ZARZĄDZENIE NR 41/19
BURMISTRZA MIASTA I GMINY DOLSK

z dnia 29 marca 2019 r.

w sprawie wprowadzenia dokumentacji ochrony danych osobowych u Administratora

Na podstawie art. 24 ust. 1 i ust. 2 oraz art. 32 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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), Burmistrz Miasta i Gminy Dolsk zarządza, co następuje:

§ 1. Wprowadza się do stosowania u Administratora nową dokumentację ochrony danych osobowych obejmującą w szczególności Politykę Ochronę Danych Osobowych wraz z załącznikami, a także dokumenty, w tym procedury wskazane w treści Polityki Ochrony Danych Osobowych, wydane na podstawie Polityki Ochrony Danych Osobowych lub wydane w związku z jej treścią.

§ 2. Nowe dokumenty dotyczące ochrony danych osobowych u Administratora, jak również nowe wersje dotychczasowych dokumentów, wydane przez Administratora, stają się automatycznie wiążące z chwilą ich wydania.

§ 3. Wprowadzana dokumentacja ochrony danych jest zgodna ze stanem faktycznym i prawnym panującym u Administratora, w szczególności co do wdrożonych środków organizacyjnych i technicznych ochrony danych osobowych oraz została sporządzona zgodnie z jego najlepszą wiedzą, w oparciu o informacje przekazane przez personel zatrudniony lub współpracujący z Administratorem.

§ 4. Zobowiązuje się wszystkie osoby przetwarzające dane osobowe z upoważnienia Administratora oraz podmioty, którym Administrator powierzył przetwarzanie danych osobowych, do bezwzględnego przestrzegania zasad, praw i obowiązków wynikających z dokumentów, o których mowa w niniejszym Zarządzeniu, jak również wytycznych i poleceń dotyczących ochrony danych osobowych wydawanych przez Administratora, a także przez inspektora ochrony danych i administratora systemów informatycznych.

§ 5. Polityka Ochrony Danych Osobowych stanowi załącznik do niniejszego Zarządzenia.

§ 6. Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Miasta i Gminy
Dolsk

Barbara Wierzbińska

POLITYKA OCHRONY DANYCH OSOBOWYCH U ADMINISTRATORA

GMINA DOLSK

SPIS TREŚCI

1. WPROWADZENIE

Celem niniejszej Polityki Ochrony Danych Osobowych (zwanej dalej: **Polityka**) jest opisanie zasad ochrony danych osobowych oraz dostarczenie podstawowej wiedzy z tego zakresu, w celu spełnienia wymagań 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 (zwanego dalej: **RODO** lub **ogólne rozporządzenie o ochronie danych osobowych**).

W celu zwiększenia świadomości obowiązków i odpowiedzialności osób przetwarzających dane osobowe, a tym samym skuteczności ochrony przetwarzanych zasobów, w niniejszym dokumencie opisano podstawy prawne przetwarzania danych osobowych.

Uzupełnieniem oraz rozwinięciem Polityki są procedury, wytyczne i polityki dotyczące zasad przetwarzania i ochrony danych osobowych przyjęte i wdrożone przez Administratora. Polityka obowiązuje z dniem wydania zarządzenia o jej wdrożeniu. Stanowi ona jeden ze środków organizacyjnych mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z RODO.

2. PODSTAWOWE ZAGADNIENIA OCHRONY DANYCH OSOBOWYCH

2.1. DEFINICJE

W Polityce przyjmuje się następujące definicje stosowanych pojęć zgodnie z RODO:

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

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

2.1.3. **ograniczenie przetwarzania** to oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

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

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

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

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

2.1.8. **podmiot przetwarzający** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;

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

2.1.10. **strona trzecia** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, Administrator, podmiot przetwarzający czy osoby, które – z upoważnienia Administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;

2.1.11. **zgoda** osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne wyrażenie woli tej osoby potwierdzające, że zezwala ona na przetwarzanie danych osobowych;

2.1.12. **naruszenie ochrony danych osobowych** oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

2.1.13. **dane genetyczne** oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;

2.1.14. **dane biometryczne** oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;

2.1.15. **dane dotyczące zdrowia** oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;

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

2.1.17. **organ nadzorczy** oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51 RODO, w Polsce organem nadzorczym jest Prezes Urzędu Ochrony Danych Osobowych;

2.1.18. **organizacja międzynarodowa** oznacza organizację i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy.

2.2. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

Administrator przetwarza dane osobowe zgodnie z następującymi zasadami:

2.2.1. legalności;

Zasada legalności oznacza przetwarzanie danych zgodnie z prawem. Realizując tę zasadę, dane osobowe przetwarzane są na podstawie co najmniej jednej z przesłanek przetwarzania danych osobowych.

2.2.2. rzetelności;

Zasada rzetelności wymaga, by dane były przetwarzane z uwzględnieniem interesów i uzasadnionych oczekiwań osób, których dane dotyczą.

2.2.3. przejrzystości;

Zasada przejrzystości wymaga by osoba, której dane dotyczą została należycie poinformowana o istotnych dla niej aspektach tego przetwarzania, tj. w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.

2.2.4. ograniczenia celu;

Zasada ograniczenia celu polega na przetwarzaniu danych osobowych jedynie w celu zgodnym z odpowiednią przesłanką dopuszczalności przetwarzania danych osobowych.

2.2.5. minimalizacji danych;

Zasada minimalizacji danych oznacza, że Administrator przetwarza tylko te dane osobowe, które są niezbędne do osiągnięcia celu przetwarzania.

2.2.6. prawidłowości danych;

Zasada prawidłowości danych oznacza, że Administrator przetwarza dane osobowe prawidłowe i uaktualnia je w razie potrzeby.

2.2.7. ograniczenia przechowywania;

Zasada ograniczenia przechowywania oznacza, że Administrator przechowuje dane osobowe w dokumentacji tworzącej akta spraw przez okres wynikający z przepisów prawa.

2.2.8. integralności i poufności;

Zasada integralności i poufności jest realizowana przez dopuszczenie do przetwarzania danych osobowych jedynie osób upoważnionych oraz zastosowanie takich środków technicznych i organizacyjnych, by dane nie były zmieniane przez osoby nieupoważnione lub by dane nie były udostępniane osobom nieupoważnionym.

2.2.9. ochrony danych osobowych w fazie projektowania;

Zasada ochrony danych osobowych w fazie projektowania oznacza, że ochrona prywatności jest realizowana na etapie projektowanych działań skutkujących przetwarzaniem danych osobowych.

2.2.10. domyślnej ochrony danych osobowych.

Zasada domyślnej ochrony danych osobowych oznacza, że domyślne ustawienia przetwarzania danych osobowych umożliwią przetwarzanie jedynie danych niezbędnych do osiągnięcia każdego konkretnego celu przetwarzania. Jednocześnie ustawienia systemów przetwarzania danych nie powinny umożliwiać udostępnienia danych nieokreślonej liczbie osób fizycznych bez interwencji osoby, której dane dotyczą.

2.3. PODSTAWY PRAWNE PRZETWARZANIA DANYCH OSOBOWYCH

2.3.1. Przetwarzanie danych osobowych zwykłych

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

2.3.1.1. osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów (art. 6 ust. 1 lit. a RODO);

2.3.1.2. 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 (art. 6 ust. 1 lit. b RODO);

2.3.1.3. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze (art. 6 ust. 1 lit. c RODO);

2.3.1.4. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej (art. 6 ust. 1 lit. d RODO);

2.3.1.5. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi (art. 6 ust. 1 lit. e RODO);

2.3.1.6. 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 (art. 6 ust. 1 lit. f RODO).

Przesłanka ta nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

2.3.2. 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. Zakaz ten nie ma zastosowania, jeżeli spełniony jest co najmniej jeden z poniższych warunków:

2.3.2.1. osoba, której dane dotyczą, udzieliła wyraźnej zgody na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą nie może uchylić zakazu (art. 9 ust. 2 lit. a RODO);

2.3.2.2. przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą (art. 9 ust. 2 lit. b RODO);

2.3.2.3. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody (art. 9 ust. 2 lit. c RODO);

2.3.2.4. przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą (art. 9 ust. 2 lit. d RODO);

2.3.2.5. przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą (art. 9 ust. 2 lit. e RODO);

2.3.2.6. przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy (art. 9 ust. 2 lit. f RODO);

2.3.2.7. przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą (art. 9 ust. 2 lit. g RODO);

2.3.2.8. przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia (art. 9 ust. 2 lit. h RODO);

2.3.2.9. przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową (art. 9 ust. 2 lit. i RODO);

2.3.2.10. przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą. (art. 9 ust. 2 lit. j RODO).

3. PROCEDURA ANALIZY RYZYKA/OCENA SKUTKÓW

3.1. ANALIZA RYZYKA

Celem analizy ryzyka jest zastosowanie środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku wynikającemu z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

3.2. OCENA SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH

Jeżeli dany rodzaj przetwarzania, który zamierza zacząć stosować Administrator, w szczególności z użyciem nowych technologii, ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.

3.2.1. Konsultacje z Inspektorem Ochrony Danych

Przy ocenie skutków Administrator zasięga opinii Inspektora Ochrony Danych.

Administrator konsultuje z Inspektorem Ochrony Danych następujące kwestie:

3.2.1.1. potrzebę przeprowadzenia oceny skutków dla ochrony danych, metodologii przeprowadzenia oceny skutków dla ochrony danych;

3.2.1.2. zasadność przeprowadzenia wewnętrznej oceny lub zlecenia jej podmiotowi zewnętrznemu;

3.2.1.3. skuteczność zabezpieczeń (w tym środków technicznych i organizacyjnych) stosowanych do łagodzenia wszelkich zagrożeń praw i interesów osób, których dane dotyczą;

3.2.1.4. prawidłowość przeprowadzonej oceny skutków dla ochrony danych i zgodności jej wyników z RODO (czy należy kontynuować przetwarzanie, czy też nie, oraz jakie zabezpieczenia należy zastosować).

3.2.2. Elementy oceny skutków dla ochrony danych

Ocena skutków dla ochrony danych zawiera co najmniej:

3.2.2.1. systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez Administratora;

3.2.2.2. ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;

3.2.2.3. ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1; oraz

3.2.2.4. środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

W przypadku, gdy Administrator nie zgadza się z zaleceniami Inspektora Ochrony Danych, dokumentacja oceny skutków dla ochrony danych osobowych powinna zawierać pisemne uzasadnienie nieuwzględnienia zaleceń.

Jeżeli ocena wykaże, że przetwarzanie może powodować wysokie ryzyko przy braku zastosowania przez Administratora środków dla zminimalizowania tego ryzyka, to zgodnie z art. 36 RODO Administrator konsultuje się w tej sprawie z organem nadzorczym.

4. PRAWA OSOBY, KTÓREJ DANE DOTYCZĄ

4.1. OBOWIĄZEK INFORMACYJNY

Osoba, której dane dotyczą, jest informowana o prowadzeniu operacji przetwarzania i o jego celach. Ponadto Administrator podaje wszelkie inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania, uwzględniając konkretne okoliczności i kontekst przetwarzania danych osobowych.

Dodatkowo Administrator informuje o fakcie profilowania oraz o konsekwencjach. W przypadku zbierania danych od osoby, której dane dotyczą, wskazuje, czy ma ona obowiązek je podać, oraz o konsekwencjach ich niepodania.

Administrator, w przypadku, gdy zbiera dane osobowe, od osoby której dane dotyczą zgodnie z art. 13 ust. 1 i 2 RODO informuje o:

4.1.1. swojej tożsamości i danych kontaktowych oraz tożsamości i danych kontaktowych swojego przedstawiciela, jeżeli istnieje;
4.1.2. danych kontaktowych Inspektora Ochrony Danych;
4.1.3. celach przetwarzania, do których mają posłużyć dane osobowe;
4.1.4. podstawie prawnej przetwarzania;
4.1.5. prawnie uzasadnionym interesie realizowanym przez Administratora lub przez stronę trzecią – jeżeli przetwarzanie odbywa się na podstawie prawnie usprawiedliwionego interesu Administratora (art. 6 ust. 1 lit. f RODO);
4.1.6. odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
4.1.7. transferze danych do państwa trzeciego, w tym o:
4.1.7.1. zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
4.1.7.2. stwierdzeniu lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony;
4.1.7.3. odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych w przypadku przekazania danych do państwa trzeciego, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO;
4.1.8. okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
4.1.9. prawie do:
4.1.9.1. 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;
4.1.9.2. 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 (art. 6 ust. 1 lit. a) RODO) lub szczególnej kategorii (art. 9 ust. 2 lit. a RODO);
4.1.9.3. wniesienia skargi do organu nadzorczego;

4.1.9.4. 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;

4.1.9.5. informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotnych informacji o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

4.2. PRAWO DOSTĘPU DO DANYCH

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:

4.2.1. cele przetwarzania;

4.2.2. kategorie odnośnych danych osobowych;

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

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

4.2.5. prawo do żądania od Administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;

4.2.6. prawo wniesienia skargi do organu nadzorczego;

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

4.2.8. informacje o zautomatyzowane podejmowanie decyzji, w tym profilowanie, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także znaczenie i przewidywane konsekwencje takiego przetwarzania dla osoby, której dane dotyczą.

4.3. PRAWO DO SPROSTOWANIA DANYCH

Osoba, której dane dotyczą, ma prawo żądania od Administratora niezwłocznego sprostowania jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

4.4. PRAWO DO USUNIĘCIA DANYCH („PRAWO DO BYCIA ZAPOMNIANYM")

Osoba, której dane dotyczą, ma prawo żądania od Administratora niezwłocznego usunięcia dotyczących jej danych osobowych, o ile zachodzi jedna z przesłanek wskazana w art. 17 RODO.

4.5. PRAWO DO OGRANICZANIA PRZETWARZANIA

Osoba, której dane dotyczą, ma prawo żądania od Administratora ograniczenia przetwarzania w następujących przypadkach:

4.5.1. osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający Administratorowi sprawdzić prawidłowość tych danych;

4.5.2. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;

4.5.3. Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;

4.5.4. osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

4.6. POWIADOMIENIE O SPROSTOWANIU LUB USUNIĘCIU DANYCH

Administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał zgodnie z art. 16, art. 17 ust. 1 i 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.

4.7. PRZENOSZENIE DANYCH

Prawo to zapewnia osobom, których dane dotyczą, możliwość otrzymywania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, danych osobowych, które dostarczyły Administratorowi, oraz możliwość przesłania tych danych osobowych innemu Administratorowi bez przeszkód.

Zgodnie z treścią art. 20 ust. 1 lit. a) RODO, prawo do przenoszenia danych znajduje zastosowanie wobec operacji przetwarzania danych na podstawie:

4.7.1. zgody osoby, której dane dotyczą;

4.7.2. umowy, której stroną jest osoba, której dane dotyczą.

Wykonując prawo do przenoszenia danych, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez Administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

Prawo do przenoszenia danych nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi.

Realizacja prawa do przenoszenia danych nie może niekorzystnie wpływać na prawa i wolności innych.

5. MONITOROWANIE I PRZEGLĄD ZASAD OCHRONY DANYCH U ADMINISTRATORA

5.1. DZIAŁANIA PODEJMOWANE PRZEZ ADMINISTRATORA

Stosowane przez Administratora zasady ochrony danych osobowych, w tym przyjęte przez Administratora polityki, procedury i wytyczne, są monitorowane przez Administratora pod kątem ich

prawidłowości, aktualności i zgodności z zaleceniami i wskazówkami organu nadzorczego i Europejskiej Rady Ochrony Danych, w szczególności poprzez podejmowanie następujących działań:

5.1.1. audyty wewnętrzne weryfikujące stosowanie przyjętych przez Administratora polityk, procedur i wytycznych;
5.1.2. wykonywanie okresowych przeglądów stosowanej dokumentacji;
5.1.3. dokonywanie analizy ryzyka;
5.1.4. sprawowanie bieżącej kontroli prawidłowości przetwarzania danych osobowych.

5.2. AUDYTY

Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Przy przeprowadzaniu audytów wewnętrznych Administrator może korzystać z pomocy Inspektora Ochrony Danych.

Audyty przeprowadzane są cykliczne, nie rzadziej niż 1 raz w roku.

Celem audytów wewnętrznych jest ocena, czy dane osobowe są należycie chronione, a wdrożone przez Administratora polityki, procedury i wytyczne zostały skutecznie wdrożone i funkcjonują zgodnie z wymaganiami RODO. Audyty prowadzone są w sposób obiektywny i bezstronny.

Szczegółowy zakres każdego audytu ustalany jest z uwzględnieniem ważności procesów przetwarzania oraz audytowanych obszarów, jak też wyników wcześniejszych audytów.

6. SZKOLENIA OSÓB PRZETWARZAJĄCYCH DANE OSOBOWE

Administrator zapewnia, aby każda osoba upoważniona przez niego do przetwarzania danych osobowych została odpowiednio przeszkolona i zapoznana z przepisami z zakresu ochrony danych osobowych.

Administrator zapewnia co najmniej następujące rodzaje szkoleń:

6.1. szkolenia wstępne – których odbycie potwierdzane jest dokumentem (np. certyfikatem, podpisem na liście obecności na szkoleniu, zdanym testem wiedzy);
6.2. szkolenia okresowe – przeprowadzane nie rzadziej niż 1 raz na rok.

7. ODPOWIEDZIALNOŚĆ ZA ZGODNOŚĆ Z PRAWEM PRZETWARZANIA DANYCH OSOBOWYCH

Na potrzeby Polityki przedstawiono poniższy schemat ról, w którym zdefiniowano role mające szczególne obowiązki w obszarze ochrony danych osobowych.

7.1. ADMINISTRATOR

Administrator wykonuje wszelkie obowiązki określone w przepisach prawa, w tym w szczególności:

7.1.1. wprowadza, zarządza i sprawuje nadzór nad stosowaniem Polityki, a także szczegółowych procedur, wytycznych i polityk;
7.1.2. określa rodzaje zasobów podlegających ochronie;
7.1.3. decyduje o celach i środkach przetwarzania danych;

7.1.4. prowadzi komunikację z osobami, których dane dotyczą i przekazuje im informacje w sposób zwięzły, przejrzysty, zrozumiały i łatwo dostępny;
7.1.5. ułatwia osobom, których dane dotyczą wykonywanie ich praw;
7.1.6. nieodpłatnie udziela osobom, których dane dotyczą informacji, również na ich żądanie;
7.1.7. weryfikuje tożsamość osób wnoszących żądania udzielenia informacji;
7.1.8. informuje osobę, której dane dotyczą, o działaniach jakie podjął, w związku z jej żądaniami opartymi o art. 15-22 RODO;
7.1.9. realizuje żądania osoby, której dane dotyczą, jeśli istnieją przesłanki do ich realizacji;
7.1.10. uzasadnia odrzucenie żądania osoby, której dane dotyczą i poucza ją o prawie skargi.

7.2. INSPEKTOR OCHRONY DANYCH

Zakres zadań Inspektora Ochrony Danych zawiera art. 39 ust. 1 RODO. Wyliczenie zawarte w tym przepisie nie jest jednak katalogiem zamkniętym, ponieważ jeden z obowiązków Inspektora Ochrony Danych można wywodzić też z art. 38 ust. 4 RODO (pełnienie roli punktu kontaktowego, dla osób, których dane dotyczą).

Wobec powyższego zadania Inspektora Ochrony Danych obejmują:

7.2.1. informowanie Administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
7.2.2. monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk Administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków;
7.2.3. działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
7.2.4. udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
7.2.5. współpraca z organem nadzorczym;
7.2.6. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;
7.2.7. 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 RODO;
7.2.8. pomoc Administratorowi w prowadzeniu rejestru czynności lub rejestru kategorii czynności.

7.3. ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

Administrator Systemów Informatycznych realizuje zadania, które zostały mu powierzone przez Administratora, w szczególności w procedurach, politykach i wytycznych. W przypadku, gdy Administrator nie wyznaczył Administratora Systemów Informatycznych, zadania te są realizowane przez osobę wyznaczoną przez Administratora, a gdy brak takiej osoby – przez Administratora.

Niezależnie od zadań wskazanych powyżej, zadaniem Administratora Systemów Informatycznych jest śledzenie osiągnięć w dziedzinie zabezpieczania systemów informatycznych i wdrażanie takich

narzędzi, metod pracy oraz sposobów zarządzania systemem informatycznym, które zwiększą bezpieczeństwo ochrony danych u Administratora.

Działania szczegółowe, jakie Administrator Systemów Informatycznych powinien podejmować uzależnione powinny być w szczególności od:

7.3.1. architektury systemu informatycznego, w którym dane są przetwarzane;
7.3.2. zastosowanych narzędzi w ramach oprogramowania systemowego;
7.3.3. użytych narzędzi do zarządzania bazą danych oraz przyjętych rozwiązań w stosowanych aplikacjach użytkowych.

7.4. PODMIOT PRZETWARZAJĄCY

Administrator korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

W celu zapewnienia ochrony danych w przypadku powierzenia przetwarzania danych, Administrator dochowuje należytej staranności przy wyborze podmiotu przetwarzającego. Administrator podpisuje z podmiotami przetwarzającymi umowy spełniające wszystkie wymogi wynikające z RODO, a także w możliwie najszerszy sposób gwarantujące ochronę praw osób, których dane dotyczą.

8. POSTANOWIENIA KOŃCOWE

Polityka jest dokumentem wewnętrznym.

Każda osoba przetwarzająca dane osobowe zapoznaje się z treścią Polityki oraz zobowiązuje się do bezwzględnego stosowania postanowień w niej zawartych.