pieczątka

Załącznik nr 2

do Zarządzenia nr 5/2021
Przewodniczącego Zarządu Związku
Gmin Krajny
z dnia 2 listopada 2021 r.

Polityka Ochrony Danych Osobowych podczas przetwarzania dokumentacji w postaci tradycyjnej oraz elektronicznej

Administrator Danych Osobowych *Związek Gmin Krajny w Złotowie, ul. Wawrzyniaka 4a, 77-400 Złotów*

Instytucja objęta dokumentem*:*
Związek Gmin Krajny w Złotowie, ul. Wawrzyniaka 4a, 77-400 Złotów

Zgodnie z art. 32 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 RODO) oraz zgodnie z USTAWĄ z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781)Administrator Danych Osobowych wdraża dokument o nazwie: „**Polityka Ochrony Danych Osobowych podczas przetwarzania dokumentacji w postaci tradycyjnej oraz elektronicznej**".

Modele architektury bezpiecznego przetwarzania dokumentacji osobowej w postaci elektronicznej

Modele architektury przetwarzania dokumentacji osobowej w postaci elektronicznej przez usługodawców.

1. Model Klasyczny - ADO posiada pełną kontrolę nad posiadaną infrastrukturą i oprogramowaniem. Jednak w wielu wypadkach jego samowystarczalność jest ograniczona koniecznością korzystania z usług dostawców łączy internetowych.
2. Kolokacja - ADO przekazuje firmie zewnętrznej serwery lub inne urządzenia teleinformatyczne do przeznaczonych do tego celu pomieszczeń (serwerowni). Podmiot zewnętrzny odpowiada również za zapewnienie odpowiedniego łącza.
3. Hosting - ADO dzierżawi od podmiotu zewnętrznego serwer lub część jego przestrzeni dyskowej.

4. Chmura obliczeniowa typu laaS - infrastruktura informatyczna jest wynajmowana od podmiotu zewnętrznego. ADO zachowuje kontrolę nad danymi i oprogramowaniem.
5. Chmura obliczeniowa typu Paas —podmiot zewnętrzny dostarcza środowisko, w którym ADO może instalować aplikacje i zarządzać nimi.
6. Chmura obliczeniowa typu SaaS — całość infrastruktury wraz z oprogramowaniem pozostają pod kontrolą podmiotu zewnętrznego, który odpowiada za ich bezawaryjne działanie.

ADO dokonuje analizy wykorzystania danego modelu z uwzględnieniem wszystkich indywidualnych okoliczności wdrożenia.

Decydując się na wybór określonego modelu przetwarzania danych ADO określa podział odpowiedzialności pomiędzy siebie a podmiot zewnętrzny, nad wykorzystywanymi zasobami IT zakresie zapewnienia bezpieczeństwa. lm więcej obowiązków zostanie powierzonych, tym mniejszą będzie miał ADO odpowiedzialność, ale jednocześnie mniejszą kontrolę.

Zasady przetwarzania danych

Art. 5 ust. 1 RODO wskazuje na sześć zasad przetwarzania danych osobowych:

1) **Zasada zgodności z prawem, rzetelności i przejrzystości przetwarzania** - wszelkie przetwarzanie danych osobowych powinno być zgodne z prawem, rzetelne i przetwarzane w sposób zrozumiały dla osoby, której dane dotyczą. Jest to podstawowa zasada określająca relacje pomiędzy podmiotem danych i ich administratorem. Oznacza ona, że podmiot przetwarzający dane zawsze i na każdym etapie przetwarzania danych jest zobowiązany dbać o interesy osoby, której dane dotyczą. Musi spełniać co najmniej jeden z przewidzianych prawem warunków dopuszczalności przetwarzania danych (np. osoba, której dane dotyczą, wyrazi na to zgodę lub świadczeniem innych usług osobowych, zarządzania udzielaniem usług osobowych). Jednocześnie musi dołożyć staranności w zabezpieczeniu interesów osoby której przetwarzane dane dotyczą (zapewnić bezpieczeństwo danych między innymi poprzez ich pseudonimizację i szyfrowanie) oraz zagwarantować tej osobie kontrolę nad procesem przetwarzania (przekazywanie informacji do których ma prawo umożliwiających podejmowanie decyzji, między innymi: kto jest administratorem danych, w jakim celu i zakresie dane są zbierane i przetwarzane, jakie jest źródło danych, w jaki sposób są udostępniane itd.).
2) **Zasada ograniczoności celu** – dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 RODO za niezgodne z pierwotnymi celami. Oznacza to, że administrator jest związany celem ustalonym na początku procesu przetwarzania i nie może go dowolnie zmieniać. Przepisy prawa zezwalają jednak wykorzystywać dane do celów archiwalnych i w interesie publicznym, do celów badań naukowych lub historycznych oraz do celów statystycznych, jednak pod warunkiem, że działania te są zgodne z ustalonymi w tym zakresie wymaganiami.
3) **Zasada minimalizacji danych** - przetwarzane dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

Nie wolno zbierać i przetwarzać danych, które nie są niezbędne do osiągnięcia celu przetwarzania i są w stosunku do niego nadmiarowe.

4) **Zasada prawidłowości** - przetwarzane dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane. Obowiązkiem administratora jest dbałość o to, aby dane były prawidłowe i aktualizowane oraz zapewnienie, że dane które są nieprawidłowe względem celów przetwarzania zostaną niezwłocznie usunięte lub sprostowane.

5) **Zasada ograniczoności przechowywania** - dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy rozporządzenia RODO w celu ochrony praw i wolności osób, których dane dotyczą.

6) **Zasada integralności i poufności** – dotyczy stosowania odpowiednich środków technicznych i organizacyjnych, które zapewnią bezpieczeństwo przetwarzanych danych osobowych. Między innymi chodzi o ochronę przed niedozwolonym przetwarzaniem lub przetwarzaniem niezgodnym z prawem, a także zabezpieczenie danych przed ich utratą, zniszczeniem lub uszkodzeniem.

Prawa osób których dane są przetwarzane:

1) Prawo do informacji i dostępu do danych - Każda osoba fizyczna ma prawo dostępu do zebranych danych jej dotyczących oraz ma możliwość łatwego wykonywania tego prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem. Dlatego też każda osoba, której dane dotyczą, ma prawo do wiedzy i informacji, w szczególności w zakresie celów, w jakich dane osobowe są przetwarzane, w miarę możliwości okresu, przez jaki dane osobowe są przetwarzane, odbiorców danych osobowych, założeń ewentualnego zautomatyzowanego przetwarzania danych osobowych oraz, przynajmniej w przypadku profilowania, konsekwencji takiego przetwarzania.

Administrator zwraca szczególną uwagę aby system informatyczny, w którym dane bedą przetwarzane zapewniał odnotowanie:

a) daty pierwszego wprowadzenia danych do systemu;
b) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;
c) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;
d) informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych.

Odnotowanie informacji, o których mowa w pkt. a i b, musi następować automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system musi zapewniać sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa powyżej.

W zakresie realizacji prawa do informacji i dostępu do danych, jego zakresu oraz sposobu zbierania i przechowywania, osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:

a) cele przetwarzania;
b) kategorie odnośnych danych osobowych;
c) odbiorcy lub kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu — np. przepis prawa lub czas trwania kampanii marketingowej;
e) prawo do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
f) prawie wniesienia skargi do organu nadzorczego;
g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą - wszelkie dostępne informacje o ich źródle;
h) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, 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;
i) jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przekazaniem.

Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.

Prawo do uzyskania kopii, o której mowa powyżej (art. 15 ust. 3 RODO), nie może niekorzystnie wpływać na prawa i wolności innych.

2) Prawo do poprawienia danych — prawo to zwane także prawem do sprostowania polega na tym, że osoba, której dane dotyczą, ma prawo żądać od administratora niezwłocznego uzupełnienia dotyczących jej danych osobowych, które są niekompletne, uaktualnienia danych jeżeli są nieaktualne oraz sprostowania danych jeżeli są one nieprawdziwe, w tym poprzez przedstawienie dodatkowego oświadczenia.

Warunkiem skorzystania z prawa jest wykazanie przez zainteresowanego, że dane są niepełne, nieaktualne, nieprawdziwe, zostały zebrane z naruszeniem prawa, bądź są już niepotrzebne do realizacji celu, dla którego były gromadzone.

Na podstawie art. 16 RODO osoba, której dane dotyczą może żądać od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Zgodnie z art. 19 RODO administrator jest zobowiązany do informowania o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał zgodnie z art. 16, art. 17 ust. 1 lub art. 18 RODO każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

3) Prawo do żądania usunięcia danych — zwane także prawem do bycia zapomnianym.

Zgodnie z RODO osoba, której dane dotyczą, ma prawo żądać od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
c) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania w przypadku jeżeli jej dane przetwarzane są na potrzeby marketingu bezpośredniego w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim;
d) dane osobowe były przetwarzane niezgodnie z prawem;
e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;
f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego tj. w przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.

Aby wzmocnić prawo do „bycia zapomnianym" w Internecie, rozszerzono prawo do usunięcia danych poprzez zobowiązanie administratora, który upublicznił te dane osobowe, do poinformowania administratorów, którzy przetwarzają takie dane osobowe o usunięciu wszelkich łączy do tych danych, kopii tych danych osobowych lub ich replikacji. Spełniając ten obowiązek administrator podejmuje racjonalne działania z uwzględnieniem dostępnych mu technologii i środków, w tym dostępnych środków technicznych, w celu poinformowania administratorów, którzy przetwarzają dane osobowe, o żądaniu osoby, której dane dotyczą.

Przepisy art. 17 ust. l i 2 RODO nie mają zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:

a) do korzystania z prawa do wolności wypowiedzi i informacji;
b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

c) z uwagi na względy interesu publicznego;
d) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania;
e) do ustalenia, dochodzenia lub obrony roszczeń.

Administrator informuje o usunięciu danych osobowych lub ograniczeniu przetwarzania, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

4) Prawo sprzeciwu — osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych. By skorzystać z tego uprawnienia musi złożyć pisemne umotywowane żądanie zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację. W tej sytuacji administrator jest zobowiązany do zaprzestania przetwarzania, chyba że wykaże istnienie ważnych i prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych nad interesami osoby, której dotyczą. W przypadku danych przetwarzanych w celach marketingowych lub kiedy osoba, której dane dotyczą, chce je przekazać innemu administratorowi, powołanie się na szczególną sytuację nie jest konieczne i w tej sytuacji sprzeciw ma charakter bezwzględny i oznacza, że administrator nie ma prawa podważania sprzeciwu. Osoba, której dane dotyczą nie może skorzystać z prawa sprzeciwu gdy administrator przetwarza dane na podstawie przepisów prawa lub gdy jest to konieczne dla realizacji umowy, której podmiot danych jest stroną.
Zgodnie z art. 21 RODO osoba, której dane dotyczą ma prawo w dowolnym momencie wnieść sprzeciw z przyczyn związanych z jej szczególną sytuacją — wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f) RODO tj. wtedy gdy: przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, 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, w tym profilowania na podstawie tych przepisów. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych, prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń. Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane marketingiem bezpośrednim. Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów. W związku z korzystaniem z usług społeczeństwa informacyjnego i bez uszczerbku dla dyrektywy 2002/58/WE osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne.

Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, osoba, której dane dotyczą, ma prawo wnieść sprzeciw z przyczyn związanych z jej szczególną sytuacją — wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

5) **Prawa związane z podejmowaniem zautomatyzowanych decyzji** - Są to przypadki, w których decyzja opiera się wyłącznie na operacjach na danych osobowych, wykonywanych automatycznie przez system informatyczny tj. bez udziału czynnika ludzkiego. Do takiego przetwarzania zalicza się „profilowanie" które polega na dowolnym zautomatyzowanym przetwarzaniu danych osobowych pozwalającym ocenić czynniki osobowe osoby fizycznej, a w szczególności analizować lub prognozować aspekty dotyczące efektów pracy, sytuacji ekonomicznej, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą — o ile wywołuje skutki prawne względem tej osoby lub w podobny sposób znacząco na nią wpływa. Przetwarzanie takie powinno zawsze podlegać odpowiednim zabezpieczeniom, obejmującym informowanie osoby, której dane dotyczą, prawo do uzyskania interwencji człowieka, prawo do wyrażenia własnego stanowiska, prawo do uzyskania wyjaśnienia co do decyzji wynikłej z takiej oceny oraz prawo do zakwestionowania takiej decyzji. Takie przetwarzanie nie powinno dotyczyć dzieci.
   W przypadku kiedy jednak podjęto zautomatyzowane decyzje zgodnie z obowiązującymi przepisami prawa, osoba w sprawie której decyzje podjęto ma szczególne prawo pozwalające jej na kontrolowanie omawianego procesu: **prawo do uzyskania informacji o przesłankach - podjęcia rozstrzygnięcia; prawo do żądania ponownego, indywidualnego rozpatrzenia sprawy.**

6) **Prawo do przenoszenia danych** - zgodnie z art. 20 RODO - jeżeli przetwarzanie danych: odbywa się na podstawie zgody osoby, której dane dotyczą lub umowy, której stroną jest osoba, której dane dotyczą oraz przetwarzanie odbywa się w sposób zautomatyzowany, osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe. Wykonując prawo do przenoszenia danych osoba, której dane dotyczą może zażądać od administratora danych by jego dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe. Z tego prawa można skorzystać jedynie wtedy kiedy dane mają postać elektroniczną i tylko wtedy, kiedy administrator przetwarza te dane na podstawie zgody podmiotu danych lub na podstawie zawartej z tym podmiotem umowy. Wykonanie prawa do przenoszenia danych, pozostaje bez uszczerbku dla prawa do usunięcia danych. Prawo do przenoszenia danych nie powinno w szczególności skutkować usunięciem danych osoby, której dane dotyczą, a które osoba ta dostarczyła do wykonania umowy, o ile i w takim zakresie, w jakim te dane osobowe są niezbędne do wykonania tej umowy.

Monitorowanie przestrzegania zgodności przetwarzania danych

Monitorowanie przestrzegania zgodności przetwarzania danych z przepisami o ochronie danych osobowych wiąże się z przeprowadzaniem audytów ochrony danych osobowych. Przepisy RODO jedynie nakreślają ogólny zakres działań, które ADO musi podjąć, aby zapewnić bezpieczeństwo przetwarzania danych. Zgodnie z ogólną zasadą podejścia opartego na ryzyku, podmiot przetwarzający dane osobowe jest zobowiązany wdrożyć odpowiednie zabezpieczenia zarówno w warstwie systemowej, organizacyjnej i technicznej, które zapewnią należytą ochronę danych osobowych.

Ocena skutków ochrony danych osobowych - analiza oparta na ryzyku

Ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze zagrożeń, może wynikać z przetwarzania danych osobowych mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności gdy:

a) przetwarzanie może skutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia;
b) naruszeniem poufności danych osobowych chronionych tajemnicą zawodową,
c) nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną;
d) osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi;
e) 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;
f) 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;
g) 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.

Niezbędne elementy oceny skutków określa przepis art. 35 ust. 7 RODO.

Ocena skutków przetwarzania obligatoryjnie zawiera co najmniej:

a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie - prawnie uzasadnionych interesów realizowanych przez administratora;
b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać

przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

Zagrożenia i odpowiedzialność wynikająca z przetwarzania dokumentacji osobowej

Zagrożenia wystepuiące podczas przetwarzania dokumentacji osobowej

Naruszenie podstawowych atrybutów bezpieczeństwa przetwarzania informacji tj. naruszenie poufności, integralności i dostępności danych osobowych obejmuje poniższe zagrożenia:

1) Nieuprawniony dostęp przez użytkowników polegający na zaistnieniu sytuacji, w której użytkownicy korzystają z kont do których sami nie mają uprawnień, albo korzystania przez wielu użytkowników z tego samego loginu użytkownika i hasła.
2) „Pragmatyzm zwyczajowy" stanowi naruszenie zasad bezpiecznego uwierzytelniania użytkownika. Przykładem takiego zwyczaju mogą być sytuacje, w których jeden pracownik merytoryczny może zastąpić innego na stanowisku pracy i kontynuuje prace na już zalogowanym koncie poprzednika co skutkuje brakiem potrzeby przelogowania. Pierwsze logowanie użytkownika pozwala na pracę w systemie i jednocześnie bez uprzedniego wylogowania pozwala na pracę przez innych użytkowników na koncie bieżącego użytkownika. Powyższy przykład zachowania powoduje poważne naruszenia poufności i niezaprzeczalności.
3) Nieuprawniony dostęp przez użytkowników (w tym usługodawcy uprawnieni na podstawie umów - personel obsługi technicznej - administratorzy oprogramowania i sprzętu, którzy mogą mieć uzasadniony powód dostępu do systemów i danych) posiadających uprzywilejowany dostęp do systemów i urządzeń polegający na uzyskaniu nieautoryzowanego dostępu do danych. Działanie takie jest naruszeniem bezpiecznych rozwiązań wynikających z umów outsourcingowych. Nieuprawniony dostęp przez usługodawców może być także źródłem poważnych naruszeń poufności informacji w tym danych osobowych.
4) Nieuprawniony dostęp przez osoby z zewnątrz organizacji - zaistnieje w sytuacji, w której nieuprawnione osoby trzecie (hakerzy) posiadają dostęp do danych lub zasobów systemowych, albo poprzez podszywanie się jako autoryzowany użytkownik stanie się upoważnionym użytkownikiem (na przykład przez tak zwany atak wykorzystujący metody socjotechniczne).
5) Przypadek nieuprawnionego dostępu przez użytkowników z zewnątrz może świadczyć o pominięciu kontroli bezpieczeństwa w zakresie:
   a) identyfikacji użytkownika;
   b) uwierzytelniania użytkownika;
   c) identyfikacji użytkownika z uwierzytelnieniem zaufanego sprzętu;
   d) uwierzytelniania pochodzenia;
   e) kontroli dostępu i zarządzania uprawnieniami.
6) Osadzanie złośliwego kodu. Zagrożenie to obejmuje wirusy przesyłane w wiadomościach e-mail i wykorzystanie złośliwego kodu mobilnego. Zwiększenie wykorzystania technologii bezprzewodowych i komórkowych przez pracowników zwiększa potencjał tego zagrożenia. Osadzanie złośliwego kodu stanowi brak skutecznego stosowania kontroli oprogramowania antywirusowego lub kontroli zapobiegania włamaniom.

7) Przekierowanie połączenia. Zagrożenie to obejmuje możliwość, że informacje przesyłane przez sieć informatyczną mogą być dostarczone do niewłaściwego adresata. Przypadkowe przekierowanie połączenia może stanowić uchybienie w działaniu systemu lub niemożność utrzymania integralności informacji przetwarzanych w dokumentacji osobowej.
8) Awaria techniczna systemu lub infrastruktury sieciowej. Zagrożenia te obejmują awarie sprzętu, awarie sieci lub braki w bazach danych. Takie problemy zwykle stanowią o awarii jednego lub większej liczby elementów powodując jego ograniczone działanie lub niedostępność.
9) Awaria środowiska wsparcia, w tym awarie zasilania i zakłócenia wynikające z oddziaływania fizycznego lub katastrof spowodowanych przez człowieka. Te same katastrofy mogą jednak spowodować duże zniszczenia w systemach wsparcia środowisk niezbędnych do utrzymania działalności.
10) Awaria systemu lub oprogramowania sieciowego. Ataki DOS są znacznie ułatwione dzięki słabościom lub błędom systemu operacyjnego lub oprogramowaniu sieciowemu. Awaria systemu lub sieci może być spowodowana awarią oprogramowania do sprawdzania integralności i testowania systemu kontroli lub konserwacji oprogramowania.
11) Błędne operacje. Błędy operatora odpowiadają za niewielki, ale znaczący procent niezamierzonych ujawnień poufnych informacji. Błędy operatora stanowią o braku jednego lub więcej czynników takich jak: kontrola operacji, bezpieczeństwo personelu (w tym brak skutecznego szkolenia).

Odpowiedzialność

Najważniejszym i jednocześnie najbardziej dotkliwym rodzajem sankcji przewidzianych w RODO są administracyjne kary pieniężne, o których mowa w art. 83 rozporządzenia.

1) Katalog naruszeń, które będą dawały podstawę do nałożenia administracyjnej kary pieniężnej w kwocie do 10 mln euro lub - gdy kara nakładana jest na przedsiębiorstwo do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego zostały wskazane w art. 83 ust. 4 RODO. Należą do nich między innymi:
   a) niestosowanie mechanizmów uwzględniania ochrony danych w fazie projektowania (tzw. privacy by design) oraz domyślnej ochrony danych (tzw. privacy by default), o których mowa w art. 25 RODO,
   b) naruszenie zasad współpracy pomiędzy współadministratorami danych, o których mowa w art. 26 RODO,
   c) naruszenie obowiązków w zakresie powierzania do przetwarzania danych osobowych (w tym obowiązek korzystania przez administratorów danych wyłącznie z usług takich podmiotów przetwarzających, które spełniają wymagania RODO, czy też wymagania odnośnie formy i zakresu umowy, na podstawie której dochodzi do powierzenia przetwarzania danych),
   d) naruszenie obowiązku prowadzenia rejestru czynności przetwarzania danych, o którym mowa w art. 30 RODO,
   e) niestosowanie odpowiednich środków bezpieczeństwa zapewniających wymagany poziom ochrony danych osobowych (zgodnie z przeprowadzaną analizą ryzyka) art. 32 RODO,
   f) niezgłaszanie faktu naruszenia ochrony danych osobowych do organu kontrolnego oraz nieprzekazanie informacji o tym fakcie osobom, których te dane dotyczą (art. 33 i 34 RODO),

g) niestosowanie się do obowiązku przeprowadzania oceny skutków dla ochrony danych w sytuacjach gdy jest to wymagane (art. 35 RODO),
h) niewyznaczenie inspektora ochrony danych w przypadkach gdy to wyznaczenie jest obligatoryjne (art. 37 RODO) i wiele innych.

2) Katalog naruszeń, które będą dawały podstawę do nałożenia kary pieniężnej w kwocie do 20 mln euro lub — gdy kara nakładana jest na przedsiębiorstwo - do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego zostały wskazane w art. 83 ust. 5 RODO.

Należą do nich między innymi:

a) niestosowanie się do podstawowych zasad przetwarzania danych, o których mowa w art. 5, 6,7 oraz 9 RODO (chodzi między innymi o znane z polskiej ustawy o ochronie danych osobowych, aczkolwiek zmodyfikowane na gruncie RODO zasady legalności i celowości przetwarzania danych, wymagania prawne wobec zgody jako podstawy prawnej przetwarzania danych, czy też warunki przetwarzania danych sensytywnych),
b) naruszenie praw osób, których dane dotyczą, określonych w art. 12-22 RODO (m.in. wymagania wobec obowiązków informacyjnych jakie należy spełniać wobec tych osób, uprawnienia tych osób do dostępu, żądania sprostowania oraz w określonych w RODO),
c) przypadkach żądania usunięcia ich danych, czy też prawo do przenoszenia danych pomiędzy różnymi administratorami danych,
d) naruszenie wymagań prawnych związanych z transferem danych osobowych do tzw. państw trzecich, o których mowa w art. 44-49 RODO.

Zalecenia dotyczące bezpiecznego przetwarzania dokumentacji osobowej

Prowadzenie dokumentacji osobowej w podmiocie wymaga spełnienia poniższych wymagań:

1) zabezpieczenie dokumentacji przed uszkodzeniem lub utratą;
2) integralność treści dokumentacji i metadanych polegającą na zabezpieczeniu przed wprowadzaniem zmian, z wyjątkiem zmian wprowadzanych w ramach ustalonych i udokumentowanych procedur;
3) stały dostęp do dokumentacji dla osób uprawnionych oraz zabezpieczenie przed dostępem osób nieuprawnionych;
4) identyfikacja osoby dokonującej wpisu oraz osoby udzielającej świadczeń i dokumentowanie dokonywanych przez te osoby zmian w dokumentacji i metadanych;
5) przyporządkowanie cech informacyjnych dla odpowiednich rodzajów dokumentacji,
6) udostępnienie, w tym przez eksport w postaci elektronicznej dokumentacji albo części dokumentacji będącej formą dokumentacji określonej w rozporządzeniu, w formacie, w którym jest ona przetwarzana (XML albo PDF);
7) funkcjonalność wydruku dokumentacji.

Dokumentacja prowadzona w postaci elektronicznej jest właściwie zabezpieczona, jeżeli w sposób ciągły są spełnione łącznie następujące warunki:

1) jest zapewniona jej dostępność wyłącznie dla osób uprawnionych,

2) jest chroniona przed przypadkowym lub nieuprawnionym zniszczeniem,
3) wprowadzono metody i środki ochrony dokumentacji, których skuteczność w czasie ich zastosowania jest powszechnie uznawana.

Zabezpieczenie dokumentacji w postaci elektronicznej wymaga w szczególności:

1) systematycznego dokonywania analizy zagrożeń,
2) opracowania i stosowania procedur zabezpieczania dokumentacji i systemów ich przetwarzania, w tym procedur dostępu oraz przechowywania,
3) stosowania środków bezpieczeństwa adekwatnych do zagrożeń,
4) bieżącego kontrolowania funkcjonowania wszystkich organizacyjnych i technicznoinformatycznych sposobów zabezpieczania, a także okresowego dokonywania oceny skuteczności tych sposobów,
5) przygotowania i realizacji planów przechowywania dokumentacji w długim czasie, w tym jej przenoszenia na nowe informatyczne nośniki danych i do nowych formatów danych, jeżeli tego wymaga zapewnienie ciągłości dostępu do dokumentacji.

Zasady ewidencjonowania procesów przetwarzania danych osobowych

1) Kierownik komórki organizacyjnej zgłasza ADO zamiar rozpoczęcia nowego procesu przetwarzania danych osobowych.
2) Kierownik komórki organizacyjnej wraz z ADO określają wymagane parametry procesu, tj. cel, zakres danych, podstawę prawną, okres przetwarzania, odbiorców, przekazywanie do państw trzecich.
3) ADO wpisuje nowy proces w **„Rejestr Czynności Przetwarzania" – ZAŁĄCZNIK NR 1**.
4) Dla każdego nowego, planowanego procesu przeprowadzane jest szacowanie ryzyka wraz z oceną skutków, w razie potrzeb ADO określa minimalne wymagania zabezpieczeń dla ochrony danych w nowym procesie na podstawie tego szacowania. Ponadto na etapie planowania uwzględnia się realizacje wszystkich wymagań mających zastosowanie do nowego procesu, m.in. realizowanie obowiązku informacyjnego.

Zasady udostępniania danych osobowych

1) Dane osobowe w podmiocie mogą być udostępniane na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie odrębnych przepisów, na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępniania danych oraz na podstawie wniosku osoby uprawnionej, której dane dotyczą.
2) Dane osobowe w podmiocie udostępnia się na pisemny, umotywowany wniosek, chyba, że inny przepis stanowi inaczej.
3) Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać tylko zgodnie z przeznaczeniem.
4) Wniosek o udostępnienia danych przekazywany jest do Kierownika komórki organizacyjnej, w którym wnioskowane dane są przetwarzane. Kierownik komórki organizacyjnej podejmuje decyzje o udostępnieniu i odnotowuje fakt w rejestrze udostępnionych danych.

5) Kierownik komórki organizacyjnej odpowiedzialny jest za przygotowanie danych osobowych zgodnie z obowiązującą podstawą prawną do udostępnienia w zakresie wskazanym we wniosku.
6) Informacje zawierające dane osobowe są przekazywane uprawnionym podmiotom lub osobom listem poleconym za potwierdzeniem odbioru lub za pomocą elektronicznych kanałów komunikacji z wykorzystaniem środków ochorny kryptograficznej.

Zasady powierzania danych osobowych

1) Powierzenie przetwarzania danych osobowych w podmiocie odbywa się zgodnie z art. 28 ust. 3 Rozporządzenia, na podstawie umowy zawartej na piśmie pomiędzy ADO, a danym podmiotem, któremu zleca się czynności związane z przetwarzaniem danych osobowych.
2) Decyzję powierzenia danych osobowych podejmuje Kierownik komórki organizacyjnej, który będzie zlecać podmiotom zewnętrznym czynności związane z przetwarzaniem danych osobowych.
3) Kierownik komórki organizacyjnej odpowiedzialny jest za informowanie ADO o zamiarze powierzenia danych osobowych do przetwarzania.
4) Projekt umowy parafują Kierownik komórki organizacyjnej przygotowującej umowę i/lub Radca Prawny – **ZAŁĄCZNIK NR 2 „Umowa powierzenia danych osobowych".**
5) Zaparafowany projekt umowy jest przedkładany do akceptacji i podpisu ADO.
6) Umowa powierzenia jest wymagana w każdym przypadku, kiedy następuje przekazanie danych osobowych lub ich gromadzenie przez podmiot zewnętrzny.
7) W przypadkach, kiedy pracownik podmiotu zewnętrznego uzyskuje dostęp do danych osobowych, jednak przetwarzanie odbywa się w obszarze ADO wystarczające jest zastosowanie upoważnienia.
8) Zawarta umowa musi zawierać poniższe elementy:
   a) cel przetwarzania, z zastrzeżeniem zakazu wykorzystania danych w innym celu,
   b) zakres, kategorie oraz charakter powierzanych danych,
   c) odpowiedzialność stron, w tym za przestrzeganie postanowień umownych oraz przestrzeganie obowiązujących przepisów prawa — zwłaszcza w zakresie wdrożenia odpowiednich środków technicznych i organizacyjnych zabezpieczających dane osobowe,
   d) konieczność upoważniania przez podmiot, osób przetwarzających w imieniu Podmiotu oraz zobowiązanie ich do zachowania poufności,
   e) zakaz korzystania z innych podmiotów - podwykonawców - bez pisemnej zgody lub aneksu do umowy,
   f) konieczność uczestniczenia Podmiotu w wypełnianiu obowiązków ciążących na ADO, w tym realizacji praw osób, których dane dotyczą oraz przekazywania informacji o sposobach przetwarzania oraz informacji potrzebnych do szacowania ryzyka i oceny skutków naruszeń,
   g) zgłaszanie wszelkich incydentów lub podejrzeń incydentów, z zapewnieniem wszystkich niezbędnych informacji do poprawnej realizacji zgłaszania incydentów zgodnie z przepisami prawa,
   h) sposób potwierdzania przestrzegania przepisów prawa i zasad bezpieczeństwa tj. umożliwienie monitorowania, audytowania podmiotu,

i) konieczność usunięcia lub zwrócenia powierzonych danych osobowych w przypadku wygaśnięcia umowy lub jej rozwiązania.

9) Każdy podmiot przetwarzający oraz ewentualnie podwykonawcy zostają wpisani do rejestru umów powierzenia danych.

Środki organizacyjne ochrony danych osobowych

W celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych w podmiocie, Administrator Danych Osobowych wprowadza określone poniżej środki organizacyjne.

1) Przetwarzanie danych osobowych może odbywać się wyłącznie ramach wykonywania zadań służbowych. Zakres uprawnień wynika z zakresu tych zadań.
2) Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych.
3) Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie.
4) Zabrania się przetwarzania danych poza wyznaczonym obszarem.
5) Pracownik upoważniony do przetwarzania danych potwierdza pisemnie fakt zapoznania się z niniejszą dokumentacją i zrozumieniem wszystkich zasad bezpieczeństwa. Podpisany dokument wraz z upoważnieniem do przetwarzania danych jest dołączany do akt osobowych.
6) Obszar przetwarzania danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.
7) Przebywanie osób, nieuprawnionych w ww. obszarze jest dopuszczalne za zgodą Administratora Danych Osobowych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
8) Pomieszczenia stanowiące obszar przetwarzania danych powinny być zamykane na klucz.
9) Przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna, usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach.
10) Nie należy gromadzić w podręcznej dokumentacji danych osobowych. Wszystkie dane niezbędne do prawidłowej pracy powinny znajdować się w zbiorach.
11) Dokumenty zawierające dane osobowe należy niszczyć w niszczarkach.
12) Każdorazowe zbieranie danych rodzi obowiązek informacyjny. Obowiązek należy realizować umieszczając odpowiednią treść informacyjną pod formularzem z danymi.
13) Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
14) Dokumenty w wersji elektronicznej, które zapisywane są na nośniki zewnętrzne, przenoszone poza siedzibę placówki lub przesyłane pocztą elektroniczną, należy zabezpieczyć poprzez nadanie im haseł odczytu.
15) Zbiory osobowe przetwarzane elektronicznie należy zabezpieczać poprzez wykonywanie kopii bezpieczeństwa, zapisywanych na zewnętrznych nośnikach i przechowywanych pod zamknięciem.

16) Komputery, które przetwarzają zbiory osobowe, za wyjątkiem komputerów służących jedynie do edycji tekstu, należy wyposażyć w urządzenia podtrzymujące napięcie na wypadek braku zasilania.
17) Pliki edytorów tekstu lub arkuszy kalkulacyjnych należy traktować jak kopie zbiorów, z których pochodzą przetwarzane w nich dane i odpowiednio zabezpieczać stosując wytyczne zawarte w Instrukcji Zarządzania Systemem Informatycznym będącej częścią niniejszej dokumentacji.

Środki techniczne ochrony danych osobowych

Potencjalne środki ochrony technicznej danych osobowych w podmiocie:

1) Ogólna ochrona budynku - gaśnice, systemy p-poż., system alarmowy, monitoring.
2) Zabezpieczenie drzwi - drzwi tradycyjne zamykane na klucz. Dostęp do kluczy posiadają upoważnione osoby.
3) Zabezpieczenia zbiorów tradycyjnych (papierowych) - szafy tradycyjne zamykane na klucz, szafy metalowe lub sejfy (dla danych szczególnie ważnych).
4) Dane przeznaczone do zniszczenia niszczone są w niszczarkach.
5) Zabezpieczenia zbiorów elektronicznych - w systemy antywirusowe.

Postanowienia końcowe

W sprawach nieuregulowanych niniejszą Polityką Ochorny Danych Osobowych odpowiednie zastosowanie mają reguły i procedury zawarte w dokumentach powiązanych podmiotu.

Zapisy tego dokumentu wchodzą w życie z dniem 2 listopada 2021 r.

Sporządził: *Marcin Misztal – Inspektor Ochrony Danych Osobowych.*

Administrator Danych Osobowych: *Związek Gmin Krajny w Złotowie, ul. Wawrzyniaka 4a, 77-400 Złotów*

……..

Data, podpis i pieczątka