Kiedy należy przeprowadzić DPIA, czyli kilka słów o preDPIA

Ocena skutków dla ochrony danych (ang. *data protection impact assessment*, DPIA) to szczególna postać analizy ryzyka. Pozwala ona administratorom opisać dokonywanie przetwarzanie i ocenić jego konieczność i proporcjonalność. Poprzez ocenę ryzyka i określenie środków pozwalających zaradzić jego czynnikom, wspomaga ona również zarządzanie ryzykiem naruszania praw i wolności osób fizycznych.

RODO nie wymaga jednak przeprowadzenia DPIA w odniesieniu do każdej operacji przetwarzania. Kiedy zatem dokonanie takiej oceny jest obligatoryjne?

DPIA – co na to RODO

Zgodnie z art. 35 ust. 1 RODO, przeprowadzenie oceny skutków dla ochrony danych jest obowiązkowe zawsze, gdy dany rodzaj przetwarzania, ze względu na swój charakter, zakres, kontekst i cele, może z dużym prawdopodobieństwem powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Warunkiem aktualizacji obowiązku dokonania DPIA jest zatem stwierdzenie, że:

1) istnieje **duże prawdopodobieństwo wystąpienia ryzyka** naruszenia praw lub wolności osób fizycznych, oraz

2) **ryzyko to jest wysokie**.

RODO nie definiuje ani pojęcia *"dużego prawdopodobieństwa"*, jak i *"wysokiego ryzyka"*. W art. 35 ust. 3 RODO podaje się natomiast **przykłady sytuacji**, gdy operacja przetwarzania „*może powodować wysokie ryzyko*", a więc przeprowadzenie oceny będzie w jej zakresie obowiązkowe. Są to przypadki:

1) 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,

2) przetwarzania na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych,

3) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

RODO przewiduje również (art. 35 ust. 4 RODO) obowiązek ustanowienia i podania do publicznej wiadomości przez krajowe organy nadzorcze **wykazu rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych**.

Tyle przepisy RODO. Na ich podstawie, administrator musi samodzielnie dokonać oceny, czy dany rodzaj operacji przetwarzania będzie wymagał od niego przeprowadzenia DPIA. Jak zatem ma to zrobić?

Analiza preDPIA – czym jest?

Analiza preDPIA, to nic innego jak ocena, czy dany rodzaj operacji przetwarzania będzie podlegał obowiązkowi przeprowadzenia DPIA.

Jako, że administrator jest zobowiązany wykonać DPIA jeszcze przed rozpoczęciem przetwarzania, analiza preDPIA powinna zostać przeprowadzona w jak najwcześniejszej fazie projektowania danej operacji. Tak, aby w razie takiej konieczności, czynności związane z oceną skutków dla ochrony danych zostały podjęte w odpowiednim czasie.

Biorąc pod uwagę ogólne obowiązki w zakresie rozliczalności określone przez przepisy RODO, analizą preDPIA powinny zostać objęte wszystkie operacje ujawnione w rejestrze czynności przetwarzania.

Należy pamiętać o tym, że przetwarzanie danych osobowych jest procesem dynamicznym i może ulegać ciągłym zmianom. Każda przeprowadzona analiza preDPIA powinna podlegać zatem systematycznym przeglądom i w razie potrzeby, aktualizacjom.

preDPIA w praktyce

Oceniając, czy dany rodzaj operacji będzie podlegał obowiązkowi przeprowadzenia DPIA, administrator powinien wziąć pod uwagę, wskazane na wstępie, przesłanki. Jeżeli jakakolwiek z nich zostanie spełniona, dokonanie DPIA będzie obligatoryjne. Ze względów praktycznych, warto przesłanki te analizować od ich końca.

I tak, **pierwszy etap preDPIA** powinno stanowić sprawdzenie, czy dany rodzaj operacji przetwarzania został ujawniony w wykazie ustanowionym przez organ nadzorczy jako podlegający wymogowi dokonana oceny skutków dla ochrony danych.

Ogłoszony przez Prezesa UODO wykaz zawiera 12 kategorii rodzajów operacji przetwarzania wraz z przykładami operacji, w których może wystąpić wysokie ryzyko naruszenia praw lub wolności oraz przykładami potencjalnych obszarów obejmujących te operacje.

Przykład:

Zbieranie danych o przeglądanych stronach, wykonywanych operacjach bankowych, zakupach w sklepach internetowych, a następnie ich analiza w celu tworzenia profilu osoby (pozycja 8 wykazu).

Systemy służące do zgłaszania nieprawidłowości (związanych np. z korupcją, mobbingiem) – w szczególności gdy przetwarzane są w nim dane pracowników (pozycja 9 wykazu).

DPIA dla operacji wskazanej w wykazie organu przeprowadzana powinna zostać obowiązkowo. W takim wypadku dalsza analiza nie będzie już konieczna.

Jeżeli badana operacja przetwarzania nie widnieje w wykazie Prezesa UODO, konieczne jest przeprowadzenie dalszych czynności. **Drugi etap preDPIA** stanowi ocena, czy dany rodzaj przetwarzania może z dużym prawdopodobieństwem powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Jak to sprawdzić?

Wskazywaliśmy już przykłady takich operacji podawane w RODO. Przykłady nie stanowią jednak wyczerpującego wykazu. Mogą występować operacje przetwarzania związane z „*wysokim ryzykiem*", których w przepisach RODO nie uwzględniono. Jak je zatem zidentyfikować?

Na pomoc administratorom przyszła Europejska Rada Ochrony Danych. W *Wytycznych dotyczących oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679* EROD podaje **9 kryteriów oceny operacji**.

Jakie to kryteria?

1. **Ocena lub punktacja**, w tym profilowanie i prognozowanie w szczególności na podstawie „aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą.

> Przykład:
>
> *Ocena zdolności kredytowej, referencyjna baza danych w zakresie przeciwdziałania praniu pieniędzy i zwalczania finansowania terroryzmu lub baza danych zawierająca informacje o nadużyciach finansowych, badania genetyczne w celu oceny i prognozowania ryzyka wystąpienia choroby lub zagrożeń dla zdrowia, tworzenie profili zachowań lub profili marketingowych w oparciu o wykorzystanie lub nawigację na swojej stronie internetowej.*

2. **Automatyczne podejmowanie decyzji o skutku prawnym lub podobnie znaczącym skutku**

> Przykład:
>
> *Ocena zdolności kredytowej na potrzeby zawarcia umowy kredytu z bankiem, gdzie oceny dokonuje się w oparciu o zdefiniowany zestaw reguł i algorytmów, a konsekwencją dokonanej oceny jest automatyczna zgoda na zawarcie umowy lub automatyczna odmowa zawarcia umowy, prowadzenie rekrutacji z wykorzystaniem systemu, który w oparciu o ustalone kryteria dokonuje automatycznego odrzucenia kandydata w toku postępowania rekrutacyjnego, profilowanie dokonane w ramach procesów marketingowych, gdzie na podstawie oceny czynników behawioralnych np. pozostawione przez klienta „ślady" na stronie internetowej sklepu, prowadzić będą do dyskryminacyjnego różnicowania wyświetlanych temu klientowi cen produktów i usług*.

3. **Systematyczne monitorowanie**

Przykład:

Monitoring wizyjny obejmujący miejsca publiczne, stały i systematyczny monitoring aktywności użytkowników w sieci teleinformatycznej.

4. Dane wrażliwe lub dane o charakterze wysoce osobistym

Przykład:

Przechowywanie dokumentacji medycznej pacjentów przez szpital lub przechowywanie szczegółowych danych przestępców przez prywatnego detektywa.

5. Dane przetwarzane na dużą skalę

Przy ustalaniu, czy przetwarzanie danych odbywa się na dużą skalę, wziąć pod uwagę w szczególności następujące czynniki: liczbę osób, których dane dotyczą, ilość danych lub zakres poszczególnych przetwarzanych pozycji danych, czas trwania lub trwałość czynności przetwarzania danych oraz zakres geograficzny czynności przetwarzania.

Przykład:

Przetwarzanie danych pacjentów przez szpital w ramach prowadzonej działalności, przetwarzanie danych dotyczących podróży osób korzystających ze środków komunikacji miejskiej (np. śledzenie za pośrednictwem kart miejskich), przetwarzanie danych geolokalizacyjnych klientów w czasie rzeczywistym przez wyspecjalizowany podmiot na rzecz międzynarodowej sieci fast food do celów statystycznych, przetwarzanie danych klientów przez banki albo ubezpieczycieli w ramach prowadzonej działalności, przetwarzanie danych do celów reklamy behawioralnej przez wyszukiwarki, przetwarzanie danych (dotyczących treści, ruchu, lokalizacji) przez dostawców usług telefonicznych lub internetowych.

6. Dopasowywanie lub łączenie zbiorów danych

Przykład:

Łączenie baz marketingowych z różnych źródeł (własne, zakupione, pobrane ze źródeł powszechnie dostępnych).

7. Dane dotyczące osób wymagających szczególnej opieki

Przykład:

Do osób wymagających szczególnej opieki, których dane dotyczą, można zaliczyć m.in. dzieci oraz bardziej wrażliwe grupy społeczne wymagające szczególnej ochrony (osoby chore psychicznie, osoby ubiegające się o azyl lub osoby starsze, pacjenci itp.).

8. Innowacyjne wykorzystanie lub stosowanie nowych rozwiązań technologicznych lub organizacyjnych

Przykład:

Połączenie technologii rozpoznającej odcisk palca i twarz w celu poprawy fizycznej kontroli dostępu.

9. Przetwarzanie uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy

Przykład:

Monitoring wizyjny przy wejściu do sklepu / hotelu, gdzie bez wkroczenia w obszar monitorowany (przetwarzanie danych w ramach monitoringu) nie jest możliwe dokonanie zakupu / zawarcia umowy na usługę, uzależnianie świadczenia usług od pozytywnej weryfikacji zdolności kredytowej, techniczne ograniczenia w realizacji praw do usunięcia danych ("prawa do bycia zapomnianym").

Za operacje mogące powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych uważa się, w szczególności operacje, które spełniają **co najmniej dwa ze wskazanych kryteriów**. Administrator może jednak uznać, że:

1) przetwarzanie spełniające **tylko jedno z kryteriów będzie wymagało** przeprowadzenia DPIA,

2) przetwarzanie spełniające **dwa lub więcej kryteriów nie będzie wymagało** przeprowadzenia DPIA.

We wskazanych wyżej przypadkach, należy szczegółowo uzasadnić przyjęte stanowisko. W szczególności może to nastąpić poprzez powołanie się na decyzje organów nadzorczych, wytyczne Europejskiej Rady Ochrony Danych, orzecznictwo, praktykę doktryny lub na własne doświadczenia w tym zakresie.

Mając na uwadze zasadę rozliczalności, przeprowadzenie preDPIA powinno zostać oczywiście właściwie udokumentowane.

Nie wiesz jak to zrobić? Skorzystaj z naszego wzoru!

Pobierz nasz sprawdzony szablon preDPIA

POBIERZ

preDPIA – kto ją przeprowadza?

Za zapewnienie przeprowadzenia oceny skutków dla ochrony danych osobowych odpowiada administrator. Analogiczną odpowiedzialność należy przyjąć w stosunku do analizy preDPIA. Trudno sobie jednak wyobrazić sytuację, w której Prezes Zarządu spółki będącej administratorem

samodzielnie dokonuje takiej oceny. Tak jak DPIA, tak i preDPIA wymaga szczegółowej wiedzy na temat danej operacji przetwarzania. Stąd też w analizie uczestniczyć powinny osoby taką wiedzę posiadające, tj. przede wszystkim pracownicy / współpracownicy administratora biorący udział w planowanym lub trwającym już przetwarzaniu.

Nie można w tym zakresie oczywiście zapomnieć o roli IOD. Jeżeli został on wyznaczony, to powinien on również uczestniczyć w analizie preDPIA, chociażby w zakresie konsultacji. W praktyce, często administratorzy pozostawiają inspektorom ochrony danych koordynację całego procesu.

Ostateczną decyzję o przeprowadzeniu lub nieprzeprowadzeniu DPIA dla danej operacji przetwarzania, na podstawie przedstawionej mu analizy, podejmuje oczywiście administrator.

Podsumowanie

Tak samo jak DPIA, tak i analiza preDPIA stanowi ważne narzędzie rozliczalności. Ułatwia administratorowi wykazanie przestrzegania wymogów określonych w RODO. Analiza preDPIA stanowi również jeden z elementów stosowania przez administratora zasady podejścia opartego na ryzyku (ang. *risk-based approach*). Jej przeprowadzenie nie jest czasochłonne (zestawiając ją z np. z DPIA), a daje administratorom wymierne korzyści w zakresie zgodności z przepisami RODO.

Autor artykułu:

Małgorzata Guðfinnsson, ekspert ds. ochrony danych osobowych

Źródła:

- 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)
- Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679
- Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony
- Wytyczne dotyczące inspektorów ochrony danych („DPO")