Dnia 25 maja 2018 roku we wszystkich krajach należących do Unii Europejskiej zacznie być stosowane Ogólne Rozporządzenie o Ochronie Danych Osobowych 2016/679 (RODO).

Photo by Matthew Henry on Unsplash

RODO

INFORMATOR

RODO obejmuje swoim zastosowaniem wszystkie podmioty prywatne i publiczne, które przetwarzają dane osobowe i w praktyce większość procesów przetwarzania danych. Regulacje RODO pomagają również osobom przebywającym na terytorium Polski egzekwować ich prawo do ochrony danych osobowych. Zgodnie z nowymi przepisami, dane osobowe to takie dane, które pozwalają zidentyfikować osobę fizyczną. Mogą to być informacje takie jak: imię, nazwisko, numer PESEL, płeć, adres e-mail, ale również mniej oczywiste jak numer IP, dane o lokalizacji, kod genetyczny, poglądy polityczne czy historia zakupów. Wszelkie informacje zbierane na temat osoby, które pozwalają na ustalenie jej tożsamości, są danymi osobowymi, niezależnie od tego, czy są przetwarzane w formie papierowej czy cyfrowej.

Informator zawiera odpowiedzi na najczęściej zadawane pytania dotyczące wdrażania przepisów RODO w sektorze prywatnym i publicznym. Na końcu opisów poszczególnych zagadnień znajdą Państwo odniesienia do numerów artykułów i motywów preambuły RODO, które pozwolą na pogłębienie wiedzy w danym obszarze. Informator przybliża następujące kwestie:

1. Rejestr czynności przetwarzania danych osobowych.
2. Prawo do bycia zapomnianym.
3. Prawo do przenoszalności danych.
4. Uzyskiwanie zgody dziecka.
5. Obowiązek aktualizowania uzyskanej już raz zgody na przetwarzanie danych po wejściu w życie RODO.
6. Różnice między anonimizacją oraz pseudonimizacją.
7. Obowiązek zgłaszania naruszeń przepisów RODO.

REJESTR CZYNNOŚCI PRZETWARZANIA
DANYCH OSOBOWYCH

Rejestr czynności zastąpi obowiązek zgłaszania zbiorów danych do organu nadzorczego (obecnie GIODO). Rejestr będzie sporządzany wewnątrz przedsiębiorstwa albo innej instytucji prywatnej bądź publicznej, a dokumentacja z rejestru pozwoli rozliczać się przed organem nadzoru w przypadku kontroli.

Rejestr jest niczym innym jak dokumentacją związaną z przetwarzaniem danych osobowych. W rejestrze powinny być zapisane wszystkie czynności związane z przetwarzaniem danych osobowych. **„Czynności związane z przetwarzaniem danych" nie są tym samym co „operacje przetwarzania"** (operacje przetwarzania czyli m.in. zbieranie, porządkowanie, usuwanie danych osobowych zdefiniowane w słowniczku, art. 4 pkt 2 RODO).

Posługiwanie się kategorią czynności przetwarzania wymaga szerokiego spojrzenia na przetwarzane dane osobowe w organizacji, na przykład poprzez kategorie podmiotów danych, których dane przetwarzamy albo celów, dla których je przetwarzamy. Kształtując rejestr na podstawie kategorii podmiotów danych, można wyróżnić np. pracowników i klientów. Następnym krokiem jest określenie czynności przetwarzania danych w danej kategorii. W kategorii pracowników mogą to być czynności przetwarzania dotyczące np.: zatrudniania, wypłaty wynagrodzenia, organizacji wyjazdów służbowych, ubezpieczenia społecznego, ubezpieczenia chorobowego. Każdej kategorii czynności, powinny być przypisane operacje przetwarzania. Ponadto, w rejestrze powinien zostać zamieszczony szereg innych informacji – te, które muszą zostać zamieszczone w rejestrze prowadzonym odpowiednio przez administratora danych i przetwarzającego, określone zostały w przepisie art. 30 RODO.

To, w jakiej formie rejestr będzie prowadzony, jest sprawą indywidualną organizacji – **może to być dowolny typ pliku w wybranym programie komputerowym.** W tym względzie RODO nie narzuca konkretnych rozwiązań, tylko wskazuje kryteria, jakie każdy rejestr musi wypełniać. Istotne jest to, aby rejestr czynności był na bieżąco aktualizowany, a jego zawartość odpowiednio chroniona przed nieuprawnionymi osobami.

<u>Wyjątki</u>

Rejestr czynności, nie musi być prowadzony w przedsiębiorstwach zatrudniających mniej niż 250 osób, chyba że:

- przetwarzanie może naruszać prawa lub wolności osób, których dane przetwarzamy np. może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości,
- przetwarzanie obejmuje szczególne kategorie danych (np. dane biometryczne) lub dane dotyczące wyroków skazujących i naruszeń prawa,
- przetwarzanie nie ma charakteru sporadycznego, np. przetwarzanie danych związanych z zarządzaniem Klientami, zarządzaniem Personelem.

<u>Podstawa prawna</u>
Preambuła: motywy 13, 82 i 89
art. 4 pkt 1 i 2, art. 30

Photo by Joel Filipe on Unsplash

PRAWO DO USUNIĘCIA DANYCH

(PRAWO DO BYCIA ZAPOMNIANYM)

Photo by Remy_Loz on Unsplash

RODO przyznaje osobom, których dane dotyczą, prawo do usunięcia danych, w tym prawo do bycia zapomnianym. Zgodnie z przepisami RODO osoba taka ma prawo w przypadkach opisanych w RODO (wskazanych poniżej) żądać od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki te dane osobowe usunąć. Prawo do bycia zapomnianym obejmuje także prawo do żądania od administratora, który upublicznił dane (np. wyszukiwarkę internetową), aby ten podjął działania w celu poinformowania innych administratorów przetwarzających te dane, że podmiot danych żąda ich usunięcia.

Administrator musi zapewnić odpowiednie techniczne i organizacyjne środki pozwalające na całkowite usunięcie danych osoby, która korzysta z prawa do bycia zapomnianym. **Należy usunąć dane ze wszystkich miejsc, czyli z m.in.: serwera, poczty, plików Word i Excel, dysków zewnętrznych i przenośnych, ale również z papierowych kopii.** Samo przechowywanie przez administratora danych nadal kwalifikowane jest jako przetwarzanie danych osobowych. Dane osobowe muszą być także usuwane ze wszystkich kopii zapasowych oraz logów.
**Jeżeli usuwanie z kopii zapasowych pojedynczych rekordów grozi naruszeniem integralności pozostałych gromadzonych danych, to administrator może manualnie przywracać kopie do bazy głównej,
a następnie usuwać z nich pojedyncze rekordy i „backupować" bazy zmniejszone o ten rekord, choć jest to dość czasochłonny proces.**

Niezbędna jest także wiedza komu, w czasie trwania współpracy, przekazano przetwarzanie danych osoby, która wnosi o prawo do bycia zapomnianym. Obowiązkiem administratora jest poinformowanie podmiotów przetwarzających (np. dostawców, firmę obsługującą newslettera), by także usunęli dane tej osoby.

<u>Kiedy powstaje – na podstawie „prawa do bycia zapomnianym" – obowiązek usunięcia danych:</u>

- dane osobowe nie są już niezbędne do celów, do których je zebrano,
- podmiot danych wycofał zgodę i nie istnieje inna podstawa prawna dla przetwarzania tych danych,
- podmiot danych wniósł sprzeciw do dalszego przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania,
- dane osobowe były przetwarzane niezgodnie z prawem,
- dane osobowe muszą być usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w unijnym bądź krajowym przepisie prawnym (np. przepisach dotyczących niszczenia dokumentacji medycznej),
- dane zostały zebrane w celu świadczenia usług internetowych dziecku.

<u>Przykłady</u>

1. Usuwanie danych z kopii zapasowych

Serwis internetowy zajmuje się sprzedażą odzieży używanej online, przetwarzając dane niezbędne do dokonania sprzedaży, w tym doręczenia

ubrań kupującemu. Pan Cyfrowy, realizując przysługujące mu na podstawie RODO „prawo do bycia zapomnianym" niezwłocznie po dokonaniu zakupów, zażądał usunięcia swoich danych z wszystkich baz oraz kopii zapasowych sklepu.

Czy sklep ma obowiązek usunąć dane?

Sklep będzie mógł przetwarzać dane Pana Cyfrowego w bazie głównej oraz archiwalnej, a także w kopiach zapasowych, mimo skierowanego żądania usunięcia danych w celu wykazania, że sprzedaż ubrań została dokonana. Zasadniczym celem kopii zapasowych jest jednak zapewnienie ciągłości funkcjonowania systemów informatycznych, nie mogą być one więc utożsamiane z bazami archiwalnymi. Dane w kopiach zapasowych są więc przechowywane krótkotrwale i usuwane chociażby przez nadpisywanie danych.

Dane podane przez kupującego jak: imię, nazwisko, adres dostawy oraz dane kontaktowe mogą być wykorzystywane m.in. przy realizacji jego prawa do gwarancji bądź do ochrony sprzedawcy przed ewentualnymi przyszłymi roszczeniami. Dopóki istnieją podstawy do przetwarzania danych, to sklep może je w tych miejscach przetwarzać. Jednakże gdy przestaną one istnieć, będzie on musiał usunąć dane ze wszystkich wspomnianym miejsc.

2. Usuwanie danych osób trzecich

Kwiaciarnia internetowa, zbierając zamówienia na doręczenia bukietów, gromadzi m.in. dane osobowe nadawcy oraz odbiorcy kwiatów, w tym adresy do doręczeń. Kobieta, której kwiaty zostały doręczone, dowiedziawszy się o przekazaniu jej danych przez przesyłającego kwiaty przyjaciela, zażądała natychmiastowego usunięcia jej danych, w tym z wszelkich posiadanych przez kwiaciarnię baz danych oraz kopii. Kwiaciarnia odmówiła usunięcia danych z wszystkich kopii wskazując, że w razie ewentualnej przyszłej kontroli organu nadzorczego, będzie musiała przedstawić, w jaki sposób realizuje prawo do usunięcia danych. W ocenie kwiaciarni nie da się tego zrobić, bez przetwarzania danych osób, które występują z takimi żądaniami.

Czy kwiaciarnia miała prawo odmówić takiego żądania?

Realizacja obowiązków wynikających z RODO nie powinna być uzasadnieniem gromadzenia nadmiernej ilości danych osobowych. Kwiaciarnia realizując zasadę rozliczalności może gromadzić dane niezbędne do wykazania, że dane usunęła. W tym przypadku mogą być to jednak logi, które nie prowadzą do konkretnego żądania, identyfikując daną osobę. Kwiaciarnia chcąc dalej przetwarzać dane, nie może uzasadniać więc tego koniecznością rozliczenia się przed organem z wykonania obowiązków wynikających z RODO. Jedynym uzasadnieniem mogłaby być ochrona przed ewentualnymi przyszłymi roszczeniami.

Photo by Luca Iaconelli on Unsplash

<u>Wyjątki</u>
Istnieją sytuacje, kiedy administrator danych nie będzie musiał zrealizować prawa do bycia zapomnianym. Są to m.in. sytuacje, gdy przetwarzanie przez administratora jest wymagane przez prawo unijne albo krajowe bądź jest to niezbędne do ustalenia, dochodzenia lub obrony roszczeń. Przykładem może być tutaj pracodawca, który ma obowiązek gromadzenia dokumentacji pracowniczej przez 50 lat. Pełna lista wyłączeń zawarta jest w art. 17 ust. 3 RODO.

<u>Podstawa prawna</u>
Preambuła: motywy 65, 66, 156
art. 17

PRAWO DO PRZENOSZALNOŚCI DANYCH

Photo by John Simitopoulos on Unsplash

Osoba, której dane dotyczą, ma prawo żądać:

- wydania jej w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego danych osobowych jej dotyczących, które dostarczyła administratorowi oraz ma prawo samodzielnie przesłać te dane osobowe innemu („nowemu") administratorowi bez przeszkód ze strony pierwszego administratora,
- przesłania swoich danych osobowych z systemów informatycznych od administratora, któremu je wcześniej przekazała, innemu, „nowemu", administratorowi, o ile jest to technicznie możliwe.

Prawo do przenoszenia danych osobowych dotyczy danych osobowych przetwarzanych w systemach informatycznych (tj. w sposób zautomatyzowany).

Objęte prawem do przenoszenia są dane przetwarzane w systemach IT w związku z korzystaniem przez osobę, której dane dotyczą, z usług lub urządzeń – jak na przykład historia logowania. **Prawo do przeniesienia danych nie obejmuje jednak „danych wywnioskowanych" i „danych wywiedzionych", a są nimi np. wyniki algorytmiczne, które administrator pozyskał na podstawie analizy danych osoby, której dane dotyczą.** Przykładowo, dane które posiada służba zdrowia na nasz temat, są przez nas przekazane, ale to, że lekarz je analizuje i wyciąga wnioski to już dane wywiedzione i wywnioskowane. Kolejnym przykładem może być też ocena wiarygodności kredytowej oraz ryzyka ubezpieczeniowego.

Prawo do przeniesienia danych stosuje się, jeśli przetwarzanie opiera się podstawie zgody lub umowy. Nie obejmuje ono administratorów, którzy przetwarzają dane niezbędne do wykonania zadania realizowanego w interesie publicznych lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

Zakres danych podlegających przeniesieniu obejmuje też dane poddane pseudonimizacji. Zdarza się, że administratorzy danych przetwarzają informacje, które zawierają dane osobowe kilku osób. W takich przypadkach nie powinni oni zbyt wąsko interpretować tego, kogo te dane dotyczą i traktować taką informację jako dane osobowe osoby wnioskującej, np. rejestry połączeń telefonicznych bądź przelewów bankowych. Mimo że zawierają dane nie tylko osoby wnioskującej czy dokonującego przelewu, ale też innych osób, to abonent lub nadawca przelewu powinien mieć możliwość ich otrzymania. Gdy przekazywane dane osobowe dotyczą osób trzecich, to „nowy" administrator nie może ich wykorzystywać do własnych celów (np. oferowania im produktów).

Dane osobowe powinny być przekazywane w powszechnie używanym formacie, który pozwoli je odczytać maszynowo, np. w formacie XML, CSV albo JSON.

Administrator we współpracy ze swoimi ewentualnymi podwykonawcami powinien jasno wskazać procedury tak, aby był on w stanie odpowiedzieć na wnioski o przeniesienie danych, podobnie współadministratorzy powinni jasno określić zasady współpracy w tym obszarze. Administratorzy powinni także ustalić procedury identyfikacji osób żądających przeniesienia danych.

„Nowy" administrator danych będzie odpowiedzialny za zapewnienie, aby przekazane mu dane osobowe nie były nadmierne w stosunku do nowego celu przetwarzania danych, dlatego ważne jest wyraźne i bezpośrednie określenie celów, dla których będzie przetwarzał dane osobowe.

Prawo do przeniesienia danych nie jest tym samym co prawo do bycia zapomnianym. „Stary" administrator danych nie będzie miał automatycznie obowiązku usunięcia przeniesionych danych, jednak na żądanie podmiotu danych będzie musiał przeniesione już dane usunąć. Przeniesienie danych nie może niekorzystnie wpływać na prawa i wolności innych osób, czyli np. uniemożliwiać im realizacji prawa do dostępu.

Wyjątki

Przenoszalność danych nie ma zastosowania do ich przetwarzania w zakresie:

- niezbędnym do wykonania zadania realizowanego w interesie publicznym,
- niezbędnym w ramach sprawowania władzy publicznej powierzonej administratorowi.

Podstawa prawna

Preambuła: motywy 68, 73, 156

art. 13 ust. 2 pkt b, art. 14 ust. 2 pkt c, art. 20

Wytyczne Grupy Roboczej art. 29 dotyczące prawa do przenoszenia danych, dostępne na: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

UZYSKIWANIE ZGODY DZIECKA

Dzieci, które korzystają z usług internetowych, np. portali społecznościowych, są często narażone na wykorzystanie swoich danych osobowych bez ich świadomej zgody, np. w celach marketingowych. Kierując się potrzebą większej ochrony osób małoletnich, RODO reguluje szczególną formę zgody dziecka w stosunku do usług społeczeństwa informacyjnego. Za taką usługę uważa się każdą odpłatną usługę świadczoną na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług. Wielu administratorów mylnie identyfikuje obowiązek odbierania zgody rodzica zawsze, gdy usługa świadczona jest w sieci Internet. **Ma on jednak zastosowanie tylko w ograniczonym zakresie tam, gdzie podstawą przetwarzania danych jest zgoda, a nie np. umowa.** W ogromnej ilości przypadków podstawą korzystania z usługi jest akceptacja regulaminu świadczenia usług drogą elektroniczną, np. przy zakładaniu kont na portalach społecznościowych bądź zakładaniu konta e-mail. **W takich przypadkach zgoda rodzica na przekazanie danych osobowych z punktu widzenia RODO nie jest wymagana**, jednak wymagana może okazać się zgoda rodzica na zawarcie umowy zgodnie z przepisami prawa cywilnego – nie mająca jednak nic wspólnego ze zmianami wynikającymi z RODO. Trzeba odróżniać wyrażenie zgody na przekazanie danych osobowych od wyrażenia zgody na zawarcie umowy.

RODO nakazuje administratorowi podjęcie rozsądnych działań w celu weryfikacji zgody lub aprobaty rodzica lub opiekuna prawnego. **Administrator może w tym celu na przykład wprowadzić zasadę uwierzytelniania przez inne konto, która pozwoli dziecku przesłać prośbę o zgodę do sprawdzonego konta rodzica na tym samym portalu.**

Przykłady

1. Uzyskiwanie zgody dziecka

10-letni Jaś chce wziąć udział w konkursie internetowym na najlepszy komiks. W formularzu zgłoszeniowym trzeba podać numer telefonu, można też wyrazić zgodę na cele marketingowe.

Czy organizatorzy mogą uzyskać zgodę Jasia na cele marketingowe?

Po pierwsze należy zaznaczyć, że do udziału Jasia w konkursie niezbędne będzie na gruncie prawa cywilnego wyrażenie zgody przez jego rodziców.

Odnosząc się natomiast do wyrażenia przez Jasia zgody na cele marketingowe, to Jaś nie będzie mógł takiej zgody udzielić samodzielnie. Jaś musi o to poprosić rodzica bądź opiekuna prawnego. Jednak to na administratorze ciąży obowiązek podjęcia rozsądnych starań w celu zweryfikowania, czy osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem wyraziła zgodę lub ją zaaprobowała. Dlatego organizatorzy konkursu powinni wyświetlić komunikat z zapytaniem o wiek. Natomiast po zaznaczeniu opcji wskazującej, że Jaś ma poniżej 16 lat (propozycja Ministra Cyfryzacji w nowym projekcie ustawy o ochronie danych osobowych obniża granicę do lat 13), powinien się wyświetlić następny komunikat, w którym zgodę na udział oraz na cele marketingowe może wyrazić tylko rodzic lub opiekun prawny.

Podstawa prawna

Preambuła: motywy 38, 58, 65

art. 4 pkt 25, art. 8, art. 12 ust. 1, art. 40 ust. 2 pkt g

RODO

OBOWIĄZEK AKTUALIZOWANIA UZYSKANEJ JUŻ RAZ ZGODY NA PRZETWARZANIE DANYCH PO WEJŚCIU W ŻYCIE RODO

Zgodnie z RODO, jeżeli przetwarzanie ma za podstawę zgodę w myśl dyrektywy 95/46 i odpowiada ona warunkom przewidzianym w ustawie o ochronie danych osobowych z 1997 r. będzie ona ważna również po 25 maja 2018 r. W takim przypadku administrator może kontynuować przetwarzanie w oparciu o „starą" zgodę.

Grupa Robocza art. 29 w wytycznych przyjętych 28 listopada 2017 r. w sposób jasny stwierdziła, że zgody zbierane przed rozpoczęciem stosowania RODO i zgodnie z krajowymi przepisami o ochronie danych osobowych nie muszą być automatycznie zbierane ponownie po 25 maja 2018 r. Ale zgoda zachowa ważność wyłącznie wtedy, jeżeli jest zgodna z zasadami określonymi w RODO. Na te zasady składa się szereg elementów, takich jak np. konieczność przekazania szeregu informacji przy zbieraniu danych osobowych. Grupa stwierdziła wyraźnie, że niepodanie przy zbieraniu danych informacji, które trzeba podawać na gruncie RODO, a których wcześniej podawać nie trzeba było, nie powoduje automatycznie, że tak udzielone zgody stracą ważność. Przykładem takiej sytuacji może być właśnie kwestia informowania o możliwości odwołania zgody.

Przepisy RODO nakładają na administratorów nieistniejący dzisiaj obowiązek poinformowania o prawie do odwołania zgody, na etapie gromadzenia danych. **W ocenie Ministra Cyfryzacji zasada aktualności obowiązująca w prawie administracyjnym wyłącza uznanie, że pozyskanie zgodne z prawem zgody przed 25 maja 2018 r. powinny być po tej dacie uzupełniane o obowiązek poinformowania o prawie do ich odwołania.** Przemawia za tym również orzecznictwo NSA. W wyroku z 8 lipca 2011 r. I OSK 389/11, NSA wskazał, że późniejsza zmiana przepisów stanowiących podstawę rozstrzygnięcia administracyjnego nie ma znaczenia dla oceny prawidłowości wydanej pod rządami poprzednio obowiązującej regulacji decyzji. Należy jednak wnieść zastrzeżenie, że polski organ nadzorczy bądź instytucje unijne mogą wyrazić inne stanowisko w sprawie, co będzie rodziło wątpliwości Ministra Cyfryzacji, ale może prowadzić do odmiennego rozumienia tego obowiązku.
Definicja zgody w RODO zawiera dwie nowe przesłanki w porównaniu do zgody określonej w dyrektywie 95/46, a więc i w ustawie o ochronie danych osobowych z 1997 roku, są to: 1) przesłanka jednoznacznego okazania woli; 2) przesłanka oświadczenia pisemnego, elektronicznego bądź wyraźnego działania potwierdzającego okazanie woli (którą można nazwać „okazaniem woli w sposób afirmatywny").

Zgodnie z RODO spełnienie przesłanki afirmatywnej formy okazania woli może natomiast polegać między innymi na:

- zaznaczeniu okienka wyboru podczas przeglądania strony internetowej,
- wyborze ustawień technicznych do korzystania z usług społeczeństwa informacyjnego,
- innym oświadczeniu bądź zachowaniu, które w danym kontekście jasno wskazuje, że osoba, której dane dotyczą, zaakceptowała proponowane przetwarzanie jej danych osobowych.

Zgodnie z RODO: milczenie, okienka zaznaczone domyślnie lub niepodjęcie działania, nie powinny oznaczać zgody. Dlatego też, jeżeli administrator zbierał zgody w takiej formie, to będzie musiał zbierać nowe zgody. Istotne jest także

wdrożenie nowych mechanizmów i rozwiązań, takich jak zapewnienie rozliczalności, czy danie możliwości łatwego odwołania zgody, na co zwraca uwagę w opinii Grupa Robocza.

Podstawa prawna

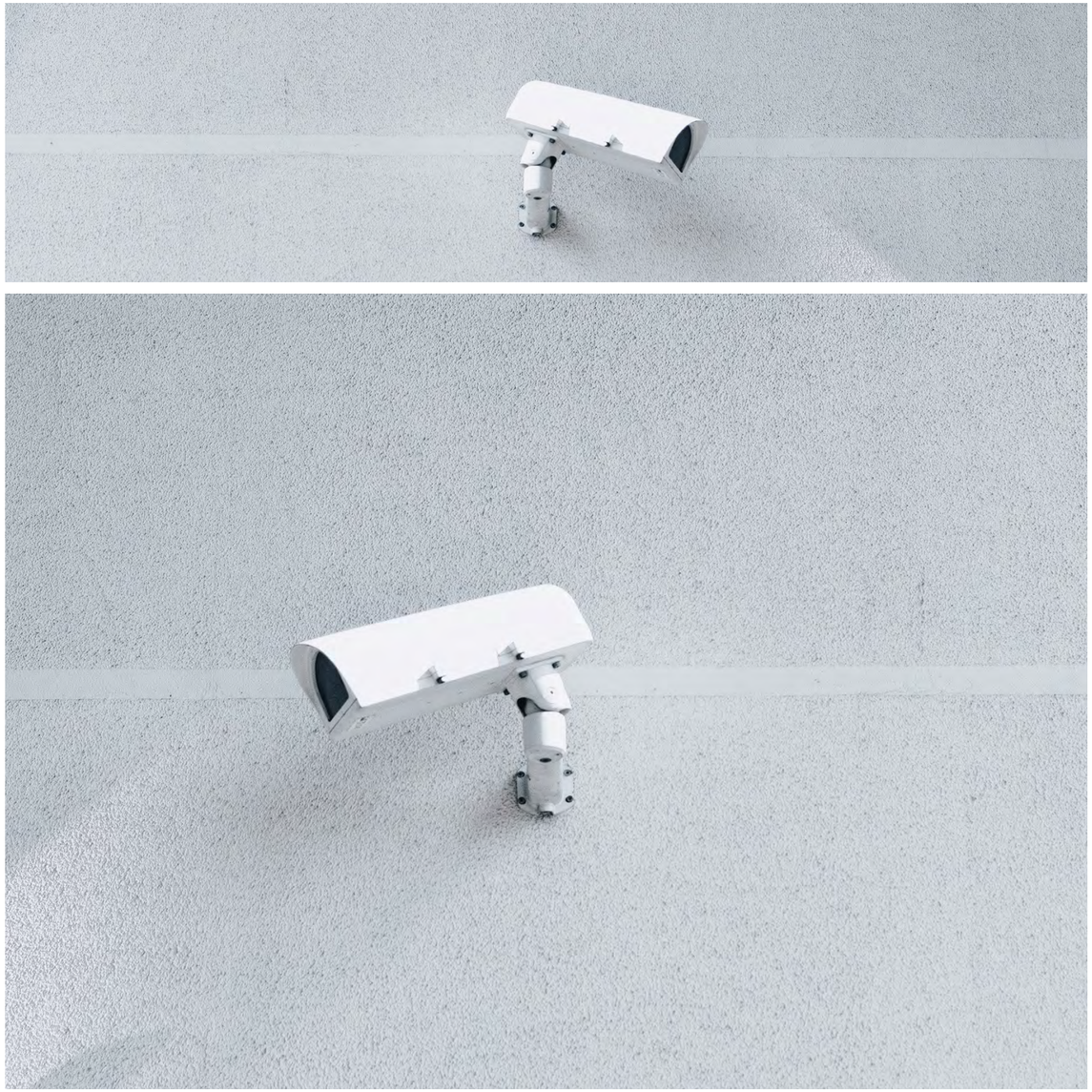

Photo by Siarhei Horbach on Unsplash

Preambuła: motywy 32, 40-57, 171

art. 4 pkt 11, art. 6, art. 9-11

Projekt wytycznych Grupy Roboczej art. 29 dotyczące zgody na przetwarzanie danych osobowych, dostępne na: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

ANONIMIZACJA A PSEUDONIMIZACJA

Photo by Lane Jackman on Unsplash

Anonimizacja pozwala na usunięcie powiązań między danymi osobowymi a osobami, których dane dotyczą. Zanonimizowane dane nie są danymi osobowymi, ponieważ nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. **W związku z tym, zasady ochrony danych nie powinny mieć zastosowania do danych zanonimizowanych, co oznacza, że RODO nie stosuje się do przetwarzania takich anonimowych informacji.**

Natomiast pseudonimizacja to „ukrycie" danych osobowych, ponieważ nadal istnieje narzędzie, które pozwala je odczytać. Dane osobowe, które są spseudonimizowane, pozostają danymi osobowymi. Poddając je pseudonimizacji, tylko na jakiś czas „ukrywamy" informacje pozwalające zidentyfikować osobę, której dane dotyczą. **Aby dokonać skutecznie czynności pseudonimizacji istotne jest to, aby klucz pozwalający odczytać dane był przechowywany osobno, tj. w innym miejscu, niż same dane. Ponadto, klucz musi być odpowiednio zabezpieczony w sposób techniczny i organizacyjny.**

Różnica między tymi dwoma procesami wymaga analizy tego, czy dana osoba fizyczna jest nadal możliwa do zidentyfikowania. Dlatego trzeba wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby, co do których istnieje możliwość, że zostaną wykorzystane przez administratora lub inną osobę w celu zidentyfikowania tożsamości tej osoby fizycznej. W tym celu należy wziąć pod uwagę wszelkie czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny.

Podstawa prawna

Preambuła: motywy 26, 28, 29, 75, 78, 85, 156

art. 4 pkt 5

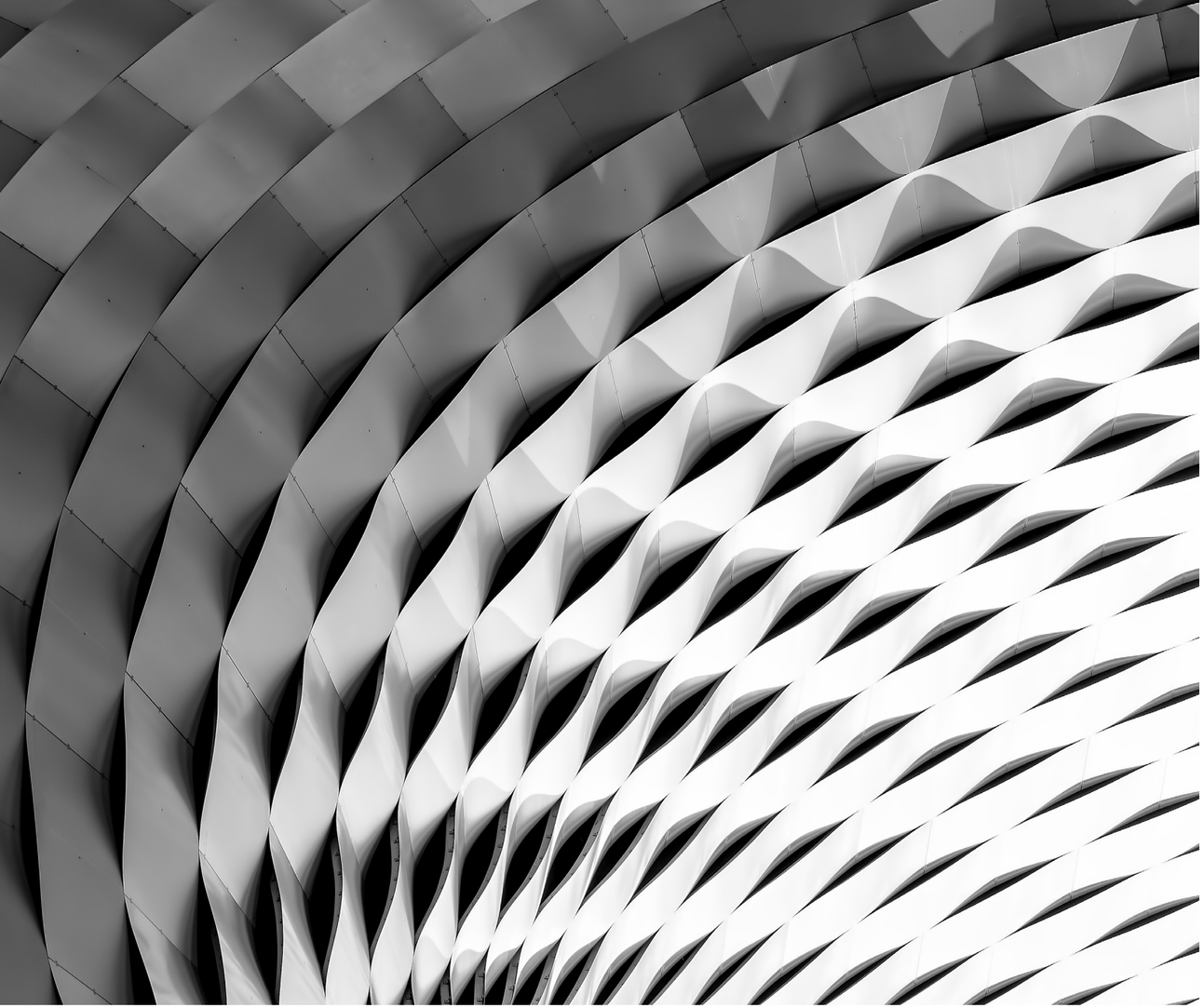

Photo by Ricardo Gomez Angel on Unsplash

OBOWIĄZEK ZGŁASZANIA NARUSZEŃ

Administrator danych osobowych jest zobowiązany do dokumentowania naruszeń ochrony danych osobowych. Zgodnie z RODO naruszenie ochrony danych osobowych, należy bezwzględnie zgłosić w ciągu 72 godzin od stwierdzenia naruszenia, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. **W ocenie Ministra Cyfryzacji nie zawsze występuje konieczność zgłoszenia przypadków naruszenia bezpieczeństwa danych osobowych. Takich przypadków, które nie wywołują bezpośredniego skutku względem osób, których dane dotyczą nie trzeba zgłaszać.** Taka sytuacja ma miejsce wtedy, gdy – przykładowo – doszło do przypadkowego zniszczenia nośnika z danymi osobowymi przez osobę upoważnioną do przetwarzania, jednak istniałyby jednocześnie inne nośniki, na których przechowywane są te same dane. Mogłaby być to również sytuacja, gdy poza obszar przetwarzania danych dane nawet w dużych zasobach są wyniesione przez osobę mającą prawo do ich dostępu, ale nie zostały ujawnione i niedługo potem bezpiecznie wróciły na swoje miejsce.

Zgłoszenie musi zawierać m.in.:

- opis naruszenia, kategorię danych, przybliżoną liczbę osób, których dane dotyczą, liczbę wpisów, których dotyczy naruszenie,
- opis konsekwencji naruszenia danych,
- opis środków jakie zastosowano lub jakie administrator proponuje, w celu naprawy sytuacji lub zminimalizowania negatywnych konsekwencji naruszenia.

W przypadku, kiedy naruszenie może spowodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator musi bez zbędnej zwłoki zawiadomić osobę, której dane dotyczą.

Przykłady

1. Naruszenie nie powodujące wysokiego ryzyka naruszenia praw lub wolności

Kadrowa firmy X przekopiowała listę płac na niezaszyfrowanego pendrive'a, po czym zabrała go poza siedzibę firmę, by dokończyć pracę w domu. Niestety zgubiła go w drodze do domu. **Czy firma powinna zgłosić takie naruszenie?**

W powyższej sytuacji naruszenie trzeba zgłosić, bo niezaszyfrowane dane mogły zostać odczytane przez nieuprawnione do tego osoby. Należy także bezwzględnie pouczyć kadrową i podjąć koniecznie wewnętrzne działania, aby takie sytuacje nie miały miejsca w przyszłości.

Gdyby dane z pendrive'a były szyfrowane, nie dostały się w nieuprawnione do tego ręce i następnego dnia bezpiecznie wróciły do firmy, to nie byłoby potrzeby zgłaszania incydentu, ponieważ dane nie zostały udostępnione osobom nieupoważnionym do przetwarzania. Zostałyby tylko narażone na takie ryzyko.

Wyjątki

Przypadki kiedy nie musimy zgłaszać naruszeń osobom, których dane przetwarzamy są następujące:

- administrator zastosował odpowiednie środki techniczne i organizacyjne dla danych których dotyczy naruszenie, takie jak szyfrowanie, aby uniemożliwić osobom nieuprawnionym odczytanie danych,
- administrator w dalszej kolejności użył środków, które eliminują prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
- administrator musiałby dokonać niewspółmiernie dużego wysiłku by powiadomić osobę której dane dotyczą o naruszeniu, wówczas wydawany jest publiczny komunikat lub inny podobny środek by poinformować osoby w skuteczny sposób.

Natomiast niezależnie od tego, przypadki takich naruszeń trzeba będzie udokumentować i przedstawić w razie kontroli organu nadzoru.

Podstawa prawna

Preambuła: motywy 73, 75, 85-88

art. 33-34

Wytyczne Grupy Roboczej art. 29 dotyczące oceny skutków dla ochrony danych, dostępne na: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

RODO

INFORMATOR

Ministerstwo
Cyfryzacji