

1. INFORMACJE OGÓLNE

Niniejsza Polityka bezpieczeństwa przetwarzania danych osobowych (dalej zwana „Polityka”) została wdrożona w **P.H.U ALGO Jarosław Bartos** 98-300 Wieluń, ul. Krótka 3 tel.438432504 (dalej zwanym „Administratorem”), będącej Administratorem Danych Osobowych, i opisuje zasady ochrony i nadzoru nad przetwarzaniem danych osobowych.

Każde naruszenie Polityki może być uznane za poważne naruszenie podstawowych obowiązków pracowniczych lub wynikających z umów cywilnych o współpracy i może skutkować konsekwencjami, zgodnie z Kodeksem Pracy lub odpowiednimi przepisami regulującymi zasady współpracy, jak również odpowiedzialnością przewidziana w ustawie o ochronie danych osobowych.

Celem powstania niniejszej Polityki jest realizacja obowiązków wynikających w przepisów dotyczących ochrony danych osobowych, jak również spełnienie wymagań chroniących prywatność i godność osób, których dane osobowe są przetwarzane przez Administratora danych.

Przedmiotem Polityki jest określenie, opisanie i zawarcie, w tym i załączonych dokumentach, zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych osobowych objętych ochroną, a w szczególności zabezpieczeń danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. PODSTAWA PRAWNA ORAZ ZAKRES OBOWIĄZYWANIA

Polityka została zastosowana aby spełnić wymogi :

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
- USTAWA z dnia 10 maja 2018 r. o ochronie danych osobowych
- Rozporządzenie ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024)

Polityka obowiązuje przy przetwarzaniu wszelkich danych osobowych w **P.H.U ALGO Jarosław Bartos**. Sposób postępowania przy przetwarzaniu danych opisany jest w osobnych procedurach i instrukcjach. Podmioty zewnętrzne, które będą przetwarzać dane osobowe na zlecenie Administratora danych, zgodnie z art. 31 ustawy o ochronie danych osobowych, są obowiązane opracować własną dokumentację i zabezpieczyć przetwarzane dane osobowe zgodnie z wymogami prawa.

3. DEFINICJE

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

2) „**przetwarzanie**” oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

3) „**ograniczenie przetwarzania**” oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

4) „**profilowanie**” oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

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

6) „**zbiór danych**” oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

7) „**administrator**” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

8) „**podmiot przetwarzający**” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

9) „**odbiorca**” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

10) „**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;

- 11) „**zgoda**” osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
- 12) „**naruszenie ochrony danych osobowych**” oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
- 13) „**dane genetyczne**” oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;
- 14) „**dane biometryczne**” oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
- 15) „**dane dotyczące zdrowia**” oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;
- 16) „**przedsiębiorca**” oznacza osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą;
- 17) „**grupa przedsiębiorstw**” oznacza przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa przez nie kontrolowane;
- 18) „**organ nadzorczy**” oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51; 4.5.2016 L 119/34 Dziennik Urzędowy Unii Europejskiej PL
- 19) „**usługa społeczeństwa informacyjnego**” oznacza usługę w rozumieniu art. 1 ust. 1 lit. b) dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/1535 (1); 26) „**organizacja międzynarodowa**” oznacza organizację i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy.
- 20) **IODO** – Inspektor Ochrony Danych Osobowych, rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, decydującą o celach i środkach przetwarzania danych osobowych.
- 21) **Prezes Urzędu Ochrony Danych Osobowych** - organ nadzorczy do spraw ochrony danych osobowych

4. PODSTAWOWE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. Dane osobowe muszą być:

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

Zgodność przetwarzania z prawem

Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

- a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
- b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
- c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
- d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
- e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

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

Jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.

Jeżeli osoba, której dane dotyczą, wyraża zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie niniejszego rozporządzenia nie jest wiążąca

Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie

Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy

- c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);
- d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”); 4.5.2016 L 119/35 Dziennik Urzędowy Unii Europejskiej PL (1) Dyrektywa (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz.U. L 241 z 17.9.2015, s. 1).
- e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania”);
- f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).

6. ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANIA DANYCH

Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator **P.H.U ALGO Jarosław Bartos** wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z rozporządzeniem i obowiązującymi przepisami prawa oraz aby móc to wykazać. Środki te są w razie potrzeby będą poddawane przeglądowi i uaktualniane, aby zapewnić :

- a) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania
- b) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
- c) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

2. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Zabezpieczenia organizacyjne

1. sporządzono i wdrożono Politykę Bezpieczeństwa;
2. do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez Administratora danych bądź osobę przez niego upoważnioną;
3. stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych;
4. osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;
5. osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
6. przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
7. przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych;

Zabezpieczenia techniczne

1. stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową,
2. komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkownika i cykliczne wymuszanie zmiany hasła,
3. dostęp do systemu informatycznego służącego do przetwarzania danych osobowych, może uzyskać wyłącznie osoba (użytkownik) zarejestrowana w tym systemie przez administratora systemu.
- 4) dostęp do systemów operacyjnych serwerów i stacji roboczych jest chroniony przez nazwę użytkownika i hasło.
- 5) Na terenie zakładu w celu zapewnienia bezpieczeństwa pracowników oraz przetwarzanych danych został wprowadzony szczególny nadzór w postaci monitoringu wizyjnego.
- 6) Dokumenty w formie papierowej zawierające dane osobowe przechowywane są w szafkach zamykanych na klucz.
- 7) W budynku zainstalowany został system alarmowy.

6. PRAWA I OBOWIĄZKI WOBEC OSÓB FIZYCZNYCH, KTÓRYCH DANE SĄ PRZETWARZANE

Niniejsza polityka oraz instrukcje wdrożone w **P.H.U ALGO Jarosław Bartos** stosują się do przepisów mających na celu zapewnienie osobom fizycznym, których dane są przetwarzane :

- Prawa do bycia poinformowanym o operacjach przetwarzania
Osobie fizycznej, której dane są przetwarzane przez administratora danych, przysługuje prawa bycia poinformowanym o tym przetwarzaniu.
- Prawa dostępu do danych
Każda osoba fizyczna, której dane osobowe są przetwarzane ma prawo dostępu do przetwarzanych danych
- Prawa do sprostowania – uzupełnienia danych
Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
- Prawa do usunięcia danych
Osoba, której dane dotyczą może żądać od administratora niezwłocznego usunięcia dotyczących jej danych osobowych. W takim przypadku, ze strony administratora powstaje obowiązek usunięcia danych bez zbędnej zwłoki.
- Prawa do ograniczenia przetwarzania danych
- Prawa sprzeciwu
Osoba fizyczna, której dane są przetwarzane, mocą oświadczenia woli powstrzymać przetwarzanie danych jej dotyczących.
- Prawa do przenoszenia danych
Prawo to polega na możliwości otrzymania przez osobę, której dane dotyczą, w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego danych osobowych jej dotyczących, które dostarczyła administratorowi i możliwości przesłania tych danych innemu administratorowi.

Osoby fizyczne, których dane osobowe są przetwarzane w sposób związany przejrzysty i zrozumiały zostały poinformowane o celu i sposobie przetwarzania danych.

Uwzględniając powyższe oraz stosując się do obowiązujących przepisów wszyscy pracownicy zostali na piśmie poinformowani kto jest administratorem ich danych osobowych, w jakim celu przetwarzane są ich dane osobowe.

7. WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH.

Wykaz zbiorów danych osobowych, gromadzonych i przetwarzanych w **P.H.U ALGO Jarosław Bartos** stanowi Załącznik do niniejszej Polityki,

8. STRUKTURA ZBIORÓW DANYCH WSKAZUJĄCYCH ZAWARTOŚĆ POSZCZEGÓLNYCH PÓŁ INFORMACYJNYCH

Struktura zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych dla programów i systemów stosowanych w **P.H.U ALGO Jarosław Bartos** adekwatna jest do zakresu przetwarzanych danych stanowi Załącznik i przedstawia się w sposób następujący:

1. W ramach zbioru **Kontrahenci** przetwarzane są dane osobowe : imię i nazwisko, nazwa firmy, adres, NIP, REGON, numer telefonu lub adres e-mail, numer rachunku bankowego. Dane te są niezbędne do dokonywania transakcji handlowych, realizacji zamówienia oraz dokonywania płatności bieżących związanych z realizacją zadań związanych z działalnością firmy **P.H.U ALGO Jarosław Bartos**
2. W ramach zbioru **Pracownicy** przetwarzane są dane byłych i obecnych pracowników **P.H.U ALGO Jarosław Bartos** : imię i nazwisko, adres zamieszkania, numer telefonu, wysokość wynagrodzenia, staż pracy, wykształcenie, urlopy, zwolnienia, numer PESEL, numer dowodu osobistego, numer konta, imiona rodziców, miejsce urodzenia, informacje o odbytych szkoleniach, imię i nazwisko, PESEL dziecka lub członka rodziny , dane o stanie zdrowia, dane dotyczące zainteresowań.
3. W ramach zbioru **Monitoring** przetwarzany jest wizerunek pracowników oraz osób przebywających na terenie zakładu.
4. W ramach zbioru **Sklep internetowy** przetwarzane są dane związane z transakcjami kupna-sprzedaży oraz dostawy towaru : imię i nazwisko, nazwa firmy, adres dostawy, NIP, REGON, numer telefonu, adres e-mail.

9. OBSZAR W KTÓRYM PRZETARZANE SĄ DANE OSOBOWE

Obszar, w którym przetwarzane są dane osobowe, w **P.H.U ALGO Jarosław Bartos** przy ulicy Krótkiej 3 zabezpieczony jest przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są w **P.H.U ALGO Jarosław Bartos** dane osobowe jest treścią osobnego dokumentu stanowiącego Załącznik

Informacje są przedstawione z zachowaniem podziału na :

- strefę przetwarzania danych osobowych, czyli pomieszczenia Administratora danych w których dane są przetwarzane przez Administratora danych,
- strefę w której przetwarzane są dane osobowe powierzone przez Administratora Danych do przetwarzania innym podmiotom, w tym w oparciu o pełnomocnictwo do dalszego powierzania przetwarzania.

10. POSTĘPOWANIE W SYTUACJI NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie **72 godzin** po stwierdzeniu naruszenia – zgłasza je organowi nadzorcemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorcemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

Każda osoba przetwarzająca dane osobowe po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza Inspektorowi Ochrony Danych Osobowych lub bezpośrednio administratorowi.

Zgłoszenie, naruszenia danych osobowych musi:

- a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
- d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Administrator **P.H.U ALGO Jarosław Bartos** dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

Do typowych zagrożeń bezpieczeństwa danych osobowych należą:

- Niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
- Niewłaściwe zabezpieczenie sprzętu, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
- Nieprzestrzeganie zasad ochrony danych osobowych przez pracowników.

Do typowych incydentów bezpieczeństwa danych osobowych należą:

- Zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
- Zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/ zagubienie danych);
- Umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

Formy naruszeń bezpieczeństwa danych osobowych zawiera tabela stanowiąca Załącznik do Polityki

W przypadku stwierdzenia wystąpienia zagrożenia, Administrator Danych prowadzi postępowanie wyjaśniające w toku którego:

- Ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki;
- Inicjuje ewentualne działania dyscyplinarne;
- Rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości;
- Dokumentuje prowadzone postępowania.

W przypadku stwierdzenia naruszenia, Administrator Danych prowadzi postępowanie wyjaśniające, w toku którego:

- Ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały;
- Zabezpiecza ewentualne dowody;
- Ustala osoby odpowiedzialne za naruszenie;
- Podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody);
- Wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości;
- Dokumentuje prowadzone postępowania zgodnie ze wzorem Raportu z naruszenia bezpieczeństwa danych osobowych stanowiących Załącznik do Polityki Bezpieczeństwa.

11. ZGODNOŚĆ

Niniejsza Polityka będzie aktualizowana wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi w ramach prowadzonej działalności **P.H.U ALGO Jarosław Bartos**, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.

12. POSTANOWIENIA KOŃCOWE

1. Administrator Danych ma obowiązek zapoznać z treścią Polityki każdego użytkownika.
2. Wszystkie regulacje dotyczące systemów informatycznych, określone w Polityce dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
3. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce.
4. Wobec osoby, która w przypadku naruszenia lub domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
5. W sprawach niuregulowanych w Polityce mają zastosowanie przepisy ustawy oraz rozporządzenia.