RODO

ZMIANY W PRZEPISACH O OCHRONIE DANYCH OSOBOWYCH

Autor: Ewa Kamila Cecko

SPIS TREŚCI

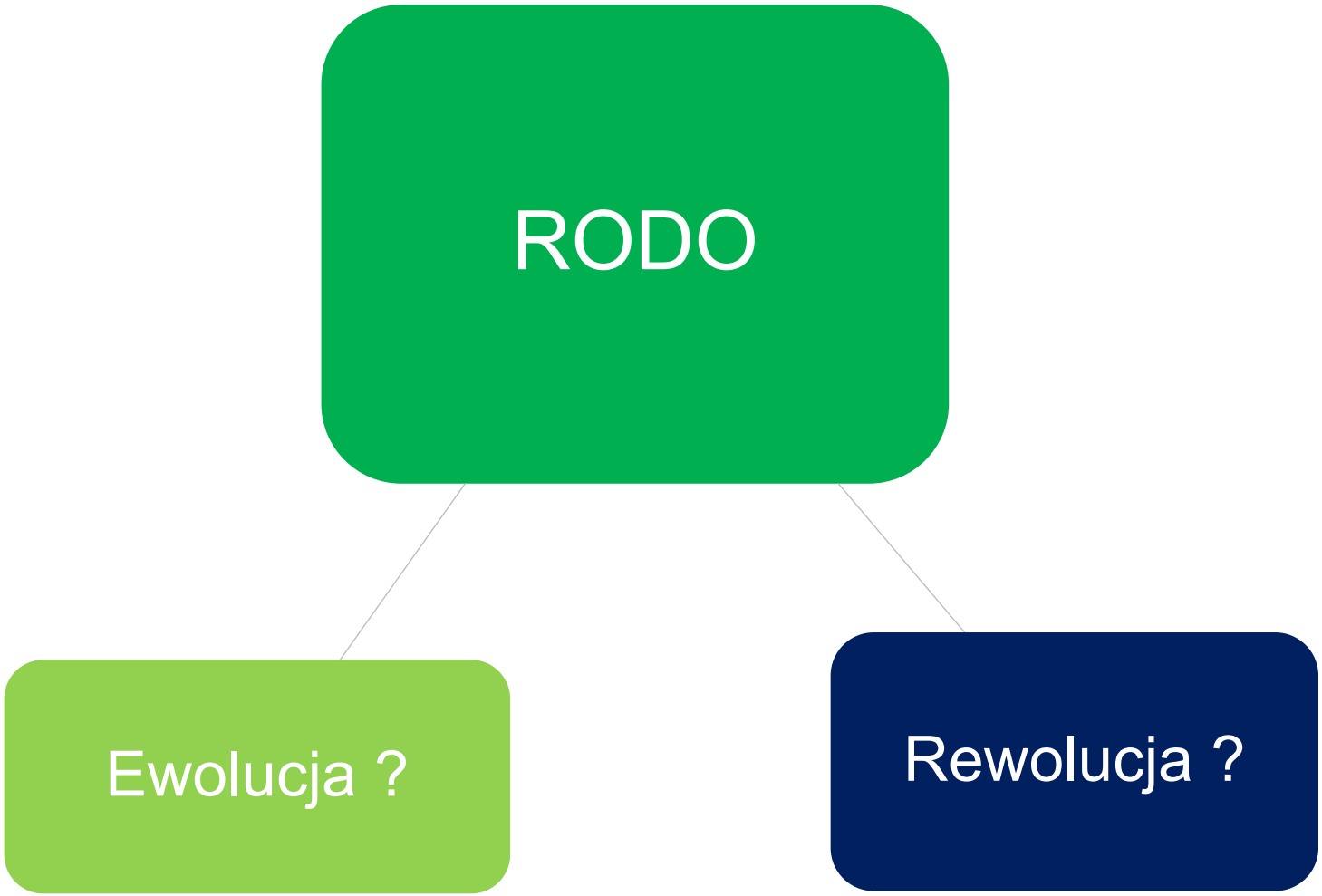
WSTĘP

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. - zacznie obowiązywać od 25 maja 2018 r.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r.

WSTĘP

WSTĘP



CO SIĘ ZMIENIA W PRZEPISACH SZCZEGÓLNYCH

Ustawa o samorządzie pielęgniarek i położnych:

Administratorem danych osobowych zawartych w rejestrach pielęgniarek i rejestrach położnych są okręgowe rady pielęgniarek i położnych.

Ustawa o zawodach pielęgniarki i położnej:

Postępowanie w sprawach określonych w ust. 1 – 6 [**ustalenie niezdolności do wykonywania zawodu]** jest poufne i odbywa się z zachowaniem przepisów o ochronie danych osobowych.

Administratorem danych osobowych zawartych w rejestrze [**centralnym rejestrze pielęgniarek i położnych**] jest Naczelna Rada Pielęgniarek i Położnych.

Kodeksie pracy:

Zmienia się zakres przetwarzanych danych przed zatrudnieniem oraz podczas zatrudnienia.

Pojawia się kwestia wideomonitoringu i danych biometrycznych.

WSTĘP

Fakty i Mity nt. RODO

Wysokie kary finansowe dla każdego kto nie wdroży RODO,

Ogromne wyzwanie dla administratorów danych;

Duże zmiany;

W końcu każdy będzie wiedział kto przetwarza jego dane;

Rewolucja w przetwarzaniu danych;

Co jeszcze ?

WSTĘP

Fakty i Mity nt. RODO

1. Lepsza ochrona danych osobowych;
2. Harmonizacja przepisów;
3. Wzmocnienie praw osób fizycznych;
4. Uatrakcyjnienie rynku UE względem państw trzecich;
5. Usprawnienie wymiany informacji i procedur wewnątrzwspólnotowych;
6. Wyznaczenie standardów bezpieczeństwa adekwatnych do wyzwań XXI wieku.

OGÓLNE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

- Brak konieczności rejestracji zbiorów danych osobowych przez GIODO/UPODO.
- Obowiązek prowadzenia rejestru czynności przetwarzania wewnątrz organizacji.
- Podmiot przetwarzający, również będzie zobowiązany do prowadzenia wspomnianego rejestru. Będzie też w niektórych okolicznościach zobowiązany powołać Inspektora Ochrony Danych (IOD).

OGÓLNE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

- Zgodność z prawem, rzetelność i przejrzystość.
- Ograniczenie celu.
- Minimalizacja danych.
- Prawidłowość.
- Ograniczenie przechowywania.
- Integralność, poufność i rozliczalność.

OGÓLNE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

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

OGÓLNE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

KRÓTKIE PRZYPOMNIENIE

Dane osobowe to wszelkie informacje odnoszące się do **zidentyfikowanej** lub **możliwej do zidentyfikowania** osoby fizycznej.

Osobą zidentyfikowaną jest taka osoba, której tożsamość znamy, którą możemy wskazać spośród innych osób. Osobą możliwą do zidentyfikowania jest taka osoba, której tożsamości nie znamy, ale możemy poznać, korzystając z tych środków, które mamy.

Możliwość uznania informacji za dane osobowe nie zależy ani **od wieku** danej osoby, ani **od jej narodowości**.

OGÓLNE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

Osoba zidentyfikowana:

a) pracownik, którego dane osobowe przetwarza pracodawca;
b) klient sklepu internetowego, który podał swoje dane osobowe do wysyłki zamówienia;
c) osoba, która w formularzu kontaktowym podaje swoje imię, nazwisko i adres e-mail.

Osoba możliwa do zidentyfikowania:

a) potencjalny kontrahent, którego posiadamy tylko numer ewidencyjny w CEIDG;
b) nadawca listu poleconego na podstawie numeru przesyłki.

PAMIĘTAJ !!!

Dane osób prowadzących **jednoosobową działalność gospodarczą** stanowią dane osobowe **podlegające ochronie**.

Zgodnie z RODO, do **kategorii danych osobowych zwykłych** należą także dane osobowe dotyczące **wyroków skazujących**.

OGÓLNE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

Dane osobowe to informacje o **osobach fizycznych** – osoby prawne nie mają danych osobowych.

Pracownicy osób prawnych mogą mieć dane osobowe, jak każda inna osoba fizyczna:

a) informacja „XYX sp. z o. o.” – nie stanowi danych osobowych tego podmiotu,

b) informacja „Jan Kowalski, pracownik XYZ sp. z o. o.” – może stanowić dane osobowe Jana Kowalskiego.

PAMIĘTAJ !!!

Danymi osobowymi są:

- Imię i nazwisko;
- Numer identyfikacyjny;
- Dane o lokalizacji;
- Identyfikator Internetowy.

Czynniki określające:

- Fizyczną;
- Fizjologiczną;
- Genetyczną;
- Psychiczną;
- Ekonomiczną;
- Kulturową lub społeczną tożsamość

JAKIE DANE MOŻNA PRZETWARZAĆ

PRZEPISY SZCZEGÓLNE WSKAZUJĄ JAKIE DANE MOŻE PRZETWARZAĆ ADMINISTRATOR DANYCH

LUB

TE DANE, KTÓRE SĄ NIEZBĘDNE DO OSIĄGNIĘCIA CELU PRZETARZANIA

PAMIĘTAJ

Podmiot przetwarzający dane na zlecenie powinien zawrzeć z administratorem danych odpowiednią umowę, tzw. **umowę powierzenia**, w której określone zostaną zasady przetwarzania danych.

W danej organizacji, dane osobowe faktycznie przetwarzają konkretne osoby fizyczne – pracownicy lub współpracownicy administratora lub podmiotu przetwarzającego dane. Takie osoby powinny posiadać **upoważnienie do przetwarzania danych osobowych**.

KIEDY MOŻNA PRZETWARZAĆ DANE OSOBOWE

Dane osobowe można przetwarzać **wyłącznie** wtedy, gdy istnieje tzw. **podstawa prawna przetwarzania danych**.

W przypadku przedsiębiorców, typowymi podstawami przetwarzania danych zwykłych są:

a) zgoda osoby, której dane dotyczą,

b) przetwarzanie danych jest niezbędne do wykonania umowy lub do podjęcia działań poprzedzających zawarcie umowy,

c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze,

d) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią.

PAMIĘTAJ

Zawsze to administrator danych powinien **móc wykazać**, **że dysponuje odpowiednią podstawą przetwarzania danych**. Jest to prawny obowiązek administratora danych wynikający z tzw. **zasady rozliczalności**.

JAK WIELE DANYCH MOŻNA ZBIERAĆ ZGODNIE Z RODO

RODO wprowadza tzw. **zasadę minimalizacji danych osobowych**.

Przetwarzanie danych powinno wiec zostać ograniczone do takich danych, bez których nie można osiągnąć celu przetwarzania danych.

Przykład

Jeżeli celem przetwarzania danych jest realizacja zamówienia w sklepie internetowym, przetwarzanie danych o sytuacji rodzinnej, czy finansowej klienta, nie będzie dopuszczalne. Przetwarzanie takich danych byłoby dopuszczalne, ale w innym celu, np. w celu marketingowym, na innej podstawie prawnej.

JAK ZBIERAĆ ZGODY NA PRZETWARZANIE DANYCH

Każda zgoda na przetwarzanie danych powinna charakteryzować się następującymi cechami:

a) **dobrowolność**

b) **konkretność**

c) **świadomość**

d) **jednoznaczność**

PAMIĘTAJ

Zgoda może zostać wyrażona w **dowolnej formie.**

Zgoda może być wyrażona poprzez **czynność.**

JAKIE INFORMACJE NALEŻY PRZEKAZYWAĆ

RODO **nakazuje**, aby przy gromadzeniu danych przekazywać osobie, której dane dotyczą, szereg informacji:

- o tożsamości administratora danych,
- o danych kontaktowych IOD,,
- o celach i podstawie przetwarzania danych,
- o odbiorcach danych osobowych lub o kategoriach odbiorców,
- informacje o zamiarze przekazania danych osobowych do państwa trzeciego,

JAKIE INFORMACJE NALEŻY PRZEKAZYWAĆ

RODO **nakazuje**, aby przy gromadzeniu danych przekazywać osobie, której dane dotyczą, szereg informacji:

- o okresie czasu, przez który dane osobowe będą przechowywane,
- o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą,
- ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania,
- o prawie do przenoszenia danych,
- jeżeli przetwarzanie odbywa się na podstawie zgody – o prawie do cofnięcia zgody w dowolnym momencie,
- o prawie wniesienia skargi do organu nadzorczego,

JAKIE INFORMACJE NALEŻY PRZEKAZYWAĆ

RODO **nakazuje**, aby przy gromadzeniu danych przekazywać osobie, której dane dotyczą, szereg informacji:

- o tym, czy podanie danych osobowych jest wymogiem ustawowym lub umownym,
- o profilowaniu,
- o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

KIEDY NIE TRZEBA ZBIERAĆ ZGODY

Zgody na przetwarzanie danych **nie trzeba zbierać** w szczególności wtedy, gdy:

a) przetwarzanie danych jest niezbędne do wykonania umowy,

b) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze,

c) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią.

PRZETWARZANIE SZCZEGÓLNEJ KATEGORII DANYCH OSOBOWYCH

Do szczególnych kategorii danych osobowych zaliczamy dane:

- ujawniające pochodzenie rasowe lub etniczne,
- poglądy polityczne, przekonania religijne lub światopoglądowe,
- przynależność do związków zawodowych,
- dane genetyczne,
- dane biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej,
- dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

PRZETWARZANIE SZCZEGÓLNEJ KATEGORII DANYCH OSOBOWYCH

W przypadku szczególnych kategorii danych, **typowe podstawy** przetwarzania danych to:

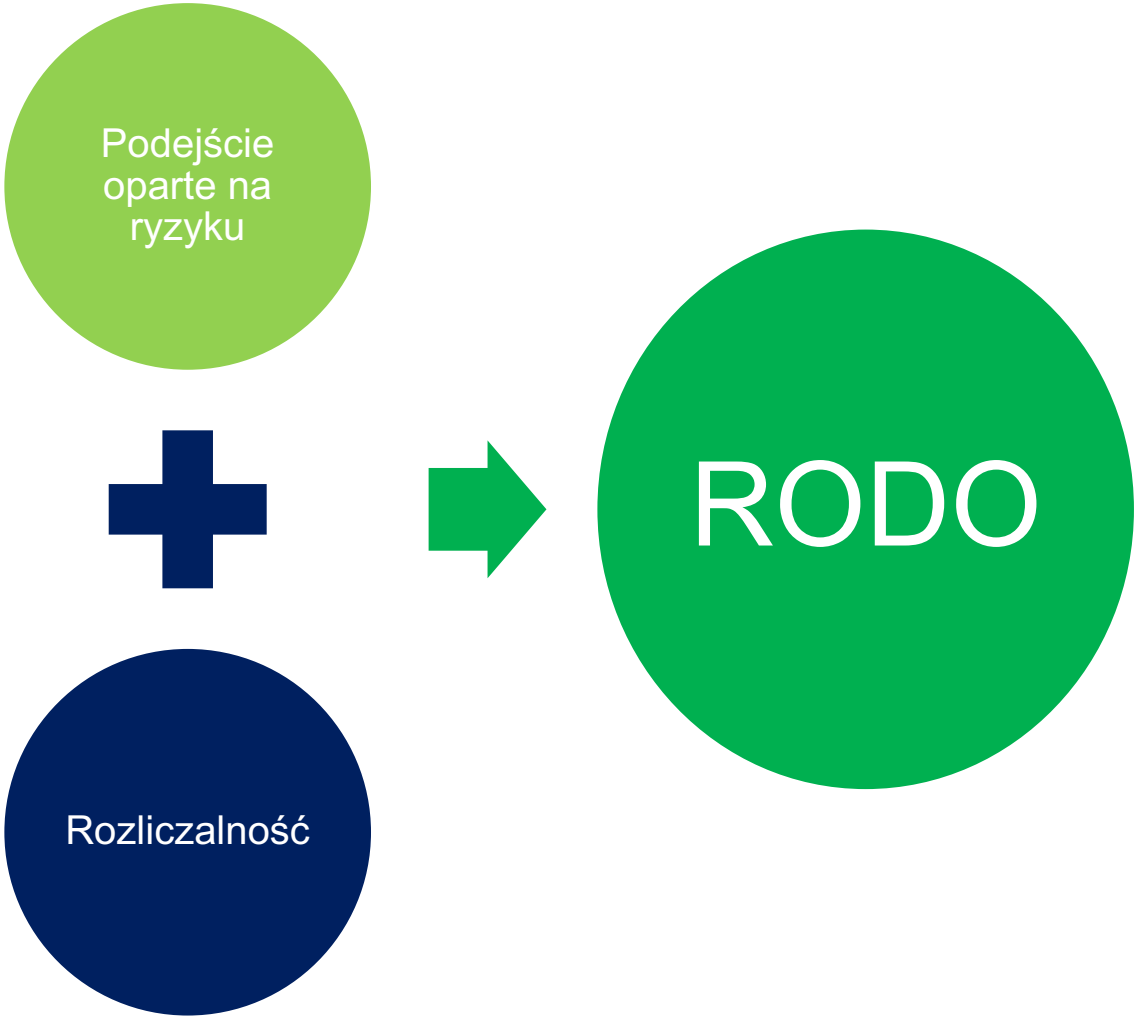
a) wyraźna zgoda osoby, której dane dotyczą,

b) przetwarzanie danych jest niezbędne do wykonania zadań związanych z zatrudnieniem, ubezpieczeniem społecznym pracowników,

c) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy,

d) przetwarzanie danych jest niezbędne w celu dochodzenia praw przed sądem.

OBOWIĄZKI ADMINISTRATORA DANYCH



OBOWIĄZKI ADMINISTRATORA DANYCH

RODO odchodzi od praktyki polegającej na wskazywaniu w przepisach prawa konkretnych środków zabezpieczenia danych osobowych, jakie mają zostać wdrożone przez administratora lub podmiot przetwarzający.

RODO wprowadza tzw. **podejście oparte na ryzyku.**

Istota podejścia opartego na ryzyku sprowadza się do tego, że każdy podmiot przetwarzający dane osobowe powinien **samodzielnie** określić, jakie konkretne środki zabezpieczenia danych należy wdrożyć.

OBOWIĄZKI ADMINISTRATORA DANYCH

Każdy podmiot przetwarzający dane osobowe powinien więc:

a) ustalić, jakie dane osobowe, w jakim charakterze, po co i w jakim środowisku przetwarza,

b) określić ryzyko naruszenia praw lub wolności osób fizycznych związane z takim przetwarzaniem,

c) dobrać odpowiednie środki zabezpieczenia danych, uwzględniając istniejące możliwości techniczne i własne możliwości finansowe.

PAMIĘTAJ

Podejście oparte na ryzyku zakłada, że każdy podmiot przetwarzający dane w **sposób świadomy podejmie decyzję** o stosowanych środkach zabezpieczenia.

Ma to tym większe znaczenie, że podmiot ten ponosi odpowiedzialność w przypadku naruszenia bezpieczeństwa danych osobowych.

REJESTR CZYNNOŚCI PRZETWARZANIA

Rejestr czynności przetwarzania danych osobowych jest **elementem dokumentacji ochrony danych**.

Rejestr powinien być **prowadzony odrębnie dla każdego procesu** przetwarzania danych – i niektóre z tych procesów występujących w typowych organizacjach mogą być zwolnione z prowadzenia rejestru.

Obowiązek prowadzenia rejestru czynności przetwarzania danych osobowych dotyczy **administratora danych** oraz **podmiotu przetwarzającego dane.**

PAMIĘTAJ

Rejestr może być prowadzony w formie pisemnej bądź w postaci elektronicznej.

Rejestr czynności **nie musi** być prowadzony przez przedsiębiorców zatrudniających mniej **niż 250** osób, chyba że:

a)przetwarzanie może naruszać prawa lub wolności osób, których dane dotyczą,

b)przetwarzanie obejmuje szczególne kategorie danych lub dane dotyczące wyroków skazujących,

c)przetwarzanie nie ma charakteru sporadycznego.

OBOWIĄZEK ZGŁASZANIA NARUSZEŃ

O wystąpieniu incydentu należy poinformować organ nadzorczy (PUODO).

Informacja powinna zostać przekazania niezwłocznie, lecz nie później, niż w ciągu 72 godzin od stwierdzenia naruszenia.

W pewnych przypadkach należy również informować o incydencie osoby, których dane dotyczą – będzie tak wtedy, gdy naruszenie może powodować wysokie ryzyko naruszenia praw i wolności osoby, której dane dotyczą.

OBOWIĄZEK ZGŁASZANIA NARUSZEŃ

Przykłady zgłoszenie do PUODO:

- zagubienie nośnika z danymi osobowymi,
- uzyskanie dostępu do danych przez osobę do tego nieuprawnioną,
- włamanie do systemu służącego do przetwarzania danych osobowych.

Przykłady poinformowania osoby:

- uzyskanie przez osoby nieuprawnione dostępu do loginów i haseł klientów systemu bankowości elektronicznej,
- zagubienie nośnika zawierającego dokumentację medyczną pacjentów.

DOKUMENTACJA

Ustawa z 29 sierpnia 1997 r. nakładała na administratorów danych obowiązek przygotowania i wdrożenia tzw. dokumentacji ochrony danych osobowych, na którą składały się:

- polityka bezpieczeństwa danych osobowych,
- instrukcja zarządzania systemem informatycznym, w którym przetwarzane są dane osobowe.

RODO podobnego obowiązku już nie nakłada, zgodnie z podejściem opartym na ryzyku. Z drugiej strony, RODO wielokrotnie odwołuje się do „polityk ochrony danych" stosowanych przez administratora. Z tego względu zaleca się dalsze stosowanie dokumentacji ochrony danych osobowych, po jej dostosowaniu do przepisów RODO – w szczególności, po uwzględnieniu rejestru czynności przetwarzania danych.

PRAWO DO BYCIA ZAPOMNIANYM

Prawo do bycia zapomnianym można wykonać, jeżeli spełniona jest choć jedna z następujących przesłanek:

a) jeżeli dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane,

b) jeżeli osoba, której dane dotyczą, wycofała zgodę na przetwarzanie danych osobowych i nie istnieje inna podstawa przetwarzania danych,

c) jeżeli osoba, której dane dotyczą, zgłosiła sprzeciw wobec przetwarzania swoich danych w związku ze swoją szczególną sytuacją albo wobec przetwarzania danych dla celów marketingowych,

PRAWO DO PRZENOSZENIA DANYCH

Prawo do przenoszenia danych to prawo do:

a) otrzymania przez osobę, której dane dotyczą, w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, danych osobowych jej dotyczących, które dostarczyła administratorowi,

b) prawo przesłania przez osobę, której dane dotyczą, danych osobowych jej dotyczących, które dostarczyła administratorowi, innemu administratorowi, bez przeszkód ze strony administratora danych.

PRAWO DO PRZENOSZENIA DANYCH

Format danych nadający się do odczytu maszynowego to format pliku zorganizowany tak, aby aplikacje komputerowe mogły łatwo zidentyfikować, rozpoznać i uzyskać określone dane.

Przykład:

– pliki w formacie XML, JSON, CSV.

PROFILOWANIE

Profilowanie to szczególny rodzaj przetwarzania danych osobowych, który:

- odbywa się w sposób automatyczny,
- ma na celu ocenę osoby fizycznej lub przewidywanie jej zachowania.

Przykłady:

- automatyczny dobór reklam na stronie internetowej w oparciu o wcześniejszą aktywność na tej stronie,
- automatyczne obliczenie składki ubezpieczeniowej w oparciu o dane podane na stronie internetowej.

Profilowanie zawsze wymaga poinformowania o tym osób, które są profilowane.

ODWOŁANIE ZGODY

Zgodę na przetwarzanie danych osobowych można zawsze odwołać. Odwołanie zgody powinno być równie łatwe, jak jej udzielenie.

Przykład:

– jeżeli zgody są zbierane przy pomocy dedykowanej strony internetowej, odwołanie zgody powinno być możliwe w ten sam sposób.

Odwołanie zgody wywołuje wyłącznie skutki na przyszłość – oznacza to, że od chwili otrzymania oświadczenia o odwołaniu zgody, nie można już opierać na zgodzie przetwarzania danych; wszystkie te czynności, które opierały się na zgodzie i miały miejsce wcześniej pozostają ważne.

DŁUGOŚĆ PRZECHOWYWANIA DANYCH

Dane osobowe nie powinny być przechowywane w nieskończoność, bez ograniczenia czasowego.

Jeżeli podstawą przetwarzania danych osobowych jest zgoda, wówczas dane osobowe mogą być przetwarzane tak długo, aż zgoda nie zostanie odwołana.

Po odwołaniu zgody, przez okres czasu odpowiadający okresowi przedawnienia roszczeń, jakie może podnosić administrator danych i jakie mogą być podnoszone wobec administratora danych. Obecnie okres ten wynosi 10 lat.

POWIERZENIE PRZETWARZANIA DANYCH

W działalności większości przedsiębiorców dochodzi do powierzenia przetwarzania danych osobowych.

Przykłady:

- korzystanie z usług zewnętrznego podmiotu świadczącego usługi księgowe,
- korzystanie z usług podmiotu zapewniającego usługi poczty elektronicznej,
- zlecenie zewnętrznemu podmiotowi zniszczenia dokumentów zawierających dane osobowe,
- zlecenie zewnętrznemu podmiotowi archiwizacji dokumentów zawierających dane osobowe.

INSPEKTOR OCHRONY DANYCH