EMG POLAND SP. Z O.O. I TELOC POLSKA SP. Z O.O.

POLITYKA BEZPIECZEŃSTWA

Przetwarzania danych osobowych w EMG Poland Sp. z o.o. i Teloc Polska Sp. z o.o.

Wg. ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

SPIS TREŚCI: **STRONA**

DOKUMENTACJA DOTYCZĄCA SPOSOBU PRZETWARZANIA DANYCH OSOBOWYCH

Definicje :

1) **„RODO”**

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);

2) **„ustawa”**

Ustawa z dnia……. o ochronie danych osobowych (Dz.U. z 2018 r. , poz……);

3) **„inspektor ochrony danych „**

osoba , podmiot powołany przez administratora danych do realizacji zadań wynikających z RODO celem skutecznej ochrony danych osobowych ;

4) **„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;

5) **„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;

6) **„incydent”**

naruszenie ochrony danych osobowych w sposób zamierzony lub niezamierzony , które może powodować stratę oraz skutki negatywne dla bezpieczeństwa zasobów;

7) **„ograniczenie przetwarzania”**

oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

8) **„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;

9) „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;

10) „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;

11) „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;

12) „podmiot przetwarzający”

oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

13) „odbiorca”

oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

14) „strona trzecia”

oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;

15) „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;

-

16) „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;

17) „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;

18) „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;

19) „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;

20) „przedstawiciel”

oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający na mocy art. 27 do reprezentowania administratora lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z niniejszego rozporządzenia;

21) „przedsiębiorca”

oznacza osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą;

22) „organ nadzorczy”

oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51;

23) „zgodność przetwarzania danych osobowych „

1. 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.

24) „warunki wyrażenia zgody"

1. 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.

2. Jeżeli osoba, której dane dotyczą, wyrażą 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.

3. 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.

4. 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.

25) „przetwarzanie szczególnych kategorii danych osobowych"

Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby. Powyższe nie dotyczy wówczas gdy został jeden z warunków zawartych w art.9 ust.2 RODO

WPROWADZENIE

Niniejszy dokument opisuje reguły dotyczące zapewnienia bezpieczeństwa danych osobowych zawartych w *EMG Poland Sp. z o.o. i Teloc Polska Sp. z o.o.*.

Opisane reguły określają granice dopuszczalnego zachowania wszystkich , którzy przetwarzają dane osobowe w jednostce.

Dokument zwraca uwagę na konsekwencje , jakie mogą wynikać z niewłaściwego przetwarzania danych osobowych oraz procedury postępowania dla zapobiegania i minimalizacji skutków zagrożeń.

Dokument „ Polityka bezpieczeństwa" przetwarzania danych osobowych zgodnie z RODO , określa sposób postępowania celem minimalizacji naruszenia bezpieczeństwa przy przetwarzaniu danych osobowych a także sposób postępowania w sytuacji wystąpienia incydentu.

-

Potrzeba opracowania „Polityki bezpieczeństwa„ wynika z przepisów art.24 RODO , który do obowiązków administratora zalicza wdrażanie odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie danych osobowych odbywało się zgodnie z rozporządzeniem i aby móc to wykazać.

Zasady stosowanych środków powinny uwzględniać charakter, zakres i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia.

Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki , o których mowa powyżej obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

PRZEPISY OGÓLNE

1. Celem „Polityki bezpieczeństwa „ jest wdrażanie odpowiednich metod, które spowodują właściwe postępowanie i zabezpieczenie zasobów związanych z przetwarzaniem danych osobowych;
2. „Polityka bezpieczeństwa „ określa tryb i zasady postępowania w przypadku , gdy:
    1) ujawnione zostaną sytuacje wskazujące na wystąpienie incydentu z naruszeniem ochrony danych osobowych;
    2) zostały zanalizowane określone ryzyka naruszenia celem minimalizacji ryzyka.

3. Realizacja zapisów w „Polityce bezpieczeństwa” ma zapewnić właściwą i skuteczną reakcję , ocenę i dokumentowanie przypadków wystąpienia incydentów ;

4. Administrator swoją decyzją nie wyznacza inspektora ochrony danych osobowych;

ZADANIA ADMINISTRATORA OCHRONY DANYCH

1) informowanie pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia (RODO) oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

2) monitorowanie przestrzegania przepisów krajowych , rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora w dziedzinie ochrony danych osobowych;

3) podejmowanie działań zwiększające świadomość pracowników przetwarzających poprzez szkolenia personelu uczestniczącego w operacjach przetwarzania;

4) prowadzenie okresowych przeglądów stanu zabezpieczenia danych osobowych , audytów ;

5) realizacja zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania ;

6) współpraca z organem nadzorczym;

7) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami , oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;

-

8) w przypadku incydentu związanego z naruszeniem ochrony danych osobowych pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy rozporządzenia (RODO);

9) prowadzenie dokumentacji o ochronie danych osobowych;

10) prowadzenie spraw związanych z incydentami , w przypadku ich wystąpienia;

11) dokonywanie oceny i szacowania ryzyka celem zastosowania skutecznych metod organizacyjnych i technicznych dla właściwej ochrony danych osobowych u administratora danych osobowych, a w przypadku potrzeby oceny skutków naruszenia ochrony danych osobowych;

12) przygotowywanie poleceń -upoważnień do przetwarzania danych osobowych oraz prowadzenie ewidencji osób poleceń- upoważnionych .

PRZETWARZANIE DANYCH OSOBOWYCH – ZASADY OGÓLNE

1) wszelkie przetwarzanie danych osobowych powinno być zgodne z prawem i rzetelne.;

2) dla osób fizycznych powinno być przejrzyste, że dotyczące ich dane osobowe są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim stopniu te dane osobowe są lub będą przetwarzane;

3) zasada przejrzystości wymaga, by wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem.;

4) zasada ta dotyczy w szczególności informowania osób, których dane dotyczą, o tożsamości administratora i celach przetwarzania oraz innych informacji mających zapewnić rzetelność i przejrzystość przetwarzania w stosunku do osób, których sprawa dotyczy, a także prawa takich osób do uzyskania potwierdzenia i informacji o przetwarzanych danych osobowych ich dotyczących;

5) osobom fizycznym należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem;

6) konkretne cele przetwarzania danych osobowych powinny być wyraźne, uzasadnione i określone w momencie ich zbierania.;

-

7) dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane. Wymaga to w szczególności zapewnienia ograniczenia okresu przechowywania danych do ścisłego minimum.;

8) dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami;

9) aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu.;

10) należy podjąć wszelkie rozsądne działania zapewniające sprostowanie lub usunięcie danych osobowych, które są nieprawidłowe;

11) dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu **.**

UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH PRZEZ PRACOWNIKÓW

1) zgodnie z art. 29 RODO - podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego;

2) wzór polecenia -upoważnienia stanowi załącznik nr 1 do Polityki .

PODMIOT PRZETWARZAJĄCY - UMOWA POWIERZENIA

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) podmiot przetwarzający zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;

5) umowa powierzenia jest podpisana na piśmie lub w formie elektronicznej;

6) wzór umowy powierzenia stanowi załącznik nr 2.

REJESTROWANIE CZYNNOŚCI - ZASADY

1) **zgodnie z Rozporządzeniem ogólnym UE w sprawie ochrony danych osobowych, administrator danych prowadzi rejestr czynności przetwarzana danych osobowych. Jest to dokument, który ma pokazywać w szczególności w jakich procesach w organizacji są przetwarzane dane osobowe, w jakim celu, kogo dotyczą oraz jak są zabezpieczane. Dokument ten będzie musiał zostać udostępniony na każde wezwanie RODO;**

2) rejestr czynności przetwarzania nie jest prowadzony gdyż firma ma mniej niż 250 pracowników oraz przetwarzanie :

- nie może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą;
- ma charakter sporadyczny;
- nie obejmuje szczególne kategorie danych osobowych ;
- nie obejmuje danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o których mowa w art. 10 RODO.

INCYDENTY

1) 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 nakłada na administratora danych obowiązek dokumentowania wszelkich naruszeń ochrony danych osobowych;

2) zasady zgłaszania naruszenia ochrony danych organowi nadzorczemu określone są w artykule 33 RODO;

3) administrator danych osobowych ma obowiązek zgłoszenia organowi nadzorczemu przypadek naruszenia ochrony danych osobowych w ciągu 72 godzin. Jeżeli zgłoszenie przekazane zostanie po 72 godz. należy wówczas dołączyć wyjaśnienie przyczyn opóźnienia.;

4) zwolnienie z obowiązku zgłoszenia naruszenia, organowi nadzorczemu możliwe jest, jeżeli jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych;

-

5) jeżeli naruszenie dotyczy podmiotu przetwarzającego, to podmiot przetwarzający bez zbędnej zwłoki zgłasza je administratorowi danych;

6) jeżeli informacji nie możemy udzielić w tym samym czasie możemy je przekazywać organowi nadzorczemu sukcesywnie bez zbędnej zwłoki;

7) administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania artykułu 33 RODO;

8) administrator prowadzi rejestr incydentów – wzór rejestru stanowi załącznik nr 3 do Polityki.

ZAWIADAMIANIE OSOBY, KTÓREJ DANE DOTYCZĄ, O NARUSZENIU OCHRONY DANYCH OSOBOWYCH.

1) jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu;

2) zawiadomienie, jasnym i prostym językiem powinno opisywać charakter naruszenia ochrony danych osobowych oraz zawierać przynajmniej niżej wymienione informacje;

- imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
- 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.

Zawiadomienie nie jest wymagane w następujących przypadkach:

1. Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych.

2. Administrator zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w pkt. 1.

3. Wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

4. Jeżeli administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, organ nadzorczy – biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko – może od niego tego zażądać lub może stwierdzić, że spełniony został jeden z warunków, wymienionych wyżej;

5. Wzór zawiadomienia stanowi załącznik nr 4 do Polityki.

-

OBOWIĄZEK INFORMACYJNY –ZASADY

Jakie informacje należy przekazać osobom, których dane dotyczą?

1. Motyw 60 preambuły RODO wskazuje nam, że osoba, której dane dotyczą, musi być poinformowana o **prowadzeniu operacji przetwarzania i o jego celach**. Poza tym administrator powinien podać wszelkie inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania, uwzględniając konkretne okoliczności i kontekst przetwarzania danych osobowych.

2. Dodatkowo należy poinformować o fakcie **profilowania** oraz o konsekwencjach takiego profilowania. W przypadku zbierania danych od osoby, której dane dotyczą, należy wskazać, czy ma ona obowiązek je podać, oraz o konsekwencjach ich niepodania.

O czym powinniśmy poinformować zbierając dane od osoby, której dane dotyczą?

W przypadku, gdy zbieramy dane osobowe, od osoby której dane dotyczą zgodnie z art. 13 ust. 1 i 2 RODO powinniśmy poinformować ją o:

a) swojej tożsamości i danych kontaktowych oraz tożsamość i danych kontaktowych swojego przedstawiciela, jeżeli istnieje;

b) danych kontaktowych inspektora ochrony danych (jeżeli go powołaliśmy);

c) celach przetwarzania, do których mają posłużyć dane osobowe;

d) podstawie prawnej przetwarzania;

f) prawnie uzasadnionym interesie realizowanym przez administratora lub przez stronę trzecią – jeżeli przetwarzanie odbywa się na podstawie prawnie usprawiedliwionego interesu ADO ;

g) odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;

h) transferze danych do państwa trzeciego, w tym o:

- zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej ,
- stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony ,
- lub wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych w przypadku przekazania danych do państwa trzeciego ,

i) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

j) prawie do:

- żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą,
- ich sprostowania, usunięcia lub ograniczenia przetwarzania lub

---

-

- wniesienia sprzeciwu wobec przetwarzania, a także
- przenoszenia danych;

k) prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem jeżeli przetwarzanie odbywa się na podstawie zgody na przetwarzanie danych zwykłych lub szczególnej kategorii ;

l) prawie wniesienia skargi do organu nadzorczego;

m) informacji, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;

n) informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

O CZYM POWINNIŚMY POINFORMOWAĆ ZBIERAJĄC DANE Z INNEGO ŹRÓDŁA NIŻ OSOBA, KTÓREJ DANE DOTYCZĄ?

W przypadku, gdy zbieramy dane osobowe, od innego źródła niż od osoby której dane dotyczą zgodnie z art. 14 ust. 1 i 2 RODO powinniśmy poinformować ją o:

a) informacjach z punktów a-l oraz n wskazanych powyżej;

b) kategoriach odnośnych danych osobowych

c) źródle pochodzenia danych osobowych, a jeżeli ma to zastosowanie, o pochodzeniu ich ze źródeł powszechnie dostępnych.

W jakiej formie mamy spełniać obowiązek informacyjny?

1. Powyższe informacje administrator danych powinien przekazać w **formie zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej** oraz jasnym i prostym językiem w szczególności gdy informacje są kierowane do dziecka (art. 12 ust. 1 RODO),

2. Klauzulę informacyjną można opatrzyć też **standardowymi znakami graficznymi**, które w widoczny, zrozumiały i czytelny sposób przedstawią sens zamierzonego przetwarzania (Art. 12 ust. 7 RODO),

3. Obowiązek informacyjny możemy spełnić **na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie**. Jednak jeżeli w treści obowiązku informacyjnego zastosowano znaki, a są one przedstawione elektronicznie, muszą nadawać się do odczytu maszynowego. Dodatkowo spełnienie obowiązku informacyjnego w stosunku do osób musi być wolne od opłat.

WZÓR

-

Zgodnie z art.13 ust.1 i ust.2 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 (ogólnego rozporządzenia o ochronie danych), informujemy ,że:

1) **administratorem Pani/Pana danych osobowych jest** … (**nazwa ADO*) z siedzibą w … (*adres*) (*dodatkowo należy podać dane przedstawiciela jeżeli istnieje*);

2) **inspektorem ochrony danych w** … (*nazwa ADO*) **jest Pan/Pani** (**imię i nazwisko inspektora*) … (*e-mail lub inne dane kontaktowe*) … ;

3) **Pani/Pana dane osobowe przetwarzane będą w celu** … (**należy podać cel przetwarzania*) na podstawie … (*należy podać podstawę prawną przetwarzania np. art. 6 ust 1 pkt a/b/c/d/e/f. *Przy podpunkcie f należy wskazać uzasadniony interes ADO lub strony trzeciej*);

4) **odbiorcą Pani/Pana danych osobowych będą** … (*można wymienić kategorię odbiorców o ile istnieją*);

5) **Pani/Pana dane osobowe będą przekazywane do państwa trzeciego/organizacji międzynarodowej na podstawie**:

wybrać odpowiednią podstawę:

1. **Na podstawie decyzji Komisji Europejskie stwierdzającej odpowiedni stopień ochrony** … (*wskazać odpowiednią decyzję*)
2. **W tym zakresie nie został stwierdzony przez Komisję Europejską odpowiedni stopień ochrony w drodze decyzji niemniej dane będą odpowiednio zabezpieczone za pomocą**:

a) **prawnie wiążącego i egzekwowalnego instrumentu między organami lub podmiotami publicznymi w postaci** …(*wskazać jakiego*);

b) **wiążących reguł korporacyjnych** … (*wskazać jakie*) zatwierdzonych przez GIODO;

c) **standardowych klauzul ochrony danych przyjętych przez Komisję Europejską** … (*wskazać jakie*);

d) **standardowych klauzul ochrony danych przyjętych przez GIODO i zatwierdzonych przez Komisję Europejską** (*wskazać jakie*);

e) **zatwierdzonego przez GIODO kodeksu postępowania** (*wskazać jakiego*);

f) **certyfikatu ochrony danych osobowych** (*wskazać jakiego*);

g) **zezwolenia GIODO na klauzule umowne** … (*klauzule umowne między ADO lub procesorem a ADO, procesorem lub odbiorcą danych w państwie trzecim lub organizacji międzynarodowej*);

h) **zezwolenia GIODO na postanowienia administracyjne między organami lub podmiotami publicznymi**.

Może Pan/ Pani uzyskać kopię danych osobowych przekazywanych do państwa trzeciego … *(wskazać sposób uzyskania kopii danych lub miejsce udostępnienia danych)*

6) **Pani/Pana dane osobowe będą przechowywane przez okres** … *(jeżeli nie ma możliwości wskazania okresu przechowywania należy podać kryterium ustalania tego okresu np. do czasu wyłonienia zwycięscy konkursu, do czasu zakończenia rekrutacji itd.)*;

7) **posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do**

-

cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania *(jeżeli przetwarzanie odbywa się na podstawie zgody)*, którego dokonano na podstawie zgody przed jej cofnięciem;

8) **ma Pan/Pani prawo wniesienia skargi do GIODO gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r**.;

9) **podanie przez Pana/Panią danych osobowych jest** … *(wybrać odpowiednio: wymogiem ustawowym/warunkiem umownym/warunkiem zawarcia umowy)*. Jest Pan/Pani zobowiązana do ich podania a konsekwencją niepodania danych osobowych będzie … *(jeżeli osoba, której dane dotyczą, jest zobowiązana do ich podania należy wskazać ewentualne konsekwencje niepodania danych)*;

10) **Pani/Pana dane będą** / *nie będą*/ **przetwarzane w sposób zautomatyzowany w tym również w formie profilowania**. /*jeżeli będą*/ **Zautomatyzowane podejmowanie decyzji będzie odbywało się na zasadach** … , **konsekwencją takiego przetwarzania będzie** … *(należy wskazać istotne informacje o zasadach zautomatyzowanego podejmowania decyzji oraz informacje o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą. Np. w jaki sposób będą oceniane czynniki osobowe osoby fizycznej, natomiast przykładową konsekwencją takiego przetwarzania może być automatyczne odrzucenie elektronicznego wniosku kredytowego czy elektroniczne metody rekrutacji bez interwencji ludzkiej.*

KAŻDY CZYJE DANE OSOBOWE SĄ PRZETWARZANE MA PRAWO DO KONTROLI

Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dotyczące jej dane osobowe. Jeżeli dane są przez dany podmiot przetwarzane, to może wnioskować o udzielenie następujących informacji:

1) cele przetwarzania;

2) kategorie danych osobowych;

3) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;

4) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

5) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;

6) informacje o prawie wniesienia skargi do organu nadzorczego;

7) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;

-

8) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą;

9) jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach związanych z przekazaniem.

OBOWIĄZEK UŁATWIANIA KONTROLI

Administrator ma obowiązek ułatwiania osobie, której dane dotyczą, wykonanie praw przysługujących jej na mocy art. 15–22:

1. Prawo dostępu do swoich danych ,
2. Prawo do sprostowania,
3. Prawo do usunięcia,
4. Prawo do ograniczenia,
5. Prawo do przenoszenia,
6. Prawo do sprzeciwu,
7. Prawo do informacji o profilowaniu.

Również w przypadkach przetwarzania niewymagającego identyfikacji, administrator nie może odmawiać podjęcia działań na żądanie osoby chcącej zrealizować prawa przysługujące jej na mocy art. 15–22, chyba że wykaże, iż nie jest w stanie zidentyfikować osoby, której dane dotyczą.

OBOWIĄZEK INFORMOWANIA –TERMINY

TERMINY NA WYWIĄZANIE SIĘ Z TEGO OBOWIĄZKU TO:

1) **bez zbędnej zwłoki** – a w każdym razie w terminie miesiąca od otrzymania żądania- zasadniczo,

2) **trzy miesiące** – w razie potrzeby ww. termin jednego miesiąca można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań,

3) w terminie miesiąca od otrzymania żądania administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia,
4) Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

OBOWIĄZEK UZASADNIENIA ODRZUCENIA ŻĄDANIA - POUCZENIE O PRAWIE SKARGI

Jeżeli administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o:

1) powodach niepodjęcia działań; oraz

2) możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

WOLNOŚĆ OD OPŁAT

Prawo do kontroli jest wolne od opłat jednakże:

-

jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może:

1) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo

2) odmówić podjęcia działań w związku z żądaniem.

Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.

OBOWIĄZKI OSOBY, KTÓREJ DANE DOTYCZĄ, WZGLĘDEM ADMINISTRATORA

1) Jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą,
2) To, że wątpliwości muszą być uzasadnione, oznacza że administrator powinien skorzystać z wszelkich rozsądnych środków w celu zweryfikowania tożsamości żądającej dostępu osoby, której dane dotyczą, w szczególności w kontekście usług internetowych i identyfikatorów internetowych. Administrator nie powinien zatrzymywać danych osobowych wyłącznie w celu reagowania na ewentualne żądania,
3) Jeżeli administrator przetwarza duże ilości informacji o osobie, której dane dotyczą, może zażądać, przed podaniem informacji, by osoba, której dane dotyczą, sprecyzowała informacje lub czynności przetwarzania, których dotyczy jej żądanie.

ANALIZA I SZACOWANIE RYZYKA

Zgodnie z art.24 RODO na administratora oraz podmiot przetwarzający nałożony został obowiązek zastosowania zabezpieczeń danych osobowych zgodnie z oceną zagrożeń.

Obowiązki administratora

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. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

3. Stosowanie zatwierdzonych kodeksów postępowania, o których mowa wart. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa wart. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.

Artykuł 25 RODO

Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu

---

-

sposobów przetwarzania, jak i w czasie samego przetwarzania –wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.

2. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

3. Każda organizacja przetwarzająca dane narażona jest na wpływ czynników wewnętrznych oraz zewnętrznych, które mogą spowodować naruszenie bezpieczeństwa, prowadzące do przypadkowego lub niezgodnego z prawem:

   - **zniszczenia,**
   - **utracenia,**
   - **zmodyfikowania,**
   - **nieuprawnionego ujawnienia,**
   - **nieuprawnionego dostępu**

4. Ocenę ryzyka w zakresie bezpieczeństwa przetwarzania danych osobowych przeprowadzamy biorąc pod uwagę potencjalnie negatywne skutki (straty) zarówno dla administratora jak i dla osób , których dane dotyczą.

UWAGA ! Gdyby istniało wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą , wówczas należy dodatkowo przeprowadzić ocenę skutków dla ochrony danych osobowych.

DEFINICJE:

Ryzyko – możliwość zaistnienia zdarzenia, które będzie miało wpływ na realizację założonych celów. Ryzyko jest mierzone wpływem (skutkami) i prawdopodobieństwem wystąpienia". W przypadku ryzyka naruszenia praw i wolności osób, których dane dotyczą, celem będzie ochrona tych praw i wolności.

Szacowanie ryzyka – całościowy proces identyfikacji ryzyka, analizy ryzyka oraz oceny ryzyka (definicja przyjęta zgodnie z normą PN-ISO/IEC 25005:2011)

Identyfikacja ryzyka - jest to czynność polegająca na określeniu, co może się zdarzyć (kiedy, gdzie, jak i dlaczego) i spowodować stratę.

Kryteria akceptacji ryzyka – są to kryteria, które określają dopuszczalność danego ryzyka. Zwykle definiuje się je poprzez wartość progową, np. przy przedziałach ryzyka 0-2, 3-5 oraz 6-8, akceptowalną wartością jest ryzyko tylko w zakresie 0-2.

-

Kryteria oceny ryzyka - są to kryteria, które określają poziomy odniesienia, względem których określa się ważność ryzyka.

Podatność - jest to słabość, która może być wykorzystana przez zagrożenie, powodując niekorzystne skutki, np. luka w systemie informatycznym.

Zabezpieczenie - jest to środek, którego celem jest zmniejszenie ryzyka poprzez obniżenie prawdopodobieństwa zrealizowania zagrożenia (czyli wykorzystania istniejącej podatności) lub też minimalizację potencjalnych strat związanych ze zrealizowanym zagrożeniem, np. program antywirusowy, drzwi antywłamaniowe, stosowanie procedury bezpieczeństwa.

Zagrożenie - jest to źródło potencjalnej szkody, np. zagrożenie naruszenia integralności danych.

Proces przetwarzania danych osobowych – zespół operacji (czynności) wykonywanych na danych osobowych lub zestawach danych osobowych w celu osiągnięcia określonego celu przetwarzania.

Operacja przetwarzania danych osobowych - każda czynność wykonywana na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka 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.

Anonimizacja – oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było przypisać konkretnej osobie, której dane dotyczą, za pomocą dodatkowych informacji lub wszelkich innych środków, jakimi dysponuje administrator lub podmiot przetwarzający. Zabieg ten ma charakter trwały i nieodwracalny, powodujący, że po jego przeprowadzeniu nie mamy do czynienia z danymi osobowymi.

Pseudonimizacja - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji. Te dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. W przeciwieństwie do anonimizacji, której skutkiem jest nieodwracalne uniemożliwienie identyfikacji osoby, pseudonimizacja jest procesem odwracalnym.

Grupa Robocza Art. 29 - Grupa Robocza Art. 29 to powołany na mocy Dyrektywy 95/46 zespół roboczy do spraw ochrony osób fizycznych mający charakter doradczy i działający w sposób całkowicie niezależny. Jej misją jest służenie radą Komisji Europejskiej, i przyczynianie się do jednolitego stosowania przepisów krajowych przyjętych na mocy dyrektywy. Grupę tworzą przedstawiciele krajowych organów nadzorczych, przedstawiciele organów ustanowionych dla instytucji i organów unijnych (po jednym dla każdej z instytucji i organu) oraz przedstawiciele Komisji Europejskiej. Działania Grupy sprowadzają się głównie do wydawania niemających mocy wiążącej zaleceń, rekomendacji oraz opinii w sprawach unijnych aktów normatywnych z zakresu ochrony prywatności.

RODO - 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), które będzie stosowane od 25 maja 2018 r.; jego celami są skuteczna ochrona podstawowych praw i wolności osób fizycznych, w szczególności prawa do ochrony danych osobowych osób fizycznych oraz uregulowanie zasad i zapewnienie swobodnego przepływu danych osobowych w UE w taki sposób, by ochrona praw jednostki nie stała temu na przeszkodzie.

-

OGÓLNE WYMOGI BEZPIECZEŃSTWA

Przetwarzanie danych osobowych w EMG Poland Sp. z o.o. i Teloc Polska Sp. z o.o. odbywa się w postaci:

- elektronicznej (np.: pliki na dysku komputera, w pamięci operacyjnej komputera),
- papierowej (wydruki).

Aby zapewnić bezpieczeństwo przetwarzania danych osobowych należy stosować:

- środki ochrony fizycznej stanowiska komputerowego oraz wydruków przed nieuprawnionym dostępem,
- środki ochrony technicznej stanowiska komputerowego (np.: hasła dostępu do stacji roboczej, program antywirusowy).

AKTYWA

1. Przetwarzanie danych osobowych odbywa się w EMG Poland Sp. z o.o. i Teloc Polska Sp. z o.o. z siedzibą w Warszawie ul. Stradomska 66, 04-608.
2. Dane osobowe przetwarzane są przez osoby uprawnione , posiadające upoważnienie wydane przez administratora danych osobowych .
3. Osoby upoważnione do przetwarzania danych osobowych odbywają obowiązkowe szkolenie z zakresu procedur i obowiązków związanych z prawidłowym przetwarzaniem danych osobowych . Po odbyciu szkolenia osoby przeszkolone składają pisemne oświadczenie o zapoznaniu z przepisami oraz o zachowaniu tajemnicy .
4. Prowadzona jest ewidencja wydanych upoważnień do przetwarzania danych osobowych oraz rejestr osób , które podpisały oświadczenie o zapoznaniu z przepisami .
5. Prowadzony jest wykaz pomieszczeń stanowiących obszar przetwarzania danych osobowych wg.

	Budynek ..... **Nazwa jednostki** ..... **ul**.....		
L.P.	**Nazwa pomieszczenia**	**Nazwa stanowiska**	**Miejsce ,położenie**

poniższego wzoru:

-

Prowadzony jest rejestr czynności przetwarzania danych osobowych .

6. Rejestr czynności przetwarzania prowadzony przez ADO wg.RODO jest prowadzony wówczas gdy przetwarzanie :

- może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą;
- nie ma charakteru sporadycznego;
- obejmuje szczególne kategorie danych osobowych .

		DANE KONTAKTOWE
NAZWA ADMINISTATORA		
NAZWY WSPÓŁADMINISTATORÓW		
NAZWA PRZEDSTAWICIELA		
IMIĘ I NAZWISKO INSPEKTORA		

Kategorie osób, których dane dotyczą	**Kategorie danych osobowych**	**Kategorie odbiorców, którym dane ujawniono lub zostaną ujawnione**	**Nazwa państwa trzeciego, do którego dane są przekazywane**	**Planowane terminy usunięcia danych**	**Sposób Zabezpiecze-nia *(alternatywnie)***

EWENTUALNE KOSZTY ZWIĄZANE Z UTRATĄ AKTYWÓW

1. Koszty związane z odtworzeniem aktywów,
2. Koszty utraty zaufania do administratora danych osobowych,
3. Koszty związane z utratą:
   - poufności,
   - integralności,
   - dostępności danych ,
4. Możliwość nałożenia kary przez organ nadzorczy,
5. Koszty związane z możliwością nakazania przez organ nadzorczy całkowitego zaprzestania lub czasowego zaprzestania przetwarzania danych osobowych , np. w sytuacji niezastosowania przez administratora odpowiednich środków bezpieczeństwa.

-

ZAGROŻENIA DLA SYSTEMU INFORMATYCZNEGO

Podstawowe zagrożenia dla systemu informatycznego, przeznaczonego do przetwarzania danych osobowych:

I. utrata poufności (pozyskanie danych przez osoby nieupoważnione):

- ✓ nieuprawniony dostęp do pomieszczenia gdzie znajdują się dane osobowe(wydruki)
- ✓ nieuprawniony dostęp do stacji roboczej (komputera) gdzie znajdują się dane osobowe (np. poprzez ujawnienie hasła dostępu),
- ✓ nieuprawnione skopiowanie danych osobowych na inny nośnik,
- ✓ zgubienie nośnika zawierającego dane osobowe,
- ✓ niedostateczne zniszczenie wydruku zawierającego dane osobowe,
- ✓ klęska żywiołowa powodująca utratę poufności danych.

II. utrata integralności (zmiany w systemie informatycznym przeprowadzone przez osoby nieupoważnione):

- ✓ nielegalny dostęp do dokumentów zawierających dane osobowe (w formie papierowej i elektronicznej),
- ✓ błędy ludzkie,
- ✓ działania wirusów (brak programów antywirusowych i firewalli),
- ✓ awarie oprogramowania komputerów,

III. utrata rozliczalności (brak możliwości przypisania danemu podmiotowi konkretnych działań) :

- ✓ brak mechanizmu uniemożliwiającego usunięcie logów o pracy danej osoby na komputerze,
- ✓ brak kontroli nad kopiowaniem dokumentów z komputera na nośniki zewnętrzne.

Do głównych źródeł zagrożeń dla stanowisk komputerowych, na których przetwarzane są dane osobowe przedstawia poniższa tabela:

ŹRÓDŁO ZAGROŻENIA		SPOSÓB ZABEZPIECZENIA
Siły wyższe – naturalne -niezależne od jednostki ludzkiej	• pożar np.: będący skutkiem uderzenia pioruna, • starzenie się sprzętu, • powódź, • katastrofa budowlana, • wilgoć, kurz,	Skutki zagrożeń wynikających z sił natury można starać się ograniczyć poprzez odpowiednia zabezpieczenie budynku, w którym znajdują się dane osobowe.
Działalność człowieka	• błędy użytkowników. • zgubienie nośnika informacji, • niewłaściwe usunięcie danych z nośnika informacji,	Zagrożenia wynikające z działalności człowieka mogą zostać ograniczone poprzez

---

-

	• terroryzm, • utrata prądu, • szpiegostwo, • kradzież, • wandalizm, • podsłuch, • ataki socjotechniczne.	rygorystyczne przestrzeganie zasad ochrony danych osobowych obowiązujących w EMG Poland Sp. z o.o. i Teloc Polska Sp. z o.o. oraz systematyczne szkolenia użytkowników.

ANALIZA ZAGROŻEŃ I RYZYKA

1. Analiza zagrożeń i ryzyka polega na identyfikacji ryzyka wystąpienia niepożądanego czynnika (ujawnienia, przechwycenia itd.), określenia jego wielkości i zidentyfikowania obszarów wymagających zabezpieczeń tak, aby to ryzyko zminimalizować lub całkowicie go zlikwidować.

2. Zagrożenia i ryzyka w zakresie ochrony danych osobowych:
   - Niedostateczne kwalifikacje Inspektora (w tym brak podnoszenia kwalifikacji),
   - Brak procedur ochrony danych osobowych,
   - Niezgodne z wymogami prawnymi, nieaktualne, nieadekwatne do zagrożeń procedury ochrony danych osobowych,
   - Brak aktualnego wykazu zbiorów będących w zasobach jednostki,
   - Brak lub wady upoważnień do przetwarzania danych osobowych,
   - Udzielanie upoważnienia do przetwarzania danych osobowych osobom postępującym nieetycznie,
   - Brak lub wady ewidencji wydanych upoważnień,
   - Brak lub wady szkoleń z zakresu ochrony danych osobowych,
   - Wady nadzoru nad przetwarzaniem i ochroną danych osobowych,
   - Brak lub wady identyfikacji i analizy ryzyka w zakresie przetwarzania i ochrony danych osobowych,
   - Brak reakcji lub nieprawidłowa reakcja na zagrożenie bezpieczeństwa danych osobowych lub systemów i sieci teleinformatycznych.

POJĘCIE I CELE RYZYKA

1. Ryzyko jest mierzone wpływem (skutkami) i prawdopodobieństwem wystąpienia". Rozporządzenie w Artykule 32 definiuje cele w zakresie bezpieczeństwa przetwarzania i są to:

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

2. W związku z powyższym ryzyko w przetwarzaniu danych jest związane z potencjalną sytuacją, w której określone zagrożenie wykorzysta podatność (np. niezabezpieczony hasłem sprzęt komputerowy), powodując w ten sposób szkodę dla jednostki organizacyjnej (np. kradzież lub upublicznienie informacji).

IDENTYFIKACJA RYZYKA (ZAGROŻEŃ I PODATNOŚCI)

1. Zgodnie z zapisem 75 punktu preambuły Rozporządzenia, wyszczególnione zostały zagrożenia związane z przetwarzaniem danych z wyszczególnieniem prowadzących do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności:

   - jeżeli przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną,
   - jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi,
   - jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa,
   - jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych,
   - lub jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci,
   - jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

-

POMIAR I ANALIZA RYZYKA

Prawdopodobieństwo w terminologii zarządzania ryzykiem to możliwość wystąpienia jakiegoś zdarzenia (np. jako prawdopodobieństwo lub częstość w określonym przedziale czasu).

Zdefiniowanie poziomu ryzyka realizujemy wykorzystując macierz ryzyka , która daje możliwość zobrazowania poziomu zagrożeń.

PRAWDOPODOBIEŃSTWO /RYZYKO/	NISKI	**1-20**
	ŚREDNI	**21-60**
	WYSOKI	**61-80**
	KRYTYCZNY	**81-100**

POZIOM RYZYKA	SPOSÓB DZIAŁANIA
N - niski	**Poziom ryzyka akceptowany** Działania podejmowane są w zależności od wymaganych nakładów
Ś - średni	**Poziom ryzyka nieakceptowany** Działanie może zostać przesunięte w czasie , lecz wymagany jest okresowy nadzór i monitorowanie
W – wysoki	**Poziom ryzyka nieakceptowany** Działanie może zostać przesunięte w czasie , lecz wymagany jest stały nadzór i monitorowanie
K – krytyczny	**Poziom ryzyka nieakceptowany** Wymagana jest niezwłoczna reakcja i działanie

RYZYKO SZCZĄTKOWE:

Ryzyko szczątkowe – ryzyko, które pozostaje po wprowadzeniu zabezpieczeń, często zwane również ryzykiem pozostałym lub ryzykiem akceptowalnym.

Po analizie zagrożeń i podatności wszystkich czynników występujących czy też mogących wystąpić opisanych dotychczas, niewątpliwie istnieje jeszcze pewne ryzyko dla bezpieczeństwa przetwarzania danych osobowych . w celu bardziej przejrzystego zidentyfikowania pozostałego ryzyka niżej przedstawiono proces analizy ryzyka w oparciu o podaną macierz. W rzędach macierzy wyszczególnione są zasoby podlegające ochronie.

-

Analiza dotyczy ryzyka jakie zagrażają:

- **INTEGRALNOŚCI,**
- **POUFNOŚCI ,**
- **DOSTĘPNOŚCI.**

INTEGRALNOŚĆ	właściwość zapewniająca, że informacje nie zostały zmienione lub zniszczone w sposób nieautoryzowany – **pożar, katastrofa budowlana, błąd ludzki przy przetwarzaniu danych osobowych, zniszczenie płyty zawierającej jedyną kopię danych osobowych.**
POUFNOŚĆ	właściwość zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom – **nieuprawniony dostęp klientów do danych osobowych, zagubienie wydruku .**
DOSTĘPNOŚĆ	właściwość bycia dostępnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot .

Skutek	rezultat niepożądanego incydentu, następstwa zaistnienia zagrożeń, szkody mierzone wysokością strat, jakie poniosłaby jednostka organizacyjna w wyniku ujawnienia, utraty lub modyfikacji informacji lub zasobu systemu.
Podatność	słabość zasobów, która może być wykorzystana przez zagrożenie – charakteryzuje łatwość, z jaką dane zagrożenie może wyrządzić szkodę.
Ryzyko	prawdopodobieństwo, że określone zagrożenie wykorzysta podatność zasobów, aby spowodować ich straty lub zniszczenie.

RYZYKO (iloczyn) : **PODATNOŚĆ X SKUTEK = RYZYKO**

PRZYJĘTE WARTOŚCI ZWIĄZANE Z OCENĄ ZAGROŻENIA:

- **1 - 3** - nie ma realnej szansy wystąpienia zidentyfikowanego zagrożenia; zagrożenie nigdy nie wystąpiło,
- **4 - 7** - zagrożenie jest mało realne, jednak zagrożenie jednak może się pojawić,
- **8 - 9**- zagrożenie jest realne i może pojawić się w nieoczekiwanym momencie, pomimo iż nie wystąpiło w okresie ostatnich 24 miesięcy,
- **10** -zagrożenie jest realne lub bardzo realne; zagrożenie wystąpiło w okresie ostatnich 24 miesięcy.

SZACOWANIE „RYZYKA INTEGRALNOŚCI"

W analizie ustalono cztery poziomy zagrożeń dotyczących zachowania integralności oraz zakres wartości liczbowych (1-10) dla tych poziomów:

Poziomy zagrożeń zachowania INTEGRALNOŚCI informacji	**Zakres wartości liczbowych skutków utraty integralności odpowiadający danemu poziomowi zagrożeń**
Niskie - **N**	1-3
Średnie- **Ś**	4-7
Wysokie - **W**	8-9
Krytyczny – **K**	10

-

MACIERZ OSZACOWANIA „RYZYKA INTEGRALNOŚCI”

ZASOBY (miejsce)	SZACOWANIE	ZAGROŻENIA							
		Nielegalny dostęp	Błędy, pomyłki	Celowe uszkodzenia	Nielegalne oprogramowanie	Wirusy	Personel	Awarie	Klęski żywiołowe
Nośniki informacji	SKUTKI	8	6	8	6	5	4	5	4
	PODATNOŚĆ	3	5	3	3	5	6	5	3
	RYZYKO	**24**	**30**	**24**	**24**	**25**	**24**	**25**	**12**
Zgromadzone dane – zbiory	SKUTKI	4	5	6	6	6	5	6	5
	PODATNOŚĆ	6	5	4	4	5	6	5	4
	RYZYKO	**24**	**25**	**24**	**24**	**30**	**30**	**30**	**20**
Oprogramowanie	SKUTKI	6	5	7	5	6	7	6	4
	PODATNOŚĆ	5	6	4	6	7	7	6	5
	RYZYKO	**30**	**30**	**28**	**30**	**42**	**49**	**36**	**20**
Sprzęt komputerowy	SKUTKI	6	6	5	6	6	7	6	4
	PODATNOŚĆ	6	5	4	5	6	7	5	4
	RYZYKO	**36**	**30**	**20**	**30**	**36**	**49**	**30**	**16**

OSZACOWANIE RYZYKA INTEGRALNOŚCI

W wyniku wymnożenia w wierszach poszczególnych zasobów liczb będących szacunkiem „skutków” i „podatności” dla poszczególnych zagrożeń, otrzymaliśmy liczby, które stanowią wynik szacowanego ryzyka dla zasobów w ujęciu integralności, informacji . Zgodnie z przyjętą metodyką szacowania ryzyka **poziom wielkości ryzyka** dla obliczonych wartości liczbowych wynosi:

NISKI	**1-20**
ŚREDNI	**21-60**
WYSOKI	**61-80**
KRYTYCZNY	**81-100**

Analizując otrzymane wyniki należy stwierdzić, że nie zanotowano poziomu ryzyka wysokiego i krytycznego.

-

SZACOWANIE „RYZYKA POUFNOŚCI ”

W analizie szacowania ryzyka przyjęto cztery poziomy zagrożeń zachowania „poufności” i 10-cio stopniową skalę skutków utraty „poufności”:

Poziomy zagrożeń zachowania POUFNOŚCI informacji	**Zakres wartości liczbowych skutków utraty POUFNOŚCI odpowiadający danemu poziomowi zagrożeń**
Niskie –**N**	1-3
Średnie- **Ś**	4-7
Wysokie- **W**	8-9
Krytyczny –**K**	10

MACIERZ OSZACOWANIA „RYZYKA POUFNOŚCI”

ZASOBY (miejsce)	**SZACOWANIE**	**ZAGROŻENIA**									
		Nielegalny dostęp	Błędy, pomyłki	Pokonanie i omijanie zabezpieczeń	Nielegalne kopiowanie	Nieuprawnione naprawy	Rotacja personelu	Awarie	Klęski żywiołowe	Podsłuch i pogląd	Niedyskrecja
Nośniki informacji	SKUTKI	9	6	6	8	6	5	4	4	5	9
	PODATNOŚĆ	3	5	6	7	7	7	4	4	5	6
	RYZYKO	**27**	**30**	**36**	**56**	**42**	**35**	**16**	**16**	**25**	**54**
Zgromadzone dane	SKUTKI	8	8	8	7	8	6	6	3	7	8
	PODATNOŚĆ	6	5	7	6	5	4	5	3	3	5
	RYZYKO	**48**	**40**	**56**	**42**	**40**	**24**	**30**	**9**	**21**	**40**
Oprogramowanie	SKUTKI	8	8	9	9	7	5	5	4	6	6
	PODATNOŚĆ	3	6	6	5	3	4	4	4	4	4
	RYZYKO	**24**	**56**	**54**	**45**	**21**	**20**	**20**	**16**	**24**	**24**
Sprzęt komputerowy	SKUTKI	8	7	8	2	8	4	6	4	6	6
	PODATNOŚĆ	7	7	7	3	7	5	7	3	6	4
	RYZYKO	**56**	**49**	**56**	**6**	**56**	**20**	**42**	**12**	**36**	**24**

-

OSZACOWANIE RYZYKA POUFNOŚCI

W wyniku wymnożenia w wierszach poszczególnych zasobów liczb będących szacunkiem „skutków" i „podatności" dla poszczególnych zagrożeń, otrzymaliśmy liczby, które stanowią wynik szacowanego ryzyka dla zasobów w ujęciu integralności, poufności i dostępności informacji . Zgodnie z przyjętą metodyką szacowania ryzyka **poziom wielkości ryzyka** dla obliczonych wartości liczbowych wynosi:

NISKI	**1-20**
ŚREDNI	**21-60**
WYSOKI	**61-80**
KRYTYCZNY	**81-100**

Analizując otrzymane wyniki należy stwierdzić, że nie zanotowano poziomu ryzyka wysokiego i krytycznego.

SZACOWANIE „RYZYKA DOSTĘPNOŚCI”

W analizie „ryzyka dostępności” przyjęto cztery poziomy zagrożeń zachowania „dostępności” i 10-cio stopniową skalę skutków utraty „dostępności”:

Poziomy zagrożeń zachowania „dostępności” informacji	**Zakres wartości liczbowych skutków utraty „dostępności” odpowiadający danemu poziomowi zagrożeń**
Niskie – **N**	1-3
Średnie – **Ś**	4-7
Wysokie – **W**	8-9
Krytycznego – **K**	10

MACIERZ OSZACOWANIA „RYZYKA DOSTĘPNOŚCI”

ZASOBY (miejsce)	**SZACOWANIE**	**ZAGROŻENIA**						
		Błędy, pomyłki	Celowe uszkodzenia	Nielegalne oprogramowanie	Infekcja wirusowa	Rotacja personelu	Awarie	Klęski żywiołowe
Nośniki informacji	SKUTKI	2	2	3	3	3	3	4
	PODATNOŚĆ	2	1	2	3	3	3	4
	RYZYKO	**4**	**2**	**6**	**9**	**9**	**9**	**16**
Zgromadzone dane	SKUTKI	6	6	6	6	6	6	6
	PODATNOŚĆ	7	3	3	5	2	2	2
	RYZYKO	**42**	**18**	**18**	**30**	**12**	**12**	**12**
Oprogramowanie	SKUTKI	3	4	2	2	3	3	2
	PODATNOŚĆ	2	3	2	3	2	3	4
	RYZYKO	**6**	**12**	**4**	**6**	**6**	**9**	**8**
Sprzęt komputerowy	SKUTKI	3	4	2	2	3	5	3
	PODATNOŚĆ	4	2	3	3	3	5	2
	RYZYKO	**12**	**8**	**6**	**6**	**9**	**25**	**6**

-

OSZACOWANIE RYZYKA DOSTĘPNOŚCI

W wyniku wymnożenia w wierszach poszczególnych zasobów liczb będących szacunkiem „skutków" i „podatności" dla poszczególnych zagrożeń, otrzymaliśmy liczby, które stanowią wynik szacowanego ryzyka dla zasobów i dostępności informacji . Zgodnie z przyjętą metodyką szacowania ryzyka **poziom wielkości ryzyka** dla obliczonych wartości liczbowych wynosi:

NISKI	**1-20**
ŚREDNI	**21-60**
WYSOKI	**61-80**
KRYTYCZNY	**81-100**

Analizując otrzymane wyniki szacowania ryzyka w zakresie integralności, poufności , dostępności należy stwierdzić, że zanotowano średni poziom zagrożeń , natomiast nie zanotowano poziomu ryzyka wysokiego i krytycznego.

WNIOSKI :

1) Wyniki ryzyka związanego z Bezpieczeństwem Informacji w EMG Poland Sp. z o.o. i Teloc Polska Sp. z o.o. w Warszawie są na poziomie nieakceptowanym,
2) Dla minimalizacji możliwości utraty danych osobowych oraz zmniejszenie oszacowanego ryzyka istotnym wsparciem w zakresie doboru odpowiednich do charakteru ryzyka środków i rozwiązań powinien być szkolenie pracowników i zwiększanie ich świadomości z zakresu RODO oraz Administrator danych osobowych powinien zabezpieczyć niezbędne środki oraz zasoby do wykonywania zadań związanych z ochroną danych osobowych.

Ponadto dla skutecznej realizacji zadań związanych z minimalizacją ryzyka należy zwracać szczególną uwagę na:

1. SPRZĘT

1) Nieuprawnione kopiowanie danych z dysku twardego,
2) Korzystanie z oprogramowań nie posiadających licencji,
3) Uszkodzenie sprzętu komputerowego (drukarka, karta sieciowa, jednostka centralna, klawiatura, mysz itp.) oraz łączy transmisyjnych,
4) Uszkodzenie fizyczne nośników danych,
5) Starzenie się nośników,
6) Wejście do systemu operacyjnego z wykorzystaniem obcego identyfikatora.

Nieuprawniony dostęp do procesu przetwarzania danych :

1) Włamanie do pomieszczeń po godzinach pracy.

2. LUDZIE

1) Kradzież dokumentów papierowych lub elektronicznych przechowywanych na stanowiskach pracy,
2) Kradzież dysku twardego komputera,
3) Zagubienie dokumentów lub utrata w czasie awarii , pożaru, zalania itp.,
4) Zagubienie dokumentów lub utrata przetwarzanych danych osobowych,
5) Stosowanie korupcji , szantażu w celu wydobycia określonych informacji od pracowników jednostki,
6) Infiltracja środowiska przez wyszukiwanie osób uważających się za pokrzywdzonych przez pracodawcę, zwalnianych lub poszukujących zatrudnienia w innej komórce,
7) Podglądanie zawartości danych znajdujących się na ekranie monitora,
8) Włamanie do systemu – podszycie się pod uprawnionego użytkownika,
9) Wyłudzenie , fałszowanie dokumentów, kart dostępu , haseł dostępu itp.,
10) Nieuprawniona świadoma modyfikacja oprogramowania zainstalowanego na komputerze przez innych użytkowników,
11) Skorzystanie z cudzego identyfikatora i hasła,
12) Błędy popełniane przez użytkowników,
13) Wejście osoby nieupoważnionej do strefy przetwarzania danych osobowych,
14) Utrata lub odczytanie informacji przez osoby nieuprawnione podczas napraw gwarancyjnych , konserwacji sprzętu ,
15) Odczytanie danych z nośników przewidzianych do naprawy,
16) Podgląd danych przetwarzanych przez poprzedniego użytkownika,
17) Zapisywanie danych na prywatne nośniki użytkownika,
18) Nieuprawnione kopiowanie danych,
19) Przeglądanie (przeszukiwanie) pamięci operacyjnej i zewnętrznej komputerów w celu uzyskania określonych informacji,
20) Pozostawienie przez pracownika dokumentów , nośników informacji na biurku po godzinach pracy,
21) Utrata kluczowych pracowników,
22) Brak możliwości rozliczania działań użytkowników – brak kontroli nad dostępem do przetwarzanych danych osobowych,
23) Dostęp do informacji przez osoby nieuprawnione podczas ponownego wykorzystania używanych nośników danych,
24) Obserwacja bezpośrednia poprze filmowanie, fotografowanie, nagrywanie .

3. APLIKACJE

-

1) Nieuprawnione instalowanie urządzeń służących do naruszenia poufności przetwarzanych informacji,
2) Nieuprawniona , świadoma modyfikacja oprogramowania zainstalowanego na komputerze przez innych użytkowników,
3) Korzystanie z nielicencjonowanego oprogramowania,
4) Przypadkowa zmiana ustawień konfiguracyjnych ,
5) Stosowanie niewłaściwego systemu plików,
6) Wykorzystanie przechowywanych dokumentów na dysku twardym,

4. POMIESZCZENIA

1) Katastrofy budowlane,
2) Ekstremalne czynniki środowiskowe (temperatura, wilgotność, zapylenie),
3) Awaria klimatyzacji ,
4) Pożar w pomieszczeniach, w których są przetwarzane dane osobowe,
5) Zalanie pomieszczeń , w których są przetwarzane dane osobowe,
6) Zamach terrorystyczny,

5. DODATKOWE INNE NIEBEZPIECZEŃSTWA

1) Celowe lub przypadkowe zniszczenie zbiorów i programów zewnętrznym impulsem elektromagnetycznym;
2) Podsłuch emisji akustycznych na zewnątrz budynku z obszaru przetwarzania danych osobowych;
3) Awaria zasilania;
4) Awaria systemu operacyjnego lub ujawnienie wady oprogramowania aplikacyjnego;
5) Zbieranie się ładunków elektrostatycznych;
6) Nierzetelna kontrola rejestrowanych zdarzeń systemowych;
7) Wykorzystanie błędów w obiegu dokumentów;
8) Ponowne wykorzystywanie nośników , które powinny być wcześniej skutecznie zniszczone ;
9) Nieprawidłowości w przypadku kserowania , powielania – brak nadzoru lub uprawnień;
10) Niepełny , niedokładny opis procedur w instrukcjach bezpiecznej eksploatacji.

6. PRZETWARZANIE ZAUTOMATYZOWANE:

W odniesieniu do zautomatyzowanego przetwarzania należy wdrożyć po ocenie ryzyka środki, które:

1) uniemożliwią osobom nieuprawnionym dostęp do sprzętu używanego do przetwarzania (kontrola dostępu do sprzętu);
2) zapobiegną nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu nośników danych (kontrola nośników danych);

-

3) zapobiegną nieuprawnionemu wprowadzaniu danych osobowych oraz nieuprawnionemu oglądaniu, zmienianiu lub usuwaniu przechowywanych danych osobowych (kontrola przechowywania);
4) zapobiegną korzystaniu z systemów zautomatyzowanego przetwarzania przez osoby nieuprawnione, używające sprzętu do przesyłu danych (kontrola użytkowników);
5) zapewniają, że osoby uprawnione do korzystania z systemu zautomatyzowanego przetwarzania będą mieć dostęp wyłącznie do danych osobowych objętych posiadanym przez siebie uprawnieniem (kontrola dostępu do danych);
6) pozwolą zweryfikować i ustalić podmioty, którym dane osobowe zostały lub mogą zostać przesłane lub udostępnione za pomocą sprzętu do przesyłu danych (kontrola przesyłu danych);
7) pozwolą następczo zweryfikować i stwierdzić, które dane osobowe zostały wprowadzone do systemów zautomatyzowanego przetwarzania, kiedy i przez kogo (kontrola wprowadzania danych);
8) zapobiegną nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu danych osobowych podczas ich przekazywania lub podczas przenoszenia nośników danych (kontrola transportu);
9) zapewniają, że w razie awarii można będzie przywrócić zainstalowane systemy (odzyskiwanie);
10) zapewniają działanie funkcji systemu, zgłaszanie występujących w nich błędów (niezawodność) oraz odporność przechowywanych danych na uszkodzenia powodowane błędnym działaniem systemu (integralność).

Załączniki

do Polityki bezpieczeństwa

Załącznik nr 1

……

/nazwa jednostki/

POLECENIE – UPOWAŻNIENIE

zgodnie z art.29* RODO oraz zakresem czynności i złożonego oświadczenia w sprawie znajomości przepisów dotyczących ochrony danych osobowych

polecam- u p o w a ż n i a m

Pana/Panią:

……

do przetwarzania danych osobowych gromadzonych w systemie informatycznym/ nie informatycznym w …… w zbiorach :
(nazwa komórki organizacyjnej)

Lp.	PEŁNA NAZWA ZBIORU

Powyższe polecenie - upoważnienie wydaje się na okres do
…… *(wpisać na jaki okres)* /stażyści , praktykanci/

na czas zatrudnienia /pracownicy jednostki/.

Administrator Danych Osobowych

…… …… ……

/miejscowość/ */data/*

*Artykuł 29

Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.

-

Załącznik nr 2

Umowa powierzenia przetwarzania danych osobowych

Zgodnie z art.28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE zostaje zawarta umowa powierzenia w dniu ..... r. pomiędzy:

……
z siedzibą w .....,
zarejestrowaną/ym w ..... pod numerem KRS .....,
numer NIP .....,.
oraz numer REGON .....,
reprezentowaną/ym przez: .....,
zwaną/ym dalej **Zleceniodawcą**, a……
z siedzibą w .....,
zarejestrowaną/ym w .....
pod numerem KRS .....,
numer NIP .....
oraz numer REGON .....,
reprezentowaną/ym przez: .....,
zwaną/ym dalej **Zleceniobiorcą**.

§ 1

Oświadczenia stron

1. Zleceniodawca powierza Zleceniobiorcy przetwarzanie danych osobowych w zakresie i celu objętym niniejszą umową.

2. Zleceniodawca oświadcza, że jest administratorem danych osobowych w rozumieniu ustawy z dnia …… o ochronie danych osobowych (Dz.U ……), (dalej zwana ustawą), które przetwarza zgodnie z obowiązującymi przepisami prawa. Zleceniodawca oświadcza ponadto, że zawiera niniejszą umowę w celu bezpośrednio związanym z jego działalnością gospodarczą lub zawodową.

3. Zleceniobiorca oświadcza, iż dysponuje odpowiednimi środkami, w tym należytymi zabezpieczeniami umożliwiającymi przetwarzanie danych osobowych zgodnie z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE ,(dalej zwane rozporządzeniem),

§ 2

Zakres i cel przetwarzania danych osobowych

1. Zleceniobiorca może przetwarzać dane osobowe przekazane przez Zleceniodawcę wyłącznie w zakresie i w celu określonych w niniejszej umowie.
2. Dane osobowe będą przetwarzane przez Zleceniobiorcę tylko i wyłącznie w celu ……*[wskazać cel przetwarzania]*.
3. Zakres przetwarzania obejmuje następujące dane osobowe …….. *[wskazać zakres przetwarzania]*
4. Poprzez przetwarzanie danych rozumie się jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

§ 3

Zobowiązania podmiotu, któremu powierzono przetwarzanie danych osobowych

1. Zleceniobiorca zobowiązuje się przed przystąpieniem do przetwarzania powierzonych przez Zleceniodawcę danych wdrożyć i utrzymywać przez czas przetwarzania wszelkie środki i zabezpieczenia związane z przetwarzaniem danych, zgodnie z wymaganiami ustawy oraz rozporządzenia.

2. Zleceniobiorca może powierzać przetwarzanie powierzonych przez Zleceniodawcę danych osobowych innym podmiotom, takim jak:
   ……..
   [wskazać określone podmioty].

3. Zleceniobiorca odpowiada za wszelkie wyrządzone osobom trzecim szkody, które powstały w związku z nienależytym przetwarzaniem przez Zleceniobiorcę powierzonych danych osobowych.

4. Zleceniobiorca nie jest odpowiedzialny za udostępnienie powierzonych danych osobowych osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem tych danych osobowych w przypadku, gdy przyczyną powyższego jest działanie bądź zaniechanie Zleceniodawcy

§ 4

Postanowienia końcowe

1. W sprawach nieuregulowanych niniejszą umową zastosowanie znajdują przepisy ustawy oraz powiązanych z nią aktów wykonawczych, a także rozporządzenia i kodeksu cywilnego.
2. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.
3. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

…….. ……..

Zleceniodawca Zleceniobiorca

-

Załącznik nr 3

REJESTR INCYDENTÓW - NARUSZEŃ

DATA NARUSZENIA:/zgłoszenia …….

GODZ.: …….

Ilość osób, których dotyczy naruszenie : …….

Zgłoszenie do UODO: ☐ tak ☐ nie

Data zgłoszenia do UODO: ……

Godz. zgłoszenia do UODO: …….

Kategorie osób , których naruszenie dotyczy: ☐ dane zwykłe,

☐ dane podlegające szczególnej ochronie:

Proponowane środki zabezpieczeń : *np. uzupełnienie – zakup sprzętu IT, szkolenie pracowników.*

Zastosowane środki zabezpieczeń : *np. uniemożliwiono dostęp osobom nieupoważnionym.*

Sposób naruszenia: *np. włamanie.*

Konsekwencje – straty: *np. ujawnione zostały dane osobowe, adres i miejsce zamieszkania* .

ZAWIADOMIENIE OSÓB , KTÓRYCH DANE DOTYCZĄ

NIE ZAWIADOMIONO , GDYŻ:

☐ ADO wdrożył odpowiednie środki techniczne i organizacyjne,

☐ ADO zastosował działania mające na celu wyeliminowanie ryzyka naruszenia praw i wolności osób,

☐ Zawiadomienie wymagałoby niewspółmiernych środków.

ZAWIADOMIONO POPRZEZ :

☐ Wysłano pismo ze szczegółowym wyjaśnieniem,

☐ Opublikowano komunikat w środkach masowego przekazu (BIP, gazeta, radio itp.).

INSPEKTOR :

IMIĘ :……..

NAZWISKO : ……..

Podpis: ……..

-

Załącznik nr 4

ZAWIADOMIENIE O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

Dane i adres odbiorcy zawiadomienia

……

……..

Data naruszenia: …….

Godz. naruszenia: ……..

KATEGORIA OSÓB , KTÓRYCH NARUSZENIE DOTYCZY:

- np. dane z ewidencji ludności i dowodów osobistych ,

RODZAJ NARUSZENIA:

- np. niekontrolowany wypływ poprzez sieć TI.

ZASTOSOWANE SRODKI ZABEZPIECZAJACE :

- np. wdrożono dodatkowe środki techniczne i organizacyjne w tym: zabezpieczenie w dodatkowe programy antywirusowe, przeszkolono osoby przetwarzające dane osobowe

KONSEKWENCJE NARUSZENIA:

- np. ujawnienie danych osobowych i adresów , miejsca zamieszkania oraz numeru nieruchomości.

CZY ZGŁOSZONO INCYDENT DO GIODO:

- np. incydent został zgłoszony do Urzędu Ochrony danych osobowych w ciągu 72 godzin od dnia stwierdzenia naruszenia ochrony danych osobowych.

INSPEKTOR :

Imię : ……..…

Nazwisko: ……..……

Nr Tel: ……

e-mail : ……

-