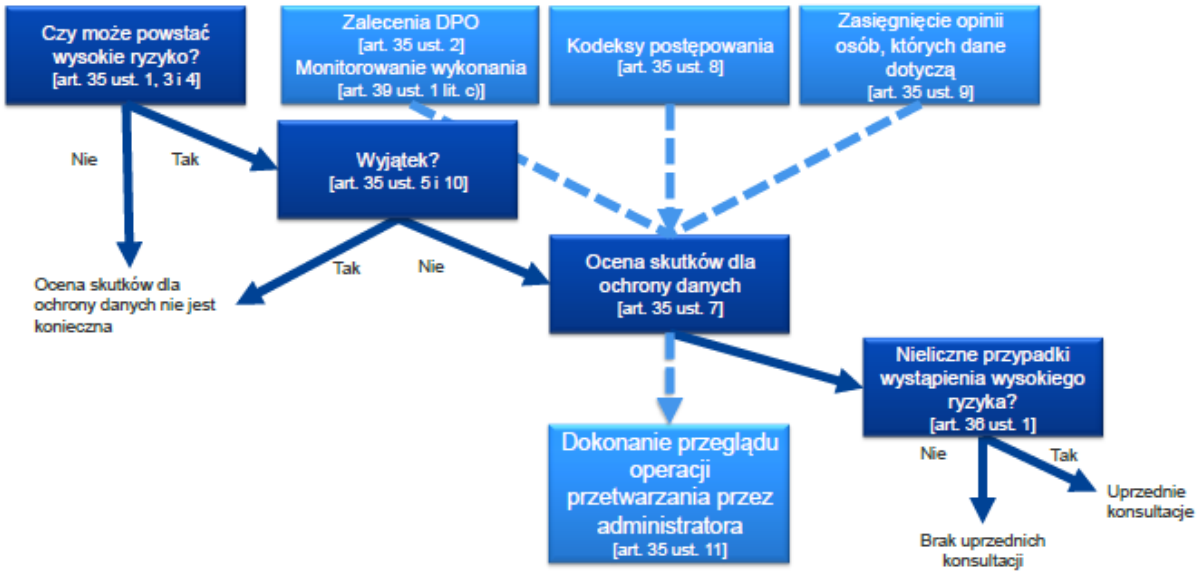
DPIA w organizacji



Jednym z częstych uchybień, które mają miejsce podczas wdrażania RODO, jest błędna ocena co do braku przesłanek do przeprowadzenia oceny skutków dla ochrony danych (Data Protection Impact Assessment, DPIA). Często może być wynikiem przeświadczenia, że skoro niejedna analiza procesu została zrobiona przed wdrożeniem RODO (np. podczas audytu), to już nic więcej nie trzeba oceniać. Natomiast brak przeprowadzenia DPIA, gdy jest wymagana, może przełożyć się na nałożenie „niższej" kary finansowej przez Prezesa UODO. Cudzysłów użyty celowo, gdyż administracyjna kara pieniężna może wynieść do 10 mln Euro, a w przypadku przedsiębiorstwa – w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Wyższe kary są możliwe odpowiednio w wysokości do 20 mln Euro oraz do 4% obrotu, ale za inne naruszenia przepisów RODO. Skupmy się jednak nad oceną przetwarzania – którą Administrator musi dokonać, aby ocenić konkretne prawdopodobieństwo i powagę możliwości zaistnienia wysokiego ryzyka przetwarzania danych osobowych.

Kiedy ocena skutków dla ochrony danych jest konieczna?

Zgodnie z brzmieniem art. 35 ust. 1 RODO oceny dokonujemy, jeżeli dany rodzaj przetwarzania – 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, wówczas Administrator danych osobowych przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. W ustępie 3 wskazanego przepisu Administrator może znaleźć doprecyzowanie. Mianowicie taka ocena skutków jest wymagana w szczególności, w przypadku:

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, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10; lub

c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

Natomiast Administrator nie musi dokonywać oceny skutków przetwarzania, jeżeli przetwarzanie danych zostało oparte na przepisie prawa albo dotyczy zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej (art. 6 ust. 1 lit. c) lub e) RODO) i ma podstawę prawną w przepisach krajowych lub unijnych, które regulują dany proces przetwarzania, a ocenę skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji legislacyjnych. Przeglądając uzasadnienia projektów ustaw, można mieć wątpliwości, czy taka ocena skutków została dokonana w oparciu o zamieszczone przez ustawodawcę następujące zdanie: Rozwiązania przyjęte w projekcie zapewniają ochronę danych osobowych w sposób zgodny z przepisami o ochronie danych osobowych. Pamiętajmy, że racjonalny ustawodawca nie zawsze bywa racjonalny.

Ciągle mam wątpliwości, czy przeprowadzenie DPIA jest wymagane w moim przedsiębiorstwie?

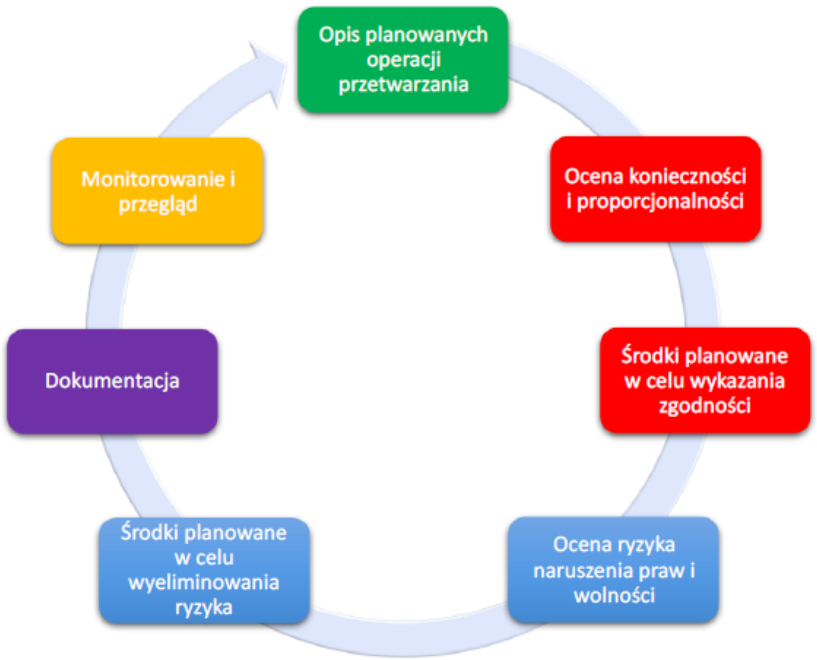
Powyższe przesłanki wymienione w art. 35 ust. 3 RODO wydają się bardziej konkretne. Lecz po ich lekturze Administrator danych wciąż może mieć wątpliwości i szukać powodów utwierdzających go w przekonaniu, że jednak nie jest zobowiązany do dodatkowej analizy. Być może twórcy RODO to przewidzieli i dlatego w art. 35 ust. 4 nakazali organowi krajowemu ds. ochrony danych osobowych upublicznić wykaz rodzajów operacji przetwarzania, które podlegają wymogowi dokonania oceny skutków dla ochrony danych. Z art. 54 ustawy o ochronie danych osobowych dowiemy się, że taki wykaz operacji jest ogłaszany w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski" – i to nie jeden wykaz, a dwa. Mianowicie Prezes Urzędu musi ogłosić listę operacji, dla których DPIA jest wymagane oraz może przedstawić operacje niewymagające DPIA. Oczywiście drugiej listy nie znajdziemy, w końcu jest fakultatywna. Natomiast będąc Administratorem danych możemy odnaleźć operacje wymagające dokonania oceny skutków przetwarzania w Komunikacie 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 [link: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WMP20190000666].
Administrator danych musi jednak pamiętać, że wyliczenia zawarte w powyższym Komunikacie, czy w art. 35 ust. 3 RODO, nie stanowią katalogu zamkniętego. Zostało to również podkreślone w treści załącznika do Komunikatu Prezesa UODO, w którym można przeczytać, że każdy z przykładów obszarów zastosowania ma charakter wyłącznie ilustracyjny, a w konsekwencji „Przykłady operacji/ zakresu danych/ okoliczności, w których może wystąpić wysokie ryzyko naruszenia dla danego rodzaju operacji przetwarzania" nie mają charakteru wyczerpującego. Zawarte w wykazie przykłady mają jedynie na celu pomoc w lepszym zrozumieniu kryteriów/rodzajów operacji mogących skutkować koniecznością przeprowadzenia oceny skutków dla ochrony danych.

Przykłady zawarte w Komunikacie warto przejrzeć, gdyż znajdują się
w nich pozycje mogące mieć zastosowanie u większości Administratorów. Jako przykład można wskazać, że wymieniono przetwarzanie danych w kontekście pracy w domu i pracy wykonywanej zdalnie.

Wiem już, że muszę wykonać DPIA. Tylko jak?

Jeżeli Administrator danych osobowych zlokalizował procesy wymagające dokonania oceny skutków dla ochrony danych, musi pamiętać, by skonsultować się z Inspektorem Ochrony Danych wyznaczonym w organizacji (art. 35 ust. 2 RODO).
W dokonaniu omawianej oceny przychodzi Administratorowi z pomocą art. 35 ust. 7 RODO, zgodnie z którym ocena skutków dla ochrony danych powinna zawierać co najmniej:

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 niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.



Dokonując oceny, należy również pamiętać o uwzględnieniu zatwierdzonych kodeksów postępowania (czyli o białych krukach), o czym stanowi art. 35 ust. 8 RODO oraz o możliwości zasięgnięcia opinii osób, których dane Administrator będzie przetwarzał, na podstawie art. 35 ust. 9 RODO.

Administrator powinien należycie przeprowadzić ocenę skutków przetwarzania z kilku powodów. Jednym z najważniejszych jest uniknięcie negatywnych konsekwencji dla osób fizycznych w związku z przetwarzaniem danych osobowych. Chroniąc osoby fizyczne Administrator może ustrzec się przed złym PR swojej marki oraz administracyjną karą finansową nałożoną przez Prezesa UODO. Kolejnym powodem jest cykliczność wykonywania takiej analizy. Jeżeli wykonamy błędnie DPIA może nie być widoczna poprawa jaka zaszła po wdrożonych środkach w celu zminimalizowania ryzyka związanego z daną operacją wykonywaną na danych osobowych. Nie możemy także zapominać o art. 36 RODO, zgodnie z którym, w określonych sytuacjach należy skonsultować się z organem nadzorczym – czyli Prezesem Urzędu Ochrony Danych Osobowych – i to przed rozpoczęciem przetwarzania, co do którego występuje wysokie ryzyko naruszenia praw lub wolności osób fizycznych, a Administrator nie jest w stanie go zminimalizować odpowiednimi środkami z punktu widzenia dostępnej technologii i kosztów wdrożenia.

Podsumowując.

Administrator w celu poprawienia przestrzegania RODO, w szczególności gdy operacje przetwarzania mogą wiązać się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, musi dokonać oceny skutków dla ochrony danych. Jest to niezbędne w celu oszacowania, w szczególności źródła, charakteru, specyfiki i powagi tego ryzyka. Wyniki dokonanej oceny Administrator powinien uwzględnić przy określaniu odpowiednich środków, które należy zastosować w jego organizacji. Dlatego należy zadbać o poprawne przeprowadzenie DPIA, by wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z RODO.

* Zdjęcia pochodzą z Wytycznych grupy roboczej art. 29 (WP 248) https://uodo.gov.pl/pl/file/17