POLITYKA

BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Uwzględniająca regulacje: Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE oraz
Ustawy o Ochronie Danych Osobowych z dnia 10 maja 2018r. (Dz.U. 2018 poz. 1000)

OPRACOWAŁ: Data: 2018-05-25 Imię i nazwisko: Wiktor Gronowicz	SPRAWDZIŁ: Data: 2018-05-25 Stanowisko: Dyrektor Finansowy Imię i nazwisko: Renata Roga	ZATWIERDZIŁ: Data: 2018-05-25 Stanowisko: Prezes Zarządu, Dyrektor Spółki Imię i nazwisko: dr inż. Andrzej Olejnik

SPIS TREŚCI

ZA**ŁĄ**CZNIKI:

1. Załącznik nr 1: Wykaz i charakterystyka procesów, czynności i rodzajów przetwarzanych danych
2. Załącznik nr 2: Aktywa Informacyjne
3. Załącznik nr 3: Ocena ryzyka
4. Załącznik nr 4: Rejestr czynności przetwarzania
5. Załącznik nr 5: Rejestr kategorii czynności przetwarzania

1. WSTĘP

Polityka Bezpieczeństwa Danych Osobowych została opracowana jako przewodnik po stosowanych regulacjach dotyczących ochrony danych osobowych. Wraz z towarzyszącymi Politykami Ochrony Danych została ona opracowana ze szczególnym uwzględnieniem przepisów:

- Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej w treści jako: RODO)
- Ustawy O Ochronie Danych Osobowych z dnia 10 maja 2018r. (Dz.U. 2018 poz. 1000) (dalej w treści jako: UODO),
- innych przepisów towarzyszących związanych z ochroną danych osobowych
- wytycznych prezentowanych przez urząd nadzoru: Urząd Ochrony Danych Osobowych – prezentowane na stronie urzędu.

Niniejsza Polityka Bezpieczeństwa Danych Osobowych zawiera lub przywołuje stosowane w firmie zabezpieczenia danych osobowych, zastosowane środki organizacyjne i techniczne oraz mechanizmy ochrony danych osobowych przetwarzanych zarówno w zbiorach w formie papierowej jak i elektronicznej, w sposób ręczny i automatyczny. Ponadto normuje mechanizmy aktualizacji dokumentacji związanej z ochroną danych osobowych, ale także pozwala monitorować proces skuteczności wdrożonego systemu bezpieczeństwa i inne aspekty związane z przetwarzaniem danych osobowych. Polityka jest wyrazem zasad istotnych dla Spółki, opracowanych z uwzględnieniem kontekstu organizacji a w szczególności praw i wolności osób, których dane przetwarza w ramach prowadzonej działalności. Polityka ma na celu usystematyzowanie i spisanie zasad związanych z ochroną danych osobowych, których stosowanie ma zapewnić odpowiednie bezpieczeństwo tym danym.

2. NADZOROWANIE POLITYKI BEZPIECZEŃSTWA DANYCH OSOBOWCH

System Bezpieczeństwa Danych Osobowych, opisany w niniejszej Polityce Bezpieczeństwa, jest nadzorowany przez Pełnomocnika ds. ochrony danych. Pełnomocnik ds. ochrony danych jest odpowiedzialny za nadzór nad opracowaniem, wydaniem, aktualizacją, rozpowszechnianiem Polityki Bezpieczeństwa Danych Osobowych oraz za nadzór nad prawidłowym stosowaniem zasad w niej ujętych. Polityka Bezpieczeństwa zatwierdza jest w imieniu Administratora Danych Osobowych przez Prezesa Zarządu.

Rozpowszechnianie, zmiany, przeglądy i weryfikacja
Zgodnie z procedurą P- 4.01 Nadzór nad dokumentacją i zapisami.

3. CEL POLITYKI BEZPIECZEŃSTWA

Celem niniejszej Polityki Bezpieczeństwa jest określenie zasad przetwarzania danych osobowych oraz ich bezpieczeństwa, jako zestaw praw, reguł, polityk ochrony i procedur oraz praktycznych

zasad regulujących sposób ich zarządzania, ochrony i dystrybucji wewnątrz Spółki jak i w kontaktach ze stronami zainteresowanymi. Polityka Bezpieczeństwa ma zapewnić kierunki działania i wsparcie kierownictwa dla bezpieczeństwa informacji. Niniejszy dokument opracowany został z poszanowaniem zasad prawa UE oraz prawa krajowego w tym z Konstytucji RP i podległych jej aktów prawnych.

Niniejsza Polityka Bezpieczeństwa zawiera w szczególności:

a) wykaz procesów /czynności i rodzajów przetwarzanych danych,

b) ocenę ryzyka w zakresie bezpieczeństwa danych osobowych,

c) rejestr czynności przetwarzania,

d) rejestr kategorii czynności przetwarzania,

e) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Niniejszy dokument ma za zadanie wskazać działania, jakie należy wykonać, aby właściwie zabezpieczyć dane osobowe przetwarzane w Spółce.

4. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

Dane osobowe w Spółce są przetwarzane z uwzględnieniem następujących zasad:

Zasada zgodności z prawem, rzetelności i przejrzystości
dane osobowe są przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.

Zasada ograniczenia celu
dane osobowe są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

Zasada minimalizacji danych
dane osobowe są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

Zasada prawidłowości
dane osobowe są prawidłowe i w razie potrzeby uaktualniane; podejmowane są wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.

Zasada ograniczenia przechowywania
dane osobowe są 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.

Zasada integralności i poufności
dane osobowe są 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 rozliczalności
Powyższe zasady jak również regulacje mających zastosowanie przepisów prawa są przestrzegane przez Spółkę w sposób umożliwiający wykazanie ich przestrzegania

5. TERMINY I DEFINICJE

Wyjaśnienie używanych pojęć:

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.

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.

ZBIERANIE. Wszelkie działania mające na celu uzyskanie danych osobowych bezpośrednio od osoby, której dane dotyczą (np. poprzez wypełnienie formularza elektronicznego), lub pośrednio (np. przez zakup bazy danych).

UTRWALANIE. Zapisanie danych osobowych na określonym nośniku, np. w pamięci komputera, na pendrivie, na papierze, na zdjęciu.

ORGANIZOWANIE. Wszelkie operacje, które służą usprawnieniu korzystania z uporządkowanych zbiorów danych, np. ułatwienie wyszukiwania danych osobowych przez opatrywanie tagami.

PORZĄDKOWANIE. Zbudowanie pewnej struktury z zebranych danych osobowych w oparciu o określone kryterium, np. kryterium alfabetyczne, kryterium wieku, kryterium płci etc.

PRZECHOWYWANIE. Wszelkie działania, które służą zachowaniu utrwalonych danych osobowych i pozwalają zapoznać się z danymi osobowymi w dowolnym momencie. Dane osobowe mogą być przechowywane na wszelkich dostępnych nośnikach, w tym również w tzw. chmurach.

ADOPTOWANIE. Dopasowanie treści danych osobowych do zmieniających się okoliczności, np. automatyczna zmiana wieku danej osoby w systemie w związku z upływem czasu.

MODYFIKOWANIE. Zmiana treści danych osobowych, np. poprzez zmianę adresu, poprawienie błędnego imienia.

POBIERANIE. Wykonanie kopii danych osobowych na jednym nośniku z innego nośnika, za pośrednictwem sieci telekomunikacyjnej. Może to być np. pobranie danych osobowych z serwera na komputer osobisty.

PRZEGL**Ą**DANIE. Zapoznawanie się z treścią danych osobowych jednej po drugiej.

WYKORZYSTYWANIE. Użycie danych osobowych do założonego celu.

UJAWNIANIE POPRZEZ PRZES**Ł**ANIE. Dowolna forma przekazania danych osobowych innej osobie, np. poprzez wysłanie pocztą, kurierem, e-mailem, przez komunikator internetowy.

UJAWNIANIE POPRZEZ ROZPOWSZECHNIANIE. Zamieszczenie danych osobowych w miejscu publicznym, np. na ogólnie dostępnej stronie internetowej, do której ma dostęp nieograniczona liczba użytkowników; na forum internetowym.

UJAWNIANIE POPRZEZ INNEGO RODZAJU UDOST**Ę**PNIANIE. Wszystkie inne czynności niż przesłanie i rozpowszechnianie.

DOPASOWYWANIE. Czynność polegająca na sprawdzeniu, czy w dwóch różnych zbiorach znajdują się dane osobowe tej samej osoby i czy są one ze sobą spójne.

ŁĄCZENIE. Scalanie danych osobowych jednej osoby, które są zamieszczone w różnych zbiorach, np. danych o aktywności w Internecie, jak również scalanie danych osobowych różnych osób pod względem określonego kryterium.

OGRANICZANIE. Oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania

USUWANIE. Usunięcie treści danych z określonego nośnika bez niszczenia nośnika, czyli np. usunięcie adresu e-mail z bazy newslettera, skasowanie nagrania z kamery.

NISZCZENIE. Fizyczna destrukcja nośnika, na którym znajdują się dane osobowe, np. poprzez spalenie lub zniszczenie papieru, zniszczenie płyty CD lub innego zewnętrznego nośnika

CZYNNO**ŚĆ** PRZETWARZANIA oznacza działanie w ramach którego są przetwarzane dane osobowe, którego realizacja jest niezbędna do osiągnięcia założonego celu. Przykładową czynnością przetwarzania jest *REKRUTACJA PRACOWNIKÓW*.

PROCES PRZETWARZANIA oznacza zestaw czynności przetwarzania, których realizacja jest niezbędna do osiągniecia jednego celu. Pojęcie procesu zostało wprowadzone między innymi w celu zapewnienia odpowiedniej efektywności i czytelności wyników oceny ryzyka oraz określenia działań odnoszących się do ryzyka, kiedy zidentyfikowane zagrożenia mają zastosowanie do

więcej niż jednej czynności przetwarzania, które łącznie są realizowane do osiągnięcia wspólnego celu.
Przykładem procesu przetwarzania może być: prowadzenie spraw pracowniczych, w ramach którego to procesu są realizowane takie czynności przetwarzania jak: rozliczanie czasu pracy, prowadzenie dokumentacji osobowej pracowników aktywnych, przechowywanie dokumentacji pracowniczej pracowników nieaktywnych, realizacja spraw dotyczących ubezpieczeń społecznych, ZFŚS itp.

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.

PODMIOT PRZETWARZAJ**Ą**CY oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

ODBIORCA oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią (wyłączenie: organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego).

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.

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.

ADMINISTRATOR SYSTEMU INFORMATYCZNEGO (ASI) – firma zewnętrzna - osoba zajmująca się zakresem działań informatyki i informatyzacji Spółki. Jest odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych.

ROZLICZALNO**ŚĆ** – jest to właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

6. INFORMACJE PODSTAWOWE O PRZETWARZANYCH DAYCH OSOBOWYCH

6.1. OGÓLNA CHARAKTERYSTYKA PRZETWARZANYCH DANYCH OSOBOWYCH

Niniejsza Polityka Bezpieczeństwa Danych Osobowych ma zastosowanie do:

a) do wszelkich informacji o zidentyfikowanych lub możliwych do zidentyfikowania osobach fizycznych;

b) danych osobowych przetwarzanych w jakiejkolwiek formie w tym elektronicznej w systemach informatycznych utrwalonych na wszelkiego rodzaju nośnikach magnetycznych, optycznych, elektronicznych itp. oraz w formie tradycyjnej – papierowej;

c) danych osobowych przetwarzanych zarówno w zbiorach danych, zestawach oraz pojedynczych informacjach osobowych

d) całkowicie lub częściowo zautomatyzowanego przetwarzania danych osobowych oraz do przetwarzania ręcznego danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.

W Spółce przetwarzane są dane osobowe następujących kategorii osób:

a) pracowników i współpracowników w tym tych aktywnych i nieaktywnych

b) członków rodzin pracowników Spółki

c) kandydatów na pracowników

d) dane kontrahentów (dostawców, klientów) i partnerów biznesowych – będących osobami fizycznymi prowadzącymi działalność gospodarczą

e) pracowników kontrahentów i partnerów biznesowych

f) gości odwiedzających Spółkę.

6.2. CELE, ZAKRES I PODSTAWA PRZETWARZANYCH DANYCH OSOBOWYCH

Cele, zakres i podstawa przetwarzania danych osobowych zależą od rodzaju procesów i czynności przetwarzania danych osobowych oraz kategorii osób, których dane są przetwarzane. W Spółce zostały zidentyfikowane wszystkie procesy i czynności przetwarzania. Zostały one przedstawione i scharakteryzowane w Załączniku nr 1 do niniejszej Polityki Bezpieczeństwa: Wykaz i charakterystyka procesów, czynności i rodzajów przetwarzanych danych.

W dokumencie tym zostały przedstawione informacje takie jak:

a) realizowane w firmie procesy i czynności przetwarzania danych osobowych,

b) rola Spółki w przetwarzaniu danych osobowych (administrator lub przedmiot przetwarzający),

c) cele przetwarzania,

d) kategorie osób, których dotyczą przetwarzane dane osobowe,

e) rodzaj i zakres przetwarzanych danych,

f) podstawa przetwarzania poszczególnych rodzajów danych osobowych,

g) sposób pozyskiwania danych,

h) okres przetwarzania poszczególnych rodzajów danych osobowych w Spółce,

i) aktywa wykorzystywane do przetwarzania danych.

Niniejsze informacje stanowią podstawę do przeprowadzenia oceny ryzyka dla bezpieczeństwa danych osobowych oraz zaplanowania i wdrożenia stosownych środków technicznych i proceduralnych jako odpowiedzi na to ryzyko. Dalsze postępowanie zostało przedstawione w pkt. 7.

6.3. ROLA FIRMY W PRZETWARZANIU DANYCH OSOBOWYCH

W zależności od realizowanych procesów i czynności przetwarzania danych osobowych oraz odpowiedzialności firmy i stron zainteresowanych, Spółka występować może jako:

a) Administrator danych osobowych

Sytuacja taka ma miejsce w przypadku, gdy Spółka ponosi odpowiedzialność za określenie celów i sposobów przetwarzania danych osobowych. Dotyczy to między innymi danych osobowych pracowników i współpracowników (aktywnych i nieaktywnych), dane kandydatów do pracy, dane kontrahentów i partnerów biznesowych.

Rola Spółki w przetwarzaniu poszczególnych rodzajów danych w ramach realizowanych procesów i czynności przetwarzania została przedstawiona w Załączniku nr 1 do niniejszej Polityki Bezpieczeństwa: Wykaz i charakterystyka procesów, czynności i rodzajów przetwarzanych danych.

6.4. INSPEKTOR OCHRONY DANYCH (IOD)

W ramach systemu bezpieczeństwa danych osobowych zgodnie z mającymi zastosowanie przepisami prawa w Spółce nie został powołany Inspektor Ochrony Danych (IOD).

Rolę koordynatora w zakresie ochrony danych osobowych w Spółce pełni Pełnomocnik ds. ochrony danych.

7. UWZGLĘDNIENIE OCHRONY DANYCH W FAZIE PROJEKTOWANIA

W celu zapewnienia odpowiedniego poziomu bezpieczeństwa danych osobowych na etapie określania sposobów przetwarzania oraz w czasie samego przetwarzania wdrażane są odpowiednie środki techniczne i organizacyjne. Są one określane z uwzględnieniem:

- stanu wiedzy technicznej,
- kosztów wdrażania,
- charakteru, zakresu, kontekstu i celów przetwarzania,
- ryzyka naruszenia prawa lub wolności osób fizycznych w wyniku przetwarzania (ryzyko o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia).

Przebieg całego procesu od ustalenia potrzeb w zakresie realizacji procesów i czynności przetwarzania do uruchomienia przetwarzania danych został przedstawiony na schemacie nr 1. Poniżej zostały scharakteryzowane poszczególne bloki schematu wraz ze wskazaniem

odpowiedzialnych za nie. W przypadku potrzeby uruchomienia realizacji nowego procesu ,czynności przetwarzania danych osobowych lub modyfikacji już istniejących należy przejść wszystkie niżej przedstawione bloki i postępować zgodnie z przedstawionymi regulacjami.

1. Określnie procesu /czynności przetwarzania danych osobowych oraz jego celu
   Po określeniu potrzeby przetwarzania danych osobowych w ramach prowadzonej działalności należy w pierwszej kolejności określić CEL PRZETWARZANIA DANYCH oraz nierozerwalnie związany z celem OKRES PRZETWARZANIA. Określając te dane należy kierować się obowiązującymi zasadami przetwarzania danych: ograniczenia celu oraz ograniczenia przechowywania (patrz pkt. 5).

   Odpowiedzialnym za realizację niniejszego działania jest osoba odpowiadająca za obszar, w którym zidentyfikowana została potrzeba realizacji dodatkowego procesu lub czynności przetwarzania danych. Cel jest określany w porozumieniu z Pełnomocnikiem ds. ochrony danych.

2. Określenie rodzaju i zakresu danych osobowych niezbędnych do realizacji celu
   Mając na uwadze określony cel przetwarzania danych należy określić jakiego rodzaju dane są nam potrzebne do tego aby cel przetwarzania został osiągnięty. Z tego względu określana jest kategoria osób, których dane będą przetwarzane oraz rodzaj i zakres tych danych. Określając te dane należy realizować to z uwzględnieniem zasad: minimalizacji danych oraz prawidłowości (patrz pkt. 5).

   Odpowiedzialny za działanie: osoba która będzie odpowiedzialna za nowy proces /czynność przetwarzania danych osobowy w porozumieniu z Pełnomocnikiem ds. ochrony danych.

3. Określenie podstawy prawnej do przetwarzania danych osobowych
   W ramach tego etapu należy określić na jakiej podstawie będziemy przetwarzali dane osobowe biorąc pod uwagę w szczególności regulacje RODO w tym: art. 6 Zgodność przetwarzania z prawem, art. 9 Przetwarzanie szczególnych kategorii danych osobowych oraz art. 10 Przetwarzanie danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

   Należy pamiętać, ze przetwarzanie poszczególnych danych jest zgodne z prawem w przypadku gdy spełniony jest jeden z przedstawionych w przepisach warunków. Oznacza to, że jeśli podstawą przetwarzania danych w ramach konkretnego celu przetwarzania jest umowa zawarta z osobą której dane dotyczą (art. 6, ust. 1 lit. b) to nie ma potrzeby ani obowiązku uzyskiwania od tej osoby zgody na przetwarzanie jej danych osobowych - z podkreśleniem, że dotyczy to celu przetwarzania, które jest niezbędne do wykonania zawartej umowy.

   Dla każdego celu przetwarzania należy określić odrębnie podstawę przetwarzania danych.

Charakterystyka procesów /czynności przetwarzania oraz danych których dotyczy powinna zostać udokumentowana w Załączniku nr 1: Wykaz i charakterystyka procesów, czynności i rodzajów przetwarzanych danych.

Odpowiedzialny za działanie: osoba która będzie odpowiedzialna za nowy proces /czynność przetwarzania danych osobowy w porozumieniu z Pełnomocnikiem ds. ochrony danych.

Ocena ryzyka dla nowego lub modyfikowanego procesu /czynności przetwarzania

Zagrożenia dla których określany jest poziom ryzyka są identyfikowane dla aktywów wykorzystywanych w Spółce do przetwarzania danych osobowych lub takich które mają wpływ na poziom ryzyka. Wszystkie aktywa w firmie zostały zidentyfikowane i wskazany został ich właściciel oraz fakt powierzenia i odbioru aktywa (tam gdzie ma to zastosowanie). Wykaz aktywów został przedstawiony w Załączniku nr 2: Aktywa Informacyjne. W załączniku tym przedstawione zostały również główne cechy poszczególnych aktywów.

Poziom ryzyka jest określony dla tych zagrożeń, które wykorzystując podatności danego aktywa mogą wywołać konkretny negatywny skutek. W przypadku braku podatności danego aktywa na konkretne zagrożenie ryzyko dla tego zagrożenia nie jest danej poddawane analizie. Każdy fakt wprowadzenia nowego aktywa, istotnej zmiany konfiguracji aktywa, jego przekazania lub odbioru od pracownika jest dokumentowany w Załączniku nr 2: Aktywa Informacyjne. Odpowiedziany za zarządzanie aktywami informacyjnymi jest Prezes Zarządu.

Dane przedstawione w powyższych punktach stanowią podstawę do przeprowadzenia oceny dla nowego procesu /czynności przetwarzania danych.

W przypadku, jeżeli w ramach tego procesu /czynności są wykorzystywane do przetwarzania aktywa stosowane w ramach innych procesów /czynności przetwarzania należy dokonać przeglądu wyników oceny ryzyka przeprowadzonej na etapie wdrażania. Jeśli jest to zasadne należy w takim przypadku dokonać aktualizacji oceny w tym zakresie.

W przypadku, jeżeli w ramach nowego procesu /czynności przetwarzania wykorzystywane będą rodzaje aktywów wcześniej nie stosowane w Spółce, biorąc pod uwagę, ze podatności tych aktywów mają wpływ na występowanie zagrożeń oraz poziom ryzyka należy dobrać je w sposób zapewniający odpowiedni poziom bezpieczeństwa.

Ocena ryzyka jest przeprowadzona zgodnie z metodyką przedstawioną w Załączniku nr 3: Ocena ryzyka. Wyniki oceny ryzyka również są dokumentowane w tym załączniku.

Odpowiedzialnym za nadzór nad oceną ryzyka jest: Pełnomocnik ds. ochrony danych., który dobiera sobie zespół osób o kompetencjach niezbędnych do przeprowadzenia rzetelnej oceny.

4. Określenie i wdrożenie środków technicznych i organizacyjnych jako odpowiedzi na ryzyko

W każdym z przypadków, gdy pomimo uwzględnienia w ocenia ryzyka obecnie stosowanych zabezpieczeń poziom ryzyka nie będzie akceptowalny należy zaplanować i wdrożyć stosowne środki techniczne lub organizacyjne.

Środki, jakie powinny zostać zastosowane powinien być adekwatny do zagrożenia i skutków jego materializacji. Rozpatrując możliwe do zastosowania rodzaje środków należy kierować się również ich skutecznością. Analizę potrzeba należy rozpocząć od najbardziej skutecznych środków i analizując ich celowość oraz możliwość zastosowania i koszty wdrożenia przechodzić do kolejnych mniej skutecznych środków. Rodzaje środków od najbardziej skutecznych:

a) środki eliminujące ryzyko poprzez zmianę procesu lub eliminację źródła zagrożenia,
b) środki zapobiegające materializacji zagrożenia
c) środki zmniejszające potencjalne skutki w przypadku wystąpienia zagrożenia
d) transfer ryzyka, czyli przeniesienie go na inny podmiot,
e) akceptacja ryzyka

Za określenie środków technicznych i organizacyjnych Pełnomocnik ds. ochrony danych. , wraz z osobami uczestniczącymi w ocenie ryzyka. Określone jako niezbędne do zastosowania środki zostają wprowadzone do: Załącznika nr 3: Ocena ryzyka.

Uwzględniając rodzaj i zakres przetwarzanych danych oraz uzyskane wyniki oceny ryzyka należy zaktualizować lub w przypadku potrzeby założyć:

- Rejestr Czynności Przetwarzania – prowadzony przez Spółkę występująca w roli Administratora (Załącznik nr 4: Rejestr Czynności Przetwarzania),
- Rejestr Kategorii Czynności Przetwarzania – prowadzony przez Spółkę występującą w roli Podmiotu Przetwarzającego, (Załącznik nr 5: Rejestr Kategorii Czynności Przetwarzania).

Za realizację niniejszego działania odpowiada: Pełnomocnik ds. ochrony danych.

5. Przygotowanie dokumentów niezbędnych do uruchomienia procesu /czynności przetwarzania

Zgodnie z przyjętymi środkami organizacyjnymi oraz w celu zapewnienia zgodności z obowiązującymi przepisami prawa opracowywane są niezbędne dokumenty:

- informacja dla osób, których dane będą przetwarzane w celu dopełnienia obowiązku informacyjnego. Wraz z tym dokumentem określany jest możliwie najbardziej skuteczny sposób przekazania tych informacji zainteresowanym.
- Treść oświadczenia o zgodzie na przetwarzanie danych osobowych -w przypadku gdy podstawą przetwarzania ma być wyrażona zgoda.

Za realizację niniejszego działania odpowiada: Pełnomocnik ds. ochrony danych.

6. Nadanie uprawnień do przetwarzania danych osobowych.

   Przed przystąpieniem do przetwarzania danych osobowych należy dokonać przeglądu nadanych w Spółce uprawnień do przetwarzania danych osobowych w celu ustalenia zakresu zmian jakie należy wprowadzić w związku z uruchomieniem nowego procesu /czynności przetwarzania). W przypadku tego działania należy postępować zgodnie z regulacjami przedstawionymi w Polityce Ochrony Danych: Zarządzanie uprawnieniami do przetwarzania danych osobowych.

7. Uruchomienie procesu przetwarzania danych osobowych

   Po zakończeniu realizacji wszystkich działań oraz przygotowaniu niezbędnych dokumentów /wprowadzeniu zmian w już funkcjonujących można przystąpić do przetwarzania danych osobowych w ramach kolejnego procesu /czynności przetwarzania.

   Realizacja ma być zgodna z przyjętymi w Spółce oraz, gdy jest to zasadne, dla tego konkretnego procesu /czynności Politykami Ochrony Danych.

8. ODPOWIEDZIALNOŚĆ W SYSTEMIE BEZPIECZEŃSTWA DANYCH OSOBOWYCH

W imieniu Administratora Danych Osobowych występują osoby zgodnie z uprawnieniami do prawomocnego reprezentowania Spółki tj.: Prezes Zarządu.

W każdym przypadku, gdy Spółka występuje w charakterze Administratora Danych Osobowych ponosi odpowiedzialność za:

- wdrożenie odpowiednich środków technicznych i organizacyjnych, określonych z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia prawa lub wolności osób fizycznych, aby przetwarzanie odbywało się zgodnie z mającymi zastosowanie przepisami prawa i aby móc to wykazać,
- przeglądy i aktualizacje (w przypadku potrzeby) wdrożonych środków technicznych i organizacyjnych,
- wdrożenie i nadzór nad stosowaniem Polityk Ochrony Danych
- korzystanie wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych by przetwarzanie spełniało wymogi aktualnych przepisów prawa i chroniło prawa osób, których dane dotyczą.

W każdym przypadku, gdy Spółka występuje w charakterze Podmiotu Przetwarzającego realizuje procesy i czynności przetwarzania zgodnie ze wskazanymi jednoznacznie wymaganiami Administratora, który powierzył Spółce te dane.
Do podstawowych, wynikających z przepisów prawa obowiązków i odpowiedzialności Podmiotu Przetwarzającego należą między innymi:

- przetwarzanie danych osobowych wyłącznie na udokumentowane polecenie administratora,
- zapewnienie, że osoby upoważnione do przetwarzania danych osobowych były zobowiązane do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,
- wdrożenie i stosowanie środków technicznych i organizacyjnych zgodnych z obowiązującymi przepisami prawa,
- korzystanie z usług innego podmiotu przetwarzającego wyłącznie po uprzedniej pisemnej zgodzie Administratora,
- wsparcie dla Administratora w wywiązywaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą w zakresie wykonywania jej praw,
- wsparcie Administratora w zakresie wywiązania się prze niego z jego obowiązków w zakresie: zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzania danych, reagowania na naruszenia bezpieczeństwa danych osobowych w tym w przypadku potrzeby w zakresie komunikacji z Urzędem Ochrony Danych Osobowych i/lub osobami których dane dotyczą,
- w zależności od decyzji Administratora: usunięcie lub zwrócenie mu wszelkich danych osobowych po zakończeniu świadczenia usług związanych z przetwarzaniem danych (chyba, że prawo stanowi inaczej w danym przypadku),
- udostępnianie Administratorowi wszelkich informacji niezbędnych do oceny poziomu bezpieczeństwa przetwarzanych przez siebie danych osobowych w tym umożliwienie audytorowi lub innej upoważnionej osobie z ramienia Administratora do przeprowadzania audytów w tym inspekcji elementów swojego systemu bezpieczeństwa danych osobowych,
- informowanie Administratora (niezwłoczne) w przypadku, gdy wydane przez Administratora polecenie stanowi naruszenie obowiązujących przepisów prawa.

Do zakresu zadań, obowiązków i odpowiedzialności Pełnomocnika ds. ochrony danych pełniącego rolę koordynatora w zakresie ochrony danych osobowych w Spółce należą między innymi:

- umożliwienie osobom, których dane dotyczą, kontaktu we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy przepisów prawa,
- zachowanie tajemnicy lub poufności co do wykonywania zadań – zgodnie z aktualnie obowiązującymi przepisami prawa,
- informowanie Administratora oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy obowiązujących przepisów prawa o ochronie danych i doradzanie im w tej sprawie,
- monitorowanie przestrzegania aktualni obowiązujących przepisów prawa o ochronie danych oraz polityk Administratora w dziedzinie ochrony danych osobowych, w tym

podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,

- opracowywanie lub opiniowanie przygotowanych dokumentów pod kątem ich zgodności z mającymi zastosowanie przepisami prawa z zakresu ochrony danych osobowych,
- koordynowanie działań związanych z uruchomieniem w Spółce realizacji nowego procesu i czynności przetwarzania danych osobowych w celu dopełnienia wszystkich obowiązków wynikających z przepisów prawa,
- współpraca z organem nadzorczym – Urzędem Ochrony Danych Osobowych,
- pełnienie funkcji punktu kontaktowego dla Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem,
- inne przedstawione w dokumentacji operacyjnej: Politykach Ochrony Danych i procedurach.

Do zakresu zadań, obowiązków i odpowiedzialności wszystkich pracowników i współpracowników firmy w zakresie ochrony danych osobowych w Spółce należą między innymi:

- zapewnienie ochrony danych osobowych przetwarzanych w ramach pełnionych obowiązków służbowych, a w szczególności zabezpieczenie ich przed dostępem osób nieupoważnionych, przed ich zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem,
- zachowanie w tajemnicy, także po ustaniu stosunku pracy /współpracy, wszelkich informacje dotyczących przetwarzania oraz sposobów zabezpieczenia danych osobowych Spółce,
- natychmiastowe zgłaszanie przełożonemu, a w przypadku potrzeby również Pełnomocnikowi ds. ochrony danych stwierdzonych prób lub faktów naruszenia bezpieczeństwa danych osobowych w Spółce,
- inne przedstawione w dokumentacji operacyjnej: Politykach Ochrony Danych i procedurach.

Dane osobowe w Spółce są przetwarzane wyłącznie przez osoby posiadające stosowne upoważnienie do tego celu. Regulacje w zakresie zarządzania uprawnieniami zostały przedstawione w Polityce Ochrony Danych: Zarządzanie uprawnieniami.

9. ODPOWIEDZIALNOŚĆ DYSCYPLINARNA

Pracownicy /współpracownicy zobowiązani są do przestrzegania zasad, Polityk Ochrony danych, procedur wynikających z dokumentów Spółki regulujących ochronę danych osobowych.

W przypadku rażącego naruszeni przez pracownika /współpracownika regulacji systemu bezpieczeństwa danych osobowych uruchomione może zostać postępowanie dyscyplinarne zgodnie z przyjętymi zasadami określonymi w Regulaminie Pracy.

10. BEZPIECZEŃSTWO PRZETWARZANYCH DANYCH OSOBOWYCH

10.1. BEZPIECZEŃSTWO DANYCH PRZETWARZANYCH W SYTEMACH INFORMATYCZNYCH

W celu zapewnienia odpowiedniego nadzoru nad siecią oraz infrastrukturą IT zostały opracowane i wdrożone oraz są stosowane następujące dokumenty:

- Regulamin użytkownika systemu IT
- Regulamin administratora systemu IT

10.2. BEZPIECZEŃSTWO DANYCH PRZETWARZANYCH W FORMIE PAPIEROWEJ

W przypadku przetwarzania danych osobowych w formie papierowej obowiązują regulacje przedstawione w:

- P- 4.01 Nadzór nad dokumentacją i zapisami

Dokumenty zawierające dane osobowe są zamykane w szafach, szufladach zamkniętych na klucz.

Nadzorowanie kluczy:

- Wszystkie duplikaty kluczy są dostępne w sekretariacie;
- Ostatnia osoba po skończonej pracy powinna sprawdzić, czy wszystkie szafy zamykane na klucz są zamknięte;
- Klucze do szaf, szuflad powinny być zabezpieczone przed dostępem osób nieuprawnionych.

10.3. BEZPIECZEŃSTWO DANYCH POZA SIEDZIBĄ SPÓŁKI

Pracownicy lub współpracownicy przetwarzający dane osobowe poza obszarem Spółki zobowiązani są zwrócić szczególną uwagę na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed ich zniszczeniem.

W przypadku przetwarzania poza siedzibą Spółki danych wszyscy realizujący tego typu działania są zobowiązani do przestrzegania regulacji przedstawionych w:

- Regulamin użytkownika systemu IT
- P- 4.01 Nadzór nad dokumentacją i zapisami

11. UDOSTĘPNIANIE W TYM POWIERZANIE PRZETWARZANIA DANYCH OSOBOWYCH

Udostępnianie danych osobowych odbiorcom oraz instytucjom spoza Spółki może odbywać się wyłącznie:

a. zgodnie z przepisami prawa dotyczącymi ochrony danych osobowych oraz

b. za zgodą Administratora Danych Osobowych (ADO)

W przypadku wątpliwości odnośnie zasadności i celowości przekazania danych osobowych fakt ten jest konsultowany przez ADO z Pełnomocnikiem ds. ochrony danych.

Dane osobowe udostępniane są przede wszystkim:

a. kontrahentom w celu realizacji przez nich zleconych im usług,

b. urzędom i instytucjom – zgodnie z mającymi zastosowanie przepisami prawa lub innymi zobowiązaniami, które Spółka musi realizować (organizacje te nie są Odbiorcami Danych w myśl aktualnie obowiązujących przepisów prawa),

c. osobom których dane dotyczą – na ich wyraźne żądanie.

Osoby zatrudnione na podstawie umowy innej niż umowa o pracę (zlecenia, umowy o współpracy):

a. na terenie siedziby Spółki są objęte takimi samymi prawami i obowiązkami jak pracownicy zatrudnieni na podstawie umowy o pracę,

b. poza siedzibą Spółki obowiązują je zasady ochrony powierzonych im danych osobowych, określone w Politykach Ochrony Danych a w przypadku gdy ma to zastosowanie w zawieranych umowach /przekazywanych zleceniach.

Powierzenie danych osobowych przez Spółkę innym podmiotom w celu realizacji określonych usług zabezpieczane jest stosownymi regulacjami zgodnie z: Polityka ochrony danych: Przetwarzanie danych w ramach kontaktów handlowych. Za ich stosowanie odpowiada osoba nadzorująca i/lub koordynująca współpracę z danym kontrahentem.

W przypadku powierzania do przetwarzania danych (w tym udostępniania) w wersji elektronicznej musi odbywać się wyłącznie z zachowaniem odpowiednich zabezpieczeń uniemożliwiających utratę poufności, integralności lub dostępności do danych.

12. ŚWIADOMOŚĆ PRACOWNIKÓW I WSPÓŁPRACOWNIKÓW

W celu zapewnienia odpowiedniej świadomości i kompetencji osobowych personelu realizującego procesy i czynności mające lub mogące mieć wpływ na Bezpieczeństwo Danych Osobowych planowane są i przeprowadzane szkolenia oraz inne działania.

Potrzeby w tym zakresie określa się między innymi na podstawie:

- występujących incydentów i naruszeń bezpieczeństwa danych osobowych,
- potrzeb zgłaszanych przez pracowników i przełożonych pracowników,
- wymagań określonych w przepisach prawnych, w szczególności mających miejsce zmian w przepisach,
- planów uruchomienia nowych procesów i czynności przetwarzania danych osobowych.

Postępowanie zgodnie z procedurą P-6.03 Szkolenia.

13. REAGOWANIE NA ŻĄDANIA OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE

Zgodnie z obowiązującymi przepisami prawa, osobom, których dane przetwarzamy przysługują następujące prawa:

a) Prawo dostępu do danych oraz informacji dotyczących celu i zakresu ich przetwarzania
b) Prawo do sprostowania danych
c) Prawo do ograniczenia przetwarzania danych
d) Prawo do przenoszenia danych
e) Prawo do usunięcia danych („prawo do bycia zapomnianym”)
f) Prawo do sprzeciwu przetwarzania danych osobowych
g) Prawo do wycofania zgody
h) Prawo do niepodlegania decyzji która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu
i) Prawo do wniesienia skargi do organu nadzorczego w zakresie ochrony danych osobowych (UODO: www.uodo.gov.pl).

W zależności od rodzaju przetwarzanych danych osobowych, celu i podstawy i przetwarzania część z tych praw osób, których dane przetwarzamy może mieć charakter typowo iluzoryczny. Oznacza to, że osobie takiej przysługują prawa i może do nas wystąpić z konkretnym żądaniem jednak ze względu np. na nadrzędność przepisów, które mogą mieć zastosowanie w konkretnej sytuacji nie możemy zrealizować danego żądania (np. żądania pracownika do „bycia zapomnianym”).

Niezależnie od sytuacji na każde żądanie dotyczące przetwarzanych przez nas danych osobowych, wpływające do nas jako do ADO (Administratora) udzielane są odpowiedzi w ustawowym terminie.

Postępowanie w tym zakresie zostało przedstawione w Polityce Ochrony danych: Reagowanie na żądanie od osoby, której dane dotyczą. Nadzór nad realizacją tej Polityki Ochrony Danych sprawuje Nadzór nad jej stosowaniem sprawuje Pełnomocnik ds. ochrony danych.

14. REAGOWANIE NA NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

W celu zapewnienia odpowiedniego postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych w Spółce została opracowana, wdrożona i jest utrzymywana Polityka Ochrony Danych: Polityka zarzadzania incydentami. Nadzór nad jej stosowaniem sprawuje Pełnomocnik ds. ochrony danych

15. ZAPEWNIENIE ZGODOŚCI Z PRZEPISAMI PRAWA

Obowiązujące Spółkę przepisy prawa i inne wymagania z zakresu bezpieczeństwa danych osobowych do których spełnienia nasza Spółka jest zobowiązana są zarejestrowane w F-3/P-4.01 Rejestrze wymagań prawnych

Dostęp do treści przepisów zapewniony jest przez portal: http://prawo.sejm.gov.pl/isap.nsf/home.xsp.

Wykaz jest na bieżąco aktualizowany. W przypadku zmian przeprowadzana jest analiza wpływu lub potencjalnego wpływu na system bezpieczeństwa danych osobowych oraz w konsekwencji zmian regulacji systemowych.

Odpowiedzialnym za nadzór nad aktualnością przepisów prawa i ich transponowaniem do regulacji wewnętrznych jest Pełnomocnik ds. ochrony danych.

16. AUDYTY I INSPEKCJE WEWNĘTRZNE ORAZ U DOSTAWCÓW USŁUG.

Postępowanie zgodnie z procedurą P-8.01 Audyt wewnętrzny.

17. OKRESOWY PRZEGLĄD SYSTEMU BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Na zakończenie każdego roku Pełnomocnik ds. ochrony danych przygotowuje dla kierownictwa sprawozdanie z funkcjonowania oraz skuteczności systemu bezpieczeństwa danych osobowych. W sprawozdaniu przedstawione zostają informacje dotyczące:

- status ustaleń z poprzedniego przeglądu systemu bezpieczeństwa danych osobowych
- zmian jakie miały miejsce w systemie w ciągu ostatnich 12 m-cy
- planowane zmiany w systemie i zalecenia do realizacji
- status oceny ryzyka i stosowanych środków
- wyniki przeprowadzonych audytów i inspekcji

- ilość i charakter naruszeń bezpieczeństwa danych osobowych
- realizacji żądań osób których dane dotyczą

Wyniki przeglądu wyżej przedstawionych rodzajów informacji zawierają

- zmiany i zalecenia do doskonalenia w systemie
- informacje dotyczące zasobów, niezbędnych do utrzymywania systemu bezpieczeństwa danych osobowych oraz wdrożenia wskazanych zmian i zaleceń do doskonalenia
- inne ustalenia dotyczące zgodności i skuteczności systemu

Sprawozdanie przedstawiane jest w formie udokumentowanej.

Prezes Zarządu, Dyrektor Spółki INSS-POL Sp. z o.o.

dr inż. Andrzej Olejnik