Informacja o zmianach w związku z wejściem w życie od 25 maja 2018

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)

Szanowni Państwo

W związku z wejściem w życie w dniu 25 maja br., ww. rozporządzenia, które na celu chronić podstawowe prawa osób fizycznych, w szczególności ich prawo do ochrony danych osobowych. Natomiast nie może ograniczać się ani, zakazywać swobodnego przepływu danych osobowych w Unii z powodów odnoszących się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

Każdy podmiot, będący Administratorem danych osobowych osób fizycznych, musi dokonać oceny skutków ochrony danych zgodnie z art. 35 rozporządzenia. Oceny można dokonać zgodnie z wytycznymi Grupy Roboczej art. 29.

Definicja osoby administratora zgodnie z rozporządzeniem

„**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."

Przesłanki legalizacyjne przetwarzania danych:

„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. Akapit pierwszy lit. f) nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.
2.**Państwa członkowskie mogą zachować lub wprowadzić bardziej szczegółowe przepisy**, aby dostosować stosowanie przepisów niniejszego rozporządzenia w odniesieniu do przetwarzania służącego wypełnieniu warunków określonych w ust. 1 lit. c) i e); w tym celu mogą dokładniej określić szczegółowe wymogi przetwarzania i inne środki w celu zapewnienia zgodności przetwarzania z prawem i jego rzetelności, także w innych szczególnych sytuacjach związanych z przetwarzaniem przewidzianych w rozdziale IX.
3.**Podstawa przetwarzania, o którym mowa w ust. 1 lit. c) i e), musi być określona**: a) w prawie Unii; lub b) w prawie państwa członkowskiego, któremu podlega administrator. Cel przetwarzania musi być określony w tej podstawie prawnej lub, w przypadku przetwarzania, o którym mowa w ust. 1 lit. e) – musi być ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Podstawa prawna może zawierać przepisy szczegółowe dostosowujące stosowanie przepisów niniejszego rozporządzenia, w tym: ogólne warunki zgodności z prawem przetwarzania przez administratora; rodzaj danych podlegających przetwarzaniu; osoby, których dane dotyczą; podmioty, którym można ujawnić dane osobowe; cele, w których można je ujawnić; ograniczenia celu; okresy przechowywania; oraz operacje i procedury przetwarzania, w tym środki zapewniające zgodność z prawem i rzetelność przetwarzania, 4.5.2016 L 119/36 Dziennik Urzędowy Unii Europejskiej PL w tym w innych szczególnych sytuacjach związanych z przetwarzaniem, o których mowa w rozdziale IX. Prawo Unii lub prawo państwa członkowskiego muszą służyć realizacji celu leżącego w interesie publicznym, oraz być proporcjonalne do wyznaczonego, prawnie uzasadnionego celu.
4.**Jeżeli przetwarzanie w celu innym niż cel, w którym dane osobowe zostały zebrane**, nie odbywa się na podstawie zgody osoby, której dane dotyczą, ani prawa Unii lub prawa państwa członkowskiego stanowiących w demokratycznym społeczeństwie niezbędny i proporcjonalny środek służący zagwarantowaniu celów, o których mowa w art. 23 ust. 1, administrator – aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane – bierze pod uwagę między innymi: a) wszelkie związki między celami, w których zebrano dane osobowe, a celami zamierzonego dalszego przetwarzania; b)kontekst, w którym zebrano dane osobowe, w szczególności relację między osobami, których dane dotyczą, a administratorem; c) charakter danych osobowych, w szczególności czy przetwarzane są szczególne kategorie danych osobowych zgodnie z art. 9 lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa zgodnie z art. 10; d) ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą; e) istnienie odpowiednich zabezpieczeń, w tym ewentualnie szyfrowania lub pseudonimizacji.”

Zgoda na przetwarzanie danych

Zgodę stosujmy, kiedy nie ma możliwości zastosowania innej przesłanki legalizacyjnej – tzn., kiedy nie spełniamy żadnego innego warunku spośród warunków wskazanych w art. 6 ust. 1 RODO.

Zgoda powinna zawierać następujące informacje:

Wytyczne Grupy Roboczej art. 29, wskazują, że zgoda powinna zawierać co najmniej:

1. Tożsamość administratora – dane podmiotu, który decyduje o celach i zasadach przetwarzania danych. W kontekście NGO będą to dane podmiotu, np. stowarzyszenia lub fundacji, a nie dane zarządu, ponieważ ten działa w imieniu osoby prawnej;

2. Cel każdej operacji przetwarzania, dla której prosi się o zgodę – tu wskazujemy po co nam dane określonej osoby: np. dla celów statystycznych, marketingu swoich usług lub wysyłania informacji o zbieraniu 1%;

3. Jakie dane będą zbierane i wykorzystywane – wskazujemy te, które osoba dostarcza bezpośrednio (np. wpisując do formularza swoje imię i nazwisko) oraz pozyskiwane pośrednio (np. adres IP);

4. Informacje o prawie do wycofania zgody *(o wycofaniu / odwołaniu zgody piszemy poniżej);*

5. Informacje na temat wykorzystywania danych do decyzji opartych jedynie na zautomatyzowanym przetwarzaniu, w tym profilowania – jeżeli przetwarzamy dane w ten sposób to należy poinformować o tym osobę, która nam dane przekazuje;

6. Jeżeli zgoda dotyczy przekazywania - informacje na temat możliwych zagrożeń związanych z przekazywaniem danych do krajów trzecich. Tę informację należy przekazać tylko w wypadku, gdy brak jest decyzji Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony w kraju, do którego dane są przekazywane.

Jeśli, już wcześniej uzyskano zgodę na podstawie Dyrektywy 95/46/WE
Stanowisko GIODO dotyczące ważności zgód na przetwarzanie danych osobowych
https://giodo.gov.pl/pl/1520281/10303

„Zgoda, która dotychczas została pozyskana, jest nadal ważna, o ile jest ona zgodna z warunkami określonymi w rozporządzeniu. Takie stanowisko wynika bezpośrednio z treści motywu 171 ogólnego rozporządzenia o ochronie danych (RODO): „*jeżeli przetwarzanie ma za podstawę zgodę w myśl dyrektywy 95/46/WE, osoba, której dane dotyczą, nie musi ponownie wyrażać zgody, jeżeli pierwotny sposób jej wyrażenia odpowiada warunkom niniejszego rozporządzenia; dzięki temu administrator może kontynuować przetwarzanie po dacie rozpoczęcia stosowania niniejszego rozporządzenia”.* RODO nie przewiduje przepisów przejściowych w stosunku do dyrektywy 95/46/WE. Ważność zachowuje zatem zgoda, która została pierwotnie zebrana w sposób gwarantujący osobie, której dane dotyczą, złożenie oświadczenia spełniającego następujące kryteria:

- **dobrowolność** – zgoda oznaczać musi możliwość realnego, swobodnego wyboru, nie może być wymuszona; brak wyrażenia zgody nie może również powodować negatywnych konsekwencji dla osoby, której dane dotyczą; motyw 43 RODO zwraca szczególną uwagę w tym kontekście na sytuację, w której istnieje wyraźny brak równowagi pomiędzy administratorem a osobą, której dane dotyczą, np. w relacji pracodawca-pracownik;
- **konkretność** – zgoda musi określać precyzyjnie cel przetwarzania danych oraz wskazywać zakres danych; niedopuszczalne jest zbieranie zgód blankietowych, ogólnych; należy również

wyraźnie oddzielić informacje związane z uzyskaniem zgody od informacji dotyczących innych kwestii;
- świadomość – przed uzyskaniem zgody należy zapewnić niezbędne informacje osobom, których dane dotyczą, aby umożliwić im podejmowanie świadomych decyzji i zrozumienie, na co wyrażają zgodę; prosząc o zgodę, administratorzy powinni upewnić się, że używają jasnego i prostego języka;
- **jednoznaczność** – ważna zgoda wymaga jednoznacznego okazania w formie oświadczenia lub wyraźnego działania potwierdzającego, co oznacza, że osoba, której dane dotyczą, musi podjąć celowe działanie w celu wyrażenia zgody na określone przetwarzanie."

Przedmiot ochrony praw osób fizycznych

Stanowią również wytyczne do przystosowania systemów IT administratora danych w, celu zapewnienia przestrzegania praw, zgodnie z rozporządzeniem**:**

1) Artykuł 15 - prawo dostępu przysługujące osobie, której dane dotyczą;

2) *Artykuł 16* - prawo do sprostowania danych;

3) *Artykuł 17* - prawo do usunięcia danych („prawo do bycia zapomnianym") ;

4) *Artykuł 18* - prawo do ograniczenia przetwarzania;

5) *Artykuł 19* - obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania;

6) *Artykuł 20* - prawo do przenoszenia danych;

7) *Artykuł 21* - prawo do sprzeciwu.

Wymogi techniczne

„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.Wywiązywanie się z obowiązków, o których mowa w ust. 1 i 2 niniejszego artykułu, można wykazać między innymi poprzez wprowadzenie zatwierdzonego mechanizmu certyfikacji określonego w art. 42".

Definicja naruszenia zgodnie z rozporządzeniem:

„**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.

Obowiązek zgłaszania naruszeń

W ciągu **72 godzin od wykrycia** naruszenia mogącego skutkować zagrożeniem praw i swobód osób, których dane zostały naruszone, trzeba zgłosić się do właściwego organu nadzoru (przypuszczalnie będzie to Urząd Ochrony Danych Osobowych).

Kary finansowe za naruszenie przepisów

1) 10 milionów euro lub do 2% wartości rocznego światowego obrotu przedsiębiorstwa,

2) 20 milionów euro lub do 4% wartości rocznego światowego obrotu przedsiębiorstwa,

3) 100 tysięcy złotych kary administracyjnej, za naruszenia spowodowane przez administrację publiczną (według projektu z dnia 13.09.2017 roku ustawy o ochronie danych osobowych).

Podstawa prawna:

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)

Dane zostały pozyskane z bazy danych GIODO:

https://giodo.gov.pl