Wydanie 1

P O L I T Y K A

O C H R O N Y D A N Y C H

D A N Y C H O S O B O W Y CH

Firmy:
P.H.U.P. Wiesław Zajączek
ul. Zdunowska 201, 63-700 Krotoszyn

Zatwierdzam

…….

Data: 25 maja 2018

Spis treści

Karta zmian

Lp.	Krótki opis zmiany oraz numer strony, na której ją wprowadzono	Data i podpis osoby dokonującej zmiany
1.	Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania RODO	25.03.2019
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		

1. INFORMACJE OGÓLNE

1.1. Administrator, cel polityki ochrony danych osobowych, podstawy prawne

Administratorem odpowiedzialnym za wdrożenie Polityki Ochrony Danych Osobowych, zwanej zamiennie również „Polityką", jest P.H.U.P. Wiesław Zajączek

Celem wdrożenia i utrzymywania Polityki Ochrony Danych Osobowych jest zapewnienie zgodności działania osób pracujących pod nadzorem z wymaganiami 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, zwanego dalej RODO, oraz z krajowymi aktami wykonawczymi wydanymi na jego podstawie

Podstawę prawną wdrożenia wymagań dotyczących przetwarzania danych osobowych stanowią:

a) 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,
b) ustawa z dnia 10.05.2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000).
c) Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania RODO

1.2. Zakres informacji objętych polityką ochrony danych osobowych oraz zakres jej zastosowania

Dokument „Polityka Ochrony Danych Osobowych" określa zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem, nieuprawnionym udostępnieniem, utratą, modyfikacją oraz zniszczeniem.

1. Politykę Ochrony Danych Osobowych tworzy zespól dokumentów o charakterze regulacyjnym oraz wynikających z nich dokumentów wykonawczych, w szczególności:
    a) wykaz zbiorów i miejsc, w których przetwarzane są dane osobowe oraz celów i podstaw prawnych ich przetwarzania(zał. 20 Analiza ryzyka),
    b) instrukcja zarządzania systemem informatycznym,
    c) instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych.
    d) opis środków technicznych i organizacyjnych zapewniających ochronę praw i wolności osób, których dane dotyczą (zał. 9),
    e) procedura szacowania ryzyka w procesie przetwarzania danych osobowych,
    f) instrukcja zbywania sprzętu IT.

1.3 Terminy i definicje

1. Administrator - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

2. Administrator Systemów Informatycznych (ASI) - osoba odpowiedzialna za funkcjonowanie systemu informatycznego oraz stosowanie technicznych i organizacyjnych środków ochrony.
3. Dane osobowe – informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
4. Główna jednostka organizacyjna oznacza miejsce, w którym znajduje się jego centralna administracja w Unii.
5. Naruszenie ochrony danych osobowych - 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.
6. Organ nadzorczy - niezależny organ publiczny ustanowiony przez państwo członkowskie UE.
7. Osoby pracujące pod nadzorem – osoby świadczące pracę na podstawie stosunku pracy (umowa o pracę), zwane dalej pracownikami, oraz w innych formach (umowy cywilnoprawne, np. umowa zlecenia, o dzieło, o zarządzanie, kontraktowa oraz inne osoby fizyczne odbywające staże, specjalizacje, szkolenia specjalizacyjne i praktyki zawodowe),
8. Przetwarzanie danych - operacja 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;
9. Profilowanie - dowolna forma zautomatyzowanego przetwarzania danych osobowych i polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się (np. według płci, zainteresowań, wieku, zadłużenia kredytowego, miejsca, zamieszkania);
10. Pseudonimizacja - to użycie zamiast np. imienia i nazwiska konkretnej osoby – liczby, znaku, symbolu, pseudonimu. Wszystko po to, by nie można ich było przypisać konkretnej osobie, której dane dotyczą bez użycia dodatkowych informacji, gdyż one powinny być przechowywane osobno i powinny być objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie określonej osobie fizycznej.
11. Podmiot przetwarzający - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;
12. Poufność danych – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.
13. Sieć rozległa - sieć publiczną w rozumieniu ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t. j. Dz. U. z 2017 r., poz. 1907).
14. 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 (w ostatnim przypadku - np. pracownik podmiotu przetwarzającego dane osobowe).
15. Użytkownik systemu - osoba upoważniona do przetwarzania danych osobowych w systemie informatycznym.

16. Zbiór danych - uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
17. „Zgoda" osoby, której dane dotyczą - dobrowolne, konkretne, świadome i jednoznaczne okazanie woli osoby, której dane dotyczą, w formie:
    a) oświadczenia
    lub
    b) wyraźnego działania potwierdzającego, przyzwalającego na przetwarzanie dotyczących jej danych osobowych.

2. ODPOWIEDZIALNOŚĆ ZA OCHRONĘ PRZETWARZANIA DANYCH OSOBOWYCH

Za przetwarzane danych osobowych, każdy w swoim zakresie, odpowiadają:

- Administrator Danych Osobowych (ADO)
- Specjalista ds. Ochrony Danych Osobowych zatrudniona na stanowisku Pracownik ds. Kadr i Finansów
- Administrator Systemów Informatycznych (ASI)- firma zewnętrzna
- Osoby wykonujące pracę pod nadzorem, które uzyskały od Administratora Danych upoważnienie do przetwarzania danych osobowych.

Całkowitą odpowiedzialność za przetwarzanie danych osobowych ponosi Administrator.

2.1 Administrator Danych Osobowych

Administratorem jest P.H.U.P. Wiesław Zajączek
ul. Zdunowska 201, 63-700 Krotoszyn
NIP: 621-000-24-39

Administrator odpowiada, między innymi, za:

1. Wdrożenie do praktyki zarządczej niniejszej Polityki Ochrony Danych Osobowych.
2. Wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających przetwarzanie danych osobowych zgodnie z RODO oraz za wykazanie tego wymagania w ramach zasady rozliczalności.
3. Poddawanie okresowym przeglądom i aktualizacji środków technicznych i organizacyjnych, o których mowa wyżej.
4. Nadawanie upoważnień do przewarzania danych osobowych osobom pracującym pod nadzorem, którzy będą przetwarzać dane osobowe
5. Prowadzenie ewidencji wydanych upoważnień osobom pracującym pod nadzorem (zał. 5)
6. Określanie celów i sposobów przetwarzania danych osobowych.
7. Udzielanie odpowiedzi na zapytania kierowane przez osoby fizyczne, dotyczące administrowanych zbiorów danych osobowych ich dotyczących oraz z zakresu praw im przysługujących.
8. Prowadzenie ewidencji umów powierzenia o przetwarzania danych osobowych oraz przechowywanie oryginałów tych umów (zał. nr 7),
9. Przeprowadzanie okresowych szkoleń personelu uczestniczącego w operacjach przetwarzania danych.
10. Przeprowadzanie okresowych audytów oraz analiz z procesu przetwarzania danych osobowych z punktu widzenia zasad przetwarzania danych osobowych oraz pozostałych wymagań zawartych w Polityce Ochrony Danych Osobowych i dokumentach regulacyjnych.

11. Zgłaszanie naruszenia ochrony danych osobowych Organowi Nadzorczemu, (niezwłocznie, nie później niż 72 godziny po stwierdzeniu naruszenia lub po powzięciu informacji).
12. Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych, gdy może to powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych (niezwłocznie),
13. Współpracę z Organem Nadzorczym (Prezesem Urzędu Ochrony Danych Osobowych).
14. Przeprowadzenie oceny skutków planowanych operacji przetwarzania danych osobowych, które mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych w celu ochrony danych osobowych.
15. Prowadzenie uprzednich konsultacji z Organem Nadzorczym, gdy ocena skutków planowanych operacji wykaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby Administrator nie zastosował środków w celu zminimalizowania tego ryzyka.
16. Udzielanie wyjaśnień Organowi Nadzorczemu, odpowiedzi na zalecenia dotyczące oceny skutków dla ochrony danych oraz monitorowanie ich wykonania,

2.2. Specjalista ds. Ochrony Danych Osobowych

Imię i nazwisko: Iwona Raźniak
Adres do korespondencji: P.H.U.P. Wiesław Zajączek, ul. Zdunowska 201, 63-700 Krotoszyn
Numer telefonu kontaktowego: 62-722-62-82
E-Mail : wzajaczek@op.pl

Powyższe dane informacyjne zamieszczone są na stronie internetowej www…..

Specjalista ds. Ochrony Danych Osobowych podlega bezpośrednio Administratorowi. Fakt jego powołania zakomunikowany zostaje wszystkim osobom pracującym pod nadzorem niezwłocznie po jego powołaniu z zastosowaniem obowiązujących środków komunikacji przyjętej w P.H.U.P. Wiesław Zajączek (zał. nr 1a).

Administrator zapewnia wsparcie Specjaliście ds. Ochrony Danych Osobowych w wypełnianiu jego zadań, udział we wszystkich zagadnieniach związanych z ochroną danych osobowych, bezstronność poprzez zakaz wydawania Specjaliście ds. Ochrony Danych Osobowych jakichkolwiek instrukcji co do wykonywania przez niego zadań przez osoby funkcyjne. Zapewnia także zakaz odwoływania i karania Specjalistę ds. Ochrony Danych Osobowych za realizowane przez niego zadania (art. 38 pkt 3 RODO).

Specjalista Ochrony Danych Osobowych składa oświadczenie o zachowaniu poufności danych osobowych (zał. nr 2a).

Specjalistą ds. Ochrony Danych Osobowych może być osoba, która:
1. Ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych.
2. Posiada odpowiednią wiedzę w zakresie ochrony danych osobowych.

Do jego obowiązków należy, między innymi (art. 39 pkt 3 RODO):

1) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz sporządzanie okresowych raportów Administratorowi;
2) informowanie Administratora, podmiotu przetwarzającego oraz osoby pracujące pod nadzorem, którzy przetwarzają dane osobowe, o ich obowiązkach wynikających z RODO, aktów prawnych wydanych na jego podstawie oraz niniejszej Polityki Ochrony Danych Osobowych i doradzanie im w sprawie przetwarzania danych osobowych;
3) koordynowanie prac przeprowadzanych przez pracowników na samodzielnych stanowiskach danych osobowych dotyczących analizy zagrożeń oraz oceny

ryzyka, na które może być narażone przetwarzanie danych w systemach informatycznych i tradycyjnych,
4) wydawanie opinii w procesie oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych i przedstawianie ich Administratorowi oraz monitorowanie wykonywania zaleceń,
5) zapoznawanie osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
6) pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw im przysługujących z mocy RODO,
7) nadzór nad aktualnością treści Polityki Ochrony Danych Osobowych, dokumentów z nią związanymi oraz z niej wynikającymi,
8) prowadzenie rejestru czynności przetwarzania danych osobowych (Analiza ryzyka – Zał. 20),
9) nadzór nad fizycznym i organizacyjnym zabezpieczeniem miejsc, w których przetwarzane są dane osobowe,
10) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych wdrożonych w celu ochrony danych osobowych,
11) określanie obowiązków personelowi z zakresu bezpieczeństwa przetwarzania danych osobowych i podnoszenie ich świadomości w tym względzie,
12) przeprowadzanie okresowych szkoleń personelu uczestniczącego w operacjach przetwarzania danych,
13) przeprowadzanie okresowych audytów oraz analiz z procesu przetwarzania danych osobowych z punktu widzenia zasad przetwarzania danych osobowych oraz pozostałych wymagań zawartych Polityce Ochrony Danych Osobowych i dokumentach regulacyjnych, a także przedkładanie sprawozdań z tej analizy Administratorowi,

2.3 Administrator systemów informatycznych

ASI, powołany przez Administratora (zał. nr 1b) realizuje zadania z zakresu zarządzania i bieżącego nadzoru nad systemem informatycznym ADO, w szczególności:
1. Zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się w uzasadnionych przypadkach hasłem dostępu Administratora.
2. Przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe.
3. Nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych.
4. Podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego.
5. Blokuje dostęp do baz danych użytkowników na polecenie Specjalisty ds. Ochrony Danych Osobowych
6. Zmienia w poszczególnych stacjach roboczych hasła dostępu, ujawniając je wyłącznie danemu użytkownikowi oraz w razie potrzeby ADO.
7. W sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje Administratora o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia.
8. Sprawuje nadzór nad wykonaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe.
9. Sprawuje nadzór nad wykonaniem kopii zapasowych, ich przechowywaniem
10. Monitoruje bezpieczeństwo przetwarzania danych oraz zapewnienia bezpieczną ich wymianę i bezpiecznej teletransmisji.
11. Nadaje upoważnienia dostępu do systemów informatycznych (zał. nr 1bb).
12. ASI składa oświadczenie o poufności danych osobowych (zał. nr 2b) .

2.4 Pracownicy na samodzielnych stanowiskach

Pracownicy na samodzielnych stanowiskach są odpowiedzialni za:

1. Przetwarzanie danych osobowych zgodnie z dokumentami regulacyjnymi dotyczącymi przetwarzania danych osobowych w P.H.U.P. Wiesław Zajączek (Polityka, Instrukcja zarządzania systemem informatycznym, Instrukcja zbywania sprzętu IT, Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych itp.).
2. Nadzór nad przetwarzaniem danych osobowych przez podległe osoby pracujące pod nadzorem.
3. Pracownicy na samodzielnych stanowiskach wspomagają Specjalistę ds. Ochrony Danych Osobowych w zakresie przetwarzania danych osobowych w tych komórkach zgodnie z niniejszą Polityką.

2.5 Osoby upoważnione do przetwarzania danych osobowych

Osoba, która uzyskała upoważnienie do przetwarzania danych osobowych, jest zobowiązana do przetwarzania danych osobowych zgodnie z niniejszą Polityką Ochrony Danych Osobowych z jednoczesnym zachowaniem wymagań zawartych w Instrukcji zarządzania systemem informatycznym, Instrukcji zbywania sprzętu IT oraz Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych.
Osoby przetwarzające dane osobowe składają oświadczenie o poufności danych osobowych (zał. nr 2c)

3. UPOWAŻNIENIA, UMOWY O PRZETWARZANIE, ZASADY BEZPIECZEŃSTWA W CZASIE PRZETWARZANIA DANYCH OSOBOWYCH, ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

3.1 Nadawanie/zmianę/zawieszanie/odebranie upoważnień do przetwarzania danych osobowych

1. Decyzję o wydaniu, zmianie, zawieszeniu lub odebraniu uprawnień do przetwarzania danych osobowych podejmuje Właściciel. Fizyczną obsługę powyższych czynności realizuje również Specjalista ds. Ochrony Danych Osobowych
2. Pisemna forma wniosku o nadanie, zmianę, zawieszenie, odebranie upoważnienia(zał. nr 3).
3. Pisemna forma upoważnienia do przetwarzania danych osobowych(zał. nr 4-dla pracowników oraz zał. nr 4a - dla osób zewnętrznych, wykonujących zlecenia/umowy lub kontrole/audyty).
4. Forma zapoznania osoby upoważnionej z zasadami ochrony danych osobowych poprzez szkolenie przeprowadzone przez Specjalistę ds. Ochrony Danych Osobowych przed pierwszym przetwarzaniem danych osobowych przez tą osobę.

3.2 Umowy powierzenia o przetwarzanie danych osobowych

1. Pisemna forma umowy.
2. Osoba odpowiedzialna za rejestrację i przechowywanie zawartych umów powierzenia: Specjalista ds. Ochrony Danych Osobowych
3. Warunki zawierania umów z podmiotem przetwarzającym:
   Powierzenie przetwarzania podmiotowi przetwarzającemu możliwe jest jedynie w sytuacji, gdy zapewni on gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych spełniających bezpieczne przetwarzanie danych osobowych zgodnie z RODO i ochronę praw osób, których dane dotyczą (zał. nr 6). Podstawa prawna: art. 28 pkt 1 RODO.

4. Ewidencję umów powierzenia przetwarzania danych osobowych oraz podmiotów, którym dane powierzono prowadzi Specjalista ds. Ochrony Danych Osobowych (zał. nr 7).

3.3. Ogólne wymagania bezpieczeństwa i zasady obowiązujące w P.H.U.P. Wiesław Zajączek w procesie o przetwarzaniu danych osobowych w miejscu stałej dyslokacji oraz poza nim

3.3.1. Ogólne wymagania dotyczące bezpieczeństwa przetwarzania danych osobowych

1. Przetwarzanie danych osobowych odbywa się wyłącznie na wyraźne polecenie ADO potwierdzone ważnym upoważnieniem do ich przetwarzania, zawierające podstawę prawną i cel przetwarzania,
2. Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze oraz indywidualną odpowiedzialność za jego ochronę ponosi każda osoba przetwarzająca te dane w określonych zbiorach.
3. Osoby przetwarzające dane osobowe nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem wynikające z zajmowanego stanowiska służbowego, w ramach udzielonego upoważnienia do przetwarzania danych.
4. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej osoby przetwarzające dane osobowe zobowiązane są do stosowania zasady tzw. „czystego biurka". Oznacza to niepozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym.
5. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe następuje w sposób uniemożliwiający odczytanie zawartej w nich treści z wykorzystaniem niszczarek.
6. Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym
1. przypadku osoba dokonująca ich wyniesienia oraz, w ramach nadzoru służbowego, jej bezpośredni przełożony. On też wydaje zgodę na ich wyniesienie, jednak tylko wtedy, gdy przetwarzanie nie może być zrealizowane w dotychczasowym miejscu pracy i pod warunkiem, że spełnione zostaną warunki skutecznej ich ochrony przed utratą poufności, dostępności oraz integralności.
7. Przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych, chyba że dane te są w odpowiedni sposób zabezpieczone przed dostępem osoby nieuprawnionej.
8. Osoby pracujące pod nadzorem zobowiązane są do zamykania na klucz wszelkich pomieszczeń oraz budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w pomieszczeniu pracy, jak i po jej zakończeniu, a klucze nie mogą być pozostawione w zamku drzwi. Osoby pracujące pod nadzorem zobowiązane są do dołożenia należytej staranności w celu zabezpieczenia posiadanych kluczy przed nieuprawnionym dostępem.
9. Wprowadza się zasady „czystego biurka", „wygaszonego ekranu komputera", co 12 miesięcy roku zmiany haseł dostępu, czystego pulpitu oraz minimalizacji udzielanych informacji przez telefon.

3.3.2 Zasady przetwarzania danych osobowych

Przetwarzanie danych osobowych w P.H.U.P. Wiesław Zajączek przeprowadza się z uwzględnieniem danych osobowych zwykłych.

3.3.2.1 Ogólne zasady przetwarzania danych osobowych

Przetwarzanie tych danych osobowych przeprowadza się według poniższych zasad:

1. Przetwarzanie zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (zasada „**zgodności z prawem, rzetelności i przejrzystości**").
   Zgodność z prawem jest zachowana, gdy spełniony zostanie przynajmniej jeden z 6 poniższych warunków:
   1) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów (zał. 8),
   2) przetwarzanie jest niezbędne do zamiaru zawarcia umowy, zawarcia umowy i jej wykonania, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy (*np. podanie danych osobowych w czasie zawierania umowy o pracę z potencjalnym administratorem*),
   3) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze – np. podstawą prawną przetwarzania jest pkt 45 RODO oraz art. 35.1, 36.1, 41.1 ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. z 2015 r., poz. 121 ze zm., oraz art. 31,33 i 35 lub art. 37–39 ustawy z 26.07.1991 r. o podatku dochodowym od osób fizycznych,
   4) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej (*interes ochrony życia, interes ochrony socjalnej),*
   5) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej - podstawą prawną jest pkt 45 RODO lub akt kraju członkowskiego, uchwała rady gminy itp.),
   6) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora, w tym z*espoły reagowania na zagrożenia komputerowe, zespoły reagowania na komputerowe incydenty naruszające bezpieczeństwo, dostawców sieci i usług łączności elektronicznej oraz dostawców technologii i usług w zakresie bezpieczeństwa - może to obejmować na przykład zapobieganie nieuprawnionemu dostępowi do sieci łączności elektronicznej i rozprowadzaniu złośliwych kodów, przerywanie ataków typu „odmowa usługi", a także przeciwdziałanie uszkodzeniu systemów komputerowych i systemów łączności elektronicznej],*

   Przejrzystość jest zachowana, gdy osoba, której dane dotyczą, jest informowana o:

   1) celu w jakim jej dane osobowe są zbierane, w jakim będą wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim stopniu te dane osobowe są lub będą przetwarzane,
   2) tożsamości Administratora firmy P.H.U.P. Wiesław Zajączek ul. Zdunowska 201, 63-700 Krotoszyn
   3) prawie do uzyskania potwierdzenia i informacji o przetwarzanych danych osobowych jej dotyczących,
   4) ryzyku, zasadach, zabezpieczeniach i prawach związanych z przetwarzaniem danych osobowych oraz o sposobach wykonywania praw w związku z przetwarzaniem.

   Wszelkie komunikaty na powyższe tematy związane z przetwarzaniem danych osobowych są łatwo dostępne i **zrozumiałe** oraz formułowane **jasnym i prostym językiem.**

2. Zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (zasada „**ograniczenia celu**");
3. Adekwatne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (zasada „**minimalizacji danych**");

4. Prawidłowe i w razie potrzeby uaktualniane co do celu ich przetwarzania, w razie rozbieżności powinny zostać niezwłocznie usunięte lub sprostowane (zasada „**prawidłowości -** integralności");
5. Przechowywane przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane 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 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 (zasada „**ograniczenia czasu przechowywania**");
6. 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 (zasada „**integralności i poufności**"),
7. ADO musi być w stanie wykazać przestrzeganie zasad (zasada „**rozliczalności**").

4. PRZETWARZANIE DANYCH OSOBOWYCH W MIEJSCU STAŁEJ DYSLOKACJI

4.1 Zbiory danych, cele, podstawy prawne przetwarzania danych osobowych

Przetwarzanie danych osobowych w miejscu stałej dyslokacji prowadzi się w zbiorach danych z uwzględnieniem zasad opisanych w punktach 3.3.1 i 3.3.2 niniejszej Polityki Ochrony Danych Osobowych oraz środków organizacyjnych i technicznych wyszczególnionych w zał. nr 9.

4.2 Obowiązki informacyjne Administratora w czasie zbierania danych osobowych bezpośrednio od osób, których dane dotyczą lub w inny sposób

Wprowadza się obowiązek udzielania poniższych informacji osobom, których dane dotyczą, w zależności od źródła pozyskania danych osobowych (patrz poniżej 4.2.1 oraz 4.2.2).

4.2.1 W przypadku zbierania danych od osoby, której dane dotyczą

1. Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, Administrator podczas pozyskiwania danych osobowych podaje jej poniższe informacje:
   a) swoją tożsamość i dane kontaktowe (nazwa, adres, siedziba, KRS lub CEIDG) oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
   b) cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania;
   c) prawnie uzasadnione interesy Administratora - jeżeli przetwarzanie odbywa się na podstawie prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią (*zapobieganie oszustwom, klienci Administratora, marketing bezpośredni*);
   d) informacje o odbiorcach danych osobowych, w tym o przekazaniu danych osobowych podmiotowi przetwarzającemu, jeżeli ma to miejsce, a także o kategoriach odbiorców, jeżeli istnieją;

3. Poza informacjami, o których mowa w punkcie 1, podaje jeszcze inne informacje, takie jak:

a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
b) informacje o prawie do żądania od Administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
c) informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem - jeżeli przetwarzanie odbywa się na podstawie zgody w jednym lub większej liczbie celów wyrażonej przez osobę, które dane dotyczą;
d) informacje o prawie wniesienia skargi do organu nadzorczego;
e) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
f) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą,

3. Wymagania zawarte w punktach 1 i 2 nie mają zastosowania, gdy:
a) osoba, której dane dotyczą, dysponuje już tymi informacjami,
b) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku,
c) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

4.2.2. Obowiązki informacyjne Administratora po otrzymaniu żądania wykonania praw przysługujących osobie, które dane dotyczą

Administrator zapewnia realizację prawa kontroli przetwarzania danych osobie, której dane dotyczą.
W tym celu wprowadza się obowiązek **niezwłocznego** udzielania udokumentowanej informacji osobie, której dane dotyczą, jednak w terminie nie dłuższym niż miesiąc, gdy osoba ta zwróci się z żądaniem/wnioskiem o:

1. Potwierdzenie czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, to jest uprawniona również do uzyskania dostępu do nich oraz do następujących informacji:

a) cele przetwarzania,
b) kategorie odnośnych danych osobowych,
c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych,
d) planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
e) 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,
f) informacje o prawie wniesienia skargi do organu nadzorczego,
g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle,

h) 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. Sprostowanie danych, jeżeli są nieprawidłowe. Ma również prawo do żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
3. Usunięcie danych („prawo do bycia zapomnianym"),jeżeli zachodzi jedna z następujących okoliczności:
   a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane,
   b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania,
   c) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania,
   d) dane osobowe były przetwarzane niezgodnie z prawem,
   e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega Administrator.
4. Ograniczenie przetwarzania w następujących przypadkach:
   a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający Administratorowi sprawdzić prawidłowość tych danych,
   b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
   c) Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
   d) osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.
5. Sprostowanie lub usunięcie danych osobowych lub o ograniczenie przetwarzania.
6. Przeniesienie danych osobowych, które dostarczyła Administratorowi, innemu Administratorowi lub przesłania jej samej.
7. Zaprzestanie przetwarzania danych osobowych w momencie zgłoszenia sprzeciwu przez osobę, której dane dotyczą.
8. Zaprzestanie profilowania jej danych osobowych.

Decyzję o udzieleniu odpowiedzi na powyższe żądania podejmuje ADO, dekretuje na Specjalistę ds. Ochrony Danych Osobowych, który jest odpowiedzialny za załatwienie sprawy.
Forma odpowiedzi: identyczna, w jakiej zwróciła się osoba, które dane dotyczą.
Kopie odpowiedzi przechowywane są w komórce organizacyjnej osoby upoważnionej do przetwarzania danych osobowych, która treść odpowiedzi przygotowała.

W celu zapewnienia wysokiego poziomu bezpieczeństwa przenoszenia danych osobowych opisanych w punkcie 6 podrozdziału 4.3.3, niezależnie od obowiązku weryfikacji tożsamości osoby wnioskującej o przeniesienie jej danych osobowych, wprowadza się poniższe uregulowania:

a) wprowadza się zasadę zgodnie z którą dane osobowe przenosi się bezpośrednio do osoby której dane dotyczą albo do innego Administratora wskazanego przez tą osobę we wniosku, w formacie umożliwiającym jego odczyt (czytelność) przez inne systemy i umożliwiającym dalsze przetwarzanie danych osobowych. Nie spełnia tego warunku

format, do którego dostęp zabezpieczony jest kosztowną licencją lub przesłanie w formacie PDF,

b) przenoszenie danych osobowych zaliczanych do szczególnej kategorii („dane wrażliwe") realizowane jest z wykorzystaniem techniki szyfrowania. Informację o takiej formie przenoszenia danych osobowych przekazywana jest osobie, której dane dotyczą, w momencie, gdy zwróci się z żądaniem przeniesienia jej danych. Osobą informującą jest pracownik przetwarzający dane osobowe osoby wnioskującej.

c) w sytuacji braku technicznych możliwości odbioru przesyłanych danych osobowych przez osobę, której dane dotyczą lub przez wskazanego przez nią nowego Administratora, dane osobowe przekazywane są bezpośrednio osobie wnioskującej. Osobą przekazującą jest pracownik przetwarzający dane osobowe osoby wnioskującej.

Notatkę służbową z przekazania danych osobowych załącza się do akt osobowych osoby wnioskującej.

4.2.3Obowiązki informacyjne Administratora po stwierdzeniu lub powzięciu informacji o naruszeniu ochrony danych osobowych

Zawiadomienie o naruszeniu ochrony danych osobowych

1. ADO zawiadamia osobę, której dane dotyczą, o naruszeniu ochrony jej danych osobowych, ale tylko w tych sytuacjach, gdy naruszenie to spowodowało wysokie ryzyko naruszenia praw i wolności tej osoby.
   Termin informowania: niezwłocznie.
   W zawiadomieniu podaje się:
   a) imię nazwisko oraz dane kontaktowe Specjalisty ds. Ochrony Danych Osobowych (osoby nadzorującej zabezpieczenie danych osobowych) lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
   b) opis możliwych konsekwencji naruszenia ochrony danych osobowych,
   c) opis środków zastosowanych lub proponowanych przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym, w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków (wzór zawiadomienia– zał. 11, a zgłoszenia do Organu Nadzorczego – zał. nr 12).

2. Zawiadomienie powyższe **nie jest wymagane**, gdy:
   a) Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,
   b) Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą.
   W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób

3. Jeżeli ADO nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, Organ Nadzorczy – biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje **wysokie** ryzyko – może zażądać od Administratora lub może stwierdzić, że spełniony został jeden z warunków, o których mowa w punkcie 2.

5. POSTĘPOWANIE WERYFIKACYJNE PROWADZONE PRZEZ SPECJALISTĘ DS. OCHRONY DANYCH OSOBOWYCH PO OTRZYMANIU WNIOSKU/ŻĄDANIA WYKONANIA PRAW PRZYSŁUGUJĄCYCH OSOBIE, KTÓRE DANE DOTYCZĄ

5.1 Postępowanie weryfikacyjne po otrzymaniu żądania/ wniosku w wersji elektronicznej (drogą elektroniczną)

Wprowadza się obowiązek weryfikacji tożsamości osoby występującej z żądaniem/wnioskiem o udzielenie jej informacji z zakresu przysługujących praw opisanych w punkcie 4.2.3. niniejszej Polityki Ochrony Danych Osobowych.
Weryfikację przeprowadzają osoby, które przetwarzają dane osobowe osoby, która z wnioskiem/żądaniem wystąpiła.
Weryfikacja obejmuje cyfrową identyfikację osoby, której dane dotyczą, na przykład poprzez mechanizm uwierzytelniania, taki jak te same dane uwierzytelniające, których osoba, której dane dotyczą, używa, by zalogować się do usług internetowych oferowanych przez Administratora.

Jeżeli z żądaniem/wnioskiem udzielenia informacji w formie *mail lub sms* wystąpiła osoba, której dane osobowe były przetwarzane w przeszłości (np. osoba ta świadczyła pracę na rzecz Administratora , tok postępowania jest następujący:

1) analiza wniosku pod względem merytorycznym i formalnym,
2) wezwanie osoby, która złożyła wniosek w wersji *sms lub mail*, o ponowne przesłanie wniosku z powodu braków formalnych lub/i merytorycznych (jeżeli wystąpiły),
3) zweryfikowanie tożsamości osoby, która wniosek złożyła, w sytuacji niejasności bądź wątpliwości co do tożsamości tej osoby poprzez:
   - wysłanie pytań sprawdzających osobie wnioskującej z żądaniem udzielenia odpowiedzi na nie w zakresie: numer PESEL osoby wnioskującej, lub
   - wysłanie pytań sprawdzających osobie wnioskującej z żądaniem udzielenia odpowiedzi na nie w zakresie: data oraz miejsce urodzenia osoby wnioskującej.
4) w sytuacji udzielenia błędnej odpowiedzi, chociażby w jednym przypadku, żądać należy podania kolejnej informacji, takiej jak datę zawarcia z tą osobą umowy o pracę/ o wykonanie usługi.
5) transmisja odpowiedzi osobie wskazanej w żądaniu/wniosku (osobie, której dane dotyczą lub innej osobie/podmiotowi wskazanej we wniosku) w wersji „mail" lub „*sms*", gdy osoba, której dane dotyczą została poprawnie zweryfikowana),
6) wstrzymanie transmisji danych osobowych osoby, której dane dotyczą, do osoby wnioskującej z jednoczesnym wysłaniem jej powiadomienia o tym fakcie i podaniem przyczyny odmowy oraz konieczności złożenia wniosku/żądania na nośniku papierowym.
   UWAGA: Jeżeli dane osobowe przetwarzane przez Administratora nie pozwalają zidentyfikować osoby fizycznej, Administrator nie ma obowiązku uzyskania dodatkowych informacji w celu zidentyfikowania osoby, której dane dotyczą, wyłącznie po to, by zastosować się do przepisów RODO.

   Administrator nie może odmawiać przyjęcia dodatkowych informacji od osoby, której dane dotyczą, aby ułatwić jej wykonywanie jej praw.

5.2 Postępowanie weryfikacyjne po otrzymaniu żądania/ wniosku w wersji papierowej

1) Kroki postępowania identyczne, jak w punkcie 5.1.
2) Transmisja informacji zwrotnej do osoby, która się o nią zwróciła, następuje w trybie, w jakim zażądała/wystąpiła, tj:

- drogą pocztową za zwrotnym poświadczeniem odbioru lub osobiście przez osobę, która wniosek złożyła. Dokument potwierdzenia odbioru danych osobowych przez tą osobę podlega archiwizacji według zasad przewidzianych w Organizacji
lub
- drogą elektroniczną (mail-ową). Potwierdzenie otrzymania maila podlega archiwizacji wg zasad jak w punkcie 1).
Koszty administracyjne (kopiowanie, transmisja itp.) ponosi wnioskodawca. Oryginały danych osobowych przechowywane są przez jeden rok kalendarzowy w Organizacji, po tym okresie są przekazywane do archiwum.

5.3 Postępowanie po otrzymaniu żądania/wniosku złożonego ustnie

1) Odebranie żądania osoby, której dane dotyczą, przy udziale świadka .
2) dalsze postępowanie identyczne jak w punkcie 5.1, jeżeli jest to uzasadnione,
3) przesyłanie danych osobowych następuje w trybie, w jakim osoba zażądała, tj:
   - drogą pocztową za zwrotnym poświadczeniem odbioru lub osobiście przez osobę, która wniosek złożyła. Dokument potwierdzenia odbioru danych osobowych przez tą osobę podlega archiwizacji według zasad przewidzianych w P.H.U.P. Wiesław Zajączek
   - drogą elektroniczną (mail-ową).

Koszty administracyjne (kopiowanie, transmisja itp.)są obliczane według zasad obowiązujących w P.H.U.P. Wiesław Zajączek. Oryginały danych osobowych przechowywane są w P.H.U.P. Wiesław Zajączek.

6. SZACOWANIE RYZYKA NARUSZENIA PRAW I WOLNOŚCI OSÓB W PROCESIE PRZETWARZANIA DANYCH OSOBOWYCH

6.1 Podstawa szacowania

1. Szacowanie ryzyka naruszenia praw i wolności osób, których dane dotyczą, w procesie przetwarzania danych osobowych przeprowadza się zgodnie z procedurą „Ocena ryzyka naruszenia praw i wolności osób, których dane dotyczą, w procesie przetwarzania danych osobowych".
2. Wyniki szacowania stanowią podstawę zaplanowania i wdrożenia środków ochrony adekwatnych i proporcjonalnych do zidentyfikowanego ryzyka.
3. Wobec ryzyka nieakceptowalnego (w procedurze oznaczonego, jako „Wysokie"), podejmuje się działania w celu zredukowania jego poziomu lub eliminacji.

6.2 Środki organizacyjne i techniczne zastosowane dla zapewnienia bezpieczeństwa przetwarzania danych osobowych

W celu skutecznej ochrony przetwarzania danych osobowych wprowadza się, między innymi, następujące środki ochrony:

a) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych.

Opis wszystkich środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzania danych osobowych (zał. nr 9).

7. ZGŁASZANIE NARUSZEŃ PRZETWARZANIA DANYCH OSOBOWYCH I RODZAJE ODPOWIEDZIALNOŚCI ZA NIE

1. Wprowadza się obowiązek zgłaszania naruszeń przetwarzania danych osobowych skutkujących:

- utratą lub zniszczeniem danych,
- nieuprawnioną modyfikacją danych
- nieuprawnionym dostępem do danych,
- nieuprawnionym udostępnieniem danych.

Obowiązek zgłoszenia naruszenia ochrony danych osobowych ciąży na wszystkich osobach pracujących pod nadzorem.
Zgłoszenia naruszenia dokonuje ADO lub Specjalista ds. Ochrony Danych Osobowych, lub pracownik bezpośredniemu przełożonemu, ten zaś ADO.
Przełożeni wszystkich szczebli przekazują zgłoszenie ADO.
Zgłoszenia dokonuje się w formie ustnej lub pisemnej (w drugim przypadku nie ustala się wzoru formularza zgłoszeniowego, układ treści może być dowolny).
Zgłoszenia naruszenia przetwarzania danych osobowych do Organu Nadzorczego dokonuje ADO.

2. Wprowadza się zasadę odpowiedzialności pracowników za powyższe naruszenia wg poniższych kryteriów:

a) za naruszenia zasad przetwarzania danych osobowych:
   - wypowiedzeniem stosunku pracy,

b) za spowodowanie „wycieku" danych osobowych pracownik podlega poniższym sankcjom:
   - wypowiedzenie stosunku pracy,
   - zwolnienie z pracy w trybie dyscyplinarnym na podstawie art. 52 Kodeksu pracy.

   Ponadto pracownik zobowiązany zostaje do zapłaty odszkodowania wypłaconego przez Administratora pracownikom których wyciek danych osobowych doprowadził do powstania szkody majątkowej oraz niemajątkowej, a także, w ramach regresu, zapłaty kary, którą Administrator uiścił organowi nadzorczemu z tytułu „wycieku" danych osobowych,

3. Szczegółowy opis postępowania w sytuacji naruszenia ochrony danych osobowych zawarto w „Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych".

8. KONTROLA PRZETWARZANIA DANYCH OSOBOWYCH I ŚRODKÓW ICH ZABEZEPIECZEŃ

1. Nadzór i kontrolę nad ochroną danych osobowych sprawują Specjalista ds. Ochrony Danych Osobowych oraz Właściciel- w odniesieniu do technicznych aspektów przetwarzania danych osobowych w systemach informatycznych.
2. Specjalista ds. Ochrony Danych Osobowych wykonuje czynności kontrolne/audyty/ w ramach sprawdzeń zgodności przetwarzania danych osobowych z wymaganiami niniejszej Polityki Ochrony Danych Osobowych oraz innych aktów regulacyjnych z nią związanych, jak również z punktu widzenia skuteczności zabezpieczeń procesu przetwarzania danych osobowych.
3. Kontrole/audyty/ są planowane i przeprowadzane przez Specjalistę ds. Ochrony Danych Osobowych.
4. Mogą być prowadzone kontrole dla Organu Nadzorczego, gdy ten zwróci się o to do Administratora.

4. Specjalista ds. Ochrony Danych Osobowych przeprowadza kontrole w trybie:
   a) kontroli planowej – raz w roku;

b) kontroli doraźnej - w sytuacji przekazania informacji o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia, niezwłocznie po otrzymaniu takich informacji;
c) kontroli w przypadku zwrócenia się o to przez Organ Nadzorczy

5. Czynności kontrolne Specjalisty ds. Ochrony Danych Osobowych podlegają udokumentowaniu w 3 dokumentach:
a) „Analiza ryzyka stopnia stosowania zasad przetwarzania danych osobowych w roku bieżącym. (zał. nr20).
b) „Protokół kontroli zgodności przetwarzania i stanu zabezpieczenia danych osobowych z wymaganiami przepisów o ochronie danych osobowych", w którym dokonuje się ustaleń z zakresu zasad przetwarzania danych osobowych oraz skuteczności zabezpieczeń tych danych (zał. nr 13),
c) „Raport z przeprowadzonych audytów zgodności przetwarzania i stanu zabezpieczenia danych osobowych z wymaganiami przepisów o ochronie danych osobowych", który przedstawiany jest ADO(zał. nr 14).
d) „Raport z naruszenia ochrony danych osobowych", ale tylko w sytuacji, gdy w czasie audytu stwierdzono, że doszło do naruszenia ochrony danych osobowych zakwalifikowanych do ryzyka „WYSOKIE" (zał. nr 15).

9. UDOSTĘPNIANIE DANYCH OSOBOWYCH ZE ZBIORU DANYCH PODMIOTOM ZEWNĘTRZNYM

Wprowadza się obowiązek udokumentowanej formy udostępniania danych osobowych podmiotom zewnętrznym, tj. innym niż upoważnionym /publicznym/ z uwzględnieniem poniższych zasad.

a) udostępnienie danych osobowych, w jakiejkolwiek postaci, jednostkom nieuprawnionym wymaga pisemnego upoważnienia ADO,
b) udostępnienie danych osobowych nie może być realizowane drogą telefoniczną,
c) udostępnienie danych osobowych może nastąpić wyłącznie po przedstawieniu wniosku o udostępnienie danych osobowych zatwierdzonego przez Właściciela P.H.U.P. Wiesław Zajączek zawierającego co najmniej uzasadnienie żądania, cel oraz zakres udostępnianej informacji ze zbioru(zał. nr 10).

Aplikacje wykorzystywane do obsługi baz danych osobowych zapewniają odnotowanie informacji o udzielonych odbiorcom danych. Zakres informacji powinien obejmować co najmniej: dane odbiorcy, datę wydania, zakres udostępnionych danych.

10. ŚRODKI OCHRONY PRAWNEJ PRZYSŁUGUJĄCE OSOBIE, KTÓREJ DANE DOTYCZĄ

1. Osobie, której dane dotyczą, osoba świadcząca pracę na rzecz ADO pod nadzorem przysługują 3 środki ochrony prawnej:
a) środki administracyjne,
b) środki sądowe,
c) pozasądowe.

2. Osobie, której dane dotyczą przysługują 4 rodzaje praw:
a) wniesienie skargi do Organu Nadzorczego, jeżeli sądzi, że przetwarzanie jej danych osobowych narusza RODO (skarga wniesiona według kryterium pobytu, swojego miejsca pracy lub miejsca popełnienia domniemanego naruszenia),

b) wystąpienie z powództwem przeciwko prawnie wiążącej decyzji jej dotyczącej wydanej przez Organ Nadzorczy. Dotyczy to tylko sytuacji, gdy Organ Nadzorczy nie rozpatrzył skargi lub nie poinformował osoby, której dane dotyczą, w terminie trzech miesięcy o postępach lub efektach rozpatrywania skargi wniesionej,
c) wystąpienie z powództwem przeciwko ADO, gdy uzna, że prawa przysługujące jej na mocy RODO zostały naruszone w wyniku przetwarzania jego danych osobowych z naruszeniem RODO,
d) uzyskania od Administratora odszkodowania za poniesioną szkodę majątkową lub niemajątkową, będącą skutkiem naruszenia RODO.

3. Osoba, której dane dotyczą ma również prawo do udzielenia pełnomocnictwa podmiotowi, organizacji lub zrzeszeniu – które nie mają charakteru zarobkowego, zostały należycie ustanowione zgodnie z prawem państwa krajowego i działają w dziedzinie ochrony praw i wolności osób, których dane dotyczą do:

a) wniesienia w jej imieniu skargi oraz
b) wykonywania w jej imieniu praw jej przysługujących oraz,
c) żądania w jej imieniu odszkodowania, o którym mowa w art. 82 RODO, jeżeli przewiduje to prawo państwa członkowskiego.

11. DOKUMENTY POWIĄZANE Z POLITYKĄ OCHRONY DANYCH OSOBOWYCH

1. Procedura szacowanie ryzyka w procesie przetwarzania danych osobowych - Zał.20.
2. Instrukcja zarządzania systemem informatycznym.
3. Instrukcja zbywania sprzętu IT.