POLITYKA BEZPIECZEŃSTWA

MGT

MARTA TATAJ, ANDRZEJ DYMEK SP. J.
UL. BOLIMOWSKA 75, 99-400 ŁOWICZ

Data i miejsce sporządzenia dokumentu:	… /…/……
Ilość stron:	

SPIS TREŚCI

1. WSTĘP

1.1. INFORMACJE OGÓLNE

1. Administratorem danych osobowych jest:
MGT Marta Tataj, Andrzej Dymek Sp. j. w Łowiczu, ul. Bolimowska 75, 99-400 Łowicz, REGON 750187450, NIP 834-157-10-50.

2. Celem niniejszej Polityki Bezpieczeństwa jest zapewnienie ochrony danych osobowych przetwarzanych przez Administratora przed wszelkiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.

3. Polityka została opracowana zgodnie z wymogami określonymi w § 4 rozporządzenia 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. Nr 100, poz. 1024) oraz Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO), ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych i ustawy o ochronie danych osobowych z dnia 10 maja 2018 r.

1.2. ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ BEZPIECZEŃSTWA ORAZ ZAKRES ZASTOSOWANIA

1. Dokument Polityki Bezpieczeństwa opisuje zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem.

2. Załącznikiem do niniejszej polityki jest między innymi opracowana i wdrożona **Instrukcja zarządzania systemem informatycznym** służącym do przetwarzania danych osobowych, zwaną dalej **„Instrukcją”.** Określa ona sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem zapewnienia ich bezpieczeństwa.

3. Ochrona danych osobowych jest realizowana poprzez: **zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez przeszkolonych użytkowników**. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

    a) **poufność danych** - rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,

b) **integralność danych** - rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

c) **rozliczalność danych** - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,

d) **integralność systemu** - rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej,

e) **legalność** przetwarzania danych – rozumianą jako możliwość przetwarzania danych osobowych wyłącznie na podstawie adekwatnych do celów przetwarzania podstawach prawnych,

4. Integralną częścią niniejszej Polityki są również załączniki wskazujące na **budynki, pomieszczenia lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe**, załączniki zawierające **opisy zbiorów danych osobowych** wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz **struktury zbiorów danych** wskazujące zawartość poszczególnych pól informacyjnych i powiązania między nimi, a także jeżeli to konieczne **sposób przepływu danych pomiędzy poszczególnymi systemami.**

1.3. WYJAŚNIENIE TERMINÓW UŻYWANYCH W DOKUMENCIE POLITYKI BEZPIECZEŃSTWA

1. Przez użyte w Polityce określenia należy rozumieć:

a. **polityka** – rozumie się przez to Politykę bezpieczeństwa ochrony danych osobowych.

b. **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; **ustawa** – rozumie się przez to ustawę o ochronie danych osobowych,

c. **rozporządzenie** – 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)

d. **RODO** - Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.

e. **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;

f. **ograniczenie przetwarzania** oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

g. **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;

h. **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;

i. **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;

j. **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;

k. **podmiot przetwarzający (procesor)** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

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

m. **strona trzecia** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą

n. **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;

o. **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;

p. **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

q. **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;

r. **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,

s. **organ nadzorczy** oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie

t. **zabezpieczenie systemu informatycznego** – należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą,

u. **nośnik komputerowy (wymienny)** – nośnik służący do zapisu i przechowywania informacji, np. taśmy, dyskietki, dyski twarde.

2. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

2.1. INFORMACJE OGÓLNE

1. Osobami odpowiedzialnymi za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami Rozporządzenia, Ustawy, Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemami informatycznymi są:
    a. Administrator Danych Osobowych (ADO),
    b. Inspektor Ochrony Danych Osobowych (IOD),
    c. Administrator Systemu Informatycznego (ASI),
    d. Osoby przetwarzające dane osobowe na podstawie udzielonego przez administratora upoważnienia do przetwarzania danych osobowych.

2.2. ADMINISTRATOR DANYCH

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszą Polityką oraz powołanymi w niej aktami prawnymi i aby móc to wykazać.

2. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

2.3. INSPEKTOR OCHRONY DANYCH OSOBOWYCH

1. Administrator i podmiot przetwarzający obligatoryjnie wyznaczą inspektora ochrony danych, w przypadku gdy:
    a) główna działalność administratora lub podmiotu przetwarzającego będzie polegała na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę;
    b) główna działalność administratora lub podmiotu przetwarzającego będzie poległa na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10. 2.

Grupa przedsiębiorstw może wyznaczyć jednego inspektora ochrony danych, o ile można będzie łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej.

2. Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w przepisach RODO
3. Inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług.
4. Administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora ochrony danych i zawiadamiają o nich organ nadzorczy.
5. Inspektor ochrony danych ma następujące zadania:
    a. informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
    b. monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
    c. udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania
    d. współpraca z organem nadzorczym;
    e. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami.

2.4 ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

1. Wyznaczenie Administratora Systemów Informatycznych jest fakultatywne.

2. Do uprawnień i obowiązków Administratora Systemów Informatycznych należy w szczególności:

    a. nadawanie/nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych,

b. nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,

c. podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,

d. identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych i tradycyjnych,

e. sprawowanie nadzoru nad przechowywanymi kopiami zapasowymi opisanymi w Instrukcji zarządzania systemem informatycznym.

2.5. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych zobowiązana jest do ich ochrony w sposób zgodny z przepisami RODO, Ustawy, Rozporządzenia, Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym.

2. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia.

3. UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Upoważnienia do przetwarzania, w imieniu Administratora, danych osobowych nadaje Administrator Danych Osobowych lub Inspektor Ochrony Danych.

2. Upoważnienie nadawane jest każdemu nowo zatrudnionemu pracownikowi oraz osobom, które na podstawie odrębnych umów świadczą na rzecz Administratora usługi, których charakter i cel wymaga przetwarzania określonych, powierzonych przez Administratora danych osobowych.

3. Ustanie stosunku pracy lub rozwiązanie umowy z Administratorem stanowią podstawę do natychmiastowego anulowania udzielonego danej osobie upoważnienia.

4. Upoważnienie udzielane jest wyłącznie w formie pisemnej. Administrator prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych.

5. Osoba upoważniona zobowiązana jest do zapoznania się z regulaminem przetwarzania danych osobowych obowiązującym u Administratora.

4. UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

1. Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą.

2. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.

3. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

4. Umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:

    a. przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;

    b. zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;

    c. podejmuje wszelkie środki wymagane na mocy art. 32 RODO;

    d. przestrzega warunków korzystania z usług innego podmiotu przetwarzającego;

e. biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw;

f. uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków dotyczących bezpieczeństwa przetwarzania;

g. po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;

h. udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym przepisie oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

5. Jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego – te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym. Jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym.

6. Administrator danych osobowych lub Inspektor danych osobowych prowadzi rejestr podmiotów upoważnionych do przetwarzania danych osobowych.

5. OGÓLNE ZASADY BEZPIECZEŃSTWA OBOWIĄZUJĄCE PRZY PRZETWARZANIU DANYCH OSOBOWYCH

1. W celu zapewnienia prawidłowego przetwarzania danych osobowych Administrator Danych Osobowych ustala ogólne zasady bezpieczeństwa przetwarzania.
2. Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze, indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych.
3. Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
4. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. „czystego biurka". Zasada ta oznacza nie pozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników.
5. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści, np. 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 przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.
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.
8. Pracownicy zobowiązani są do zamykania na klucz wszelkich pomieszczeń lub 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 w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia posiadanych kluczy przed nieuprawnionym dostępem.

6. INSTRUKCJA POSTĘPOWNIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Procedura postępowania przypadku stwierdzenia naruszenia ochrony danych osobowych ma na celu wdrożenie generalnych reguł dotyczących zachowania się pracowników Administratora Danych Osobowych w przypadku wystąpienia naruszenia zasad ochrony danych osobowych. Celem niniejszej procedury jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.
    a. każda osoba, która poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe bądź posiada informacje mogące mieć wpływ na bezpieczeństwo danych osobowych, jest zobowiązana fakt ten niezwłocznie zgłosić Administratorowi/Inspektorowi Ochrony Danych i/lub Administratorowi Systemów Informatycznych (w odniesieniu do danych przetwarzanych w systemach informatycznych).
    b. do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratorowa/Inspektora Ochrony Danych i/lub Administratorowa Systemów Informatycznych lub upoważnionej przez nich osoby, osoba powiadamiająca powinna:
        - niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków, a następnie ustalić przyczyny, lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe,
        - zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
        - udokumentować wstępnie zaistniałe naruszenie,
        - nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia.

    c. Po przybyciu na miejsce naruszenia ochrony danych osobowych, Administrator/Inspektor Ochrony Danych, Administrator Systemów Informatycznych lub osoba ich zastępująca:
        - zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metod dalszego postępowania,
        - wysłuchuje relacji osoby zgłaszającej z zaistniałego naruszenia, jak również relacji każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,

    d. Administrator Bezpieczeństwa Informacji i/lub Administrator Systemów Informatycznych dokumentuje zaistniały przypadek naruszenia oraz sporządza raport.

2. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu, Administrator Bezpieczeństwa Informacji i/lub Administrator Systemów Informatycznych, zasięga niezbędnych opinii i proponuje postępowanie naprawcze (w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń) i zarządza termin wznowienia przetwarzania danych.

3. Do typowych **zagrożeń bezpieczeństwa** danych osobowych należą:
   a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
   b) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych
   c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek)

4. Do typowych **incydentów bezpieczeństwa** danych osobowych należą:
   a) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
   b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych)
   c) 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)

7. KONTROLA PRZETWARZANIA I STANU ZABEZPIECZENIA DANYCH OSOBOWYCH (PRIVACY BY DEFAULT)

1. Nadzór i kontrolę nad ochroną danych osobowych przetwarzanych u Administratora sprawuje Administrator/Inspektor Ochrony Danych oraz/lub Administrator Systemów Informatycznych – w odniesieniu do danych osobowych przetwarzanych w systemach informatycznych służących do przetwarzania danych osobowych.
2. Administrator/Inspektor Ochrony Danych dokonuje czynności kontrolnych w ramach sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
3. Sprawdzenia dokonywane są przez Administratora/Inspektora Ochrony Danych oraz/lub Administratora Systemów Informatycznych dla Administratora bądź organu nadzoru, gdy ten na podstawie przysługujących mu kompetencji zwróci się o to do Administratora.
4. Administrator/Inspektor Ochrony Danych przeprowadza sprawdzenie w trybie:
   a. sprawdzenia planowego - według opracowanego planu sprawdzeń;
   b. sprawdzenia doraźnego - w przypadkach nieprzewidzianych w planie sprawdzeń, w sytuacji powzięcia informacji o naruszeniu ochrony danych osobowych lub

uzasadnionego podejrzenia wystąpienia takiego naruszenia, niezwłocznie po powzięciu przez takich informacji;

c. sprawdzenia w przypadku zwrócenia się o to przez organ nadzoru.

5. Administrator/Inspektor Ochrony Danych opracowuje plan sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
6. W toku sprawdzenia Administrator/Inspektor Ochrony Danych dokonuje i dokumentuje czynności, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania.
7. Po zakończeniu sprawdzenia, Administrator/Inspektor Ochrony Danych przygotowuje sprawozdanie w tym zakresie. Sprawozdanie sporządzane jest w postaci elektronicznej albo w postaci papierowej.
8. Administrator/Inspektor Ochrony Danych ma prawo do kontroli podmiotów, którym powierzono przetwarzanie danych osobowych w trybie określonym w Polityce Bezpieczeństwa, o ile w umowie o powierzeniu przetwarzania danych osobowych istnieją stosowne zapisy w tym zakresie.
9. **Raz w roku** Administrator/Inspektor Ochrony Danych przygotowuje sprawozdanie roczne stanu funkcjonowania systemu ochrony danych osobowych. W spotkaniu sprawozdawczym uczestniczą: IOD, Kierownicy działów, w których przetwarzane są dane osobowe, Informatyk. Raport przedstawiany jest kierownictwu jednostki.

8. OPIS STRUKTURY ZBIORÓW DANYCH

1. Dla każdego zidentyfikowanego zbioru danych Administrator tworzy w formie załącznika do niniejszej Polityki opis struktury zbioru wraz z zakresem informacji gromadzonych w danym zbiorze.

2. Informacje wskazane niniejszym przepisem zawarte są w załączniku stanowiącym indywidualny opis przetwarzania poszczególnych zbiorów danych.

9. SPOSÓB PRZEPŁYWU DANYCH OSOBOWYCH POMIĘDZY SYSTEMAMI INFORMATYCZNYMI

1. Dla każdego zidentyfikowanego zbioru danych Administrator – jeżeli zachodzi taka sytuacja - tworzy w formie załącznika do niniejszej Polityki opis przepływu danych pomiędzy systemami informatycznymi. Przedmiotowy opis określa systemy pomiędzy, którymi przesyłane są dane, zbiory danych, które podlegają takiemu przesyłaniu, formę przepływu danych oraz formę ich przechowywania.

2. Informacje wskazane niniejszym przepisem zawarte są w załączniku stanowiącym indywidualny opis przetwarzania poszczególnych zbiorów danych.

10. OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

1. Określenie obszaru pomieszczeń, w których przetwarzane są dane osobowe, Administrator określa w zbiorczym rejestrze przetwarzanych zbiorów danych.

11. ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH OSOBOWYCH

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

2. Zabezpieczenia organizacyjne
    a. administrator danych sam wykonuje czynności IODO,
    b. została opracowana i wdrożona polityka bezpieczeństwa,
    c. została opracowana i wdrożona instrukcja zarządzania systemem informatycznym,
    d. do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych,
    e. prowadzona jest ewidencja osób upoważnionych do przetwarzania danych,
    f. osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego,
    g. osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy,
    h. przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych,
    i. 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,
    j. stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe.

3. Zabezpieczenia ochrony fizycznej danych osobowych zostały opisane w stanowiącym indywidualny opis przetwarzania poszczególnych zbiorów danych.

4. Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej.

    a. Zabezpieczenia stosuje się dla fizycznych elementów systemu, ich połączeń oraz systemów operacyjnych. Szczegółowy opis zabezpieczeń zawarty jest w instrukcji zarządzania systemem informatycznym.

    b. Zabezpieczenia (techniczne i programowe) stosuje się dla procedur, aplikacji, programów i innych narzędzi programowych przetwarzających dane osobowe. Szczegółowy opis zabezpieczeń zawarty jest w instrukcji zarządzania systemem informatycznym.

12. SZKOLENIA UZYTKOWNIKÓW

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
2. Za przeprowadzenie szkolenia odpowiada Administrator Danych Osobowych, a za jego zorganizowanie – jeżeli został wyznaczony - odpowiada przełożony użytkowników.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u ADO, a także o zobowiązaniu się do ich przestrzegania.
4. Szkolenie zostaje zakończone podpisaniem przez słuchacza Oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.
5. Dokument ten jest przechowywany w aktach osobowych użytkowników i stanowi podstawę do podejmowania działań w celu nadania im uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe.