POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

W

JOB-JOB Sp. z o.o.

TYTUŁ I
POSTANOWIENIA OGÓLNE

Rozdział 1
Intencje administratora danych osobowych

§ 1

JOB-JOB Sp. z o.o. deklaruje:

1. zamiar podejmowania wszystkich działań niezbędnych dla ochrony praw i usprawiedliwionych interesów jednostki związanych z bezpieczeństwem danych osobowych;
2. zamiar stałego podnoszenia świadomości oraz kwalifikacji osób przetwarzających dane osobowe;
3. zamiar traktowania obowiązków pracowników przy przetwarzaniu danych osobowych jako należących do kategorii podstawowych obowiązków pracowniczych;
4. zamiar stanowczego egzekwowania ich wykonania przez pracowników,
5. stałe doskonalenie i rozwój organizacyjny w celu skutecznego zapobiegania zagrożeniom powstawania naruszeń praw lub wolności podmiotów danych w postaci przypadkowego lub niegodnego z prawem: zniszczenia, utraty, modyfikacji, nieuprawnionego dostępu, nieuprawnionego ujawnienia – danych, a w szczególności:
   a. związanym z infekcjami wirusów i koni trojańskich, które instalując się na komputerze mogą wykradać zasoby tego komputera (zarówno stacjonarne, jak i sieciowe);
   b. związanym ze spamem, posiadającym niekiedy programy pozwalające wykradać zasoby komputera;
   c. związanym z dostępem do stron internetowych, na części, których zainstalowane są skrypty;
   d. pozwalające wykradać zasoby komputera;
   e. związanym z ogólnie dostępnymi komunikatorami internetowymi, w których występują luki, przez które można uzyskać dostęp do komputera;
   f. związanym z użytkowaniem oprogramowania do wymiany plików, mogącym służyć do łatwego skopiowania pliku;

g. związanym z możliwością niekontrolowanego kopiowania danych na zewnętrzne, przenośne nośniki;
h. związanym z możliwością podsłuchiwania sieci, dzięki któremu można zdobyć hasła i skopiować objęte ochrona dane;
i. związanym z lekceważeniem zasad ochrony danych polegającym na pozostawianiu pomieszczenia lub stanowiska pracy bez ich zabezpieczenia;
j. związanym z brakiem świadomości niebezpieczeństwa dopuszczania osób trzecich do swojego stanowiska pracy;
k. związanym z atakami z sieci stanowiącymi zagrożenie dla przetwarzania danych;
l. związanym z działaniami mającymi na celu zaburzenie integralności danych, w celu uniemożliwienia ich przetwarzania lub osiągnięcia korzyści;
m. związanym z kradzieżą sprzętu lub nośników z danymi;
n. związanym z kradzieżą tożsamości umożliwiającą podszywanie się pod inna osobę;
o. mogącym wystąpić w przyszłości w związku z rozwojem technik i metod przetwarzania danych.

§ 2

JOB-JOB Sp. z o.o. jest świadoma zagrożeń związanych z przetwarzaniem danych osobowych, w szczególności zagrożeń wynikających z dynamicznego rozwoju metod i technik przetwarzania danych osobowych w systemach informatycznych oraz sieciach telekomunikacyjnych.

§ 3

Mając na względzie obowiązki nałożone na administratora danych osobowych na mocy obowiązujących regulacji prawnych dotyczących ochrony danych osobowych, w szczególności rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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) – Dz.Urz. UE L 119 z 4.5.2016 (dalej

jako: RODO), JOB-JOB Sp. z o.o. przyjmuje dokument pt. „Polityka bezpieczeństwa danych osobowych JOB-JOB Sp. z o.o.” (dalej jako: Polityka).

§ 4

1. Polityka stanowi zbiór reguł określających sposoby przetwarzania i ochrony danych osobowych.
2. Polityka zawiera opis środków technicznych i organizacyjnych służących zapewnieniu zgodnego z prawem przetwarzania danych osobowych, o których mowa w art. 24 RODO.

§ 5

Integralną część niniejszej Polityki stanowi:

a) Rejestr czynności przetwarzania (Załącznik nr 1 do Polityki);
b) Rejestru kategorii czynności przetwarzania (Załącznik nr 2 do Polityki);
c) wzór upoważnienia do przetwarzania danych osobowych (Załącznik nr 3 do Polityki);
d) wzór oświadczenia o zapoznaniu się z Polityką i zobowiązaniu do jej stosowania (załącznik nr 3a do Polityki);
e) Ewidencja osób upoważnionych do przetwarzania danych osobowych (Załącznik nr 4 do Polityki);
f) wzór raportu dotyczącego naruszenia ochrony danych osobowych (Załącznik nr 5 do raportu);
g) wzór zgłoszenia naruszenia ochrony danych osobowych do podmiotu danych osobowych (Załącznik nr 6);
h) wzór zgłoszenia naruszenia ochrony danych osobowych do Prezesa Urzędu Ochrony Danych Osobowych (Załącznik nr 7);
i) określenie Zasad przechowywania danych (Załącznik nr 8);
j) Instrukcja zarządzania systemem informatycznym (Załącznik nr 9).

Rozdział 2
Cele i obszary przetwarzania danych osobowych

§ 6

1. JOB-JOB Sp. z o.o. z siedzibą w z siedzibą w Nowym Targu (34-400), ul. Królowej Jadwigi 17 jest administratorem danych osobowych przetwarzanych w szczególności w następujących obszarach:
   a. pozyskaniu osób do pracy (rekrutacja);
   b. udzielaniu pomocy w legalizacji pobytu, pracy oraz zakwaterowania;
   c. realizacji stosunków pracy oraz innych stosunków zatrudnienia nawiązywanych przez Spółkę;
   d. realizacji umów z kontrahentami/klientami;
   e. księgowości i rozliczeń.

§ 7

1. JOB-JOB Sp. z o.o. przetwarza dane osobowe w sposób tradycyjny (papierowy) oraz w systemach informatycznych.
2. Dane osobowe, których administratorem jest JOB-JOB Sp. z o.o. są co do zasady przetwarzane na terenie Europejskiego Obszaru Gospodarczego, który tworzą państwa Unii Europejskiej oraz Islandia, Norwegia i Lichtenstein. Przekazanie danych do państwa trzeciego lub organizacji międzynarodowej może nastąpić wyłącznie na zasadach określonych w Tytule V niniejszej Polityki, czyli po zapewnieniu wymaganego przez RODO stopnia ochrony osób fizycznych.

Rozdział 3
Pojęcia związane z ochroną danych osobowych

§ 8

Ilekroć w niniejszej Polityce jest mowa o:

a) **Administratorze Danych Osobowych** (dalej jako: **ADO**) – należy przez to rozumieć JOB-JOB Sp. z o.o. z siedzibą w Nowym Targu (34-400), ul. Królowej Jadwigi 17;
b) **danych osobowych** – należy przez to rozumieć wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (przez osobę możliwą do zidentyfikowania należy rozumieć osobę, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, identyfikator internetowy lub jeden bądź kilka szczególnych

czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej);

c) **naruszenie ochrony danych osobowych** – należy przez to rozumieć naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do przesyłanych, przechowywanych lub w inny sposób przetwarzanych danych osobowych;
d) **odbiorca danych osobowych** – należy przez to rozumieć osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią, z wyłączeniem organów publicznych otrzymujących dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego;
e) **ograniczeniu przetwarzania** – należy przez to rozumieć oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
f) **organie nadzorczym** – należy przez to rozumieć Prezesa Urzędu Ochrony Danych Osobowych;
g) **osobie upoważnionej** – należy przez to rozumieć każdego pracownika lub współpracownika ADO (niezależnie od postawy prawnej zatrudnienia), która posiada imienne upoważnienie do przetwarzania danych osobowych, nadane przez ADO;
h) **podmiocie przetwarzającym** – należy przez to rozumieć podmiot, który w imieniu ADO przetwarza dane osobowe, i któremu ADO w drodze umowy powierzył przetwarzanie danych osobowych;
i) **pracowniku**– należy przez to rozumieć każdą osobę zatrudnioną przez ADO, bez względu na podstawę jej zatrudnienia;
j) **przetwarzaniu danych osobowych** – należy przez to rozumieć jakiekolwiek operacje na danych osobowych lub zestawach danych osobowych wykonywane w sposób zautomatyzowany lub niezautomatyzowany, takie 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;
k) **pseudonimizacji** – należy przez to rozumieć 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;

l) **systemie informatycznym** – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

m) **użytkowniku** – należy przez to rozumieć pracownika ADO, który posiada imienne upoważnienie do przetwarzania danych osobowych w systemach informatycznych, nadane przez ADO;

n) **zbiorze danych osobowych** – należy przez to rozumieć uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

o) **zgodzie na przetwarzanie danych osobowych** – należy przez to rozumieć 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;

p) **RODO** – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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), Dz.Urz. UE L 119, s. 1;

q) **ustawie** – ustawa z 10 maja 2018 r. o ochronie danych osobowych, t.j. Dz.U. z 2019 r. poz. 1781 ze zm.

TYTUŁ II
ZASADY PRZETWARZANIA I OCHRONY DANYCH OSOBOWYCH
Rozdział 1
Zasady przetwarzania danych osobowych

§ 9

ADO dokłada wszelkich starań, aby dane osobowe były:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („**zgodność z prawem, rzetelność i przejrzystość**”);
b) zbierane wyłącznie dla oznaczonych, wyraźnych i zgodnych z prawem celów oraz niepoddawane dalszemu przetwarzaniu niezgodnie z tymi celami („**ograniczenie celu**”);
c) adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, w których są przetwarzane („**minimalizacja danych**”);
d) poprawne i w razie potrzeby uaktualniane („**prawidłowość**”);
e) przechowywane w postaci umożliwiającej identyfikację osób, których dane dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia określonych celów przetwarzania („**ograniczenie przechowywania**”);
f) przetwarzane w sposób zapewniający 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**”).

§ 10

1. ADO przetwarza dane osobowe wyłącznie w przypadkach wskazanych w art. 6 ust. 1 RODO, w szczególności:
   - na podstawie zgody osoby, której dane dotyczą (art. 6 ust. 1 lit. a RODO);
   - w związku z nawiązaniem lub realizacją umowy, której stroną jest osoba, której dane dotyczą, lub gdy osoba ta żąda podjęcia działań w tym zakresie (art. 6 ust. 1 lit. b RODO);
   - w związku z wykonaniem obowiązku prawnego ADO (art. 6 ust. 1 lit. c RODO);
   - na podstawie prawnie uzasadnionego interesu ADO, którym jest m.in. ustalenie, dochodzenie lub obrona roszczeń (art. 6 ust. 1 lit. f RODO).
2. ADO nie przetwarza szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO, za wyjątkiem przypadków wskazanych w art. 9 ust. 2 RODO, w szczególności:
   - na podstawie zgody osoby, której dane dotyczą (art. 9 ust. 2 lit. a RODO);
   - w związku z wykonywaniem obowiązków i szczególnych praw przez ADO lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia

społecznego i ochrony socjalnej, o ile jest to dozwolone prawem (art. 9 ust. 2 lit. b RODO);

- w związku z ustaleniem, dochodzeniem lub obroną roszczeń (art. 9 ust. 2 lit. f RODO).

3. ADO nie przetwarza danych dotyczących wyroków skazujących lub naruszeń prawa, o których mowa w art. 10 RODO, za wyjątkiem przypadków dozwolonych prawem.

Rozdział 2
Prawa podmiotu danych osobowych

§ 11

1. ADO dokłada wszelkich starań, aby przetwarzanie danych osobowych nie naruszało praw i wolności osób, których dane dotyczą (podmiotów danych osobowych).
2. W przypadku, gdy ADO zbiera dane osobowe, od osoby której dane dotyczą, podaje jej informacje określone w art. 13 ust. 1–3 RODO (pierwotny obowiązek informacyjny). W przypadku, gdy ADO pozyskał dane nie od osoby, której dane dotyczą, podaje jej informacje określone w art. 14 ust. 1, 2 i 4 RODO (wtórny obowiązek informacyjny). Pierwotny obowiązek informacyjny realizowany jest w momencie zbierania danych osobowych. Wtórny obowiązek informacyjny realizowany jest w rozsądnym terminie po uzyskaniu takich danych – najpóźniej w ciągu miesiąca, przy czym, jeżeli dane zbierane są do komunikacji z podmiotem danych, najpóźniej przy pierwszej takiej komunikacji.
3. Podmiotowi danych osobowych przysługuje również:
    a) prawo dostępu do dotyczących go danych osobowych, w tym do uzyskania ich kopii (art. 15 ust. 1 i 3 RODO);
    b) prawo do uzyskania informacji o: celu przetwarzania tych danych; kategorii danych osobowych; odbiorcach tych danych (lub ich kategoriach); planowanym okresie ich przechowywania (lub kryteriach ustalania tego okresu); prawie do żądania od ADO sprostowania, usunięcia lub ograniczenia przetwarzania tych danych lub wniesienia sprzeciwu wobec przetwarzania; prawie wniesienia skargi do organu nadzorczego; źródle pochodzenia danych (jeśli dane nie zostały zebrane od osoby, której dane

dotyczą); zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu (art. 15 ust. 1 RODO);

c) prawo żądania od ADO niezwłocznego sprostowania dotyczących go danych osobowych, jeśli są one nieprawidłowe, a także uzupełnienia niekompletnych danych osobowych (art. 16 RODO);
d) prawo żądania od ADO niezwłocznego usunięcia dotyczących go danych osobowych we wskazanych w art. 17 ust. 1 RODO okolicznościach (art. 17 RODO);
e) prawo żądania od ADO ograniczenia przetwarzania dotyczących go danych osobowych we wskazanych w art. 18 ust. 1 RODO okolicznościach (art. 18 RODO);
f) prawo do uzyskania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego danych osobowych go dotyczących, które dostarczył ADO, oraz ich przekazania innemu administratorowi danych osobowych, jeżeli przetwarzanie tych danych odbywa się na podstawie przesłanki zgody (art. 6 ust. 1 lit. a, art. 9 ust. 2 lit. a RODO) lub przesłanki umowy (art. 6 ust. 1 lit. b RODO) oraz jest dokonywane w sposób zautomatyzowany, jak również prawo żądania od ADO przekazania tych danych innemu administratorowi, o ile jest to technicznie możliwe (art. 20 RODO);
g) prawo do wniesienia sprzeciwu wobec przetwarzania dotyczących go danych osobowych we wskazanych w art. 21 RODO okolicznościach (art. 21 RODO);
h) prawo otrzymania powiadomienia o naruszeniu ochrony jego danych osobowych, które miało miejsce i które może powodować wysokie ryzyko naruszenia jego praw lub wolności (art. 34 RODO).

§ 12

1. Jeżeli podstawą prawną przetwarzania jest zgoda osoby, której dane dotyczą, jest ona wyrażana w formie oświadczenia lub wyraźnego działania potwierdzającego przyzwolenie na przetwarzanie jej danych osobowych. Takie oświadczenie woli powinno być dobrowolne, świadome, konkretne i jednoznaczne.
2. ADO umożliwia osobie, której dane dotyczą, wycofanie zgody w dowolnym momencie, w taki sam sposób, w jaki nastąpiło jej wyrażenie.

3. Wyrażenie zgody na przetwarzanie danych osobowych w innym celu niż zawarcie umowy lub świadczenie usługi nie może stanowić warunku zawarcia umowy lub świadczenia usługi. Jeżeli osoba, której dane dotyczą wyraża zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający je wyraźnie odróżnić od pozostałych kwestii.

§ 13

1. W celu realizacji praw, o których mowa w § 12 ust. 2 i 3, podmiot danych osobowych kontaktuje się z ADO na adres korespondencyjny: Nowy Targ (34-400), ul. Królowej Jadwigi 17.
2. ADO realizując prawa podmiotu danych wskazane w § 11 ust. 2 i 3 niniejszej Polityki, czyli udzielając podmiotowi danych wszelkich informacji, o których mowa w art. 13 i 14 RODO, oraz prowadząc z nim wszelką komunikację na mocy art. 12–22 i 34 RODO w sprawie przetwarzania, używa języka jasnego i prostego. Wszelkie informacje lub komunikaty związane z przetwarzaniem danych powinny mieć formę zwięzłą, przejrzystą, zrozumiałą i łatwo dostępną (zasada przejrzystości).
3. ADO udziela informacji w formie wskazanej przez podmiot danych – na piśmie lub elektronicznie, a jeżeli podmiot danych tego zażąda również w formie ustnej, o ile innymi sposobami ADO potwierdzi tożsamość osoby, której dane dotyczą.
4. ADO bez zbędnej zwłoki, a w każdym razie w terminie miesiąca od otrzymania żądania na podstawie art. 15–22 RODO, udziela osobie, której dane dotyczą informacji o działaniach podjętych w związku z tym żądaniem. Z uwagi na skomplikowany charakter żądań, ADO w razie potrzeby może wydłużyć ten termin o kolejne dwa miesiące. W takim przypadku w terminie miesiąca od otrzymania żądania ADO informuje podmiot danych o przedłużeniu terminu wraz z podaniem przyczyn opóźnienia.
5. Jeżeli żądania podmiotu danych są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, ADO może pobrać opłatę w rozsądnej wysokości albo odmówić podjęcia ich realizacji.
6. Jeżeli podstawą prawną przetwarzania danych jest zgoda podmiotu danych, o której mowa w § 12 niniejszej Polityki, ADO podejmuje działania mające na celu wykazanie, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.

Rozdział 3
Zasady udostępniania danych osobowych

§ 14

1. ADO dokłada wszelkich starań, aby dostęp do danych osobowych był realizowany zgodnie z przepisami o ochronie danych osobowych, w szczególności opierał się na jednej z podstaw prawnych przetwarzania danych określonych w art. 6 ust. 1 RODO lub art. 9 ust. 2 RODO.
2. Odbiorcą przetwarzanych przez ADO danych osobowych są w kontrahenci i klienci ADO.
3. Odbiorcą danych osobowych są również podmioty przetwarzające, które przetwarzają dane osobowe w imieniu ADO.

§ 15

1. ADO zapewnia dostęp do danych osobowych podmiotom upoważnionym na mocy odpowiednich przepisów prawa.
2. W szczególności dostęp do danych osobowych mogą mieć: Państwowa Inspekcja Pracy, Zakład Ubezpieczeń Społecznych, organy skarbowe, Policja, Straż Graniczna, Agencja Bezpieczeństwa Wewnętrznego, sądy powszechne, Najwyższa Izba Kontroli, Prezes Urzędu Ochrony Danych Osobowych i inne upoważnione przez przepisy prawa podmioty i organy, działające w granicach przyznanych im przez prawo uprawnień.

Rozdział 4
Zasady przechowywania danych (polityka retencyjności)

§ 16

1. Dane osobowe są przechowywane nie dłużej niż jest to niezbędne do celów, w których te dane są przetwarzane. Okresy przechowywania poszczególnych kategorii danych określa Załącznik nr 8 do niniejszej Polityki.

2. Po zakończeniu przetwarzania danych osobowych ADO zobowiązany jest do niezwłocznego usunięcia danych osobowych i wszelkich istniejących ich kopii, zarówno elektronicznych, jak i papierowych.
3. Usuwanie (niszczenie) zbędnych danych osobowych powinno w szczególności polegać na trwałym, fizycznym zniszczeniu danych osobowych wraz z ich nośnikami w stopniu uniemożliwiającym ich późniejsze odtworzenie przez osoby nieuprawnione przy zastosowaniu powszechnie dostępnych metod.
4. Osoby upoważnione przez ADO do przetwarzania danych osobowych mają obowiązek używania oddanych im do dyspozycji narzędzi i technik usuwania (niszczenia) zbędnych danych osobowych lub ich zbiorów.
5. Z usunięcia danych osobowych i ich kopii ADO sporządza protokół.

TYTUŁ III
OBOWIĄZKI ADMINISTRATORA DANYCH OSOBOWYCH

Rozdział 1
Współpraca z organem nadzorczym

§ 17

1. ADO współpracuje z organem nadzorczym na jego żądanie i w zakresie wykonywania przez niego swoich zadań.

§ 18

1. ADO prowadzi rejestr czynności przetwarzania, o którym mowa w art. 30 ust. 1 RODO.
2. ADO prowadzi także rejestr kategorii czynności przetwarzania, o którym mowa w art. 30 ust. 2 RODO.
3. ADO udostępnia organowi nadzorczemu, na jego żądanie, rejestry o których mowa w ust. 1 i 2 niniejszego paragrafu w celu monitorowania procesów przetwarzania danych osobowych.

Rozdział 2
Nadawanie upoważnień do przetwarzania danych osobowych

§ 19

1. Do przetwarzania danych osobowych mogą zostać dopuszczone wyłącznie osoby posiadające aktualne upoważnienie nadane przez ADO. Wzór upoważnienia stanowi Załącznik nr 3 do niniejszej Polityki.
2. Zakres upoważnienia do przetwarzania danych osobowych powinien być adekwatny do rodzaju pracy świadczonej przez osobę upoważnioną i związanego z nim zakresu obowiązków.

§ 20

Przed dopuszczeniem do przetwarzania danych osobowych osoba upoważniona powinna zapoznać się z postanowieniami niniejszej Polityki. Wzór takiego oświadczenia stanowi Załącznik nr 3a do niniejszej Polityki.

§ 21

1. ADO prowadzi i w razie potrzeby aktualizuje ewidencję osób upoważnionych do przetwarzania danych osobowych. Wzór ewidencji stanowi Załącznik nr 4 do niniejszej Polityki.
2. Ewidencja, o której mowa w ust. 1, zawiera: imię i nazwisko osoby upoważnionej, numer upoważnienia, datę nadania i datę ustania upoważnienia, zakres upoważnienia oraz identyfikator użytkownika, jeśli dane osobowe są przetwarzane w systemie informatycznym, a także określenie charakteru podmiotu nadającego upoważnienie.
3. W ewidencji, o której mowa w ust. 1, uwzględnia się również osoby, które zostały przez ADO upoważnione do przetwarzania danych innego administratora danych, co dotyczy przypadku, gdy ADO występuje w roli Podmiotu przetwarzającego na podstawie umowy o powierzenie przetwarzania danych.

§ 22

1. Upoważnienie do przetwarzania danych osobowych wygasa w przypadku ustania stosunku pracy lub innego stosunku zatrudnienia będącego podstawą jego nadania, lub ustania umowy o świadczenie usług, która rodzi konieczność powierzenia przetwarzania danych, co dotyczy przypadku gdy ADO występuje w roli Podmiotu przetwarzającego.
2. W razie zmiany rodzaju pracy lub zakresu obowiązków osoby upoważnionej, ADO dokonuje weryfikacji zakresu nadanego upoważnienia do przetwarzania danych osobowych i w razie potrzeby odwołuje dotychczasowe upoważnienie oraz nadaje nowe upoważnienie.
3. W przypadku zaistnienia podejrzenia naruszenia przez osobę upoważnioną przepisów o ochronie danych osobowych lub postanowień Polityki, ADO może zdecydować o odwołaniu upoważnienia do przetwarzania danych osobowych. Fakt ten ADO niezwłocznie odnotowuje w ewidencji osób upoważnionych do przetwarzania danych osobowych.

§ 23

Osoba upoważniona jest zobowiązana do:

a) zapoznania się z niniejszą Polityką oraz przestrzegania jej postanowień;
b) przestrzegania przepisów o ochronie danych osobowych;
c) stosowania określonych przez ADO procedur i środków mających na celu zabezpieczenie danych osobowych przed dostępem osób nieuprawnionych;
d) zachowania szczególnej staranności w procesach przetwarzania danych osobowych;
e) przetwarzania danych osobowych tylko w wyznaczonych do tego celu pomieszczeniach lub ich wydzielonych częściach;
f) przestrzegania określonych w Polityce zasad bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych;
g) stosowania się do zaleceń ADO lub pracownika odpowiedzialnego za obsługę informatyczną dotyczących bezpieczeństwa informacji przetwarzanych w systemach informatycznych;
h) niezwłocznego zawiadamiania ADO lub pracownika odpowiedzialnego za obsługę informatyczną o przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych przetwarzanych w systemach informatycznych;

i) niezwłocznego zawiadamiania ADO o wszelkich przypadkach naruszenia lub podejrzenia naruszenia ochrony danych osobowych.

§ 24

Obowiązek zachowania w tajemnicy danych osobowych, do których osoba upoważniona uzyskała dostęp w związku z wykonywaniem obowiązków na danym stanowisku pracy i stosownie do udzielonego przez ADO upoważnienia, trwa również po ustaniu stosunku pracy lub innego stosunku zatrudnienia będącego podstawą nadania upoważnienia. Dotyczy to również przypadków, gdy ADO udziela ww. upoważnienia występując w roli Podmiotu przetwarzającego.

§ 25

1. ADO zapewnia zapoznanie osób upoważnionych z przepisami o ochronie danych osobowych.
2. Zaznajomienie osób upoważnionych z przepisami o ochronie danych osobowych, postanowieniami Polityki i innymi regulacjami wewnętrznymi, a także środkami technicznymi i organizacyjnymi służącymi zabezpieczeniu danych osobowych może odbywać się w szczególności przez:
   - instruktaż na stanowisku pracy,
   - szkolenie wewnętrzne,
   - szkolenie zewnętrzne.
3. ADO organizuje szkolenia z zakresu ochrony danych osobowych dla osób upoważnionych lub zapewnia im w innych formach dostęp do wiedzy z zakresu ochrony danych osobowych w celu podnoszenia świadomości osób upoważnionych w przedmiocie aktualnych przepisów o ochronie danych osobowych.

§ 26

Naruszenie przez osoby upoważnione zasad przetwarzania danych osobowych lub odpowiedniego zabezpieczenia tych danych może zostać zakwalifikowane jako ciężkie naruszenie podstawowych obowiązków pracowniczych ze wszystkimi wynikającymi

stąd konsekwencjami, z rozwiązaniem stosunku pracy lub innego stosunku zatrudnienia włącznie.

Rozdział 3
Powierzenie przetwarzania danych osobowych

§ 27

1. ADO powierza przetwarzanie danych osobowych wyłącznie takiemu podmiotowi przetwarzającemu, który zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych lub organizacyjnych, by przetwarzanie spełniało wymogi określone przepisami RODO i chroniło prawa osób, których dane dotyczą.
2. W przypadku określonym w ust. 1 zawierana jest w formie pisemnej lub innej formie udokumentowanej umowa powierzenia przetwarzania danych lub odbywa się to na podstawie innego instrumentu prawnego, zgodnie z prawem Unii lub prawem państwa członkowskiego. ADO w rejestrze czynności przetwarzania odnotowuje umowy powierzenia przetwarzania.
3. Umowa, o której mowa w ust. 2, powinna określać:
    - przedmiot przetwarzania,
    - czas trwania przetwarzania,
    - charakter przetwarzania,
    - cel przetwarzania,
    - rodzaj powierzonych danych,
    - kategorie osób, których dane dotyczą,
    - obowiązki i prawa ADO,
    - obowiązki Podmiotu przetwarzającego,
    - warunki ewentualnego podpowierzenia przetwarzanych danych.
4. Przetwarzanie danych przez podmiot przetwarzający, z którego usług korzysta ADO, nie powoduje zmiany właściwego administratora. Podmiot przetwarzający przetwarza dane w imieniu ADO i w sposób przez niego określony.
5. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej zgody ADO.

6. Powierzenie przetwarzania danych podmiotom mającym siedzibę w państwie trzecim lub organizacji międzynarodowej wymaga spełnienia przesłanek i obowiązków określonych w Tytule V niniejszej Polityki.

§ 28

Jeżeli inny podmiot polecił ADO przetwarzanie danych osobowych w jego imieniu, ADO działając jako podmiot przetwarzający zobowiązany jest w szczególności:

- przetwarzać dane osobowe wyłącznie na udokumentowane polecenie powierzającego, co dotyczy też przekazywania tych danych do państwa trzeciego lub organizacji międzynarodowej, chyba że taki obowiązek nakłada nie niego prawo Unii lub państwa członkowskiego. W takim przypadku podmiot przetwarzający informuje powierzającego dane osobowe o tym obowiązku prawnym, o ile prawo nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;
- upoważnić osoby, którym polecił przetwarzanie powierzonych danych do ich przetwarzania oraz zobowiązać je do zachowania tajemnicy;
- podejmować wszelkie środki bezpieczeństwa przetwarzania, zgodnie z art. 32 RODO;
- przestrzegać warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w art. 28 ust. 2 i 4 RODO;
- w miarę możliwości pomagać powierzającemu przetwarzanie wywiązywać się z obowiązków względem podmiotów danych (realizacja żądań podmiotów danych);
- pomagać podmiotowi powierzającemu dane wywiązywać się z obowiązków określonych w art. 32–36 RODO;
- po zakończeniu usług związanych z przetwarzaniem usunąć lub zwrócić dane powierzającemu oraz usunąć wszelkie ich kopie – w zależności od jego decyzji, chyba że prawo Unii lub państwa członkowskiego nakazuje przechowywanie tych danych;
- umożliwić powierzającemu lub upoważnionej przez niego osobie przeprowadzanie audytów;
- prowadzić rejestr kategorii czynności przetwarzania, którego wzór stanowi Załącznik nr 2 do niniejszej Polityki.

Rozdział 4
Inne obowiązki administratora danych osobowych

§ 29

1. ADO wykonuje swoje obowiązki stosując podejście oparte na ryzyku (zasada rozliczalności). W szczególności zobowiązany jest do przeprowadzania okresowej analizy procesów przetwarzania danych, a następnie do dokonywania ogólnej oceny ryzyka, jakie wiąże się z przetwarzaniem danych w konkretnym przypadku. ADO uwzględnia przy tym ryzyko naruszenia praw lub wolności osób, których dane dotyczą.
2. ADO ocenia ryzyko, jakie wiąże się z przetwarzaniem danych, o którym mowa w ust. 1, po weryfikacji kontekstu przetwarzania danych, w szczególności określeniu procesów i zasobów, w ramach których dane są przetwarzane, celów przetwarzania, kategorii i zakresu przetwarzanych danych, podstaw prawnych przetwarzania, a także używanych narzędzi i zastosowanych zabezpieczeń.
3. ADO na bieżąco monitoruje, czy nie zachodzi konieczność realizacji innych obowiązków, jakie przepisy RODO nakładają na ADO, w szczególności obowiązku przeprowadzania oceny skutków przetwarzania, o którym mowa w art. 35 RODO.
4. ADO stosuje środki techniczne i organizacyjne służące zabezpieczeniu przetwarzanych danych osobowych, o których mowa w tytule IV niniejszej Polityki.
5. ADO dokumentuje wszelkie naruszenia ochrony danych osobowych na zasadach wskazanych w rozdziale 3 tytułu IV niniejszej Polityki.

TYTUŁ IV
ŚRODKI TECHNICZNE I ORGANIZACYJNE BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Rozdział 1
Środki organizacyjne i techniczne służące zabezpieczeniu danych osobowych

§ 30

1. ADO stosuje odpowiednie środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpiecza dane te przed:
   - ich udostępnieniem osobom nieuprawnionym,
   - zabraniem ich przez osobę nieuprawnioną,
   - przetwarzaniem ich z naruszeniem przepisów o ochronie danych osobowych,
   - ich zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Przed zastosowaniem środków, o których mowa w ust. 1, ADO przeprowadza analizę ryzyka, uwzględniając charakter, zakres, kontekst i cele przetwarzania, w tym ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze naruszenia, zgodnie z postanowieniami § 29 niniejszej Polityki.
3. ADO dokonuje okresowego przeglądu środków, o których mowa w ust. 1.

§ 31

1. Przetwarzanie danych osobowych powinno odbywać się wyłącznie w obszarze do tego celu przeznaczonym.
2. W obszarze, w którym przetwarzane są dane osobowe, mogą przebywać osoby upoważnione do przetwarzania danych osobowych oraz osoby nadzorujące przetwarzanie danych osobowych.
3. Osoby trzecie mogą przebywać w ww. obszarze wyłącznie pod nadzorem osoby upoważnionej do przetwarzania danych osobowych.

§ 32

Obszar przetwarzania danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych przez zastosowanie następujących środków:

a) system alarmowy w budynku, w którym znajduje się siedziba ADO;
b) system monitoringu przy użyciu kamer w budynku, w którym znajduje się siedziba ADO;
c) kontrolę wejścia do siedziby ADO przy użyciu klucza.

§ 33

1. ADO sprawuje kontrolę dostępu do siedziby tj. przestrzeni, w której przetwarzane są dane osobowe, poprzez stosowanie klucza.
2. Serwer znajduje się siedzibie ADO w pomieszczeniu zamykanym na klucz.
3. Szafki, w których przechowywane są dane osobowe przetwarzane w sposób tradycyjny (papierowy) są zamykane na klucz.
4. Klucze do szafek i klucz do pomieszczenia, w którym jest serwer posiadają tylko osoby upoważnione do przetwarzania danych, tj. osoby, które są zatrudnione na stanowisku związanym z dostępem do danych osobowych oraz przełożeni tych osób.
5. Klucze trzymane są w skrzynkach z zamkiem szyfrowym (kod).

§ 34

1. Całkowite opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe, powinno wiązać się z zastosowaniem dostępnych środków zabezpieczających to pomieszczenie przed wejściem osób nieuprawnionych (wylogowanie się z systemu, zamknięcie szafek, umieszczenie klucza w skrzynce z zamkiem szyfrowym).
2. Opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe, powinno wiązać się z zastosowaniem dostępnych środków zabezpieczających używane aktualnie zbiory danych osobowych. W razie planowanej, choćby chwilowej nieobecności osoby upoważnionej, obowiązana jest ona umieścić zbiory prowadzone w sposób tradycyjny (papierowy), jak również nośniki informacji zawierające dane osobowe, w odpowiednio zabezpieczonym miejscu ich przechowywania (np. w szafkach) oraz dokonać niezbędnych operacji w systemie informatycznym uniemożliwiającym dostęp do danych osobowych osobom nieuprawnionym (np. skorzystanie z mechanizmu blokowania stacji roboczej).
3. Opuszczenie przez osobę upoważnioną obszaru przetwarzania danych osobowych bez zabezpieczenia pomieszczenia oraz umiejscowionych w nim zbiorów danych osobowych lub nośników informacji jest niedopuszczalne i stanowi naruszenie podstawowych obowiązków pracowniczych.

Rozdział 2
Środki techniczne służące zabezpieczeniu danych osobowych przetwarzanych w systemie informatycznym

§ 35

1. Przyjęte przez ADO środki techniczne służące zabezpieczeniu danych osobowych przetwarzanych w systemie informatycznym określa Instrukcja zarządzania systemem informatycznym, która stanowi załącznik nr 9 do niniejszej Polityki.
2. ADO odpowiada za korygowanie zasad określonych w Instrukcji zarządzania systemem informatycznym, w przypadku uzasadnionych zmian w przepisach prawnych dotyczących przetwarzania danych osobowych w systemach informatycznych, jak również zmian organizacyjno-funkcjonalnych zachodzących w spółce.
3. Pracownicy ADO zobowiązani są do zapoznania się zasadami przetwarzania danych w systemie informatycznym określonymi w Instrukcji zarządzania systemem informatycznym.

Rozdział 3
Pozostałe środki techniczne i organizacyjne służące zabezpieczeniu danych osobowych

§ 36

1. ADO wdrożył oraz stosuje Instrukcję bezpieczeństwa pożarowego, która określa wymagania ochrony przeciwpożarowej w zakresie organizacyjnym, technicznym i porządkowym, jakie należy uwzględnić podczas eksploatacji budynku, w którym znajduje się siedziba spółki, zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z 7 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz.U. Nr 109 poz. 719).
2. ADO wdrożył oraz stosuje Instrukcję bhp, w tym stanowiskową, gdzie określa się zasady bezpiecznego wykonywania pracy z zachowaniem wymaganej technologii, zgodnie z rozporządzeniem Ministra Pracy i Polityki Socjalnej z 26

września 1997 r. w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy (t.j. Dz.U. z 2003 r. Nr 169, poz. 1650 ze zm.).

Rozdział 4
Procedura postępowania w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych

§ 37

1. Każda osoba upoważniona, która dostrzeże zdarzenie mogące spowodować naruszenie ochrony danych osobowych, jest zobowiązana niezwłocznie zgłosić ten fakt ADO, a w przypadku, gdy dotyczy to danych osobowych przetwarzanych w systemie informatycznym – także pracownikowi odpowiedzialnemu u ADO za obsługę informatyczną.
2. W przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych należy powstrzymać się od wszelkich czynności mogących skutkować zatarciem śladów tego zdarzenia oraz zastosować się do poleceń ADO lub pracownika odpowiedzialnego ADO za obsługę informatyczną.
3. W przypadku utraty lub kradzieży dokumentów zawierających dane osobowe lub nośników tych danych każda osoba upoważniona jest zobowiązana niezwłocznie zgłosić ten fakt ADO.

§ 38

1. Po otrzymaniu zgłoszenia naruszenia lub podejrzenia naruszenia ochrony danych osobowych ADO lub pracownik odpowiedzialny u ADO za obsługę informatyczną niezwłocznie podejmują czynności wyjaśniające mające na celu ustalenie, czy doszło do naruszenia ochrony danych osobowych.
2. W przypadku stwierdzenia naruszenia ochrony danych osobowych ADO lub pracownik odpowiedzialny u ADO za obsługę informatyczną niezwłocznie podejmują niezbędne czynności zabezpieczające dane osobowe przed ich utratą, uszkodzeniem lub zniszczeniem, niezgodnym z prawem przetwarzaniem bądź uzyskaniem przez osoby nieuprawnione dostępu do nich.

3. ADO dokumentuje wszelkie naruszenia ochrony danych osobowych. W tym celu sporządza raport, którego wzór stanowi Załącznik nr 5 do niniejszej Polityki. Celem raportu jest w szczególności wskazanie przyczyn naruszenia oraz osób za nie odpowiedzialnych, jak również dokonanie analizy poprawności funkcjonowania reguł ochrony danych osobowych w celu uniknięcia podobnych zdarzeń w przyszłości i podjęcia ewentualnych działań naprawczych.
4. Raporty, o których mowa w ust. 3, wchodzą w skład Rejestru incydentów, który ADO okazuje na żądanie organu nadzorczego.

§ 39

1. W terminie 72 godzin od dnia stwierdzenia naruszenia ochrony danych osobowych ADO dokonuje zgłoszenia do organu nadzorczego. Jeżeli zgłoszenie zostanie dokonane po upływie 72 godzin, należy podać wyjaśnienie przyczyn opóźnienia. Wzór takiego zgłoszenia stanowi Załącznik nr 7 do niniejszej Polityki.
2. Zgłoszenie, o którym mowa w ust. 1 nie jest wymagane, jeżeli jest mało prawdopodobne, aby naruszenie skutkowało ryzykiem naruszenia praw lub wolności osoby fizycznej. ADO odpowiada za dokonanie oceny istnienia lub nieistnienia wspomnianego ryzyka.
3. Każde naruszenie, również to, o którym mowa w ust. 2, powinno być odnotowane w Rejestrze incydentów, który składa się z raportów dokumentujących naruszenia danych osobowych. Wzór takiego raportu stanowi Załącznik Nr 5 do niniejszej Polityki.
4. W przypadku gdy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osoby fizycznej, ADO bez zbędnej zwłoki zawiadamia podmiot danych o jego wystąpieniu. Wzór takiego zawiadomienia stanowi Załącznik nr 6 do niniejszej Polityki.
5. Zawiadomienie, o którym mowa w ust. 4 nie jest wymagane w przypadku gdy:
   - zostały wdrożone odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych, których dotyczy naruszenie, w szczególności takie jak szyfrowanie uniemożliwiające odczyt osobom nieuprawnionym do dostępu do danych;
   - ADO następnie przedsięwziął środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
   - wymagałoby to niewspółmiernie dużego wysiłku – w takim przypadku należy wydać komunikat publiczny.

TYTUŁ V
TRANSFERY DANYCH DO PAŃSTW TRZECICH

§ 40

W przypadku gdy ADO przekazuje dane do państwa trzeciego lub organizacji międzynarodowej musi odnotować to w rejestrze czynności przetwarzania wraz podaniem podstawy przetwarzania oraz zapewnić nienaruszalność stopnia ochrony osób fizycznych gwarantowanego w RODO, przez co w szczególności należy rozumieć spełnienie warunków określonych w § 41.

§ 41

1. Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, gdy Komisja stwierdzi, że to państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony.
2. Przy braku decyzji Komisji, o której mowa w ust. 1, przekazanie przez ADO danych do państwa trzeciego może nastąpić jeżeli:
   a) zostały zapewnione odpowiednie zabezpieczenia danych, które nie wymagają uzyskania specjalnego zezwolenia ze strony organu nadzorczego, przez co należy rozumieć:
      - prawnie wiążący i egzekwowalny instrument między organami lub podmiotami publicznymi;
      - wiążące reguły korporacyjne zgodnie z art. 47 RODO;
      - standardowe klauzule ochrony danych przyjęte przez Komisję zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2 RODO;
      - standardowe klauzule ochrony danych przyjęte przez organ nadzorczy i zatwierdzone przez Komisję zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2 RODO;
      - zatwierdzony kodeks postępowania zgodnie z art. 40 RODO wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich

zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą; lub

- zatwierdzony mechanizm certyfikacji zgodnie z art. 42 RODO wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą;

b) zostały zapewnione odpowiednie zabezpieczenia danych, pod warunkiem uzyskania zezwolenia ze strony właściwego organu nadzorczego, przez co należy rozumieć:

- klauzule umowne między administratorem lub podmiotem przetwarzającym a administratorem, podmiotem przetwarzającym lub odbiorcą danych osobowych w państwie trzecim lub organizacji międzynarodowej; lub
- postanowienia uzgodnień administracyjnych między organami lub podmiotami publicznymi, w których przewidziane są egzekwowalne i skuteczne prawa osób, których dane dotyczą.

3. Przy braku decyzji Komisji, o której mowa w ust. 1, lub braku zabezpieczeń, o których mowa w ust. 2, jednorazowe lub wielokrotne przekazanie danych do państwa trzeciego lub organizacji międzynarodowej może nastąpić wyłącznie pod warunkiem, że:

- osoba, której dane dotyczą, została poinformowana o ewentualnym ryzyku, z którymi – ze względu na brak decyzji stwierdzającej odpowiedni stopień ochrony oraz na brak odpowiednich zabezpieczeń – może się dla niej wiązać proponowane przekazanie, wyraźnie wyraziła na nie zgodę;
- przekazanie jest niezbędne do wykonania umowy między osobą, której dane dotyczą, a administratorem lub do wprowadzenia w życie środków przedumownych podejmowanych na żądanie osoby, której dane dotyczą;
- przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, której dane dotyczą, między administratorem a inną osobą fizyczną lub prawną;
- przekazanie jest niezbędne ze względu na ważne względy interesu publicznego;
- przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń;

- przekazanie jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą, lub innych osób, jeżeli osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody; lub
- przekazanie następuje z rejestru, który zgodnie z prawem Unii lub prawem państwa członkowskiego ma służyć za źródło informacji dla ogółu obywateli i który jest dostępny dla ogółu obywateli lub dla każdej osoby mogącej wykazać prawnie uzasadniony interes – ale wyłącznie w zakresie, w jakim w danym przypadku spełnione zostały warunki takiego dostępu określone w prawie Unii lub w prawie państwa członkowskiego.

TYTUŁ VI
POSTANOWIENIA KOŃCOWE

§ 42

1. Postanowienia niniejszej Polityki wchodzą w życie z dniem ……
2. Niniejsza Polityka jest dokumentem przeznaczonym do użytku wewnętrznego i nie może być ona przekazywana osobom trzecim bez zgody ADO.
3. Wszystkie osoby upoważnione do przewarzania danych osobowych zobowiązane są do stosowania przy przetwarzaniu danych postanowień zawartych w niniejszej Polityce.
4. Osoba, o której mowa w ust. 3, zobowiązana jest złożyć oświadczenie o tym, iż została zapoznana z przepisami dotyczącym przewarzania danych osobowych (RODO) oraz postanowieniami niniejszej Polityki, a także o zobowiązaniu się do ich przestrzegania. Takie oświadczenie, złożone przez osobę która jest pracownikiem przechowuje się w jej atakach osobowych (wzór oświadczenia stanowi załącznik Nr 3a do niniejszej Polityki).
5. W sprawach nieuregulowanych w niniejszej Polityce zastosowanie mają przepisy RODO i ustawy.

Załącznik nr 1 do Polityki – Rejestr czynności przetwarzania (osobny plik excelowy)

Załącznik nr 2 do Polityki – Rejestr kategorii czynności przetwarzania (osobny plik excelowy)

Załącznik nr 3 do Polityki – wzór upoważnienia do przetwarzania danych osobowych

UPOWAŻNIENIE NR …….
do przetwarzania danych osobowych
w systemach informatycznych lub w zbiorach w wersji papierowej

W związku z art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (Dz.Urz. UE L Nr 119, s. 1),

*z dniem ……, **upoważniam Panią/Pana*……,***
jako pracownika JOB-JOB Sp. z o.o. zatrudnionego na stanowisku …….. na podstawie umowy o pracę/umowy cywilnoprawnej, **do przetwarzania danych osobowych**.*

*Zakres przedmiotowy upoważnienia wyznacza **zajmowane przez Panią/Pana* stanowisko tj. ……** oraz określony na nim zakres obowiązków.*

Upoważnienie obejmuje przetwarzanie danych w:

*I. **systemach informatycznych** w ramach nadanych dostępów (podać nazwy systemów lub programów), w tym:*

1) ……..,

2) ……..,

3) ……..,

lub

II. ***zbiorach papierowych*** *(podać nazwy tych zbiorów), w tym:*

1) ……..,

2) ……..,

3) ……..,

np. w zakresie przeglądania, wprowadzania, modyfikacji, usuwania, archiwizacji lub udostępniania innym podmiotom, ***pod warunkiem, że następuje to w związku z wykonywaniem Pani/Pana* obowiązków pracowniczych****.*

Niniejsze upoważnienie nie upoważnia do udzielania dalszych upoważnień i jest ważne do czasu zakończenia stosunku pracy/stosunku cywilnoprawnego a ponadto może być w każdym czasie zmienione lub odwołane.*

Jednocześnie zobowiązuję Panią/Pana do zachowania w tajemnicy wszystkich przetwarzanych danych osobowych oraz sposobu ich zabezpieczenia, a także do przestrzegania obowiązujących przepisów prawa o ochronie danych osobowych oraz przyjętych u administratora tj. JOB-JOB Sp. z o.o. wewnętrznych procedur dotyczących bezpieczeństwa informatycznego oraz ochrony danych osobowych, a w szczególności Polityki Ochrony Danych Osobowych.*

**Z dniem podpisania niniejszego upoważnienia traci moc upoważnienie nr ..... udzielone Pani/Pana w dniu ..... .*

……..

(podpis osoby reprezentującej administratora)

……

(data oraz podpis pracownika/współpracownika przyjmującego upoważnienie)

*Do skreślenia, gdy nie dotyczy.

Załącznik nr 3a do Polityki – wzór oświadczenia osoby upoważnionej do przetwarzania danych osobowych

……

(miejsce i data)

……

(imię, nazwisko, stanowisko pracownika, któremu nadano upoważnienie)

Oświadczenie osoby upoważnionej do przewarzania danych

Niniejszym oświadczam, że zostałem/-am zapoznany/-a z przepisami dotyczącymi przewarzania danych osobowych (RODO) oraz postanowieniami Polityki ochrony danych osobowych wdrożonej do stosowania w JOB-JOB Sp. z o.o., który to podmiot działa jako administrator danych osobowych.

Oświadczam jednocześnie, że jako osoba upoważniona do przetwarzania danych osobowych zobowiązuje się do stosowania przy przetwarzaniu danych postanowień zawartych w tej Polityce oraz we wskazanych wyżej przepisach dotyczących przewarzania danych osobowych.

……

(podpis pracownika składającego oświadczenie)

Załącznik nr 4 do Polityki – wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Ewidencja osób upoważnionych do przetwarzania danych osobowych:

L.p.	Imię i nazwisk	Numer upoważnienia	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia	Identyfikator użytkownika	Charakter podmiotu nadającego

	o						**upoważnienie (ADO/Procesor)**
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							

Załącznik nr 5 do Polityki – wzór raportu dotyczącego naruszenia ochrony danych osobowych

Raport dotyczący naruszenia ochrony danych osobowych:

1. Data powiadomienia: ..... Godzina powiadomienia: .....

2. Osoba powiadamiająca o zdarzeniu:

.....

(imię i nazwisko oraz stanowisko pracy)

3. Data naruszenia: ..... Godzina naruszenia: …….....

4. Miejsce zdarzenia:

.....

(oznaczenie lokalizacji/pomieszczenia/stanowiska komputerowego)

5. Opis naruszenia i okoliczności naruszenia (w tym udział osób trzecich):

.....

…….....

…….....

6. Podjęte działania:

.....

…….....

…….....

7. Przyczyny wystąpienia naruszenia (w tym wskazanie osób odpowiedzialnych za naruszenie):

.....

…….....

…….....

8. Ustalenia końcowe będące efektem przeprowadzonego postępowania wyjaśniającego:

.....

…….....

…….....

.....

data i podpis osoby reprezentującej ADO

Załącznik nr 6 do Polityki – wzór zawiadomienia podmiotu danych o naruszeniu ochrony danych osobowych

Zawiadomienie o naruszeniu ochrony danych osobowych

1. Data powiadomienia: .....

3. Data naruszenia: .....

4. Miejsce zdarzenia:

.....

(oznaczenie lokalizacji/pomieszczenia/stanowiska komputerowego)

5. Opis naruszenia i okoliczności naruszenia (w tym udział osób trzecich):

.....
……..
……..

6. Przyczyny wystąpienia naruszenia:

.....
……..
……..

7. Podjęte przez ADO działania (środki zastosowane lub proponowane) w celu zaradzenia zaistniałemu naruszeniu:

.....
……..
.....

8. Konsekwencje zaistniałego naruszenia dla podmiotu danych:

.....
……..
……..

1. Więcej informacji w sprawie przedmiotowego naruszenia można uzyskać pod nr tel. …….. lub e-mail …….. od …….
   (imię i nazwisko oraz dane kontaktowe IODO lub oznaczenie innego punktu kontaktowego)

.....

data i podpis osoby reprezentującej ADO

Załącznik nr 7 do Polityki – wzór zgłoszenia naruszenia do Urzędu Ochrony Danych Osobowych przygotowany przez organ nadzorczy i dostępny na stronie www.uodo.gov.pl

1. Dane wnioskodawcy
A. Podaj typ zgłoszenia
Wskaż czy zgłaszasz naruszenie ochrony danych osobowych mające charakter jednorazowego zdarzenia (np. zgubienie, kradzież nośnika danych, przypadkowe wysłanie danych osobie nieuprawnionej), czy przygotowujesz wstępne zgłoszenie, które uzupełnisz później, lub czy uzupełniasz lub zmieniasz wcześniejsze zgłoszenie.
Podaj datę poprzedniego zgłoszenia (opcjonalnie – jeśli zgłoszenie jest uzupełniające/zmieniające) ……
2. Podmiot zgłaszający
A. Dane administratora danych
Pełna nazwa administratora ……

REGON – jeśli został podany (opcjonalnie)	.....	
Sektor (opcjonalnie)	*Dla sektora publicznego:*	*Dla sektora prywatnego:* .....

B. Adres siedziby administratora danych

Państwo	.....	Miejscowość	.....
Województwo	.....	Ulica	.....
Powiat	.....	Kod pocztowy	.....
Gmina	.....	Numer domu	..... Numer lokalu ....

C. Osoby uprawnione do reprezentowania administratora

1.	Imię i nazwisko	Stanowisko	.....

(Aby dopisać kolejne osoby, należy po kliknięciu na powyższe pole kliknąć przycisk , który pojawi się po prawej stronie)

D. Pełnomocnik

☐Wniosek wypełniany przez pełnomocnika (opcjonalnie)

Pełnomocnictwo udzielone w formie elektronicznej oraz dowód uiszczenia opłaty skarbowej należy załączyć podczas składania wniosku przez portal biznes.gov.pl.

Pełnomocnictwo opatrzone kwalifikowanym podpisem elektronicznym osoby udzielającej pełnomocnictwa.

E. Inspektor ochrony danych

Imię i nazwisko	……
Numer telefonu	……
Adres e-mail	……

☐Inspektor nie został wyznaczony

Jeśli inspektor nie został wyznaczony podaj dane innego punktu kontaktowego, od którego można uzyskać więcej informacji o naruszeniu.

……

F. Inne podmioty uczestniczące w przetwarzaniu danych, których dotyczy naruszenie (opcjonalnie)

Podaj nazwy podmiotów, dane kontaktowe i wyjaśnij ich rolę w procesie przetwarzania, którego dotyczy naruszenie

……

3. Czas naruszenia

A. Wykrycie naruszenia i powiadomienie organu nadzorczego

Data stwierdzenia naruszenia Wskaż kiedy dowiedziałeś/aś się o naruszeniu. Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.	……
Sposób stwierdzenia naruszenia Np. zgłoszenie osoby której dane dotyczą czy cykliczny przegląd logów systemowych zgodnie z wdrożoną polityką bezpieczeństwa	……
Data powiadomienia przez podmiot przetwarzający (opcjonalnie)	…… ….

Jeśli nie znasz dokładnego terminu,
podaj czas przybliżony.

Powody opóźnienia powiadomienia organu nadzorczego o naruszeniu

Pole obowiązkowe jeśli czas od momentu stwierdzenia naruszenia do czasu wypełniania formularza jest dłuższy niż 72h

.....

B. Czas naruszenia

Data i czas zaistnienia/rozpoczęcia naruszenia .....

Jeśli nie znasz dokładnego terminu, podaj czas przybliżony. .....

☐Trwające naruszenie

Zaznacz to pole, jeśli naruszenie trwa nadal w momencie zgłaszania.

Data i czas zakończenia naruszenia (opcjonalnie) .....

Jeśli nie znasz dokładnego terminu, podaj czas przybliżony. .....

C. Komentarz do czasu naruszenia (opcjonalnie)

Możesz podać więcej szczegółów dotyczących czasu naruszenia i uzasadnić dlaczego nie są znane dokładne terminy zaistnienia naruszenia.

.....

4. Charakter naruszenia

A. Charakter

☐Naruszenie poufności danych

Nieuprawnione lub przypadkowe ujawnienie bądź udostępnienie danych

☐Naruszenie integralności danych

Wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania

☐Naruszenie dostępności danych

Brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez osobę do tego

uprawnioną

B. Na czym polegało naruszenie?

☐Zgubienie lub kradzież nośnika/urządzenia

☐Dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji

☐Korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy

☐Nieuprawnione uzyskanie dostępu do informacji

☐Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń

☐Złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność danych

☐Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing)

☐Nieprawidłowa anonimizacja danych osobowych w dokumencie

☐Nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora

☐Niezamierzona publikacja

☐Dane osobowe wysłane do niewłaściwego odbiorcy

☐Ujawnienie danych niewłaściwej osoby

☐Ustne ujawnienie danych osobowych

Opisz na czym polegało naruszenie.

……

……

……

……

……

C. Dzieci

☐Naruszenie dotyczy przetwarzania danych w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.

(opcjonalnie)

D. Przyczyna naruszenia

☐Wewnętrzne działanie niezamierzone

☐Wewnętrzne działanie zamierzone

☐Zewnętrzne działanie niezamierzone

☐Zewnętrzne działanie zamierzone

Inne przyczyny (w tym nieznane)

……

4.1. Kategorie danych osobowych

UWAGA: W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.

A. Kategorie danych

Szczegółowy opis kategorii danych, których dotyczy naruszenie

Wymień jakie dane uległy naruszeniu: np. w przypadku sklepu internetowego profil użytkownika, w skład którego wchodzą: nazwa użytkownika, imię, nazwisko, hasło (zapisane otwartym tekstem lub hashowane), adres e-mail, oraz historia transakcji - kwota, data i nazwa kupionego produktu.

……

…

B. Dane podstawowe

☐Dane identyfikacyjne

np. imię, nazwisko, nr dowodu osobistego, adres IP

☐Krajowy numer identyfikacyjny

np. PESEL, SSN

☐Dane kontaktowe

np. e-mail, numer telefonu, adres korespondencyjny

☐Dane ekonomiczne i finansowe

np. historie transakcji, faktury, dane o rachunkach bankowych, wnioski o wsparcie finansowe

☐Oficjalne dokumenty

np. akty notarialne, dowody osobiste, prawa jazdy, karty pobytu, legitymacje

☐Dane lokalizacyjne

np. GPS, dane o przemieszczaniu, miejsce zamieszkania

☐Inne

Opisz poniżej kategorie danych:

……

C. Dane szczególnej kategorii

☐Dane o pochodzeniu rasowym lub etnicznym

☐Dane o poglądach politycznych

☐Dane o przekonaniach religijnych lub światopoglądowych

☐Dane o przynależności do związków zawodowych

☐Dane dotyczące seksualności lub orientacji seksualnej

☐Dane dotyczące zdrowia

☐Dane genetyczne

☐Dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej

D. Dane, o których mowa w art. 10 RODO

☐Dane dotyczące wyroków skazujących

☐Dane dotyczące czynów zabronionych

☐Inne

Opisz poniżej kategorie danych:

……

E. Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie

Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie

Nie dotyczy to liczby osób. Jednej osobie można przypisać kilka wpisów (np. jednej osobie można przypisać kilka wykonanych transakcji)

……

……

4.2. Kategorie osób

UWAGA: W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.

A. Kategorie osób, których dane dotyczą

☐Pracownicy

☐Użytkownicy

☐Subskrybenci

☐Studenci

☐Uczniowie

☐Służby mundurowe (np. wojsko, policja)

☐Klienci (obecni i potencjalni)

☐Klienci podmiotów publicznych

☐Pacjenci

☐Dzieci

☐Osoby o szczególnych potrzebach (np. osoby starsze, niepełnosprawne itp.)

Szczegółowy opis kategorii osób, których dotyczy naruszenie.

Opisz np. kogo i w jakim przedziale czasowym dotyczy naruszenie

……

……

B. Liczba osób, których mogło dotyczyć naruszenie

Przybliżona liczba osób, których mogło dotyczyć naruszenie

……

5. Środki bezpieczeństwa zastosowane przed naruszeniem

A. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa stosowanych przez administratora przed naruszeniem (opcjonalnie)

Kliknij tutaj, aby wprowadzić tekst.

6. Możliwe konsekwencje

A. Uszczerbek fizyczny, majątkowy, niemajątkowy lub inne znaczące konsekwencje dla osoby, której dane dotyczą

☐Utrata kontroli nad własnymi danymi osobowymi
☐Ograniczenie możliwości realizowania praw z art. 15-22 RODO
☐Ograniczenie możliwości realizowania praw
☐Dyskryminacja
☐Kradzież lub sfałszowanie tożsamości
☐Strata finansowa
☐Naruszenie dobrego imienia
☐Utrata poufności danych osobowych chronionych tajemnicą zawodową
☐Nieuprawnione odwrócenie pseudonimizacji
☐Inne

Opisz poniżej inne skutki naruszenia prawa do ochrony danych osoby, której dane dotyczą:

……

B. Ryzyko naruszenia praw i wolności osób fizycznych

7. Środki zaradcze

A. Komunikacja z osobami, których dane dotyczą

Czy osoby, których dane dotyczą, zostały powiadomione o naruszeniu?

Czy indywidualnie?		Powód niezawiadomienia osób, których dane dotyczą: Opis tych środków …… …… …… …… …… …… …… …… …… …… ……	Jeśli jeszcze nie oceniłeś, czy zamierzasz zawiadomić podmioty danych, pamiętaj, że po podjęciu takiej decyzji będziesz musiał złożyć zgłoszenie uzupełniające.
Wskaż datę kiedy osoby, których dane dotyczą, zostały powiadomione o naruszeniu …… ……	Wskaż datę kiedy zamierzasz powiadomić osoby, których dane dotyczą, o naruszeniu …… …… ☐Nie znam jeszcze daty kiedy zamierzam powiadomić osoby, których dane dotyczą		
Liczba zawiadomionych osób, których dane dotyczą …… ……			
Środki komunikacji wykorzystane do zawiadomienia osoby, której dane dotyczą ……			
Treść zawiadomienia ……			

B. Środki w celu zaradzenia naruszeniu ochrony danych osobowych

Opisz dodatkowe środki (poza poinformowaniem osób) zastosowane lub proponowane w celu zminimalizowania ewentualnych negatywnych skutków naruszenia i jego ponownego

wystąpienia.

……

……

C. Transgraniczne przetwarzanie i inne powiadomienia

Naruszenie zostało lub zostanie zgłoszone innemu organowi nadzorczemu UE (oopcjonalnie)

☐Austria	☐Belgia	☐Bułgaria	☐ Chorwacja
☐Cypr	☐Czechy	☐Dania	☐Estonia
☐Finlandia	☐Francja	☐Grecja	☐Hiszpania
☐Holandia	☐Irlandia	☐Litwa	☐ Luksemburg
☐Łotwa	☐Malta	☐Niemcy	☐Portugalia
☐Rumunia	☐Słowacja	☐Słowenia	☐Szwecja
☐Węgry	☐Wielka Brytania	☐Włochy	

Naruszenie zostało lub zostanie zgłoszone innemu organowi nadzorczemu spoza UE (oopcjonalnie)

Wymień inne organy nadzorcze spoza UE, którym naruszenie zostało lub zostanie zgłoszone

……..

Naruszenie zostało lub zostanie zgłoszone innemu organowi nadzorczemu UE z powodu innych zobowiązań prawnych (oopcjonalnie)

Np. obowiązek zgłoszenia incydentu wynikający z ustawy o krajowym systemie cyberbezpieczeństwa. Wymień inne organy, którym naruszenie zostało lub zostanie zgłoszone z powodu innych zobowiązań prawnych.

……..

Informacja:

Administrator danych osobowych.
Administratorem Państwa danych osobowych będzie Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO) z siedzibą w Warszawie, przy ul. Stawki 2.
Można się z nami kontaktować w następujący sposób:
a) listownie: ul. Stawki 2, 00-193 Warszawa
b) przez elektroniczną skrzynkę podawczą dostępną na stronie https://www.uodo.gov.pl/pl/p/kontakt
c) telefonicznie: (22) 531 03 00
Inspektor ochrony danych.
Możecie się Państwo kontaktować również z wyznaczonym przez Prezesa UODO inspektorem ochrony danych pod adresem email IOD@uodo.gov.pl
Cele i podstawy przetwarzania.
Będziemy przetwarzać Państwa dane osobowe zawarte w formularzu w celu przyjmowania zgłoszeń o naruszeniu ochrony danych osobowych zgodnie z art. 33 ust 1 , 3 i 4 RODO, podejmowania działań określonych w art. 34 ust. 4 oraz art. 58 ust. 2 RODO[1], a także prowadzenia przez organ wewnętrznego rejestru naruszeń na podstawie art. 57 ust. 1 lit. u RODO. Następnie Państwa dane będziemy przetwarzać w celu wypełnienia obowiązku archiwizacji dokumentów wynikającego z ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

Odbiorcy danych osobowych.
Odbiorcami Państwa danych osobowych będą Minister Cyfryzacji w związku z zamieszczeniem formularza wniosku na platformie E-PUAP oraz Wojewoda Podlaski w związku z korzystaniem przez Prezesa UODO z systemu elektronicznego zarządzania dokumentacją (EZD PUW).
Okres przechowywania danych.
Będziemy przechowywać Państwa dane przez czas realizacji uprawnień Prezesa UODO wskazanych w art. 34 ust. 4 i art. 58 ust. 2 RODO, a następnie - zgodnie z obowiązującą w Urzędzie Prezesa UODO Instrukcją kancelaryjną oraz przepisami o archiwizacji dokumentów - przez okres 10 lat od końca roku, w którym zgłoszono naruszenie ochrony danych, lub - w przypadku skierowania wystąpienia lub wydania decyzji administracyjnej – wieczyście.

Prawa osób, których dane dotyczą.
Zgodnie z RODO przysługuje Państwu:
a) prawo dostępu do swoich danych oraz otrzymania ich kopii;
b) prawo do sprostowania (poprawiania) swoich danych;
c) prawo do usunięcia danych osobowych, w sytuacji, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa lub w ramach sprawowania władzy publicznej;
d) prawo do ograniczenia przetwarzania danych;
e) prawo do wniesienia skargi do Prezesa UODO (na adres Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00 - 193 Warszawa)

Informacja o wymogu podania danych.
Podanie przez Państwa danych osobowych w niniejszym formularzu jest obowiązkiem wynikającym z art. 33 ust. 3 RODO oraz z art. 63 § 2-3a ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego.

[1] Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO) oraz podjętych działań.

Załącznik nr 8 do Polityki – Zasady przechowywania danych (polityka retencyjności)

Kategorie danych	Okres przechowywania danych	Podstawa prawna przetwarzania
Lista obecności pracowników	3 lata	Prawnie uzasadniony interes w zw. m.in. z art. 149 Kodeksu pracy.
Dokumentacja w sprawach związanych ze stosunkiem pracy	10 lat (od końca roku kalendarzowego, w którym doszło do ustania zatrudnienia)	Przepis prawa (realizacja obowiązku prawnego).
Akta osobowe	10 lat (od końca roku kalendarzowego, w którym doszło do ustania zatrudnienia)	Przepis prawa (realizacja obowiązku prawnego).
Meldunki w Holandii	5 lat	Prawnie uzasadniony interes jakim jest uzyskanie meldunku dla zatrudnionego.
Obsługa umów w ramach prowadzenia bieżącej działalności	5 lat	Prawnie uzasadniony interes jakim jest korzystanie z tych danych do kontaktu z kontrahentem.
Obsługa umów zlecenia	3 lata	Realizacja umowy.
Wnioski o EKUZ/Karty pobytu	??? od momentu rozpatrzenia wniosku	Zgoda, osób, których dane dotyczą.
Dokumentacja powypadkowa (prowadzenie dokumentacji BHP)	10 lat	Przepis prawa (realizacja obowiązku prawnego).
Dokumentacja dot. zakończonego procesu rekrutacyjnego	3 lata od zakończenia danego procesu rekrutacyjnego	Zgoda osób, których dane dotyczą.
Dokumentacja dot. przyszłych rekrutacji pracowników	3 lata od zakończenia roku kalendarzowego w którym pozyskano dane rekrutacyjne	Zgoda osób, których dane dotyczą.
Dokumentacja dot. zakwaterowania zatrudnionych	5 lat	Umowa.
Dokumentacja zgłoszeniowa pracowników i członków ich rodzin do ZUS, aktualizacja zgłoszeń i przekazywanie danych o zwolnieniach	Dokumenty zgłoszeniowe: 5 lat Dane o zwolnieniach: 10 lat	Przepis prawa (realizacja obowiązku prawnego).
Dokumentacja rozliczeniowa z pracownikami, wypłata wynagrodzeń, naliczanie obciążeń oraz naliczanie składek do ZUS	10 lat	Przepis prawa (realizacja obowiązku prawnego). Umowa o pracę. Umowa zlecenia.
Rozliczenia podatkowe	5 lat	Przepis prawa (realizacja obowiązku prawnego).

Prowadzenie korespondencji elektronicznej	3 lata	Prawnie uzasadniony interes jakim jest prawo do prowadzenia komunikacji mailowej.
Komunikacja z użytkownikami strony	6 lat	Prawnie uzasadniony interes jakim jest prawo do prowadzenia komunikacji z użytkownikami strony internetowej.
Przyjęcie i rozpatrzenie zgłoszenia naruszenia prawa	3 lata (po zakończeniu roku kalendarzowego, w którym zakończono działania następcze)	Przepis prawa (realizacja obowiązku prawnego).

Załącznik nr 9 do Polityki – Instrukcja zarządzania systemem informatycznym