innych, znany jedynie Użytkownikowi Systemu informatycznego. Hasło użytkownika składa się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

15) Identyfikator użytkownika lub login

Ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym

16) Dane wrażliwe

Dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby

17) Integralność danych

Właściwość zapewniająca, że dane osobowe nie zostały zmienione, zmodyfikowane lub zniszczone w sposób nieautoryzowany.

18) Rozliczalność danych

Właściwość zapewniająca możliwość wykazania przestrzegania przepisów i przypisania działania podmiotu w sposób jednoznaczny tylko temu podmiotowi

19) Poufność danych

Właściwość zapewniająca odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych

20) Strona trzecia

Oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe.

21) 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.

22) Pseudonimizacja

Oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

23) Podmiot przetwarzający lub procesor

Oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora i na jego polecenie w oparciu o odpowiedni instrument prawny (umowę powierzenia przetwarzania danych osobowych).

24) Odbiorca

Oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.

25) Zgoda

Osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

26) 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.

27) Zasady przetwarzania danych osobowych

28) Podstawowe zasady

Przetwarzanie danych osobowych zarówno przez ADO, jak i jego personel odbywa się z poszanowaniem obowiązujących przepisów, dobrych praktyk oraz niniejszej Polityki Bezpieczeństwa.

ADO dokładana wszelkich starań, aby stosowane środki zabezpieczeń danych osobowych były adekwatne do zagrożeń wynikających ze sposobu, jak również kategorii przetwarzanych danych osobowych. W celu dostosowania odpowiednich zabezpieczeń przeprowadzono analizę ryzyka.

Dane osobowe są:

- przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);

- zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu”);

- adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);

- prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);

- przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania”);

- przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz

przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).

ADO jest odpowiedzialny za spełnienie powyższych wymogów i jest w stanie wykazać ich przestrzeganie („rozliczalność”).

29) Obowiązki związane z dopuszczeniem do danych osobowych

W celu zapewniania kontroli i zachowania zasady rozliczalności do przetwarzania danych osobowych dopuszczone są wyłącznie osoby posiadające wiążące upoważnienie do przetwarzania danych nadane przez ADO.

Kogo dotyczy?

Każdej osoby, która wykonuje czynności na danych osobowych (pracownik, współpracownik B2B, stażysta).

Co zrobić?

Zapoznać osobę z *Regulaminem przetwarzania danych osobowych* (folder nr 4).

Wystawić osobie **upoważnienie do przetwarzania danych osobowych**

Zebrać podpis pod zobowiązaniem do zachowania danych w tajemnicy.

Jak zrobić?

Na początek zapoznajemy osobę, która ma zostać upoważniona z *Regulaminem przetwarzania danych osobowych* (znajduje się folderze nr 4).

Po zapoznaniu się z Regulaminem wydajemy upoważnienie i odbieramy zobowiązanie do zachowania danych w tajemnicy i przestrzegania wprowadzonych zasad.

Wzór upoważnienia znajduje się w folderze nr 6 – Upoważnienia dla pracowników).

Do upoważnienia należy wpisać imię i nazwisko osoby, która będzie miała dostęp do danych:

Nr upoważnienia: ……..

Upoważnienie do przetwarzania danych osobowych

W celu zachowania kontroli nad dostępem do danych osobowych ADO upoważnia do przetwarzania danych osobowych:

Panią/Pana ……

Imię i nazwisko osoby upoważnianej

Następnie określamy zakres danych, do jakich ma dostęp wybierając odpowiednią czynności przetwarzania:

☐ Przetwarzanie danych pracowników
☒ Zatrudnienie współpracowników (umowa cywilno-prawna, kontrakt)
☐ Przetwarzanie danych dostawców / kontrahentów

Wyłącznie w zakresie wynikającym z zadań służbowych pracownika / personelu.
Niniejsze upoważnienie zaczyna obowiązywać od daty jego wydania i traci ważność w momencie ustania stosunku o pracę, rozwiązania umowy lub odwołania przez ADO.

.....
Administrator Danych Osobowych
Czytelny podpis i data

Oraz składamy podpis w wyznaczonym miejscu (podpis składa osoba uprawniona do reprezentowania firmy).

W dolnej części upoważnienie znajduje się Oświadczenie osoby upoważnionej o zobowiązaniu do zachowania poufności przetwarzanych danych, pod którym podpis składa osoba upoważniania (po zapoznaniu z Regulaminem przetwarzania danych osobowych:

Oświadczenie osoby upoważnionej o zobowiązaniu do zachowania poufności przetwarzanych danych

Ja, niżej podpisany/-na zobowiązuje się do zachowania w tajemnicy przetwarzanych danych osobowych i sposobów ich zabezpieczeń, w czasie jak również po ustaniu stosunku pracy, oraz do przestrzegania instrukcji i procedur związanych z ochroną danych osobowych przedstawionych mi w AMBusiness Sp. z o.o.

.....
Data i podpis osoby upoważnionej

Nie ma możliwości odmowy podpisania oświadczenia – jeśli pracownik odmawia zobowiązania do przestrzegania prawa w zakresie przetwarzania danych osobowych naraża się na ciężkie naruszenie obowiązków pracowniczych i nie możemy dopuścić takiej osoby do przetwarzania danych osobowych

30) Powierzanie danych osobowych innym firmom i podmiotom (folder nr *7 Procesorzy (powierzenie danych)*

W ramach prowadzonej działalności ADO może powierzyć dane osobowe, zgodnie z zasadami opisanymi w art. 28 RODO. W celu zachowania kontroli nad podmiotami, którym przekazywane są dane osobowe należy:

1. Prowadzić ***7.1 Ewidencję podmiotów, którym powierzono przetwarzanie danych***
2. W razie wątpliwości dotyczących tego, czy dana firma zapewnia odpowiedni poziom bezpieczeństwa danych należy przeprowadzić jej ocenę przy pomocy formularza nr ***7.3 Ocena firmy, której przekazywane są dane osobowe – formularz*** i podjąć na jego podstawie decyzję o przekazaniu danych.
3. Z podmiotami, które gwarantują odpowiedni poziom ochrony danych należy zawrzeć ***8.3 Umowę powierzenia danych osobowych.***

UWAGA – umowa, jaką posiadają Państwo w tym folderze stanowi wzór. RODO dopuszcza aby funkcję takiej umowy pełnił również inny, wiążący instrument prawny. Wiele firm, które otrzymują dużo danych decyduje się na opracowanie własnej umowy lub zawarcie zapisów dotyczących powierzenia w umowie głównej czy własnym regulaminie (dzięki temu nie muszą one weryfikować każdego otrzymanego dokumentu).

Jeśli otrzymają Państwo informację, że dana firma zawiera własną umowę lub uwzględnia powierzenie danych w regulaminie czy umowie głównej jest to poprawne rozwiązanie.

Jeśli firma nie dysponuje „swoją" umową tego rodzaju – mogą Państwo skorzystać z przygotowanego wzoru.

31) Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie

3.1 Administrator może korzystać z profilowania do celów marketingu bezpośredniego, ale decyzje podejmowane na jego podstawie przez Administratora nie dotyczą zawarcia lub odmowy zawarcia Umowy, czy też możliwości korzystania z Usług. Efektem korzystania z profilowania może być np. przyznanie danej osobie rabatu, przesłanie jej kodu rabatowego, przypomnienie o niedokończonych zakupach, przesłanie propozycji, która może odpowiadać zainteresowaniom lub preferencjom danej osoby lub też zaproponowanie lepszych warunków w porównaniu do standardowej oferty. Mimo profilowania to dana osoba podejmuje swobodnie decyzję, czy będzie chciała skorzystać z otrzymanego w ten sposób rabatu, czy też lepszych warunków i dokonać zakupu.

3.2 Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

32) Obowiązki ADO i Personelu

1) Obowiązki ADO

ADO decyduje o środkach, celach i sposobach przetwarzania danych osobowych, dlatego zobowiązany jest do:

1. **Zastosowania środków technicznych i organizacyjnych niezbędnych do zapewnienia bezpieczeństwa przetwarzanym danym w stopniu adekwatnym do potencjalnego zagrożenia wykazanego w przeprowadzonej analizie ryzyka** (odpowiedniego zabezpieczenia danych osobowych)

2. **Dopuszczenia do przetwarzania danych osobowych tylko osób upoważnionych.**

   Czyli wydania upoważnień do przetwarzania danych osobowych, zgodnie z informacjami na stronach 10-11 niniejszej Polityki).

3. **Prowadzenia dokumentacji określającej sposoby przetwarzania danych osobowych**

   Czyli:

   - Rejestru czynności przetwarzania (folder nr 1),
   - Rejestru kategorii czynności przetwarzania (ewentualnej listy firm, które przekazują dane osobowe do AMBusiness Sp. z o.o.), (plik Rejestru czynności przetwarzania – zakładka nr 2)
   - ewidencji osób upoważnionych (folder nr 6),
   - ewidencji firm, którym powierzane są dane (czyli przekazywane przez AMBusiness Sp. z o.o.), (folder nr 7)
   - Rejestru incydentów bezpieczeństwa danych (folder nr 5).
   - i pozostałej dokumentacji (w zakresie jej zgodności ze stanem faktycznym).

4. **Zapoznanie osób upoważnionych do przetwarzania danych osobowych z przepisami i zasadami przetwarzania danych osobowych.**

   Poprzez Regulamin przetwarzania danych osobowych – folder nr 4 oraz – jeśli to konieczne – z Zasadami pracy zdalnej).

5. **Zadbania o zgodne z prawem powierzanie i udostępnianie danych osobowych (**

   Czyli odnotowanie jakiej firmie powierzane są dane osobowe oraz zawieranie Umowy powierzenia przetwarzania danych osobowych – folder nr 7).

   Należy również pamiętać, że udostępnienie danych osobowych podmiotom uprawnionym (np. Policja, sąd, komornik, Państwowa Inspekcja Pracy) powinno odbywać się w oparciu o formalny wniosek.

6. **Zapewnienie fizycznych zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe, jak również kontrolę i nadzór nad osobami, które przebywają w obszarze przetwarzania** (dbałości o fizyczne zabezpieczenie biura bądź nośników danych osobowych).

7. **Nadawanie, zmianę lub pozbawienie uprawnień dostępu do systemu informatycznego, w którym przetwarzane są dane osobowe.**

   SZCZEGÓLNIE istotne w przypadku kluczowych baz danych i programów. Należy regularnie sprawdzać, czy wszystkie dostępy do oprogramowania (konta użytkowników) posiadają aktualne poziomy dostępu (dotyczy również pracowników firm zewnętrznych – np. developera, informatyka, czy firmy marketingowej).

8. **Zapewnienie ochrony antywirusowej** (włączony, aktualizowany program antywirusowy).

9. **Tworzenie kopii zapasowych danych osobowych.**

   Kopie zapasowe danych mogą być wykonywane przez dostawców usług – np. firmę hostingową lub firmę developerską. Należy jednak ZAWSZE wiedzieć jak często takie kopie są wykonywane oraz w jaki sposób mogą być odzyskane. Oprócz dostępności danych osobowych pozwala to na zachowanie ciągłości działania aplikacji i **UNIKNIĘCIE STRAT FINANSOWYCH** w sytuacji krytycznej.

10. **Zapewnienie respektowania praw osób, których dane dotyczą, a w szczególności prawa do:**

    - **Uzyskania informacji o Administratorze Danych Osobowych.**

      Przetwarzanie danych musi być przejrzyste. Każda osoba, której dane posiadamy ma prawo poprosić o podanie danych Administratora (firmy).

    - **Uzyskania informacji o celach, zakresie i sposobach przetwarzania danych.**

      Zgodnie z klauzulami informacyjnymi. Informujemy o celu przetwarzania, przekazywaniu danych podmiotom zewnętrznym, okresie, przez jaki będziemy posiadać dane, podstawie prawnej etc.

    - **Uzyskania informacji o momencie rozpoczęcia przetwarzania danych.**

      Miejsce pozyskiwania danych osobowych oznaczamy klauzulą informacyjną (np. przy formularzu) / informujemy skąd posiadamy dane osobowe.

    - **Uzyskania informacji o tym, jakie dane są przetwarzane.**

      Czyli informacji o zakresie danych konkretnej osoby, jakie posiadamy.

    - **Uzyskania informacji o źródle, z którego dane pochodzą.**

      Czyli informacji skąd pozyskaliśmy dane osobowe (np. bezpośrednio od tej osoby podczas rejestracji, z zewnętrznej bazy, powszechnie dostępnych źródeł – CEiDG, KRS, stron www, podczas kontaktu na targach / spotkaniach / meetingach towarzyskich, etc.).

    - **Uzyskania informacji o sposobie udostępniania danych oraz ich odbiorcach.**

      Czyli komu przekazujemy / udostępniamy dane osobowe (np. firmie płatniczej, aplikacji weryfikującej, partnerom biznesowym).

- **Żądania uzupełnienia, uaktualnienia, sprostowania danych.**

  Dane osobowe poprawiamy zgodnie z żądaniem osoby, której dotyczą.

  Żądanie może mieć charakter prośby o zmianę nazwiska, czy uaktualnienie adresu. Każda osoba ma prawo do poprawienia jej danych, jeśli są nieprawidłowe.

  Pamiętamy o weryfikacji osoby, która żąda danej zmiany – jeśli nie jesteśmy pewni tożsamości zgłaszającego możemy odmówić realizacji żądania.

- **Wniesienia umotywowanego wniosku do zaprzestania przetwarzania danych.**

  Jeśli otrzymamy wniosek o zaprzestanie przetwarzania danych (w tym również o ich usunięcie) musimy zidentyfikować, czy faktycznie możemy to zrobić. Jeśli nadal potrzebujemy danych (mamy podstawę prawną do ich

- **Wycofania zgody na przetwarzanie danych osobowych.**

  Dotyczy KAŻDEJ zgody, w tym zgody na działania marketingowe. Warunkiem prawidłowej zgody na przetwarzanie danych osobowych jest to, aby była możliwa do wycofania w dowolnym momencie, w równie prostu sposób, jak została wyrażona.

  Zalecane jest utrzymanie systemu pozwalającego na proste wycofanie zgody (np. wypisanie z newslettera, czy personalizacji komunikatów i wiadomości otrzymywanych z aplikacji).

- **Usunięcia danych („prawo do bycia zapomnianym").**

  Najczęściej realizowane poprzez wiadomość z żądaniem usunięcia danych osobowych konkretnej osoby.

  Takie żądanie możemy zrealizować tylko jeśli:

  - dane pozyskane zostały na podstawie zgody (automatycznie zostaje wtedy odwołana),

  - dane zostały pozyskane w ramach prawnie uzasadnionego interesu Administratora (np. działań marketingowych),

  W innym przypadku, jak np.:

  - dane pozyskaliśmy w celu realizacji umowy (w tym po akceptacji regulaminu),

  - mamy obowiązek prawny posiadania danych (np. na fakturach czy umowach),

  NIE MUSIMY usuwać danych osobowych. Naszym obowiązkiem jest jednak poinformowanie użytkownika z jakiego powodu musimy dane posiadać.

- **Ograniczenia przetwarzania.**

Czyli wstrzymania się od dalszego przetwarzania danych osobowych przez określony czas (np. przesłania newslettera, czy realizacji usługi). Takie żądanie może przesłać np. użytkownik zmieniający miejsce zamieszkania lub osoba, która ma podejrzenie, że jej dane zostały pozyskane niezgodnie z prawem.

- **Przenoszenia danych.**
- Realizowane tylko jeśli możliwe jest to technicznie.

33) Obowiązki Pracowników i Personelu

Poniższe obowiązki dotyczą Pracowników, Personelu, jak również wszystkich osób upoważnionych przez ADO do przetwarzania danych osobowych i w szczególności odnoszą się do:

1. **Zapoznania się z zasadami przetwarzania danych osobowych i przestrzegania ich.** Pracownik musi zapoznać się *Regulaminem przetwarzania danych osobowych.*
2. **Ochrony danych osobowych zgodnie z obowiązującymi przepisami prawa.**
3. **Przetwarzania danych osobowych tylko w zakresie określonym przez ADO.**
4. **Zgłaszania do ADO incydentów wynikających z naruszenia przepisów i zasad ochrony danych, w tym**:
    - Informacji o nieuprawnionym dostępie do danych osobowych.
    - Usterek i problemów technicznych urządzeń służących do przetwarzania danych osobowych.
    - Wykrycia wirusów oraz złośliwego oprogramowania, jak również wszelkich innych potencjalnych zagrożeń (w tym np. kradzież lub wyciek danych, atak na system informatyczny etc.)
    - Wszelkich innych nieprawidłowości i potencjalnych zagrożeń związanych z naruszeniem ochrony danych osobowych.
5. **Zabezpieczenie nośników i dokumentów zawierających dane osobowe przed nieuprawnionym dostępem**.
6. **Niszczenie w sposób trwały i niemożliwy do odzyskania dokumentów oraz nośników, na których przechowywane są dane osobowe, których okres przydatności minął.**
7. **Niezapisywania haseł dostępu do systemu informatycznego ADO oraz oprogramowania, w którym dane są przetwarzane w formie umożliwiającej dostęp do hasła osobom trzecim i nieuprawnionym.**

34) Rejestrowanie naruszeń w ochronie danych osobowych i informowanie osoby, której dane dotyczą o naruszeniu (folder nr 5 *Zarządzanie naruszeniami)*

Rejestrowanie i postępowanie z naruszeniami i incydentami w ochronie danych prowadzone jest zgodnie z przyjętą ***5.1 Procedurą zarządzania incydentami w ochronie danych*.**

35) Realizacja praw podmiotów danych

1. Administrator danych osobowych podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udzielić osobie, której dane dotyczą wszelkich informacji, o których mowa w art. 13 i 14 RODO (informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą, Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą).

Niezbędne klauzule informacyjne służące do spełnienia powyższego obowiązku znajdują się w folderze ***9. Klauzule informacyjne.***

1) Informacje, do których może uzyskać dostęp osoba, której dane dotyczą

1. Każda osoba, której dane osobowe przetwarzane są przez Administratora danych osobowych ma prawo do uzyskania potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce jest uprawniona do uzyskania dostępu do nich oraz uzyskania następujących informacji od ADO:
    1. jakie są cele przetwarzania jej danych;
    2. kategorie odnośnych danych osobowych;
    3. kto jest odbiorcą danych i komu zostają ujawnione w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
    4. w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
    5. informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
    6. informacje o prawie wniesienia skargi do organu nadzorczego;
    7. jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
    8. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
2. Osoba, której dane dotyczą ma prawo do uzyskania kopii danych osobowych podlegających przetwarzaniu. Jeśli osoba zwraca się o kopię drogą elektroniczną (np. przez pocztę e-mail) i nie zaznaczy innej formy, ADO przesyła kopię taką samą drogą.

2) Prawa osób, których dane dotyczą i sposób ich realizacji

2.1 Prawo do sprostowania danych

1. Osoba, której dane dotyczą, ma prawo żądania od ADO niezwłocznego sprostowania dotyczących jej danych osobowych, jeśli są one nieprawidłowe. Dla konkretnego celu osoba, której dane dotyczą może również żądać uzupełnienia niekompletnych danych.
2. W celu realizacji powyższych zadań ADO dokłada wszelkich starań, aby niezwłocznie reagować na informacje o nieprawidłowych lub niekompletnych danych i dokonać poprawienia / uzupełnienia danych.

2.2 Prawo do usunięcia danych („prawo do bycia zapomnianym")

1. W przypadku żądania osoby, której dane dotyczą usunięcia jej danych, ADO usuwa w sposób trwały dane z każdego systemu informatycznego, oraz, jeśli ma to miejsce – danych w formie papierowej oraz z kopii zapasowych, jeśli:
    - Dane nie są już niezbędne do celu ich pozyskania (np. zrealizowano zamówienie, dokonano zatrudnienia pracownika w procesie rekrutacji).
    - Osoba, której dane dotyczą cofnęła zgodę, na podstawie której dane są przetwarzane.
    - Osoba, której dane dotyczą wniesie sprzeciw co do przetwarzania jej danych, a ADO nie ma prawnie uzasadnionego celu dalszego przetwarzania danych.
2. Żądanie usunięcia nie dotyczy danych, które wymagają od Administratora ich przetwarzania na podstawie obowiązujących przepisów prawa, np. w celach księgowo-podatkowych. W takiej sytuacji dane nadal mogą być przetwarzane w celach uzasadnionych przepisami prawa.

2.3 Procedura usunięcia danych osobowych

1. Po otrzymaniu żądania osoby, której dane dotyczą usunięcia jej danych ADO dokonuje sprawdzenia lokalizacji, z jakich należy usunąć dane, a tym dla danych, których przetwarzanie powierzono innym odbiorcom.
2. Dane zostają w sposób trwały i nieodzyskiwalny usunięte, ze wszystkich miejsc, co do których żądanie usunięcia jest uzasadnione, nie później niż w terminie miesiąca od wpłynięcia żądania.
3. ADO informuje osobę, której dane dotyczą o usunięciu jej danych. W przypadku posiadania adresu korespondencyjnego, adresu e-mail lub innego zestawu danych niezbędnego do komunikacji, ADO dokonuje ich usunięcia niezwłocznie po przesłaniu komunikatu.
4. W przypadku wątpliwości ADO co do pochodzenia żądania usunięcia, nie od osoby, której dane dotyczą (np. po otrzymaniu żądania w formie mailowej nie z adresu używanego wcześniej do korespondencji), ma on prawo do wstrzymania się od usunięcia danych do czasu potwierdzenia pochodzenia żądania.

2.4 Prawo do ograniczenia przetwarzania

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

1. Jeśli osoba, której dane dotyczą zakwestionowała prawidłowość danych osobowych, ADO wstrzymuje się od przetwarzania takich danych (z wyjątkiem czynności przechowywania danych) do czasu sprawdzenia ich poprawności.
2. Jeśli dane przetwarzane są niezgodnie z prawem, a osoba, której dane dotyczą sprzeciwia się ich usunięciu.
3. W przypadku wystąpienia uzasadnionej konieczności usunięcia danych (np. wygaśnięcie celu przetwarzania), ale osoba, której dane dotyczą sprzeciwia się ich usunięciu, ze względu na ustalenie, dochodzenie lub obronę roszczeń.
4. W przypadku uchylenia ograniczenia przetwarzania (np. ustalono poprawność danych) ADO informuje osobę, której dane dotyczą, o tym fakcie przed ponownym rozpoczęciem przetwarzania danych.

2.5 Prawo do przenoszenia danych

1. Osoba, której dane dotyczą ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadających się do odczytu maszynowego dane jej dotyczące, które dostarczyła ADO, oraz ma prawo przesłać te dane innemu administratorowi.
2. W przypadku przetwarzania danych na podstawie uzyskanej zgody lub w celu realizacji umowy, osoba której dane dotyczą ma prawo żądania, by dane osobowe zostały przesłane przez ADO innemu administratorowi, o ile jest to technicznie możliwe.

36) Wykaz budynków i pomieszczeń tworzących obszar przetwarzania danych osobowych

37) Obszar przetwarzania danych osobowych

Obszarem przetwarzania danych osobowych jest siedziba firmy znajdująca się pod adresem: ul. Andrzeja 10/15, 05-800 Pruszków, gdzie dane osobowe przetwarzane są w wydzielonym pomieszczeniu mieszkania prywatnego.

Dane osobowe mogą być również przetwarzane poza wyznaczonym obszarem przy użyciu urządzeń mobilnych.

38) Środki techniczne i organizacyjnych niezbędne dla ochrony przetwarzanych danych

1) Środki organizacyjne

1. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

2. Administrator danych kontroluje jakie dane osobowe zostają zebrane oraz komu są przekazywane.
3. Administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania.
4. Opracowano i wdrożono dokumentację opisującą przyjęte zasady zabezpieczenia danych.
5. Osoby upoważnione do przetwarzania danych zobowiązane zostały do zachowania danych w tajemnicy.
6. Osoby upoważnione do przetwarzania danych zostały zapoznane z obowiązującymi procedurami, przepisami i wytycznymi dotyczącymi przetwarzana danych.
7. Osoby upoważnione do przetwarzania danych zobowiązane są do ich zabezpieczenia przed dostępem osób nieuprawnionych (w tym innych członków organizacji ADO nieposiadających upoważnienia do przetwarzania tych danych) poprzez:
    - blokadę komputera lub urządzenia używanego do przetwarzania danych w formie cyfrowej w momencie opuszczenia przez nią pomieszczenia poprzez wylogowanie się z konta / blokadę ekranu lub wyłączenie urządzenia,
    - zabezpieczenie danych przetwarzanych w formie papierowej przed dostępem osób nieuprawnionych, zwłaszcza w momencie znajdowania się takiej osoby w obszarze przetwarzania danych np. poprzez zamknięcie dokumentów w szafce, biurku, sejfie lub poprzez inne, skuteczne zabezpieczenie,
    - zabezpieczenie papierowych oraz cyfrowych nośników danych po zakończeniu pracy, jeśli dostęp do pomieszczenia może uzyskać osoba postronna (np. serwis sprzątający, serwis urządzeń, ochrona budynku itd.),
    - ustawienie ekranów komputerów i innych urządzeń, na których dane są przetwarzane w sposób uniemożliwiający wgląd w dane osobom nieuprawnionych. Dotyczy to zarówno urządzeń znajdujących się w obszarze przetwarzania danych, jak u urządzeń mobilnych, na których dane przetwarzane są poza tym obszarem (np. przez stosowanie filtra prywatyzującego).
8. Niedopuszczalne jest używanie nośników danych (pendrive, dysk zewnętrzny, telefon i inne) pochodzących z niewiadomego lub niepewnego źródła.
9. Stosowanie odpowiedniej polityki haseł dostępu do systemów zawierających dane osobowe.
10. Ustawienie monitorów komputerów, na których przetwarzane są dane osobowe w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
11. Każdy z użytkowników systemu informatycznego, w którym przetwarzane są dane osobowe pracuje na własnym, unikalnym koncie.

    Niedopuszczalne jest korzystanie kilku pracowników z jednego konta lub wymiana czy też udostępnienie hasła do takiego konta.
12. Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.

39) Środki ochrony fizycznej

1. Dane osobowe przechowywane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi), zamykanymi na klucz.
2. Dane osobowe w formie papierowej przechowywane są w zamkniętej szafie lub szufladzie.
3. Dokumenty i nośniki danych przeznaczone do utylizacji niszczonego są przy pomocy niszczarki do dokumentów (trwałe zniszczenie danych).

40) Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej

1. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
2. Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
3. Użyto system Firewall do ochrony dostępu do sieci komputerowej.
4. Stosowanie automatycznej aktualizacji wszystkich systemów i oprogramowani służących do przetwarzania danych osobowych.

41) Środki ochrony w ramach narzędzi programowych i baz danych

1. Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
2. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
3. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.