PRZEWODNIK PO RODO

DLA MAŁYCH I ŚREDNICH PRZEDSIĘBIORCÓW

Autor: dr Paweł Litwiński

MINISTERSTWO
PRZEDSIĘBIORCZOŚCI
I TECHNOLOGII

Warszawa 2018 r.

PRZEWODNIK PO RODO

DLA MAŁYCH I ŚREDNICH PRZEDSIĘBIORCÓW

MINISTERSTWO
PRZEDSIĘBIORCZOŚCI
I TECHNOLOGII

Warszawa 2018 r.

SPIS TREŚCI

WSTĘP

Dla małych i średnich przedsiębiorców mamy prosty i przyjazny przewodnik. Pomoże sprawnie poruszać się po meandrach nowego prawa ochrony danych osobowych, które będzie obowiązywać już od 25 maja 2018 roku.

Dowiecie się z niego:

- jakie obowiązki będą mieli przedsiębiorcy,
- co zmieni się w sposobie ochrony danych osobowych,
- jak przygotować firmę do stosowania nowych przepisów.

Atutem przewodnika przygotowanego są krótkie podrozdziały, podsumowująca sekcja pytań i odpowiedzi oraz wiele praktycznych przykładów mówiących o tym, jak w praktyce dostosować firmę do nowych przepisów.

Autorem poradnika jest ekspert w tej dziedzinie, dr Paweł Litwiński. Przewodnik nie powinien więc być traktowany jako oficjalna wykładnia Ministerstwa Przedsiębiorczości i Technologii w zakresie przepisów o ochronie danych osobowych.

Podstawowe informacje o RODO

1. Co to jest RODO?

Pisząc i mówiąc „RODO" mamy na myśli 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). Jest to akt prawny przyjęty przez Unię Europejską regulujący zasady ochrony danych osobowych – zastępuje dyrektywę 95/46/WE z 1995 r.

RODO tym się różni od dyrektywy 95/46/WE, że nie będzie implementowane, czyli nie będzie trzeba przepisów RODO przyjąć w polskiej ustawie, jak to się dzieje w przypadku dyrektyw. RODO będzie bezpośrednio obowiązywać, będzie bezpośrednio stosowane i bezpośrednio skuteczne. To oznacza, że – z bardzo niewielkimi wyjątkami – całe prawo ochrony danych osobowych znajdziemy bezpośrednio w tekście RODO. Ten tekst można znaleźć w Dzienniku Urzędowym Unii Europejskiej L z 2016 r. nr 119, str. 1.

RODO zastąpi obowiązującą obecnie ustawę z 29 sierpnia 1997 r. o ochronie danych osobowych.

Materiały:

- oficjalny tekst RODO:
  http://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32016R0679& from=EN

2. Od kiedy będzie się stosować RODO?

RODO będzie stosowane od 25 maja 2018 r. Do tej daty wszystkie te podmioty, które podlegają RODO, powinny być gotowe do stosowania RODO – nie będzie już żadnego dodatkowego okresu przejściowego.

3. Czy będzie polska ustawa o ochronie danych osobowych?

Tak, Ministerstwo Cyfryzacji pracuje nad polskimi przepisami uzupełniającymi RODO. Przepisy te będą regulować m.in.:

- zasady powoływania następy GIODO – Prezesa Urzędu Ochrony Danych Osobowych (PUODO),
- postępowanie przed POUDO,
- procedurę odwoławczą od decyzji PUODO.

W polskich przepisach o ochronie danych osobowych znajdzie się także regulacja tego fragmentu zasad ochrony danych osobowych, który nie został uregulowany w RODO, czyli niektórych zasad przetwarzania danych kadrowych.

Materiały:

- przebieg procesu legislacyjnego można śledzić na stronach Rządowego Centrum Legislacji: https://www.rcl.gov.pl/

4. Czy czekać z wdrożeniem RODO na polskie przepisy o ochronie danych osobowych?

Nie. Całe prawo ochrony danych osobowych znajdziemy bezpośrednio w tekście RODO, za wyjątkiem niektórych kwestii dot. ochrony danych osobowych kadrowych. Nie ma więc sensu czekać z dostosowaniem do RODO na polskie przepisy – proces wdrożenia RODO trzeba rozpocząć natychmiast.

5. Czy w nowych przepisach będzie odpowiednik GIODO?

Planuje się powołanie nowego organu nadzorczego, Prezesa Urzędu Ochrony Danych Osobowych (PUODO). Organ ten przejmie zadania i kompetencje GIODO, a także będzie wykonywał nowe, przyznane mu przez RODO.

6. Kto podlega RODO? Kto powinien wdrożyć RODO?

RODO podlega każdy przedsiębiorca, który prowadzi działalność w Unii Europejskiej. Może to być działalność w jakiejkolwiek formie prawnej: spółka, jednoosobowa działalność gospodarcza, czy nawet oddział w Unii Europejskiej przedsiębiorcy mającego siedzibę poza Unią. Nie ma znaczenia narodowość osób, których dane osobowe są przetwarzane. Nie ma znaczenia to, gdzie są przetwarzane dane osobowe (gdzie znajdują się serwery).

Przykłady:

- korzystanie przez polską spółkę z o. o. z usług przetwarzania danych w chmurze nie zwalnia tej spółki z konieczności stosowania RODO,
- polski podmiot oferujący swoje usługi obywatelom Ukrainy podlega przepisom RODO,
- oddział w Polsce przedsiębiorcy z USA podlega przepisom RODO.

RODO znajdzie zastosowanie nawet wtedy, gdy podmioty spoza Unii Europejskiej oferują swoje towary i usług osobom przebywający w Unii.

RODO nie znajduje zastosowania do działalności osobistej lub domowej. To oznacza, że osoba fizyczna prowadząca działalność gospodarczą musi stosować RODO do danych osobowych swoich klientów, czy pracowników, ale nie stosuje RODO do danych przetwarzanych w celach czysto prywatnych, np. do danych adresatów wysyłanych corocznie kartek świątecznych.

Podstawa prawna – art. 3 RODO.

7. Jakie czynności podlegają RODO?

RODO stosuje się do przetwarzania danych osobowych. Przetwarzaniem danych osobowych są jakiekolwiek operacje wykonywane na danych osobowych, takie jak:

- zbieranie danych,
- przechowywanie danych,
- usuwanie danych,
- opracowywanie danych,
- udostępnianie danych.

Co bardzo ważne, RODO obejmuje wszelkie czynności, które mają za przedmiot dane osobowe – czyli nie tylko np. usługę archiwizowania dokumentów, ale wszelkie usługi, w których dochodzi do zbierania danych osobowych. RODO powinni więc stosować:

- przedsiębiorcy zajmujący się przetwarzaniem danych – archiwizowanie danych, niszczenie dokumentów, usługi kurierskie itp.,
- przedsiębiorcy, którzy przetwarzają dane osobowe przy okazji świadczenia innych usług, np. pośrednicy ubezpieczeniowi, agenci biur podróży, księgowi, sklepy internetowe, zarządcy nieruchomości itp.

Podstawa prawna – art. 3, 4 pkt 2 RODO.

8. Co to są dane osobowe?

Dane osobowe to wszelkie informacje odnoszące się do zidentyfikowanej lub możliwej do zidentyfikowania osobie 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.

Przykłady:

- osoba zidentyfikowana: pracownik, którego dane osobowe przetwarza pracodawca; klient sklepu internetowego, który podał swoje dane osobowe do wysyłki zamówienia; osoba, która w formularzu kontaktowym podaje swoje imię, nazwisko i adres e-mail,
- osoba możliwa do zidentyfikowania: potencjalny kontrahent, którego posiadamy tylko numer ewidencyjny w CEIDG; nadawca listu poleconego na podstawie numeru przesyłki;

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

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

Wyróżnia się dwie kategorie danych osobowych:

a) tzw. dane osobowe zwykłe,
b) dane osobowe zaliczające się do szczególnych kategorii danych (dawniej zwane danymi wrażliwymi).

Do szczególnych kategorii danych osobowych zaliczamy dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej. Dane osobowe, które nie należą do żadnej z tych kategorii, to dane zwykłe. Zgodnie z RODO, do kategorii danych osobowych zwykłych należą także dane osobowe dotyczące wyroków skazujących.

Podstawa prawna – art. 4 pkt 1, art. 9 i 10 RODO.

9. Kto może przetwarzać dane osobowe?

Przetwarzanie danych osobowych to bardzo ogólne sformułowanie, oznaczające jakiekolwiek operacje wykonywane na danych osobowych, takie jak:

- zbieranie danych,
- przechowywanie danych,
- usuwanie danych,
- opracowywanie danych,
- udostępnianie danych.

Jeżeli jakiś przedsiębiorca przetwarza dane osobowe, to może to robić jako jeden z dwóch kategorii podmiotów:

- administrator danych,
- podmiot przetwarzający dane.

Administrator danych to taki podmiot, który decyduje o celach i sposobach przetwarzania danych. Innymi słowy, decyduje o tym, po co (cele) i jak (sposoby) wykorzystać dane osobowe. Przykłady:

- pracodawca w stosunku do danych osobowych swoich pracowników,
- sprzedawca w sklepie internetowym w stosunku do danych osobowych swoich klientów,
- właściciel strony internetowej w stosunku do danych osobowych osób, które zaprenumerowały newsletter.

Administratorem danych jest zawsze określony podmiot – np. spółka, a nie jego pracownik. Przykłady:

- administratorem danych jest spółka z o.o., a nie jej prezes zarządu, czy dyrektor marketingu,
- administratorem danych jest Jan Kowalski prowadzący jednoosobową działalność gospodarczą.

Podmiot przetwarzający dane osobowe nie decyduje o celach i środkach przetwarzania danych – działa na podstawie umowy z administratorem danych. Administrator danych może bowiem albo sam przetwarzać dane, albo skorzystać z usług zewnętrznego podmiotu, który te dane będzie przetwarzał dla niego. Przykłady:

- biuro rachunkowe przetwarza na zlecenie dane osobowe przekazane mu w tym celu przez klientów,
- podmiot utrzymujący na zlecenie swoich klientów konta poczty elektronicznej przetwarza na zlecenie dane osobowe,
- podmiot zajmujący się profesjonalnie niszczeniem danych osobowych przetwarza w tym zakresie dane osobowe na zlecenie swoich klientów.

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.

Podstawa prawna – art. 4 pkt 7 i 8 RODO.

Zbieranie danych osobowych.

1. 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 z osobą, której dane dotyczą lub do podjęcia działań poprzedzających zawarcie umowy, na żądanie tej osoby,
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.

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.

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

Podstawa prawna – art. 6 i 9 RODO.

2. Jak wiele danych osobowych można zbierać zgodnie z RODO?

RODO wprowadza tzw. zasadę minimalizacji danych osobowych. Zgodnie z nią, można przetwarzać wyłącznie takie dane osobowe, które są niezbędne do osiągnięcia celu przetwarzania danych. Przetwarzanie danych powinno więc 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.

Podstawa prawna – art. 5 ust. 1 pkt c) RODO.

3. Jak zbierać zgodę na przetwarzanie danych osobowych?

Każda zgoda na przetwarzanie danych powinna charakteryzować się następującymi cechami:

a) dobrowolność – zgoda może być ważna tylko jeżeli osoba, której dane dotyczą, ma możliwość dokonania rzeczywistego wyboru, przy czym nie zachodzi ryzyko wprowadzenia w błąd, zastraszenia, przymusu lub znaczących negatywnych konsekwencji, jeśli nie wyrazi zgody. Jeżeli konsekwencje wyrażenia zgody nie dają się pogodzić ze swobodą wyboru, zgoda nie jest dobrowolna (Opinia WP 187 w sprawie definicji zgody),
b) konkretność – aby zgoda była ważna, musi być konkretna. Innymi słowy, niedopuszczalna jest ogólna zgoda bez określenia dokładnego celu przetwarzania (Opinia WP 187 w sprawie definicji zgody),
c) świadomość – zgoda na przetwarzanie danych osobowych na podstawie art. 23 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych nie może mieć charakteru abstrakcyjnego, lecz winna odnosić się do skonkretyzowanego stanu faktycznego, obejmując tylko określone dane oraz sprecyzowany sposób i cel ich przetwarzania (zob. wyrok NSA z 11.04.2003 r., II SA 3942/02),
d) jednoznaczność – zgoda musi mieć charakter wyraźny, a jej wszystkie aspekty muszą być jasne dla podpisującego w momencie jej wyrażania (zob. wyrok NSA z 4.4.2003 r., II SA 2135/02).

Zgoda może zostać wyrażona w dowolnej formie – ale zawsze w razie wątpliwości to administrator danych powinien wykazać, że zgoda została udzielona. Decyzja o tym, jaki konkretnie sposób zbierania – i archiwizowania – zgód zastosować powinna być podjęta świadomie przez administratora danych.

Podstawa prawna – art. 6 RODO.

4. Jakie informacje przekazywać przy zbieraniu zgody na przetwarzanie danych osobowych?

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

- o tożsamości administratora danych i o jego danych kontaktowych,
- jeżeli administrator danych powołał Inspektora Ochrony Danych (IOD) – o danych kontaktowych IOD,
- o celach i podstawie przetwarzania danych, a jeżeli przetwarzanie odbywa się na tej podstawie, że jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią – o tych prawnie uzasadnionych interesach,
- o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją
- gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego,
- o okresie czasu, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
- 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, a także 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,

- o tym, 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,
- jeżeli dochodzi do tzw. zautomatyzowanego podejmowania decyzji lub profilowania – należy poinformować o tym fakcie oraz podać istotne informacje o zasadach automatycznego podejmowania decyzji, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Co bardzo istotne, odbiorcy danych to także podmioty przetwarzające dane osobowe na zlecenie administratora danych. Stąd konieczność poinformowania o tych podmiotach.

Te – bardzo rozbudowane – obowiązki informacyjne w przypadku zgody na przetwarzanie danych osobowych przybierają najczęściej postać tzw. klauzuli zgody na przetwarzanie danych. Przykładowo, klauzula zgodna z RODO może otrzymać następujące brzmienie:

Zgadzam się na przetwarzanie moich danych osobowych przez spółkę XYZ sp. z o. o. z siedzibą w ……., ul. ……., w celu ……. [np. marketingowym].
Podanie danych jest dobrowolne. Podstawą przetwarzania danych jest moja zgoda. Odbiorcami danych mogą być …….. [np. podmioty zajmujące się obsługą informatyczną administratora danych]. Mam prawo wycofania zgody w dowolnym momencie. Dane osobowe będą przetwarzane …….. [np. do ew. odwołania zgody, a po takim odwołaniu, przez okres przedawnienia roszczeń przysługujących administratorowi danych i w stosunku do niego].
Mam prawo żądania od administratora dostępu do moich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania [o prawie do przenoszenia danych, jeżeli przysługuje], a także prawo wniesienia skargi do organu nadzorczego.
[jeżeli dochodzi do profilowania, wówczas informacje dotyczące profilowania].
W przypadku pytań dotyczących przetwarzania danych osobowych prosimy o kontakt z Inspektorem Ochrony Danych pod adresem ……. [jeżeli został wyznaczony]

Co istotne, obowiązki informacyjne należy wykonywać w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.

Zgodnie z propozycją Ministerstwa Cyfryzacji, te rozbudowane obowiązki informacyjne mają zostać wyłączone w stosunku do przedsiębiorców zatrudniających mniej niż 250 osób, przetwarzających dane osobowe niezbędne do wykonywania działalności gospodarczej, w szczególności w celu zawierania umów i prowadzenia rachunkowości.

Podstawa prawna – art. 6, art. 12 i 13 RODO.

Materiały:

- przebieg procesu legislacyjnego można śledzić na stronach Rządowego Centrum Legislacji: https://www.rcl.gov.pl/

5. Kiedy nie trzeba zbierać zgody na przetwarzanie danych?

Zgoda na przetwarzanie danych jest jedną z podstaw prawnych przetwarzania danych – nie jedyną. Zgody na przetwarzanie danych nie trzeba zbierać w szczególności wtedy, gdy:

a) przetwarzanie danych jest niezbędne do wykonania umowy – np. sklep internetowy sprzedaje wysyłkowo książki; nie musi w takim wypadku prosić o zgodę na przetwarzanie danych, przetwarzanie danych będzie zgodne z RODO jako niezbędne do wykonania umowy (sprzedaży),
b) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze – np. przetwarzanie danych w celach związanych z prowadzeniem ksiąg rachunkowych nie wymaga zgody osób, których dane dotyczą, a jego podstawą są przepisy o rachunkowości,
c) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią – np. skierowanie do sądu pozwu o zapłatę przeciwko nieuczciwemu klientowi nie wymaga jego zgody na przetwarzanie danych, a podstawą przetwarzania danych w takim wypadku jest właśnie realizacja prawnie uzasadnionego interesu administratora danych.

Prawnie uzasadnionym interesem realizowanym przez administratora danych jest także marketing jego produktów i usług. Przetwarzanie danych w takim celu – marketingowym w stosunku do produktów i usług administratora danych – nie wymaga zgody na przetwarzanie danych osobowych. Ale uwaga – pewne formy kontaktu z osobami, których dane dotyczą, wymagają zgody. Zgody wymaga:

a) przesyłanie informacji handlowej za pomocą środków komunikacji elektronicznej, np. reklam za pomocą poczty elektronicznej,

b) wykorzystanie telekomunikacyjnych urządzeń końcowych w celu marketingu bezpośredniego, np. wysyłanie wiadomości SMS o treści reklamowej.

Podstawa prawna:

- art. 6, art. 12 i 13 RODO,
- art. 10 ustawy o świadczeniu usług drogą elektroniczną,
- art. 172 ustawy Prawo telekomunikacyjne.

6. Przetwarzanie szczególnych kategorii danych osobowych

RODO – inaczej, niż to ma miejsce na gruncie ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych – nie wymaga, aby zgoda na przetwarzanie danych zaliczonych do szczególnych kategorii danych osobowych była wyrażona na piśmie. Na gruncie RODO taka zgoda powinna być zgodą „wyraźną" – oznacza to, że zgoda może zostać udzielona np. w Internecie, poprzez zaznaczenie odpowiedniego pola wyboru. Oczywiście zbieranie zgód na piśmie w dalszym ciągu będzie dopuszczalne.

7. Czym jest 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.

Profilowanie najczęściej jest wykorzystywane jako narzędzie dla tzw. automatycznego podejmowania decyzji wobec osób, których dane dotyczą. Te decyzje to właśnie wyświetlenie konkretnej reklamy w oparciu o profil, czy obliczenie wysokości składki ubezpieczeniowej. Jeżeli jednak to automatyczne podejmowanie decyzji wywołuje skutki prawne wobec osób, których dane dotyczą, lub w podobny istotny sposób wpływa na te osoby, można taki mechanizm stosować wyłącznie wtedy, gdy spełniony jest jeden z następujących warunków:

- osoba profilowana wyrazi na to wyraźną zgodę,
- profilowanie jest niezbędne do zawarcia lub wykonywania umowy z tą osobą,
- profilowanie jest dopuszczalne przez szczególne przepisy prawa.

Przykłady:

- automatyczny dobór reklam na stronie internetowej w oparciu o wcześniejszą aktywność na tej stronie w większości przypadków nie wywołuje skutków prawnych wobec osób, których dane dotyczą, ani też nie wpływa na te osoby w podobny istotny sposób,
- automatyczne odrzucenie wniosku kredytowego złożonego za pośrednictwem strony internetowej wyłącznie w oparciu o automatyczne przetwarzanie danych wywołuje skutki prawne wobec osoby, której dane dotyczą, ponieważ wprost pozbawia ją możliwości zawarcia umowy kredytu.

Jeżeli profilowanie miałoby się odbywać w oparciu o szczególne kategorie danych osobowych, wówczas jedyną podstawą prawną, która mogłaby takie profilowanie zalegalizować, może być szczególny przepis prawa.

8. Czy można odwołać zgodę na przetwarzanie danych?

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.

Podstawa prawna – art. 7 ust. 3 RODO.

9. Jak długo mogę przechowywać dane osobowe?

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.

Jeżeli podstawą przetwarzania danych jest wykonywanie umowy, wówczas dane mogą być przetwarzane tak długo, jak jest to niezbędne do wykonania umowy, a po tym czasie przez okres czasu odpowiadający okresowi przedawnienia roszczeń, jakie może podnosić administrator danych i jakie mogą być podnoszone wobec administratora danych. W przypadku przedsiębiorców ten okres czasu co do zasady wynosi nie dłużej, niż 3 lata i różni się w zależności od tego, jakiej umowy dotyczyło przetwarzanie danych.

Jeżeli istnieją przepisy szczególne określające czas, przez jaki powinny być przechowywane dane osobowe, wówczas takie przepisy mogą wydłużać (lub w konkretnym przypadku skracać) czas przetwarzania danych osobowych.

Przykład – przepisy o rachunkowości nakazują przechowywać dowody księgowe umów handlowych, roszczeń dochodzonych w postępowaniu cywilnym lub objętych postępowaniem karnym albo podatkowym przez 5 lat od początku roku następującego po roku obrotowym, w którym operacje, transakcje, postępowanie zostały ostatecznie zakończone, spłacone, rozliczone lub przedawnione.

Podstawa prawna – art. 5 ust. 1 pkt e) RODO.

Organizacja przetwarzania danych

1. Jak należy zabezpieczać dane osobowe?

RODO odchodzi od praktyki polegającej na wskazywaniu w przepisach prawa konkretnych środków zabezpieczenia danych osobowych, jakie mają zostać wdrożone przez administratora lub podmiot przetwarzający. Zamiast tego, 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. Dobór środków zabezpieczenia powinien być oparty o:

a) charakter, zakres, kontekst i cele przetwarzania,
b) ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia,
c) stan wiedzy technicznej,
d) koszt wdrażania.

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.

Przykład – archiwizowanie danych osobowych przez specjalistyczny podmiot:

- zakres danych: ryzyko wzrasta, gdy archiwizowana jest systematycznie cała dokumentacja medyczna szpitala, a maleje, gdy archiwizowane są księgi rachunkowe księgarni internetowej,
- cele przetwarzania: ryzyko wzrasta, gdy dane są przetwarzane przez ich przechowywanie przez 50 lat, a maleje, gdy są przetwarzane wyłącznie w celu zniszczenia danych,
- ryzyko wzrasta, gdy dane są przetwarzane na zewnętrznych serwerach, z którymi komunikacja odbywa się w sposób nieszyfrowany z wykorzystaniem sieci publicznych, a maleje, gdy dane są przetwarzane na własnych serwerach.

RODO nie nakazuje stosowania żadnych konkretnych środków zabezpieczenia danych. RODO wskazuje tylko przykładowe środki techniczne i organizacyjne, które mogą służyć osiągnięciu tego celu, tj. zapewnienia stopnia bezpieczeństwa odpowiadającego ryzyku. Są nimi w szczególności:

- pseudonimizacja i szyfrowanie danych osobowych;
- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i 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.

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.

Podstawa prawna – art. 32 RODO.

Materiały:
- Jak rozumieć i stosować podejście oparte na ryzyku? – poradnik GIODO, http://www.giodo.gov.pl/pl/1520282/10294

2. Co się stanie z istniejącą dokumentacją ochrony danych osobowych?

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

3. Obowiązek rejestrowania czynności przetwarzania danych

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. Administrator danych odnotowuje w rejestrze:

a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz IOD,
g) cele przetwarzania,
c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,
d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione,
e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego,
f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa danych.

Podmiot przetwarzający natomiast odnotowuje w rejestrze:

a) imię i nazwisko lub nazwę oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający,
b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów,
c) gdy ma to zastosowanie – przekazania danych osobowych do państwa trzeciego,
d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa danych.

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.

Przykłady:

- przedsiębiorcy zatrudniający mniej niż 250 osób muszą prowadzić rejestr w odniesieniu do danych osobowych kadrowych – takie przetwarzanie nie ma charakteru sporadycznego i obejmuje szczególne kategorie danych osobowych,
- przedsiębiorca zatrudniający mniej niż 250 osób, który będzie jednorazowo przetwarzał dane osobowe nie obejmujące szczególnych kategorii danych, np. w celu organizacji eventu promocyjnego, będzie w odniesieniu do takiego procesu przetwarzania danych zwolniony z obowiązku prowadzenia rejestru.

4. Co to jest obowiązek uwzględniania ochrony danych w fazie projektowania?

Obowiązek uwzględniania ochrony danych osobowych w fazie projektowania to rodzaj podejścia do ochrony danych osobowych, które jest promowane w przepisach RODO. Ta filozofia opiera się na takich konkretnych rozwiązaniach, jak:

- proaktywne podejście do ochrony danych osobowych,
- konieczność włączania ochrony prywatności w projekty od początku ich realizacji,
- poszanowanie dla prywatności użytkowników.

W rezultacie, zasady prywatności w fazie projektowania powinny prowadzić do uczynienia prywatności domyślnym sposobem działania w organizacji przy jednoczesnym utrzymaniu pełnej funkcjonalności.

Podstawa prawna – art. 25 RODO.

5. Czym jest domyślna ochrona danych?

W rezultacie zastosowania zasady uwzględniania ochrony danych w fazie projektowania powinno być doprowadzenie do sytuacji, w której domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania.

Przykład – domyślne wyłączenie wszelkich funkcji gromadzenia danych o użytkowniku przez aplikację mobilną i konieczność ich aktywnego i świadomego uruchomienia przez użytkownika.

Podstawa prawna – art. 25 RODO.

6. Kiedy należy wyznaczyć Inspektora Ochrony Danych?

Inspektor Ochrony Danych (IOD) to następca Administratora Bezpieczeństwa Informacji (ABI). Inaczej niż w przypadku ABI, wyznaczenie IOD w pewnych przypadkach jest obowiązkowe na gruncie RODO:

a) gdy dane są przetwarzane przez podmioty z sektora publicznego,
b) gdy główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę,
c) gdy główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących.

Główną działalnością będzie działalność kluczowa z punktu widzenia osiągnięcia celów administratora albo podmiotu przetwarzającego dane. Nie każdy podmiot, którego główną działalnością jest przetwarzanie danych, musi jednak powołać IOD – a tylko taki, którego działalność polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę.

Przykład – działalnością główną podmiotu zajmującego się profesjonalnym niszczeniem danych osobowych jest przetwarzanie danych osobowych, jednak podmiot ten nie ma obowiązku powołania IOD, ponieważ ta działalność nie wymaga regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę.

Działalność główną należy rozumieć włączając w to działalność nierozerwalnie związaną z działalnością główną.

Przykład – szpital powinien powołać IOD, choć jego główną działalnością jest leczenie, a przetwarzanie danych działalnością nierozerwalnie związaną z taką działalnością główną.

Nie jest możliwe wskazanie konkretnej wartości, czy to rozmiaru zbioru danych, czy liczby osób, których dane dotyczą, która determinowałaby dużą skalę. Zaleca się jednak, aby za przetwarzanie na dużą skalę uznawać np.:

- przetwarzanie danych pacjentów przez szpital w ramach prowadzonej działalności,
- przetwarzanie danych klientów przez banki albo ubezpieczycieli w ramach prowadzonej działalności,
- przetwarzanie danych do celów reklamy behawioralnej przez wyszukiwarki.

Jednocześnie przywołuje się następujące przykłady przetwarzania danych niemieszczącego się w zakresie dużej skali:

- przetwarzanie danych pacjentów, dokonywane przez pojedynczego lekarza,
- przetwarzanie danych dotyczących wyroków skazujących lub naruszeń prawa przez adwokata lub radcę prawnego.

Podstawa prawna – art. 37 RODO.

Materiały:
- Wytyczne dotyczące inspektorów ochrony danych (WP 243), http://www.giodo.gov.pl/1520282/id_art/9740/j/pl

7. Co to jest ocena skutków dla ochrony danych osobowych i kiedy należy ją przeprowadzić?

RODO odchodzi od obowiązku rejestracji zbiorów danych osobowych w GIODO – po 25 maja 2018 r. zbiory danych osobowych nie będą podlegały rejestracji, a rejestr zbiorów danych zostanie zlikwidowany. Zamiast tego jednak, RODO wprowadza procedurę tzw. oceny skutków dla ochrony danych.

Ocena skutków dla ochrony danych to proces mający opisać przetwarzanie, ocenić niezbędność i proporcjonalność przetwarzania oraz pomóc w zarządzaniu ryzykiem naruszenia praw lub wolności osób fizycznych wynikającym z przetwarzania danych osobowych (oceniając ryzyko i ustalając środki mające mu zaradzić). Oceny skutków dla ochrony danych to narzędzia istotne dla celów rozliczalności, ponieważ pomagają administratorom nie tylko w przestrzeganiu wymogów RODO, ale również w wykazaniu, że podjęto odpowiednie środki w celu zapewnienia zgodności z rozporządzeniem. Innymi słowy, ocena skutków dla ochrony danych to proces służący do zapewnienia i wykazania zgodności przetwarzania danych z RODO.

Ocena skutków dla ochrony danych osobowych jest obowiązkowa, jeżeli dany rodzaj przetwarzania danych, 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. W przepisach RODO wskazano trzy przypadki, gdy przeprowadzenie oceny z pewnością będzie wymagane – będzie tak, jeżeli dochodzi do:

a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną,
b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących, lub
c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

Stosowanie monitoringu miejsc publicznie dostępnych powoduje, że przeprowadzenie oceny skutków dla ochrony danych staje się obowiązkowe. Podobnie w przypadku stosowania profilowania. Duża skala powinna być natomiast rozumiana w sposób analogiczny do przypadków obowiązkowego powołania IOD.

Przykłady – przeprowadzenie oceny skutków dla ochrony danych jest wymagane, jeżeli:

- przedsiębiorca oferuje swoim klientom system monitoringu wizyjnego obejmujący też miejsca publicznie dostępne, bądź sam stosuje taki system,
- przedsiębiorca świadczy usługi przetwarzania danych osobowych zawartych w dokumentacji medycznej,
- przedsiębiorca świadczy swoim klientom usługi profilowania klientów w sklepach internetowych, czy na portalach internetowych.

Ocena skutków dla ochrony danych osobowych może być przeprowadzana według różnych metodyk i na różne sposoby. W przepisach RODO wskazano wyłącznie obowiązkowe elementy takiej oceny:

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

Zaleca się sporządzanie oceny w taki sposób, żeby w razie konieczności można było przedstawić ją organowi nadzorczemu.

Podstawa prawna – art. 35 RODO.

Materiały:
- Wytyczne dotyczące oceny skutków dla ochrony danych (WP 248), http://www.giodo.gov.pl/pl/1520285/10078

8. Czym są uprzednie konsultacje z organem nadzorczym?

Jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator danych nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym. Uprzednie konsultacje są więc rodzajem postępowania administracyjnego, które należy wszcząć z w oparciu o wynik oceny skutków dla ochrony danych.

W wyniku przeprowadzonego postepowania, organ nadzorczy (PUODO) może wydać zalecenia, które ich adresat powinien wdrożyć.

Podstawa prawna – art. 36 RODO.

9. Co to jest obowiązek zgłaszania naruszeń ochrony danych?

RODO nakłada na podmioty przetwarzające dane osobowe prawny obowiązek informowania o incydentach bezpieczeństwa dotyczących danych osobowych. Jest to bardzo istotna zmiana w stosunku do ustawy z 29 sierpnia 1997 r., która tego rodzaju rozwiązania w ogóle nie zawierała.

Incydent bezpieczeństwa zwany jest w przepisach RODO naruszeniem ochrony danych osobowych i może polegać na:

a) naruszeniu bezpieczeństwa prowadzącym do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania danych osobowych
b) naruszeniu bezpieczeństwa prowadzącym do nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Przykłady:

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

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.

Przykłady:

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

W pewnych przypadkach zawiadamianie osób, których dane dotyczą, nie będzie jednak wymagane. Będzie tak w szczególności wtedy, gdy zostały wdrożone odpowiednie środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie danych.

Zgodnie z propozycją Ministerstwa Cyfryzacji, obowiązki związane ze zgłaszaniem incydentów mają zostać wyłączone w stosunku do przedsiębiorców zatrudniających mniej niż 250 osób, przetwarzających dane osobowe niezbędne do wykonywania działalności gospodarczej, w szczególności w celu zawierania umów i prowadzenia rachunkowości.

Podstawa prawna – art. 34 RODO.

10. Jak zawrzeć umowę powierzenia 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.

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

W stosunku do ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych, RODO wprowadza nowe – znacznie rozbudowane – wymagania co do treści umowy powierzenia. Są to zobowiązania podmiotu przetwarzającego do:

a) przetwarzania danych wyłącznie na udokumentowane polecenie administratora,
b) zapewniania, aby osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,
c) podejmowania środków zabezpieczenia danych wymaganych przez RODO i pomagania administratorowi wywiązać się z tych obowiązków,
d) przestrzegania warunków korzystania z usług innego podmiotu przetwarzającego – tzw. podpowierzenie przetwarzania danych jest dopuszczalne wyłącznie za zgodą administratora danych,
e) pomagania administratorowi wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w RODO,
f) usunięcia danych lub do zwrotu danych administratorowi danych po zakończeniu przetwarzania, zgodnie z decyzją administratora,
g) udostępnia administratorowi wszelkich informacji niezbędnych do wykazania spełnienia jego obowiązków oraz do umożliwiania administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów.

Umowa powierzenia może zostać zawarta w formie pisemnej oraz w formie elektronicznej, pod warunkiem zapewnienia integralności i autentyczności dokumentu w postaci elektronicznej.

Tym, co istotnie różni zasady powierzania przetwarzania danych w RODO od ustawy z 29 sierpnia, jest prawny obowiązek wyboru takiego podmiotu przetwarzającego, który gwarantuje odpowiednią ochronę danych osobowych. Administrator danych może mieć praktyczną trudność w wyborze takiego podmiotu – zwłaszcza, gdy sam administrator jest podmiotem niewielkim, a przetwarzanie danych ma się odbywać przez renomowanych dostawców. Z pomocą przychodzi w tym przypadku tzw. procedura certyfikacji podmiotów przetwarzających dane osobowe. Certyfikaty wydawane będą po to, żeby zaświadczyć o zgodności przetwarzania danych przez certyfikowany podmiot. Będzie to więc wskazówka dla tych, którzy poszukują odpowiedniego podmiotu przetwarzającego dane osobowe – wybór podmiotów posiadających certyfikat.

Podstawa prawna – art. 28, art. 42 RODO.

Prawo do bycia zapomnianym i prawo do przenoszenia danych

1. Prawo do bycia zapomnianym

Prawo do bycia zapomnianym jest jednym z nowych uprawnień przyznanych przez RODO osobom, których dane dotyczą. Prawo to składa się z dwóch uprawnień:

a) możliwości żądania przez osobę, której dane dotyczą, usunięcia jej danych osobowych przez administratora danych,
b) możliwości żądania, aby administrator danych poinformował innych administratorów danych, którym upublicznił dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych lub ich kopie .

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,
d) jeżeli dane osobowe były przetwarzane „niezgodnie z prawem”,
e) jeżeli dane osobowe „muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator”,
f) jeżeli dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego bezpośrednio dziecku.

W praktyce najważniejszym z tych przypadków będzie sytuacja, w której osoba, której dane dotyczą, wycofuje udzieloną zgodę bądź zgłasza sprzeciw.

Przykład – administrator danych osobowych przetwarza na podstawie zgody dane osobowe w celu marketingowym. Osoba, której dane dotyczą, wycofuje zgodę oraz korzysta z prawa do bycia zapomnianym.

W przypadku wykonania prawa do bycia zapomnianym, administrator danych powinien zaprzestać przetwarzania danych osobowych i usunąć dane, chyba że zachodzą szczególne przypadki ograniczające prawo do bycia zapomnianym. Wśród nich na szczególną uwagę zasługują:

a) istnienie przepisu prawa, który nakazuje przetwarzanie danych osobowych,
b) sytuacja, w której przetwarzanie danych jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń.

Przykład – klient sklepu internetowego zamówił książkę, którą otrzymał, ale za którą nie zapłacił. Następnie postanawia wykonać prawo do bycia zapomnianym – administrator danych może jednak jego dane nadal przetwarzać, ponieważ jest mu to niezbędne do dochodzenia swoich praw przed sądem.

Przykład – klient sklepu internetowego zamówił książkę, którą otrzymał i za którą zapłacił. Następnie postanawia wykonać prawo do bycia zapomnianym – administrator danych może jednak jego dane nadal przetwarzać, ponieważ obowiązek przetwarzania danych wynika z przepisów o rachunkowości.

W przypadku wykonania prawa do bycia zapomnianym, administrator danych powinien także poinformować innych administratorów danych, którym upublicznił dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje. Obowiązek ten jednak nie ma charakteru nieograniczonego – może być ograniczony przez:

a) dostępną technologię,
b) koszty,
c) konieczność ograniczenia do „rozsądnych działań".

Ograniczenie zakresu obowiązku przy użyciu kryterium kosztów powoduje, że podmioty większe, o większych możliwościach finansowych, będą zobowiązane do wykonywania tego obowiązku w szerszym zakresie niż podmioty niewielkie, mające mniejsze dostępne zasoby finansowe. Z kolei poprzez przywołanie „rozsądnych działań" ograniczono charakter obowiązku w ten sposób, że nie ma on charakteru zobowiązania rezultatu, a wyłącznie starannego działania.

Podstawa prawna – art. 17 RODO.

2. 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 może być wykonane wyłącznie wtedy, gdy:

a) przetwarzanie danych odbywa się na podstawie zgody lub w celu wykonania umowy oraz
b) przetwarzanie danych odbywa się w sposób zautomatyzowany.

Prawo do przenoszenia danych obejmuje tylko dane osobowe przetwarzane przy użyciu systemów informatycznych i nie obejmuje tradycyjnych, papierowych zbiorów danych.

Prawo do przenoszenia danych obejmuje dane osobowe dotyczące osoby, która wykonuje to prawo i które to dane ta osoba dostarczyła administratorowi. W pewnych przypadkach dane objęte prawem do przeniesienia będą jednak obejmować także dane innych osób.

Przykład – rejestry połączeń telefonicznych, historia konta bankowego.

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.

Podstawa prawna – art. 20 RODO.

Materiały – Wytyczne dotyczące prawa do przenoszenia danych (WP 242),
http://www.giodo.gov.pl/1520282/id_art/9741/j/pl

WDROŻENIE RODO

Etapy procesu wdrażania RODO w organizacji

1. Identyfikacja procesów przetwarzania danych osobowych

RODO odchodzi od podejścia opartego o kategorię zbiorów danych, do którego przyzwyczaiła nas ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych, na rzecz podejścia opartego o procesy przetwarzania danych osobowych. W pewnym uproszczeniu, proces przetwarzania danych osobowych można opisać jako ciąg następujących po sobie czynności począwszy od zebrania danych osobowych, aż do ich usunięcia.

Z tego względu, punktem wyjścia dla wdrożenia RODO w organizacji powinna być identyfikacja istniejących procesów przetwarzania danych.

Przykłady:

- w każdej organizacji – proces przetwarzania danych kadrowo – płacowych,
- w sklepie internetowym – proces przetwarzania danych związanych z transakcjami sprzedaży,
- w podmiocie zajmującym się niszczeniem danych – proces przetwarzania danych niszczonych na zlecenie klientów.

Należy także zidentyfikować te procesy, w których dochodzi do powierzenia przetwarzania danych osobowych:

a) w których podmiot wdrażający RODO jest administratorem powierzającym przetwarzanie

Przykłady:

- powierzenie przez przedsiębiorcę zewnętrznemu podmiotowi prowadzenia księgowości,
- powierzenie przez przedsiębiorcę zewnętrznemu podmiotowi obsługi kadrowo – płacowej

b) w których podmiot wdrażający RODO jest podmiotem przetwarzającym dane na zlecenie administratora.

Przykłady:

- świadczenie przez przedsiębiorcę usług archiwizacji danych osobowych,
- świadczenie przez przedsiębiorcę usług księgowych

Każdy proces przetwarzania danych osobowych powinien zostać opisany przy użyciu jak największej ilości zmiennych, aby w możliwie dokładny sposób oddać jego specyfikę.

2. Weryfikacja podstawowych parametrów procesów przetwarzania danych

Dla każdego zidentyfikowanego procesu przetwarzania danych należy co najmniej:

- określić podstawę przetwarzania danych osobowych zgodną z RODO,
- zweryfikować zakres przetwarzanych danych, zgodnie z zasadą minimalizacji,
- zweryfikować treść obowiązków informacyjnych towarzyszących gromadzeniu danych.

W przypadku, gdy przetwarzanie danych opiera się o zgody zebrane przed 25 maja 2018 r. należy zweryfikować, czy takie zgody pozostaną nadal ważne. W tym celu należy ocenić, czy zgody odpowiadają wymogom sformułowanym przez RODO w stosunku do zgody na przetwarzanie danych.

Materiały – Stanowisko GIODO dotyczące ważności zgód na przetwarzanie danych osobowych,
http://giodo.gov.pl/pl/1520281/10303

3. Wdrożenie podejścia opartego na ryzyku

Dla wszystkich procesów przetwarzania danych osobowych należy określić poziom ryzyka związanego z przetwarzaniem danych osobowych i wdrożyć odpowiednie środki zabezpieczenia danych.

Podejście oparte na ryzyku wymaga ciągłego monitorowania poziomu ryzyka związanego z przetwarzaniem danych osobowych. Nie jest więc wystarczającym jednorazowe dla danego procesu określenie poziomu ryzyka i zastosowanie środków zabezpieczenia danych – poziom ryzyka powinien być monitorowany ciągle w ramach trwających procesów przetwarzania danych.

Materiały – Jak rozumieć i stosować podejście oparte na ryzyku? – poradnik GIODO,
http://www.giodo.gov.pl/pl/1520282/10294

4. Przeprowadzenie procedury oceny skutków dla ochrony danych

Wykonanie oceny skutków dla ochrony danych osobowych może być obowiązkowe wyłącznie dla procesów przetwarzania danych, które rozpoczynają się po 25 maja 2018 r. Natomiast dla tych procesów, które w dniu rozpoczęcia stosowania RODO są w toku, przeprowadzenie oceny co do zasady nie jest obowiązkowe. Jeżeli jednak zmieni się poziom ryzyka związanego z przetwarzaniem danych w procesach będących w toku, wówczas przeprowadzenie oceny może stać się obowiązkowe na zasadach ogólnych. Dlatego rekomenduje się przeprowadzenie – w miarę możliwości – oceny skutków dla ochrony danych także dla procesów, które w dniu 25 maja 2018 r. są już w toku.

5. Powierzenie przetwarzania danych

Prawidłowe wdrożenie RODO wymaga zidentyfikowania tych wszystkich procesów przetwarzania danych, w których dochodzi do powierzenia przetwarzania danych.

RODO, w odróżnieniu od ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych, nakłada na administratora danych prawny obowiązek wyboru takiego podmiotu przetwarzającego, który zapewnia przestrzeganie RODO. Stąd w sytuacji, gdy podmiot wdrażający RODO jest administratorem powierzającym przetwarzanie danych, powinien on dla każdego podmiotu przetwarzającego dokonać sprawdzenia przestrzegania przez niego postanowień RODO i gotowości do wdrożenia RODO. Jeżeli natomiast podmiot wdrażający RODO jest podmiotem przetwarzającym dane na zlecenie administratora, wówczas powinien on być gotowy na takie sprawdzenia ze strony administratora danych.

Niezależnie od kwestii wyboru podmiotu przetwarzającego, każda umowa powierzenia powinna zostać dostosowana do nowych wymagań treściowych określonych w RODO.

6. Nowe prawa osób, których dane dotyczą

Należy wdrożyć rozwiązania umożliwiające wykonywanie nowych praw osób, których dane dotyczą, na czele z prawem do bycia zapomnianym i prawem do przenoszenia danych. Czasem może to wymagać wprowadzenia zmian w systemach informatycznych, przy współpracy z podmiotami dostarczającymi te systemy – należy więc upewnić się, że takie zmiany zostaną wprowadzone.

7. Incydenty bezpieczeństwa

Należy wdrożyć rozwiązania umożliwiające wykonywanie obowiązku zgłaszania incydentów bezpieczeństwa danych osobowych.

PRZYDATNE MATERIAŁY I LITERATURA

zasoby dostępne w Internecie:

- Generalny Inspektor Ochrony Danych Osobowych – http://www.giodo.gov.pl/
- Ministerstwo Przedsiębiorczości i Technologii – http://www.mpit.gov.pl/
- Ministerstwo Cyfryzacji – https://www.gov.pl/cyfryzacja

przydatna literatura:

- E. Bielak-Jomaa, D. Lubasz (red.), RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, Warszawa 2018,
- P. Litwiński (red.), Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz, Warszawa 2018,
- B. Fischer, M. Sakowska-Baryła (red.), Realizacja praw osób, których dane dotyczą, na podstawie rodo, Warszawa 2017.

Ochrona danych osobowych z biznes.gov.pl

Portal biznes.gov.pl. prowadzony przez Ministerstwo Przedsiębiorczości i Technologii, umożliwia realizację wielu spraw związanych z ochroną danych osobowych w firmie. Za pośrednictwem serwisu można wykonać usługi szybko i wygodnie, korzystając z gotowych formularzy. Na portalu znajdują się również aktualne informacje na temat praw i obowiązków przedsiębiorcy, wynikających z przepisów o ochronie danych osobowych. Do dyspozycji przedsiębiorców jest także Centrum Pomocy Przedsiębiorcy, w którym konsultanci i eksperci pomogą rozwiązywać problemy i wątpliwości związane z prowadzeniem firmy.

Zapraszamy na biznes.gov.pl!
https://www.biznes.gov.pl/przedsiebiorcy/

Wydawca:
Ministerstwo Przedsiębiorczości i Technologii
Plac Trzech Krzyży 3/5
00-507 Warszawa