Deloitte.

Praktyczny Przewodnik po Ogólnym Rozporządzeniu o Ochronie Danych Osobowych (RODO)

Jak dostosować funkcjonujący w firmie model bezpieczeństwa i ochrony danych osobowych do wymogów nowych przepisów?

Luty 2017

Spis treści

Słowo wstępu

Oddajemy w Państwa ręce Przewodnik po najważniejszych postanowieniach Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE. Rozporządzenie to jest kompleksową regulacją, która zrewolucjonizuje zakres obowiązków podmiotów przetwarzających dane osobowe i stworzy nową panoramę dla ochrony danych osobowych.

Celem, jaki przyświecał nam podczas tworzenia tego Przewodnika, było wskazanie od strony prawnej oraz bezpieczeństwa danych – zmian, które będą miały praktyczne znaczenie dla prowadzonej przez Państwa działalności.

1 Wstęp

1.1 Czym jest GDPR lub RODO?

„GDPR", zwane także „RODO" lub „Ogólnym Rozporządzeniem o Ochronie Danych" to 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[1].

1.2 Od kiedy GDPR zacznie obowiązywać?

Rozporządzenie weszło w życie 17 maja 2016 r. Zacznie ono obowiązywać bezpośrednio w krajowych porządkach prawnych od 25 maja 2018 r. Rozporządzenie wiązać będzie wszystkich, którzy przetwarzają dane osobowe w związku z prowadzoną działalnością gospodarczą.

1.3 Nowe Rozporządzenie – koniec ustawy o ochronie danych osobowych?

Nie oznacza to jednak, iż obowiązująca obecnie ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tj. Dz. U. z 2015 r. poz. 2135, ze zm.; „ODU" lub „Ustawa") zostanie w całości zastąpiona przepisami Rozporządzenia[2]. Wprawdzie wiele spośród przepisów Ustawy ulegnie zmianie lub w ogóle przestanie obowiązywać, jednakże – w niektórych kwestiach ODU stanowić będzie uzupełnienie lub doprecyzowanie zapisów Rozporządzenia. W praktyce - przedsiębiorcy będą sprawdzali, czy przetwarzają dane osobowe zgodnie z prawem, odwołując się wprost do przepisów Rozporządzenia, czyli aktu prawa Unii Europejskiej, a także zapewne – w ograniczonym zakresie - do przepisów znowelizowanej Ustawy.

1.4 Dlaczego rozporządzenie a nie dyrektywa, jak poprzednio?

Uregulowanie kwestii ochrony danych osobowych w Rozporządzeniu, a nie jak to było do tej pory w dyrektywie (która co do zasady wymaga implementacji do krajowego porządku prawnego np. w postaci ustawy o ochronie danych osobowych) ma na celu ujednolicenie przepisów na obszarze całej Unii Europejskiej, a tym samym - ułatwienie prowadzenia transgranicznej działalności gospodarczej. Przedsiębiorcy w mniejszym stopniu będą spotykać się bowiem z rozbieżnościami w prawie ochrony danych osobowych pomiędzy poszczególnymi państwami UE i dzięki temu np. z większą pewnością będą mogli stosować jednolity formularz zgody na przetwarzanie danych osobowych we wszystkich państwach UE, w których prowadzą swoją działalność.

Komentarz eksperta

Dlaczego warto zainteresować się treścią Rozporządzenia już teraz?

Proces dostosowania działalności do wymogów GDPR jest procesem długotrwałym. Aby dobrze się do niego przygotować przedsiębiorca powinien podjąć następujące kroki:

a) zorganizować szkolenie dla pracowników, na działalność których przepisy Rozporządzenia będą miały wpływ (a więc przede wszystkim – pracowników działów compliance, marketingu, sprzedaży oraz HR);
b) przygotować mapę wdrożenia GDPR; a następnie
c) implementować poszczególne rozwiązania o naturze organizacyjnej i technicznej do swojej struktury.

Aby zdążyć przed 25 maja 2018 r. przygotowania do wdrożenia GDPR należałoby rozpocząć już teraz.

Agata Jankowska-Galińska,
radca prawny, Managing Associate, odpowiedzialna za tematy regulacyjne w zespole Bankowości i Finansów Kancelarii Deloitte Legal

1 Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych („Dyrektywa").

2 Zgodnie z informacją Ministerstwa Cyfryzacji, założenia zmian do ODU mają zostać opublikowane do końca 2017 roku; sama ustawa będzie co do zasady regulować przede wszystkim kwestie uprawnień i obowiązków GIODO.

2 Kalendarium

3 Obowiązywanie i nadzór

3.1 W jakim zakresie i kiedy GDPR znajdzie zastosowanie?
Rozporządzenie ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych. Pod tym względem Rozporządzenie nie różni się od przepisów Dyrektywy.

3.2 Jakie podmioty zobowiązane będą stosować unijne zasad ochrony danych osobowych? Tylko z Unii, czy też spoza Unii?
Rozporządzenie ujednolica zasady ochrony danych osobowych w Unii Europejskiej. Unifikacja ma w założeniu wpłynąć także na sposób stosowania prawa przez organy ochrony danych osobowych dzięki przewidzianemu w treści Rozporządzenia - mechanizmowi spójności (uregulowanemu w art. 63 i nast. Rozporządzenia)[3].

3.2.1 Podmioty unijne
Administratorzy oraz podmioty przetwarzające dane, prowadzący działalność na terenie Unii Europejskiej, objęci obecnie zakresem Dyrektywy (i implementującej ją ODU) będą podlegać, tak jak dotychczas, unijnym regulacjom dotyczącym ochrony danych osobowych.

3.2.2 Podmioty spoza UE
Obowiązek stosowania przepisów Rozporządzenia nałożony natomiast zostanie na określone kategorie podmiotów spoza Unii Europejskiej, które dotychczas, co do zasady, nie podlegały przepisom Dyrektywy. Ma to na celu zapewnienie konkurencyjności podmiotów unijnych w stosunku do podmiotów spoza UE. Zgodnie z Rozporządzeniem podmioty spoza UE będą miały obowiązek zapewnienia zgodności z Rozporządzeniem w zakresie przetwarzania danych osobowych osób przebywających na terenie UE wtedy, gdy czynność przetwarzania wiąże się z:

- oferowaniem towarów lub usług takim osobom w UE, niezależnie, czy wymaga się od tych osób zapłaty; lub
- monitorowaniem ich zachowania, o ile do tego zachowania dochodzi w UE.

3.2.3 Obowiązki podmiotów spoza UE
Przetwarzający dane z państw trzecich, objęci zakresem Rozporządzenia, będą zobowiązani: (i) działać zgodnie z przepisami Rozporządzenia oraz (ii) wyznaczyć swojego przedstawiciela na terytorium Unii Europejskiej. Przedstawicielem może zostać osoba fizyczna lub prawna, mająca miejsce zamieszkania lub siedzibę w Unii. Przedstawiciel musi mieć siedzibę w państwie członkowskim, w którym przebywają osoby, których dane osobowe są przetwarzane w związku z oferowaniem im towarów lub usług lub których zachowanie jest monitorowane.

Na mocy upoważnienia udzielonego przedstawicielowi przez administratora lub podmiot przetwarzający organy nadzorcze i osoby, których dane dotyczą, będą mogły bezpośrednio zwracać się do przedstawiciela we wszystkich sprawach związanych z przetwarzaniem danych.

Komentarz eksperta

Kiedy mamy do czynienia z oferowaniem towarów lub usług?
Aby uznać, że administrator planuje oferować towary lub usługi osobom, których dane są przetwarzane może nie wystarczyć dostępność na terytorium UE strony internetowej administratora lub podmiotu przetwarzającego, posiadanie adresu poczty elektronicznej czy posługiwanie się na stronie językiem powszechnie stosowanym w państwie trzecim. Z drugiej strony, posługiwanie się językiem lub walutą powszechnie stosowanymi w co najmniej jednym państwie członkowskim oraz możliwość zamówienia towarów i usług w tym języku lub wzmianka o klientach lub użytkownikach znajdujących się w Unii mogą świadczyć o zamiarze oferowania towarów lub usług na terytorium Unii.

Katarzyna Sawicka,
Associate, doktorantka PAN, specjalistka od tematów regulacyjnych w zespole Bankowości i Finansów Kancelarii Deloitte Legal.

3 Zgodnie z art. 63 – na organy nadzorcze nałożony został obowiązek współpracy ze sobą, a w stosownym przypadku także z Komisją Europejską, przez stosowanie mechanizmu spójności wskazanego w sekcji 2 (Spójność) Rozdziału VII (Współpraca i Spójność) Rozporządzenia.

Wyznaczenie przedstawiciela przez administratora lub podmiot przetwarzający musi być dokonane na piśmie oraz pozostaje bez uszczerbku dla postępowań (np. sądowych, administracyjnych), które mogą zostać wszczęte przeciwko samemu administratorowi lub podmiotowi przetwarzającemu.

3.2.4 Placówki dyplomatyczne

Rozporządzenie ma zastosowanie do przetwarzania danych osobowych przez administratora niemającego jednostki organizacyjnej w Unii, ale posiadającego jednostkę organizacyjną w miejscu, w którym na mocy prawa międzynarodowego publicznego ma zastosowanie prawo państwa członkowskiego.

3.3 Co zmieni GDPR w sposobie funkcjonowania Grupy art.29?

Rozporządzenie zastępuje Grupę Roboczą ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych utworzoną na mocy art. 29 Dyrektywy nowym podmiotem – to jest Europejską Radą Ochrony Danych („EROD"), która przejmie dotychczasowe obowiązki Grupy Roboczej art. 29 w zakresie doradczym oraz w zakresie zapewniania współpracy pomiędzy organami nadzoru. EROD będzie posiadającym osobowość prawną organem Unii, działającym w sposób niezależny, powołanym w celu zapewnienia spójnego stosowania przepisów Rozporządzenia. Zadania EROD wskazane zostały w art. 70 GDPR. Należeć będą do nich w szczególności: (i) monitorowanie i zapewnienie właściwego stosowania Rozporządzenia, (ii) doradzanie Komisji Europejskiej w sprawach związanych z ochroną danych osobowych oraz w sprawach formatu i procedur wymiany informacji między administratorami, (iii) wydawanie wytycznych, zaleceń oraz określanie najlepszych praktyk zachęcających do spójnego stosowania Rozporządzenia, (iv) akredytowanie podmiotów certyfikujących oraz (v) dokonywanie okresowego przeglądu certyfikacji, wydawanie opinii.

3.4 Czym jest wprowadzona przez GDPR zasada one-stop shop?

Obecnie organy nadzorcze mają uprawnienia jedynie w stosunku do podmiotów przetwarzających dane osobowe w ich państwie członkowskim lub w inny sposób podlegającym ich jurysdykcji. Zgodnie z Rozporządzeniem, jeżeli przedsiębiorca przetwarza dane osobowe w więcej niż jednym państwie członkowskim, organ nadzoru głównej siedziby przedsiębiorcy będzie właściwy także względem transgranicznego przetwarzania danych i wszystkich obowiązków dla tego podmiotu z zakresu spójności z Rozporządzeniem.

Organy nadzoru z każdego z państw członkowskich pozostaną jednak właściwe w stosunku do skarg składanych przez osoby fizyczne, w odniesieniu do działalności administratora w tym państwie członkowskim.

Komentarz eksperta

Kiedy daną czynność możemy uznać za monitorowanie zachowania podmiotu danych?

Aby stwierdzić, czy czynność przetwarzania można uznać za „monitorowanie zachowania" osób fizycznych, należy ustalić, czy osoby fizyczne są obserwowane w internecie (np. poprzez rejestrację odwiedzanych stron), a także czy później na podstawie tak zebranych informacji administrator dokonuje profilowania takiej osoby, w szczególności w celu podjęcia decyzji jej dotyczącej (np. zaproponowania konkretnego produktu, skierowania odpowiedniej reklamy) lub prognozowania jej osobistych preferencji, zachowań i postaw.

Katarzyna Sawicka,
Associate, doktorantka PAN, specjalistka do spraw kwestii regulacyjnych w zespole Bankowości i Finansów Kancelarii Deloitte Legal.

4 Zasady przetwarzania danych osobowych – co przewiduje GDPR?

4.1 W jakim celu w GDPR wprowadzono katalog zasad przetwarzania danych osobowych?

GDPR wprowadza katalog zasad przetwarzania danych osobowych. Wprawdzie niektóre z nich funkcjonują w obecnym porządku prawnym, niemniej jednak w przewarzającej mierze ich źródłem są rekomendacje, czy dobre praktyki, a nie bezwzględnie obowiązujące przepisy prawa. Taki stan rzeczy nie gwarantuje spójnej i jednolitej ochrony prywatności osób, których dane są przetwarzane. Wskazanie wprost w Rozporządzeniu podstawowych zasad ochrony danych osobowych stanowi podstawę nowych standardów ochrony danych, obrazuje kierunek rozwoju ochrony prywatności oraz tworzy ramy dla pozostałych, szczegółowych przepisów Rozporządzenia. Dodatkowo, wprowadzenie do systemu ochrony danych osobowych jednolitego katalogu zasad jest źródłem nowych obowiązków, ciążących na podmiotach przetwarzających dane.

4.2 Zasada zgodności z prawem

4.2.1 Katalog warunków

Rozporządzenie zawiera zamknięty katalog warunków, w jakich przetwarzanie danych może zostać uznane za zgodne z prawem. Oznacza to, że każdy proces przetwarzania danych musi opierać się na co najmniej jednej podstawie prawnej, wskazanej w Rozporządzeniu. Następujące sytuacje mogą być podstawą przetwarzania danych:

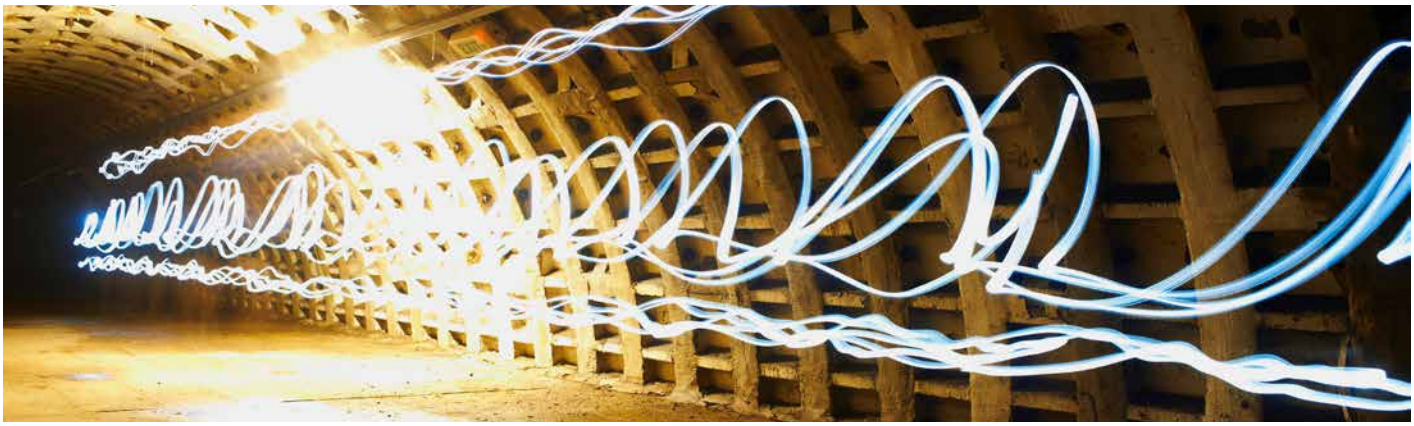
a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

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

d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;



f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

4.2.2 Nowe zasady dotyczące zgód na przetwarzanie danych osobowych

Zasadniczą zmianą, którą w praktyce odczują wszystkie podmioty, przetwarzające dane osobowe, będzie konieczność dostosowania procedur pozyskiwania zgody na przetwarzanie danych osobowych do nowych przepisów.

Rozporządzenie doprecyzowuje, jakie warunki powinna spełniać zgoda. Musi to być dobrowolne, konkretne, świadome i jednoznaczne okazanie woli. Ponadto, zgoda musi mieć charakter wyraźnego działania – oświadczenia lub potwierdzenia. W praktyce oznacza to, że formularze zgody powinny być sformułowane jasnym i czytelnym językiem, tj. w sposób zrozumiały dla osoby, której dane chcemy przetwarzać. Zawiłe, nieprecyzyjne i zbyt skomplikowane formularze mogą okazać się wadliwe, a zgoda - uznana za wyrażoną w sposób nieskuteczny.
Wymóg, aby zgoda udzielona była poprzez działanie oznacza w szczególności, że zgodnie z nowymi przepisami nie będzie dopuszczalna np. powszechna dziś praktyka domyślnie zaznaczonych okienek ze zgodą na przetwarzanie danych osobowych, czy też ze zgodą na ich przekazywanie podmiotom trzecim. Wyrażenie zgody powinno odbywać się więc jedynie poprzez faktyczne zaznaczenie każdego z okienek przez osobę, której dane dotyczą. Zgoda wiązać się będzie z aktywnym działaniem osoby fizycznej - nie będzie możliwości domniemania jej istnienia.

Aby zgoda została uznana za dobrowolną - od jej wyrażenia nie będzie można uzależniać wykonania umowy, w sytuacji, jeśli przetwarzanie danych nie będzie niezbędne dla wykonania takiej umowy.

Jeśli przedsiębiorca, zawierając umowę na dostawę towaru - pozyska zgodę na przetwarzanie danych osobowych dla celów marketingu, uzależniając od takiej zgody wykonanie umowy głównej, zgoda ta nie będzie ważna. Wynika to stąd, że przetwarzanie danych dla celów marketingu nie jest niezbędne dla wykonania umowy dostawy towaru.

W niektórych przypadkach, zgoda nie będzie uważana za dobrowolną, jeśli nie będzie możliwości wyrażenia jej osobno na różne operacje przetwarzania danych. Wyrażenie zgody nie będzie uznane za dobrowolne również wtedy, gdy osoba, której dane dotyczą, nie będzie miała rzeczywistego lub wolnego wyboru oraz nie będzie mogła odmówić ani wycofać zgody bez niekorzystnych konsekwencji.

Klauzule zgody na przetwarzanie danych osobowych często umieszczane są na formularzu lub stronie internetowej wraz z innymi informacjami kierowanymi do klientów, użytkowników, kontrahentów, itd. Należy pamiętać, że zgodnie z nowymi przepisami, jeżeli osoba, której dane dotyczą, wyraża zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
Osoba fizyczna ma bowiem zdawać sobie sprawę, że udziela zgody na przetwarzanie danych osobowych oraz w jakim zakresie.
Naruszenie powyższych przepisów oznaczać będzie nieważność zgody - na jej podstawie nie będzie można przetwarzać danych. Jeżeli dane osobowe przetwarzane będą w kilku celach, potrzebna będzie zgoda na wszystkie te cele.

Zgody będzie można udzielić zasadniczo w każdej formie, również ustnie. Rozporządzenie kładzie w tym miejscu szczególny nacisk na ochronę

Komentarz eksperta

Prawidłowe przygotowanie procesu pozyskiwania zgody oraz samych formularzy zgody, czy też odpowiednie ukształtowanie opcji zgody na stronie internetowej to zadanie, do którego należy solidnie się przygotować. Dlaczego?
Konsekwencje naruszenia przepisów w tym zakresie mogą być bardzo dotkliwe.
Po pierwsze, w przypadkach kiedy przetwarzamy dane osobowe na podstawie zgody, zgoda uzyskana nieprawidłowo będzie nieważna – a zatem przedsiębiorca nie będzie mógł na tej podstawie przetwarzać danych osobowych. Po drugie, zgodnie z nowymi regulacjami, za naruszenie przepisów dotyczących zgody - przedsiębiorcy grozić będzie nakładana przez GIODO kara administracyjna w wysokości do 20 000 000 euro lub w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, w zależności od tego, która z tych kwot będzie wyższa.

Agata Jankowska-Galinska,
radca prawny, Managing Associate odpowiedzialna za tematy regulacyjne w zespole Bankowości i Finansów Kancelarii Deloitte Legal.

użytkowników internetu - kiedy bowiem osoba, której dane dotyczą, będzie wyrażać zgodę w odpowiedzi na elektroniczne zapytanie, zapytanie takie musi być jasne, zwięzłe i nie zakłócać niepotrzebnie korzystania z głównej usługi.

Administratorzy danych będą musieli ponadto pozyskiwać i ewidencjonować zgody w taki sposób, aby np. w przypadku skargi osoby fizycznej, byli w stanie wykazać, że dana osoba rzeczywiście wyraziła zgodę na przetwarzanie swoich danych osobowych. Rozporządzenie nakłada na przedsiębiorców obowiązek zachowania należytego poziomu staranności. W przypadku, gdy administrator nie będzie w stanie wykazać, że pozyskał zgodę na przetwarzanie danych zgodnie z prawem, naraża się na karę administracyjną, a w niektórych przypadkach również na odpowiedzialność odszkodowawczą wobec osoby, której dane przetwarza.

Ponadto, osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać udzieloną zgodę. W takim przypadku, jeśli administrator danych nie ma innej podstawy przetwarzania (którą może być np. niezbędność dla wykonania umowy, szczególna podstawa prawna), należy zaprzestać przetwarzania danych. Wycofanie zgody nie wpływa jednocześnie na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. O możliwości wycofania zgody należy poinformować jeszcze przed jej wyrażeniem (np. jako część klauzuli zgody).
Wycofanie zgody musi być równie łatwe jak jej wyrażenie, np. jeśli zgoda odbierana jest telefonicznie, najlepiej umożliwić taką samą formę jej odwołania.

Na skutek wycofania zgody dane powinny zostać usunięte ze wszystkich systemów przedsiębiorcy, a więc np. nie tylko z bazy danych zbieranych w celach marketingowych, ale z każdej kolejnej bazy, do której te dane przedsiębiorca przekazał.

Rozporządzenie w sposób szczególny chroni dzieci. W przypadku tzw. usług społeczeństwa informacyjnego (usług świadczonych na odległość drogą elektroniczną), aby przetwarzać dane osobowe dziecka poniżej 16 roku życia, konieczne będzie uzyskanie zgody rodzica lub opiekuna. Państwa członkowskie będą mogły przewidzieć niższą granicę wieku, jednak nie mniej niż 13 lat. Administrator danych będzie musiał również podjąć odpowiednie starania, aby zweryfikować, czy upoważniona osoba wyraziła zgodę na przetwarzanie danych dziecka.

4.3 Zasada rzetelności i prawidłowości

Zgodnie z powyższymi zasadami, administrator danych musi zapewnić, że zgromadzone dane osobowe są poprawne i aktualne, a ich przetwarzanie przebiega bez zakłóceń. Realizacja obu zasad nakłada na administratora szereg obowiązków polegających m.in. na wdrożeniu środków technicznych i organizacyjnych, umożliwiających korektę danych, zmniejszenie ryzyka błędów oraz usunięcie nieprawidłowych danych. Wspomniane zasady nieodłącznie powiązane są z prawem osoby, której dane są przetwarzane do żądania sprostowania i uzupełnienia danych. Prawidłowość danych osobowych ma szczególne znaczenie w przypadku wykorzystywania mechanizmu profilowania. Ewentualne błędy w danych osobowych mogą stanowić ryzyko dla interesów i praw osoby, której dane dotyczą, a nawet prowadzić do dyskryminacji.

Z punktu widzenia bezpieczeństwa, w praktyce oznacza to wdrożenie odpowiednich procesów i funkcjonalności wspomagających te elementy na poziomie aplikacji, jak również baz danych.

4.4 Zasada ograniczenia celu

Zasada ograniczenia celu oznacza, że dane osobowe mogą być zbierane jedynie w konkretnym, wyraźnym i prawnie uzasadnionym celu, którego osiągnięcie nie jest możliwe przy użyciu innych sposobów. Cel przetwarzania danych musi być określony w momencie ich pozyskiwania. Jeśli podstawą przetwarzania danych

Komentarz eksperta

Na poziomie organizacyjnym założenia zasady ograniczania celu powinny określać procesy organizacji w zakresie zarządzania tożsamością i dostępem do danych, w tym proces regulujący dostęp do danych dla nowych pracowników, zmieniających jednostki wewnątrz organizacji lub odchodzących z organizacji. Jednocześnie przydzielane uprawnienia powinny być okresowo przeglądane i weryfikowane pod kątem ich aktualności, ew. korekty. Jednocześnie procesy te powinny być wspomagane przez dedykowane funkcjonalności posiadanego oprogramowania (np. przydzielanie/modyfikacja/odbiór uprawnień, przegląd uprawnień).

Marcin Ludwiszewski,
Dyrektor, Manager w dziale cyberbezpieczeństwa w Deloitte w Polsce

jest zgoda, to odnosi się ona jedynie do konkretnie wskazanego celu przetwarzania. Nowy cel przetwarzania danych wymaga pozyskania nowej zgody. Dodatkowo, to na administratorze danych ciąży obowiązek informowania osób, których dane są przetwarzane o celach przetwarzania.

4.5 Zasada minimalizacji danych

Na gruncie Rozporządzenia również zakres pozyskiwanych danych musi być adekwatny i ograniczony do minimum niezbędnego dla realizacji wskazanego celu. Minimalizacja może polegać na wyselekcjonowaniu jedynie tych danych, które są potrzebne do danej działalności oraz na ograniczeniu okresu przechowywania danych.
W praktyce realizacja zasady wymaga, aby przed rozpoczęciem procesu pozyskiwania, a następnie przetwarzania danych precyzyjnie określić cele i odpowiadające im rodzaje danych oraz ustalić termin usuwania i okresowego przeglądu danych. Należy podkreślić, że Rozporządzenie nakłada szereg obowiązków na podmioty przetwarzające dane, obwarowanych surowymi karami, a zatem chcąc zapewnić bezpieczeństwo prowadzonej działalności - warto ograniczyć zakres pozyskiwanych danych i ich przetwarzanie.

Zastosowanie się do tej zasady stanowić będzie nie lada wyzwanie. Czy w celu określenia, czy treść na stronie internetowej jest właściwa dla osób poniżej 18-stego roku życia – administrator ma prawo żądać tylko informacji o roku urodzenia użytkownika, czy też również o dniu i miesiącu? Czy w momencie, kiedy dana osoba osiągnie pełnoletniość – dane o dacie urodzenia powinny zostać skasowane?

4.6 Zasady integralności i poufności

Zasady integralności i poufności nakładają na administratora danych obowiązek przetwarzania danych w sposób gwarantujący odpowiedni poziom bezpieczeństwa. Zasada integralności odnosi się do obowiązku zapewnienia, że dane nie zostały zmodyfikowane, usunięte, dodane czy zniszczone w sposób nieautoryzowany.

Z kolei zgodnie z zasadą poufności należy zapobiegać sytuacjom, w których dane osobowe są udostępniane lub ujawniane nieautoryzowanym podmiotom czy procesom. Obie zasady wymagają dokonania analizy ryzyka właściwego dla przetwarzania danych i charakteru danych podlegających ochronie, a następnie dostosowania i wdrożenia odpowiednich środków technicznych zapewniających zachowanie integralności i poufności danych.

Z punktu widzenia procesów bezpieczeństwa zasada integralności i poufności danych oznacza konieczność wdrożenia kontroli opartych o standard polityki regulujący zasady bezpieczeństwa informacji i odporności systemów oraz usług przetwarzania na zagrożenia w organizacji oparte o zasady zarządzania ryzykiem (identyfikację, monitorowanie i ograniczanie). Na podstawie zasad określonych w standardzie polityki, organizacja powinna rozważyć wdrożenie środków bezpieczeństwa, monitorowania i reagowania, w tym m.in. elementy kontroli dostępu użytkowników do danych (zarządzanie cyklem życia), zasady bezpieczeństwa aplikacji i infrastruktury, środki dedykowane do ochrony przed wyciekiem danych, ale również środki zapewniające dostępność danych i odzyskiwanie sprawności w celu ich przetwarzania. Wdrożenie środków bezpieczeństwa powinno być poprzedzone analizą ryzyka w celu określenia wymaganych środków kontroli. Powyższe wymogi dotyczą również ochrony fizycznej posiadanych aktywów.

Jednocześnie wszystkie nowe produkty i usługi powinny odpowiadać zasadzie „security by design, security by default". Oznacza to, że organizacja powinna na podstawie analizy ryzyka wdrażać środki bezpieczeństwa w całym cyklu życia produktu – np. nowej aplikacji przetwarzającej dane osobowe, od momentu definiowania wymagań dla aplikacji, jej projektowania, tworzenia, jej testowania i wdrażania, utrzymania a także wycofywania z użycia.

Komentarz eksperta

Z punktu widzenia technicznego nie jest możliwe realizowanie zasady rozliczalności, jeśli administrator nie posiada udokumentowanej i okresowo weryfikowanej wiedzy dotyczącej danych osobowych w tym:

- Inwentaryzacji przetwarzanych danych;
- Ich lokalizacji: własności w organizacji, infrastruktury i aplikacji;
- Zapewnienia środków kontroli dostępu użytkowników (aplikacje, bazy danych) umożliwiających określenie wymaganych uprawnień dostępu ich monitorowanie i okresową weryfikację;
- Zdefiniowania i monitorowania procedur przetwarzania danych (środki kontroli przed wyciekiem danych, transfer zbiorów, współpraca z innymi dostawcami, partnerami biznesowymi);
- Posiadania środków technicznych monitorujących funkcjonowanie infrastruktury sieciowej i aplikacji;
- Procesów obsługujących wykrywanie i reagowanie na incydenty bezpieczeństwa.

Marcin Ludwiszewski,
Dyrektor, Manager w dziale cyberbezpieczeństwa w Deloitte w Polsce

4.7 Zasada rozliczalności

Administrator ma nie tylko obowiązek stosować się do wymogów Rozporządzenia, w tym do wyżej wymienionych zasad, m.in. wdrażając odpowiednie środki techniczne czy organizacyjne, ale również powinien być w stanie wykazać, że stosowane przez niego metody są zgodne z Rozporządzeniem oraz skuteczne. Zastosowanie się do zasady rozliczalności wymaga wdrożenia odpowiednich procedur i prowadzenia rzetelnej dokumentacji; warto rozważyć więc wprowadzenie odpowiednich regulacji wewnętrznych, nawet jeśli obowiązek ich posiadania nie wynika bezpośrednio z Rozporządzenia, ale dzięki którym łatwiej będzie wykazać fakt spełniania przewidzianych Rozporządzeniem wymogów. Wspomniana zasada rozliczalności jest też ściśle powiązana z obowiązkiem notyfikowania organu nadzorczego o stwierdzeniu naruszeń danych osobowych.

4.8 Zasada przejrzystości

Celem Rozporządzenia jest wzrost świadomości społeczeństwa na temat ryzyk związanych z udostępnianiem i przetwarzaniem danych osobowych. Stąd Rozporządzenie wymaga, aby wszelkie informacje, kierowane do osób fizycznych, formułowane były językiem prostym i przejrzystym. Adresat ma zrozumieć przeznaczony do niego komunikat, stąd hermetyczny język lub nadmierne skomplikowanie informacji – nie będą spełniać wymogów Rozporządzenia. Rozporządzenie kładzie nacisk na to, aby zarówno zakres udzielanych informacji jak i sposób ich przekazywania były zrozumiałe dla zainteresowanych i nie odstraszały ich swoją długością.

Zasada przejrzystości informacji w praktyce oznaczać będzie zakaz umieszczania istotnych informacji „drobnym drukiem" na innej stronie, wplatanie ich w długi i skomplikowany tekst, czy też zamieszczanie ich wśród innych, mało ważnych informacji.

Komentarz eksperta

Wywiązanie się z powyższych obowiązków – to jest zapewnienie zwięzłości i prostoty przekazu w połączeniu z rozszerzonym katalogiem udostępnianych informacji - będzie wymagało od administratorów sporo wysiłku. Przede wszystkim będą musieli oni opracować nowe metody i formy komunikacji z osobami, od których chcą pozyskać dane. To, w jaki sposób administratorzy będą realizować nałożone na nich obowiązki informacyjne, będzie oceniane przez organy nadzoru z punktu widzenia podstawowego celu Rozporządzenia – zapewnienia, że osoby udzielające zgody na przetwarzanie danych osobowych są w pełni świadome celu, procesu i konsekwencji przetwarzania ich danych.

Katarzyna Sawicka,
Associate, doktorantka PAN, specjalistka od tematów regulacyjnych w zespole Bankowości i Finansów Kancelarii Deloitte Legal

5 Ochrona osób fizycznych

5.1 Uwagi ogólne

Rozporządzenie kładzie nacisk m.in. na wzmocnienie ochrony osób fizycznych, których dane są przetwarzane. Ma tak się stać w szczególności poprzez przyznanie im dodatkowych uprawnień oraz wyposażenie w zestaw kluczowych informacji dotyczących sposobu i celu przetwarzania. W założeniu unijnego ustawodawcy - narzędzia te powinny się przyczynić do wzrostu świadomości osób fizycznych na temat tego, co dzieje się z ich danymi oraz na temat ryzyka związanego z ich przetwarzaniem.

Rozporządzenie przyznaje wprost osobom fizycznym, których dane są przetwarzane w szczególności następujące uprawnienia:

- prawo dostępu do danych i informacji,
- prawo żądania sprostowania i uzupełnienia danych,
- prawo sprzeciwu wobec przetwarzania danych,
- prawo do przeniesienia danych,
- prawo do bycia zapomnianym.

Uprawnienia te przekładają się bezpośrednio na obowiązki, którymi obciążeni zostają administratorzy danych. Nowe przepisy wymuszą na administratorach opracowanie sprawnych procedur przetwarzania danych osobowych, a w przypadkach gdy dane przetwarzane są automatycznie, dostosowanie funkcjonalności systemów.

5.2 Uprawnienia osób fizycznych

Po pierwsze, osobom wyrażającym zgodę na przetwarzanie danych osobowych przyznano prawo dostępu do danych oraz prawo do ich sprostowania, czy uzupełnienia. Na żądanie uprawnionego, administrator będzie miał obowiązek udostępnić kopię danych podlegających przetwarzaniu oraz wprowadzić odpowiednie zmiany do systemu.

Odpowiedzią na prawo dostępu do danych i informacji jest obowiązek administratorów danych do przekazywania osobie fizycznej podczas pozyskiwania jej danych, a przed rozpoczęciem ich przetwarzania, w szczególności następujących informacji:

- tożsamości i danych kontaktowych administratora,
- celu przetwarzania danych osobowych (np. w celach marketingowych),
- informacji o odbiorcach danych osobowych,
- okresu, przez jaki dane osobowe będą przetwarzane, a gdy nie można go dokładnie określić, kryteriów ustalania tego okresu (np. przez okres trwania umowy),
- informacji o wykorzystywaniu danych do profilowania,
- informacji o prawie do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
- gdy ma to zastosowanie – informacji o zamiarze przekazania danych osobowych poza Unię Europejską oraz wzmianki o odpowiednich zabezpieczeniach danych osobowych stosowanych przez podmiot, któremu dane są przekazywane.

Ponadto podmioty, których dane są przetwarzane w interesie publicznym lub w związku z uzasadnionym interesem administratora - będą mogły sprzeciwić się takiemu przetwarzaniu danych, chyba że administrator wykaże nadrzędność podstawy przetwarzania danych w stosunku do interesów jednostki. Prawo sprzeciwu będzie również przysługiwało w razie wykorzystywania danych do profilowania.

Po wejściu w życie Rozporządzenia osoba, której dane dotyczą, będzie mogła zażądać od administratora nie tylko informacji o tym, jakie dane posiada, ale także – w przypadku danych przetwarzanych elektronicznie – otrzymać je zapisane w powszechnie wykorzystywanym formacie i bez przeszkód przenieść je do innego usługodawcy.

Prawo do przeniesienia danych umożliwia również żądanie, aby to administrator posiadający dane przesłał je innemu administratorowi. Wynika to z treści art. 20 Rozporządzenia, stanowiącego, iż osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu pierwotnie dostarczono te dane. Uprawnienie to może być przez daną osobę zrealizowane, jeżeli przetwarzanie odbywa się na podstawie zgody wyrażonej przez tę osobę lub na podstawie umowy z nią zawartej oraz jeżeli przetwarzanie odbywa się w sposób zautomatyzowany. Osoba, której dane dotyczą, ma prawo również żądać, aby dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, jednak tylko o tyle - o ile jest to technicznie możliwe.

Wprawdzie wykonanie nałożonego Rozporządzeniem obowiązku przeniesienia danych na żądanie osoby, której dane dotyczą uzależnione jest od uwarunkowań technicznych, nie wiadomo jednak, do kogo należeć ma ocena tego, czy coś jest technicznie wykonalne, czy też nie. Rozporządzenie nie rozstrzyga także, czy chodzi tu o subiektywne możliwości techniczne danej instytucji, czy też o pewien standard usług, które powinien móc oferować każdy bank, instytucja płatnicza lub instytucja pożyczkowa. Omawiany przepis nie precyzuje również - pomiędzy jakimi administratorami powinno dochodzić do przekazywania danych. Nie można, zatem, wykluczyć sytuacji, w której klient zażąda, aby jego dane zostały przekazane przez instytucję płatniczą czy instytucję pożyczkową np. do urzędu, czy operatora komórkowego. W efekcie, oprócz wątpliwości interpretacyjnych, omawiany art. 20 spowodować może powstanie po stronie podmiotu zobowiązanego do jego stosowania - kolejnego kosztownego obowiązku regulacyjnego dotyczącego danych osobowych klientów.

W związku z tym, iż uprawnienia związane z przenoszeniem danych będą mogły być wykonywane przez klienta bez uszczerbku dla art. 17 Rozporządzenia, regulującego prawo do usunięcia danych (tj. „prawo do bycia zapomnianym") - klient będzie mógł zdecydować, czy przekazanie jego danych do innej instytucji nastąpi łącznie z ich wykreśleniem przez obecnego administratora, czy też nie. Opisywane uprawnienie do wykreślenia danych nie będzie mogło być egzekwowane przez klienta jedynie w sytuacjach, gdy przetwarzanie danych przez administratora jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Wydaje się, że mowa tu przede wszystkim o sytuacjach, gdy przetwarzanie danych klienta odbywa się niezależnie od jego zgody czy podpisanej przez niego umowy, na podstawie bezwzględnie obowiązujących przepisów prawa – np. w związku z archiwizowaniem danych na potrzeby procedur mających na celu przeciwdziałanie praniu pieniędzy i finansowanie terroryzmu.

Innym istotnym aspektem zastosowania art. 20 Rozporządzenia jest jego relacja do nowego rodzaju instytucji płatniczych, opierających zasadniczą część swoich usług na przetwarzaniu danych klientów. Mowa tu o TPP (ang. Third Party Providers) – czyli dostawcach usług płatniczych, którzy na mocy nowej Dyrektywy PSD2[4] oferować będą usługi płatnicze polegające na inicjowaniu płatności – PIS (ang. payment initiation service)[5] oraz zapewnianiu dostępu do informacji o rachunku – AIS (ang. account information service) [6]. W szczególności usługa AIS swym charakterem zbliżona jest raczej do usług, których przedmiotem jest przetwarzanie danych osobowych aniżeli do typowych usług płatniczych, jak np. usługa wykonania transakcji płatniczej.

W tym kontekście pojawiają się następujące pytania:

- jaki zakres danych o kliencie powinien być przekazywany na żądanie klienta wyrażone zgodnie z art. 20 Rozporządzenia?
- komu tego typu dane powinny być przekazywane?
- jak prawo do przeniesienia danych odnosi się do danych stanowiących tajemnicę bankową?

Najsilniejszym uprawnieniem przyznanym w Rozporządzeniu jest prawo do bycia zapomnianym, czyli prawo żądania usunięcia danych przez administratora. W razie skorzystania z tego prawa przez osobę, której dane dotyczą, administrator ma obowiązek, bez zbędnej zwłoki, usnąć ze wszystkich swoich systemów, dane pochodzące od tej osoby. Niemniej jednak, wskazany obowiązek odnosi się jedynie do administratorów, którzy wykorzystują dane wyłącznie na podstawie udzielonej zgody. Jeśli podstawą przetwarzania danych jest umowa, której wykonanie wymaga przetwarzania danych, wówczas prawo do bycia zapomnianym nie znajdzie zastosowania. W takiej sytuacji żądanie usunięcia danych wymagać będzie wcześniejszego rozwiązania umowy.

Powyższe uprawnienia mają sprawić, że klienci będą w pełni świadomi zakresu i celu przetwarzania danych, a także będą mieć realny wpływ na ich kształt oraz możliwość ich kontroli w każdej chwili. Dodatkowo, w razie pogwałcenia swoich praw, osoby fizyczne będą mogły dochodzić odszkodowania, jak również złożyć skargę do organu nadzoru.

4 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE.

5 Zgodnie z art. 4 pkt 15 PSD2 „usługa inicjowania płatności" oznacza usługę polegającą na zainicjowaniu zlecenia płatniczego na wniosek użytkownika usług płatniczych w odniesieniu do rachunku płatniczego posiadanego u innego dostawcy usług płatniczych.

6 Zgodnie z art. 4 pkt 16 PSD2 „usługa dostępu do informacji o rachunku" oznacza usługę online polegającą na dostarczaniu skonsolidowanych informacji na temat co najmniej jednego rachunku płatniczego posiadanego przez danego użytkownika usług płatniczych u innego dostawcy usług płatniczych albo u więcej niż jednego dostawcy usług płatniczych.

6 Istotne pojęcia

6.1 Czym są anonimizacja i pseudonimizacja danych osobowych?

Dane anonimowe to dane, które nie pozwalają na identyfikację osoby, której dotyczą dane. Nie są one objęte ochroną przewidzianą przez przepisy Rozporządzenia.

Dane spseudonimizowane to dane, które zostały poddane przetworzeniu w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie.

Pseudonimizacja danych osobowych może ograniczyć ryzyko dla osób, których dane dotyczą, oraz pomóc administratorom i podmiotom przetwarzającym wywiązać się z obowiązku ochrony danych. Aby zachęcić do stosowania pseudonimizacji podczas przetwarzania danych osobowych, należy umożliwić stosowanie u tego samego administratora środków pseudonimizacyjnych niewykluczających ogólnej analizy przetwarzanych danych. Jeśli administrator decyduje się na ochronę danych poprzez ich pseudonimizację, wówczas musi on zapewnić, że dane spseudonimizowane i dodatkowe informacje pozwalające „rozkodować" dane będą przechowywane osobno.

Pseudonimizacja traktowana jest jako istotny element zapewnienia bezpieczeństwa przetwarzania danych. Powinna być również brana pod uwagę podczas opracowywania i projektowania produktów, usług i aplikacji opierających się na przetwarzaniu danych (więcej na temat zasady privacy by default i privacy by design w pkt 6.3 niniejszego Przewodnika).

Jeżeli dane są ustrukturyzowane w taki sposób, że niemożliwa jest identyfikacja osoby, której dotyczą, wtedy, zgodnie z Rozporządzeniem, wymogi ochrony danych osobowych są znacznie złagodzone (jak w przypadku pseudonimizacji) lub nie obowiązują (jak w przypadku anonimizacji).

6.2 Czym jest profilowanie?

Nowa regulacja ułatwi osobom, których dane dotyczą wyłączenie swoich danych spod profilowania. Zmiana wpłynie więc niekorzystnie na podmioty proponujące usługi marketingu online, śledzenia konsumenta oraz reklamy online.

Zgodnie bowiem z przepisami Rozporządzenia osoba, której dane dotyczą, powinna mieć prawo do tego, by nie podlegać decyzji, która ocenia jej czynniki osobowe, opierając się wyłącznie na przetwarzaniu zautomatyzowanym. Tego typu decyzje mogą wywoływać skutki prawne lub w podobny sposób znacząco wpływać na sytuację osoby, której dane dotyczą. Skutkiem zautomatyzowanego przetwarzania danych może być na przykład odrzucenie elektronicznego wniosku kredytowego. Może być ono również wykorzystywane podczas elektronicznych metod rekrutacji niewymagającej interwencji ludzkiej. Mechanizm podejmowania takich decyzji określa się jako profilowanie.

Komentarz eksperta

Pseudonimizacja danych i szyfrowanie powinno być przeprowadzone na podstawie analizy ryzyka. Realizacja tych elementów może być stosowana poprzez różne techniki, w tym m.in. tzw. scrambling, maskowanie danych (np. w środowiskach testowych wytwarzanych aplikacji), ich zaciemnianie (obfuscation), a także ich szyfrowanie podczas przechowywania i przekazywania w celu zapewnienia poufności, integralności i autentyczności. Dotyczy to w szczególności cyklu życia tworzenia aplikacji (środowiska testowe/produkcyjne), ale również przetwarzania w aplikacjach i bazach danych.
Procesy zarządcze wspierające te elementy mogą uwzględniać m.in. sposoby zarządzania wykorzystywanym systemem kryptograficznym, w tym np. kluczami kryptograficznymi.

Marcin Lisiecki,
ekspert do spraw Cyberbezpieczeństwa, Managing Associate, Deloitte

Profilowanie jest to dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Zakazane będzie każde profilowanie które (i) wywołuje wobec osoby skutki prawne lub (ii) w podobny sposób istotnie na niego wpływa i które nie ma podstawy prawnej. Ta definicja jest znacznie szersza niż przewidziana w Dyrektywie. W rezultacie legalne obecnie czynności profilowania mogą stać się zakazane przez Rozporządzenie.

Wydaje się więc, iż w praktyce jedyną możliwością prowadzenia profilowania będzie uzyskanie wyraźnej zgody osoby na profilowanie, co oznacza że samo wyrażenie zgody na profilowanie za pomocą klauzuli zawartej w regulaminie nie będzie prawnie skuteczne.

Administratorzy wykorzystujący profilowanie będą musieli wykonać ocenę skutków tej metody przetwarzania danych pod kątem zapewnienia bezpieczeństwa danych.

6.3 Privacy by design oraz privacy by default

6.3.1 Uwagi ogólne

Rozporządzenie wprowadza do europejskiego porządku prawnego nowe zasady - privacy by design oraz privacy by default.[7]

6.3.2 Obecny stan prawny

W obecnym stanie prawnym żaden akt prawa polskiego ani unijnego nie definiuje pojęcia privacy by design (nazywanej też „zasadą prywatności w fazie projektowania") ani privacy by default (nazywanej też „zasadą prywatności w ustawieniach domyślnych"). Ich treść oraz zakres są ustalane poprzez wskazanie funkcji, jakie spełniać powinny wprowadzane do użytku programy (systemy) przetwarzające dane osobowe.

Zasada privacy by design (oraz podlegająca jej zasada privacy by default) były wielokrotnie podnoszone przez Generalnego Inspektora Ochrony Danych Osobowych (GIODO), jako konieczny element wprowadzanego w Polsce ustawodawstwa. Przykładem są zastrzeżenia GIODO, zgłaszane w związku ze stosowaniem przez organy podatkowe tzw. systemów biometrycznych umożliwiających identyfikację podatników według pobranych próbek głosu[8], czy też uwagi GIODO w toku prac nad projektem ustawy o zmianie ustawy o działalności leczniczej[9]. Warto podkreślić, że w opisywanych sytuacjach GIODO mówi wprost o konieczności uwzględniania w krajowym prawodawstwie zasady privacy by design, wskazując jednocześnie jej oparcie w konstytucyjnych normach ochrony prywatności zawartych w art. 47, 49 i 51 Konstytucji.[10]

7 Koncepcje pojęć privacy by design i privacy by default zostały po raz pierwszy użyte przez Ann Cavoukian – rzecznika ds. informacji i prywatności prowincji Ontario w Kanadzie. W swym założeniu miały one stanowić remedium na postępujące konsekwencje systemowe ICT (Information and Communication Technologies), czyli narastające problemy związane z zapewnieniem prawa do prywatności w związku z postępem technologicznym i rozwojem społeczeństwa informacyjnego.

8 http://tvn24bis.pl/z-kraju,74/fiskus-moglby-juz-identyfikowac-nas-po-glosie-ale-czeka-na-giodo,567172.html.

9 Patrz: pismo GIODO z 26 stycznia 2016 r. złożone w ramach uzgodnień nad Projektem założeń do projektu ustawy o zmianie ustawy o działalności leczniczej, Rządowe Centrum Legislacji, https://legislacja.rcl.gov.pl/projekt/12280205.

10 Art. 47 Konstytucji: „Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym."; art. 49 Konstytucji: „Zapewnia się wolność i ochronę tajemnicy komunikowania się. Ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony."; art. 51 ust. 2 Konstytucji: „Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.".

6.3.3 Koncepcje privacy by design i privacy by default

Zasada privacy by design wprowadzana jest przez art. 25 ust. 1 Rozporządzenia, zgodnie z którym „uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą". Przepis ten wprowadza generalną zasadę, na podstawie której administrator danych będzie zobowiązany zapewnić, aby już na etapie projektowania systemu oraz na etapie wykorzystywania go do przetwarzania danych wprowadzone do niego zostały odpowiednie środki techniczne i organizacyjne, które zapewnią ochronę danych użytkowników i zgodność z Rozporządzeniem. W szczególności może to dotyczyć zasad tworzenia, trzymania i wycofywania z użycia aplikacji w organizacji, przeprowadzania regularnych testów bezpieczeństwa, monitorowania bezpieczeństwa infrastruktury, przydzielania i przeglądu uprawnień użytkowników, a także zarządzania zmianą.

Zasadę privacy by default określa natomiast ust. 2 komentowanego artykułu, zgodnie z którym administrator będzie zobowiązany wdrożyć takie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne w stosunku do każdego konkretnego celu przetwarzania. Dotyczyć to będzie ilości zbieranych danych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. Omawiane środki powinny zapewniać w szczególności, aby domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych. W tym kontekście istotne jest zapewnienie inwentaryzacji danych i wdrożenie środków bezpieczeństwa zgodnie z wykonaną oceną profilu ryzyka i krytyczności danych. Warto dodać, że wywiązanie się z ww. obowiązków na gruncie art. 25 ust. 3 Rozporządzenia będzie mogło być wykazane między innymi poprzez poddanie się przez administratora dobrowolnemu mechanizmowi certyfikacji, o którym mowa w art. 42 Rozporządzenia.

6.4 Privacy impact assessment

Z powyższymi obowiązkami po stronie podmiotów przetwarzających dane związany jest art. 35 Rozporządzenia wprowadzający do systemu ochrony danych osobowych nowy mechanizm oceny wpływu przetwarzania danych osobowych na prywatność osób, których dane są przetwarzane – tzw. Privacy Impact Assessment. Zgodnie z nowymi przepisami, przed rozpoczęciem czynności przetwarzania administrator ma obowiązek dokonać oceny skutków operacji przetwarzania dla ochrony danych. Ocena powinna w szczególności uwzględniać takie czynniki jak: charakter, zakres, kontekst i cele operacji przetwarzania czy zastosowanie nowych technologii. Dokonanie rzetelnej oceny ma szczególne znaczenie w przypadku stosowania mechanizmów profilowania, a także operacji przetwarzania o dużej skali, które dotyczą znacznej ilości danych osobowych, mogą wpłynąć na dużą liczbę osób, czy też mogą powodować wysokie ryzyko ze względu na charakter danych. Ponadto, art. 35 wskazuje minimalne elementy dokonywanej oceny takie jak: opis planowanych operacji przetwarzania, ocenę ich niezbędności i proporcjonalności w stosunku do celów, ocenę ryzyka, oraz opis środków podejmowanych w celu zaradzenia ryzykom. W razie stwierdzenia ryzyka naruszenia praw lub wolności osób fizycznych, którego nie da się zminimalizować środkami rozsądnymi z punktu widzenia dostępnych technologii i kosztów wdrożenia, administrator danych ma obowiązek skonsultować się z organem nadzorczym przed rozpoczęciem czynności przetwarzania. W razie potrzeby i na żądanie podmiot przetwarzający powinien pomagać administratorowi w zapewnieniu przestrzegania obowiązków wynikających z dokonania oceny skutków przetwarzania dla ochrony danych oraz z uprzednich konsultacji z organem nadzorczym.

Komentarz eksperta

Z punktu widzenia bezpieczeństwa, ocena ryzyka prywatności powinna dotyczyć wszystkich wykorzystywanych aplikacji i wspomagającej je infrastruktury (w tym ich tworzenia, a także zmiany). Ocena ryzyka w tym zakresie powinna identyfikować potencjalne ryzyka dla zasobów, a także definiować procesy (przydzielanie uprawnień, przegląd uprawnień, procesy monitorowania i reagowania na incydenty) i środki je ograniczające (np. zasady bezpiecznego tworzenia kodu, procesy bezpieczeństwa przy tworzeniu aplikacji, testy penetracyjne, bezpieczną konfigurację infrastruktury).

Marcin Lisiecki,
ekspert do spraw Cyberbezpieczeństwa, Managing Associate, Deloitte.

7 Transfer danych osobowych do państw trzecich

7.1 Kiedy transfer do państw trzecich będzie możliwy?

Transfer danych osobowych do państw trzecich zgodnie z GDPR będzie (podobnie jak na podstawie przepisów Dyrektywy) możliwy wtedy, gdy państwa te zapewniają adekwatny poziom ochrony. Inne transfery są możliwe po zapewnieniu odpowiednich gwarancji tj. na podstawie klauzul modelowych, wiążących reguł korporacyjnych, zatwierdzonych kodeksów postępowania oraz jeśli zarówno przekazujący, jak i odbierający dane uzyskali „certyfikat europejskiej ochrony danych osobowych".

7.2 Adekwatność jurysdykcji

Adekwatność poziomu ochrony danych osobowych może być stwierdzona decyzją Komisji Europejskiej. Dotychczasowe decyzje ws. adekwatności[11] zostają utrzymane w mocy bezterminowo aż do ich uchylenia lub zmiany.

7.3 Privacy Shield

W dniu 12 lipca 2016 r. Komisja Europejska dała zielone światło dla nowych zasad przekazywania danych osobowych z UE do USA. Nowy pakiet tzw. Privacy Shield (Tarcza Prywatności) zastąpi wcześniejszy Safe Harbour, który przestał być skuteczną podstawą przekazywania danych do USA po wyroku Trybunał Sprawiedliwości Unii Europejskiej („TSUE") z 5 października 2015 r. w sprawie Schrems (C-362/14). W przywołanym wyroku TSUE stwierdził, że Safe Harbour nie gwarantował wystarczającej ochrony praw podstawowych, w szczególności prawa do prywatności w związku z przetwarzaniem danych osobowych.

7.3.1 Czym jest Privacy Shield?

Privacy Shield została przyjęta w drodze decyzji Komisji Europejskiej. Zgodnie z dyrektywą 95/46/WE, Komisja Europejska może stwierdzić, że państwo trzecie zapewnia odpowiedni stopień ochrony danych osobowych na podstawie swojego prawa krajowego lub zobowiązań międzynarodowych. W takich przypadkach przekazywanie danych osobowych do państwa trzeciego zasadniczo nie będzie wiązało się z koniecznością spełnienia dodatkowych obowiązków.

Na Privacy Shield składają się uzgodnione pomiędzy UE a USA zasady ochrony prywatności oraz zobowiązania poszczególnych organów odpowiedzialnych w USA za obszar przetwarzania danych osobowych. Dokumenty te stanowią załączniki do wspomnianej powyżej decyzji KE.

7.3.2 Główne założenia

Privacy Shield ma zapewnić skuteczniejszą ochronę prywatności w szczególności w następujących obszarach:

a) przejrzystość zasad przetwarzania danych przez administratorów/podmioty przetwarzające dane w USA: Privacy Shield funkcjonować będzie na zasadzie samocertyfikacji, tj. podmioty z USA składać będą deklarację przestrzegania zasad przetwarzania danych osobowych wypracowanych w ramach nowego porozumienia. Podmioty te będą również zobowiązane do publikowania polityk prywatności oraz przekazywania określonych informacji dotyczących przetwarzania danych osobom fizycznym;

b) skuteczny nadzór nad przetwarzaniem danych w USA: Departament Handlu USA prowadzić będzie rejestr podmiotów, które przystąpiły do Privacy Shield. Przeprowadzane będą regularne kontrole zgodności przetwarzania danych, a podmioty naruszające zasady ustalone nowym porozumieniem, będą mogły zostać wykreślone z rejestru;

c) wprowadzenie mechanizmu bezpłatnego pozasądowego rozwiązywania sporów: każdy podmiot z USA przetwarzający dane będzie musiał zapewnić wewnętrzną procedurę rozpatrywania skarg. Osoby fizyczne będą mogły skorzystać również z nieodpłatnego mechanizmu ADR lub zwrócić się o pomoc do organu nadzoru w swoim państwie. Jeśli polubowne rozwiązanie sporu okaże się nieskuteczne, przewidziano możliwość skorzystania z arbitrażu;

d) ograniczenie masowego przetwarzania danych przez organy rządowe w USA: monitorowanie danych osobowych przez organy rządowe dopuszczalne będzie jedynie w wyjątkowych sytuacjach, pod warunkiem, że będzie niezbędne i proporcjonalne. Dla rozpatrywania sporów, które mogą pojawić się w tym zakresie, powołany zostanie dedykowany Ombudsman;

e) wprowadzenie corocznego przeglądu funkcjonowania mechanizmu Privacy Shield: Komisja Europejska oraz Departament Handlu USA co roku będą dokonywały przeglądu skuteczności Privacy Shield (pierwszy przegląd ma dotyczyć m.in. zautomatyzowanego przetwarzania danych). Raport z przeglądu może wskazywać na obszary, które będą wymagać dalszego usprawnienia i negocjacji.

11 Obecnie istnieją decyzje ws. adekwatności następujących państw: Andory, Argentyny, Kanady, Szwajcarii, Izraela, wysp Guernsey, Jersey, Man, Nowej Zelandii, Urugwaju oraz EU-US Privacy Shield – struktura pozwalająca na transfer danych do Stanów Zjednoczonych.

7.3.3 Privacy Shield – podstawowe obowiązki administratorów i podmiotów przetwarzających

Podmioty z USA chcące przetwarzać dane osobowe przekazywane z UE na podstawie przystąpienia do Privacy Shield, będą musiały przestrzegać szeregu zasad pozwalających chronić prywatność osób fizycznych. Do najważniejszych z zasad można zaliczyć:

a) **prawo do informacji**
Osoby fizyczne będą musiały zostać poinformowane m.in. o rodzaju przetwarzanych danych, celu przetwarzania, prawie dostępu do danych, warunkach dalszego przekazania danych oraz zasadach odpowiedzialności za zapewnienie bezpieczeństwa przetwarzania danych osobowych.

Podmioty przetwarzające dane będą również zobowiązane opublikować swoje polityki prywatności.

b) **obowiązek zapewnienia integralności danych oraz ograniczenia celu przetwarzania**
Podmioty powinny przetwarzać jedynie dane niezbędne ze względu na cel przetwarzania przez okres, w którym takie dane są przydatne dla osiągnięcia konkretnego celu. Przetwarzane dane muszą być kompletne oraz aktualne.

c) **prawo wyboru**
Jeśli nowy cel przetwarzania jest odmienny od pierwotnego, osoba fizyczna powinna mieć możliwość sprzeciwić się przetwarzaniu jej danych osobowych (na zasadzie opt out). Ponadto, należy umożliwić sprzeciwienie się przetwarzaniu danych dla celów marketingu w dowolnym momencie.

d) **zapewnienie bezpieczeństwa przetwarzania**
Podmioty przetwarzające dane muszą przyjąć odpowiednie środki bezpieczeństwa, uzależnione m.in. od poziomu ryzyka związanego z przetwarzaniem danych oraz od rodzaju przetwarzanych danych.

e) **zapewnienie dostępu do danych**
Osoby fizyczne będą miały prawo otrzymania potwierdzenia, czy ich dane osobowe są przetwarzane przez dany podmiot oraz będą mogły żądać ich poprawienia lub usunięcia w przypadku, gdy przetwarzanie odbywa się niezgodnie z zasadami Privacy Shield.

Specjalne zasady przyjęto w zakresie zautomatyzowanego przetwarzania danych (np. profilowania), na podstawie którego podejmowane są indywidualne decyzje dotyczące poszczególnych osób fizycznych (np. decyzje kredytowe).

f) **egzekwowanie zasad przetwarzania danych i zasady odpowiedzialności**
Podmioty przetwarzające dane muszą wprowadzić wewnętrzne mechanizmy zapewniające przestrzeganie zasad wynikających z Privacy Shield oraz przeprowadzać weryfikację zgodności polityk z nowym mechanizmem przetwarzania danych. To ostatnie można osiągnąć na dwa sposoby: (i) poprzez wewnętrzny system oceny połączony z zapewnieniem szkolenia pracowników lub (ii) poprzez audyt zewnętrzny.Privacy Shield nakłada również obowiązek wprowadzenia wewnętrznego mechanizmu rozpatrywania skarg.

g) **dalsze przekazywanie danych**
Przekazywanie danych kolejnym podmiotom możliwe będzie jedynie na podstawie umowy, która gwarantować będzie taki sam poziom ochrony co Privacy Shield oraz jedynie w określonym celu. Osoby fizyczne będą musiały zostać poinformowane o podmiocie, któremu dane mają być przekazane oraz o celu przekazania. Będą miały również możliwość sprzeciwienia się takiemu przekazaniu (na zasadzie opt out), a w przypadku danych wrażliwych przekazanie będzie możliwe dopiero po udzieleniu zgody przez podmiot przetwarzania danych (na zasadzie opt in).

7.4 Środki rekompensujące brak ochrony w państwie trzecim

7.4.1 Lista środków rekompensujących

W razie braku stwierdzenia odpowiedniego stopnia ochrony danych administrator lub podmiot przetwarzający powinni zastosować środki rekompensujące brak ochrony danych w państwie trzecim, zapewniając osobie, której dane dotyczą, odpowiednie zabezpieczenia. Takie odpowiednie zabezpieczenia mogą polegać na skorzystaniu z:

a) wiążących reguł korporacyjnych,

b) standardowych klauzul ochrony danych przyjętych przez Komisję,

c) standardowych klauzul ochrony danych przyjętych przez organ nadzorczy lub

d) klauzul umownych dopuszczonych przez organ nadzorczy.

7.4.2 Odstępstwa od zakazu transferu danych

Rozporządzenie poszerza katalog odstępstw od zakazu transferu danych osobowych do państw trzecich. Wszystkie odstępstwa od zakazu zawarte obecnie w dyrektywie pozostaną w mocy. Dodatkowo transfer danych będzie możliwy również wtedy, gdy np.:

- przekazanie jest niezbędne do zawarcia umowy,
- transfer jest konieczny dla ochrony żywotnych interesów osoby, której dane dotyczą,
- przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń.

8 Wewnętrzny program compliance

8.1 Program compliance pod GDPR – czyli co?

Na skutek wejścia w życie przepisów Rozporządzenia przedsiębiorcy powinni dokonać weryfikacji obowiązujących u nich programów compliance pod kątem spójności z GDPR.

Na program compliance, zgodnie z treścią GDPR składać się będą m.in.:

- wyznaczenie inspektora ochrony danych osobowych,
- prowadzenie rejestru wewnętrznego,
- przeprowadzenie oceny skutków przetwarzania dla ochrony danych,
- wprowadzenie odpowiednich zabezpieczeń danych i procedur związanych z ochroną danych,
- uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych.

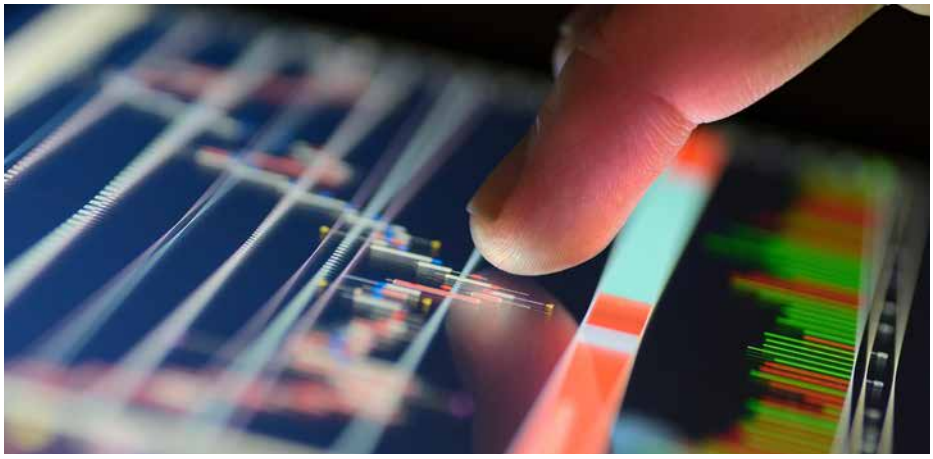
8.2 Inspektor ochrony danych

Inspektor ochrony danych zajmie miejsce ABI.Będzie wypełniał zadania z zakresu compliance oraz współpracy z organem nadzoru.

Wyznaczenie inspektora ochrony danych będzie co do zasady fakultatywne. W następujących sytuacjach będzie ono jednak obowiązkowe:

a) jeżeli główna działalność przedsiębiorcy w zakresie przetwarzania ze względu na swój charakter, zakres lub cele wymaga regularnego i systematycznego monitorowania osób na dużą skalę;

b) gdy główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu danych wrażliwych;



c) jeżeli przewidują to przepisy prawa krajowego;

d) w przypadku podmiotów publicznych.

Wyznaczony inspektor powinien posiadać kwalifikacje w zakresie ochrony danych osobowych, być właściwie i terminowo angażowany we wszystkie sprawy dotyczące ochrony danych w przedsiębiorstwie, powinien mieć zapewnione warunki działania oraz niezależność.

Możliwe będzie wyznaczenie jednego inspektora danych osobowych przez grupę przedsiębiorców, jeśli każdy z przedsiębiorców będzie mógł łatwo nawiązać z nim kontakt.

8.3 Prowadzenie wewnętrznego rejestru przetwarzania danych

Rozporządzenie znosi wymóg rejestracji zbiorów danych osobowych i zastępuje go obowiązkiem prowadzenia rejestru wewnętrznego operacji przetwarzania danych osobowych, jednak tylko w odniesieniu do niektórych przedsiębiorstw.

Obowiązek prowadzenie rejestru wewnętrznego obejmuje przedsiębiorców zatrudniających powyżej 250 pracowników, jeśli przetwarzanie danych niesie zagrożenie dla praw i wolności osób, nie ma charakteru sporadycznego lub obejmuje dane wrażliwe.

Rejestr powinien uwzględniać cel przetwarzania danych i kategorie odbiorców, których dane osobowe zostały ujawnione oraz informacje o transferze do państw trzecich. Ponadto na administratorów i podmioty przetwarzające nałożony został obowiązek udostępnienia rejestru na każde żądanie organu nadzoru.

9 Ochrona prywatności jako istotny element budowania wizerunku firmy – ewolucja podejścia do ochrony danych

Dzięki nowym technologiom pozyskiwanie danych osobowych, ich przetwarzanie, a następnie wykorzystywanie w działalności biznesowej jest zjawiskiem rozwijającym się niezwykle szybko. Coraz więcej uczestników rynku zdaje sobie sprawę z ekonomicznej wartości danych. Z drugiej strony rosnąca świadomość klientów, co do zagrożeń wynikających z udostępniania danych oraz coraz szerszy zakres prawnych regulacji powodują, że w celu efektywnego pozyskiwania dużych ilości danych osobowych, konieczne będzie nie tylko dostosowanie działalności do wymogów prawnych, ale również zapewnienie ochrony prywatności klientów i zdobycie ich zaufania. Przepisy Rozporządzenia wychodzą naprzeciw tym zmianom.

Pozyskiwanie i wykorzystywanie danych jest swego rodzaju transakcją wiązaną. Firmy zbierają ogromne ilości danych by lepiej poznać swojego klienta i w konsekwencji być bardziej konkurencyjnym na rynku, a konsumenci w zamian za swoje dane oczekują wymiernych korzyści. Obecnie wystarczy, że wraz z prośbą o zezwolenie na przetwarzanie danych osobowych, oferowany jest darmowy dostęp do artykułu, bezpłatna obsługa skrzynki pocztowej, czy możliwość ściągnięcia filmu. Dodatkowo, coraz więcej konsumentów zdaje sobie sprawę, że udostępnianie szeregu informacji na temat stylu życia, preferencji, czy potrzeb, może być źródłem oszczędności zarówno pieniężnych, jak i czasowych. Dzięki stworzeniu profilu konsumenta usługodawca może zaoferować produkty szyte na miarę pod względem ich funkcjonalności, a także ceny. Niemniej jednak, wraz z rozwojem świadomości konsumenckiej na temat ochrony danych osobowych, ich ekonomicznej wartości oraz rozwojem rynku danych personalnych, przedsiębiorca chcący pozyskać dane swojego klienta będzie musiał zaoferować „coś" więcej, a darmowy gadżet czy atrakcyjny produkt nie będą już wystarczające.

Mimo że zapewnienie zgodności prowadzonej działalności z przepisami prawa jest niezbędnym elementem budowania wizerunku firmy, to na konkurencyjnym rynku nie jest to jednak wystarczająca strategia. Konieczne jest wdrożenie dodatkowych, nawet niewymaganych prawem działań zapewniających wysokie standardy ochrony prywatności klientów.

Budowanie zaufania może bazować na działaniach mających na celu edukowanie klientów w zakresie zagrożeń płynących z przetwarzania danych osobowych, a także realizowanych przedsięwzięć gwarantujących wzrost ich bezpieczeństwa. Programy edukacyjne powinny w prosty i przyjazny sposób przekazywać niezbędne informacje, przykładowo w formie filmu czy komiksu. Niewiedza o zakresie przetwarzania danych powoduje niepewność i podejrzliwość, czego konsekwencją może być rezygnacja z usługi czy produktu. Dobrze poinformowany klient, mający zaufanie do swojego usługodawcy, zdaje sobie sprawę z konsekwencji udostępniania swoich danych personalnych, ale jednocześnie wie, że jego prywatność chroniona jest przez profesjonalistów oraz wysoko ceni sobie korzyści, które otrzymuje w zamian.

Kolejnym elementem strategii budowania zaufania jest zapewnienie klientom kontroli nad udostępnianymi przez nich danymi.

Istotny jest również przekaz, jaki podmiot pozyskujący dane kieruje do swoich klientów. Klient powinien mieć świadomość tego, że jego dane osobowe niezależnie od ich udostępnienia pozostają jego własnością, pozostają w zakresie jego kontroli, a ich przetwarzanie ma na celu jedynie polepszenie jakości świadczonych na jego rzecz usług i personalizację dostarczanych produktów.

Wiedza, kontrola i wymierne korzyści to podstawowe kroki budowania zaufania klientów i wizerunku firmy troszczącej się o ochronę prywatności. W niedalekiej przyszłości, dzięki rosnącej świadomości konsumentów na temat wartości ich danych osobowych brak tych kluczowych elementów może znacząco pogorszyć pozycję firmy na rynku.

10 Uprawnienia organów nadzorczych, skargi i sankcje

10.1 Uwagi ogólne

Dodatkowe uprawnienia organów nadzorczych oraz zwiększenie wysokości nakładanych sankcji w znaczący sposób wpłynie na działalność przedsiębiorców. Ponadto, państwa członkowskie zyskały możliwość ustanawiania przepisów przewidujących sankcje karne za naruszenie Rozporządzenia, w tym za naruszenie krajowych przepisów przyjętych na jego mocy i w jego granicach. Sankcje będą mogły również obejmować pozbawienie zysków wynikających z naruszenia Rozporządzenia.

10.2 Uprawnienia użytkowników

Zgodnie z Rozporządzeniem katalog uprawnień użytkowników, którzy uważają, że ich dane przetwarzane są niezgodnie z prawem, obejmował będzie:

a) prawo do wniesienia skargi do organu nadzorczego, jeśli użytkownik sądzi, iż przetwarzanie danych osobowych jego dotyczących narusza Rozporządzenie;

b) prawo do skutecznego środka ochrony prawnej przed sądem przeciwko prawnie wiążącej decyzji organu nadzorczego dotyczącej użytkownika;

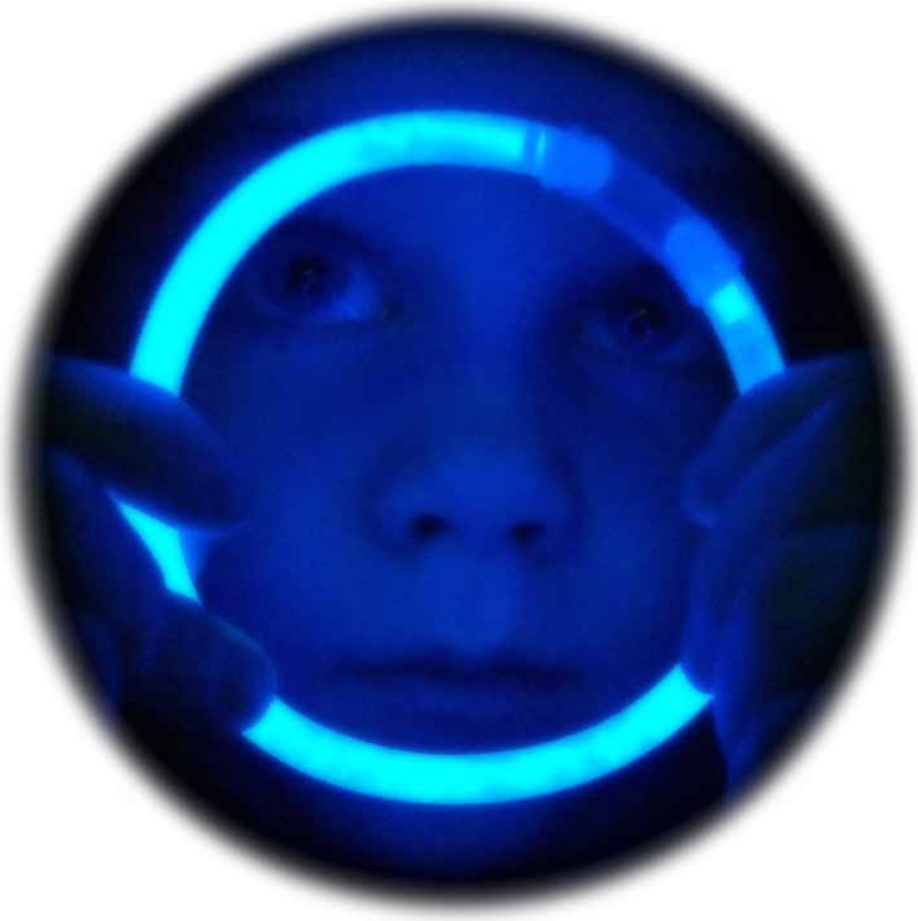
c) prawo do skutecznego środka ochrony prawnej przed sądem, przeciwko administratorowi lub podmiotowi przetwarzającemu dane.

Wszczęcie postępowania sądowego przeciwko administratorowi lub podmiotowi przetwarzającemu dane będzie możliwe niezależnie od skarg złożonych do organu nadzoru.

W związku z powyższym, administrator oraz podmiot przetwarzający dane będą musieli liczyć się z realną możliwością poniesienia odpowiedzialności administracyjnej, karnej oraz cywilnej.

10.3 Sankcje

Kary nakładane obecnie przez GIODO mają zasadniczo charakter przymuszenia tj. są nakładane w celu zmuszenia podmiotu do wykonania decyzji GIODO i nie występują często. Rozporządzenie ujednolica oraz znacząco podwyższa kary finansowe za naruszenie przepisów o ochronie danych osobowych.Maksymalna wysokość kar przewidzianych w Rozporządzeniu jest wielokrotnie wyższa niż wysokość kar nakładanych obecnie przez GIODO. Sankcje mogą wynieść do 20.000.000 EUR lub do 4% całkowitego światowego przychodu za rok poprzedni za uchybienia w ochronie danych osobowych.



Podsumowanie

Niniejszy Przewodnik opracowany został w celu zasygnalizowania najważniejszych zmian, wprowadzanych przepisami Rozporządzenia; zmiany te mają bowiem niezwykle szeroki zakres, obejmujący konieczność dostosowania się przez całą organizację – od działów prawnych, compliance, HR, poprzez marketing i IT.

Proces identyfikacji istniejących niezgodności i luk w zakresie ochrony danych osobowych w związku z nowymi wymogami GDPR (obejmujący w szczególności weryfikację dokumentacji, procedur oraz systemów IT) w celu określenia niezbędnych działań dostosowawczych należałoby więc rozpocząć już teraz.

Opracowanie nie ma charakteru porady prawnej. W celu uzyskania bardziej kompleksowych informacji prosimy o kontakt z naszymi ekspertami.

Deloitte Legal – doradztwo prawne

Zbigniew Korba
Partner
Radca prawny
Tel.: +48 22 348 35 56
Mobile: +48 500 021 990
zkorba@deloittece.com

Agata Jankowska-Galińska
Managing Associate
Radca prawny
Tel.: +48 22 348 39 93
Mobile: +48 728 459 605
ajankowskagalinska@
deloittece.com

Katarzyna Sawicka
Associate
Tel.: +48 22 511 05 33
ksawicka@deloittece.com

Zespół do spraw cyberbezpieczeństwa

Marcin Ludwiszewski
Manager
Tel: +48 22 348 36 87
Mobile: +48 538 442 815
mludwiszewski@deloittece.com

Marcin Lisiecki
Managing Associate
Tel.: +48 22 348 37 69
Mobile: +48 882 759 056
mlisiecki@deloittece.com

Deloitte.

Deloitte świadczy usługi audytorskie, konsultingowe, doradztwa podatkowego, prawnego i finansowego klientom z sektora publicznego oraz prywatnego, działającym w różnych branżach. Dzięki globalnej sieci firm członkowskich obejmującej 150 krajów oferujemy najwyższej klasy umiejętności, doświadczenie i wiedzę w połączeniu ze znajomością lokalnego rynku. Pomagamy klientom odnieść sukces niezależnie od miejsca i branży, w jakiej działają. Ponad 244 000 pracowników Deloitte na świecie realizuje misję firmy: wywierać pozytywny wpływ na środowisko i otoczenie, w którym żyją i pracują.

Specjalistów Deloitte łączy kultura współpracy oparta na zawodowej rzetelności i uczciwości, maksymalnej wartości dla klientów, lojalnym współdziałaniu i sile, którą czerpią z różnorodności. Deloitte to środowisko sprzyjające ciągłemu pogłębianiu wiedzy, zdobywaniu nowych doświadczeń oraz rozwojowi zawodowemu. Eksperci Deloitte z zaangażowaniem współtworzą społeczną odpowiedzialność biznesu, podejmując inicjatywy na rzecz budowania zaufania publicznego i wspierania lokalnych społeczności.