Warszawa, 18.11.2020 r.

Dokumentacja RODO a zasada rozliczalności. DODATEK: Pytania weryfikujące.

W ubiegłym miesiącu przedstawiliśmy Wam artykuł o dokumentacji zgodnej z RODO. Nie tylko wymieniliśmy podstawowe dokumenty niezbędne przedsiębiorcy, ale dodatkowo opisaliśmy czego one dotyczą i co powinny zawierać. Jeżeli jeszcze nie czytaliście, gorąco zachęcamy https://www.isecure.pl/blog/dokumentacja-zgodna-z-rodo/.

W międzyczasie brytyjskie Biuro Komisarza ds. Informacji (ang. Information Commissioner's Office – ICO) wydało wytyczne dotyczące zasady rozliczalności. Co prawda dokument został przedstawiony dla celów dalszej konsultacji (jego zatwierdzona wersja może mieć nieznacznie zmienioną treść), niemniej zawiera ciekawe spostrzeżenia, którymi podzielimy się z Wami. Przedstawimy głównie zasady, które pomogą w tworzeniu dokumentacji zgodnej z RODO. Zgodnej, czyli spełniającej m. in. wspomnianą zasadę rozliczalności.

Zasada rozliczalności?

O zasadzie rozliczalności pisaliśmy niedawno w kontekście Działów HR: https://www.isecure.pl/blog/rodo-w-hr-jak-zapewnic-rozliczalnosc/. Jest też często wspominana przy okazji omawiania większości artykułów. Nie powinno to dziwić, ponieważ jest jedną z najważniejszych zasad. To ona nakazuje przedsiębiorcy wykazanie, że przepisy RODO są przez niego faktycznie przestrzegane. Krótko mówiąc, kontrolerzy z Urzędu Ochrony Danych Osobowych mają ułatwione zadanie, bo zapytają czy jesteśmy zgodni z RODO, a my musimy udowodnić, że zorganizowaliśmy przetwarzanie danych osobowych w naszej organizacji w sposób prawidłowy, czyli bezpieczny, zgodny z zasadami wynikającymi z unijnego rozporządzenia.

O czym mówią wytyczne ICO?

Dokument z wytycznymi został podzielony na 10 kategorii, a one na mniejsze jednostki redakcyjne, przy czym każda mieści się na jednej stronie. Budowa dokumentu jest niezwykle przejrzysta. Oprócz wskazówek zawiera pomocne pytania sprawdzające spełnienie założeń przez przedsiębiorcę. Wytyczne dotyczą realizacji zasady rozliczalności w takich kategoriach, jak m. in. umowy i udostępnianie danych, przejrzystość, spełnianie praw osób, których dane przetwarzamy czy polityki i procedury. W niniejszym artykule skupimy się na ostatniej kategorii, aby sprawdzić co do powiedzenia ma ICO w zakresie należytego tworzenia dokumentacji zgodnej z RODO – aby była zgodna z zasadą rozliczalności. Zawiera ona 4 sekcje, które omówimy poniżej.

Kierunek i wsparcie – czyli quo vadis Polityko bezpieczeństwa?

Według brytyjskiego organu ramy Polityki powinny wynikać z ustalonego przez kierownictwo planu biznesowego obejmującego procesy, w których występuje przetwarzanie danych osobowych i zarządzanie informacją. Najpierw należy spojrzeć całościowo na organizację, a następnie **objąć dokumentacją wszystkie obszary (działy, czynności) przetwarzania danych**, czyli dostosować treści procedur do operacji występujących w firmie. Innymi słowy - opisać sposób bezpiecznego zarządzania danymi osobowymi w każdym procesie i każdej jednostce organizacyjnej. Powinno w tym uczestniczyć kierownictwo wyższych szczebli, aby przykład czynnego zaangażowania w sprawdzanie procesów (audyt) i tworzenie procedur szedł z góry. W tym punkcie ICO wskazuje, że wszelkie procedury czy wytyczne powinny być łatwo dostępne dla wszystkich pracowników, a kierownictwo

powinno bezpośrednio udzielać wskazówek swojemu personelowi.
Dodatkowo Polityka powinna wyraźnie wskazywać na **role i obowiązki** w zakresie ochrony danych, w tym **osoby odpowiedzialne za realizację poszczególnych działań np. wdrażanie procedur**.

Przegląd i zatwierdzanie dokumentacji.

Tworząc dokumentację należy pamiętać, aby wyrażenia były spójne. Poszczególne załączniki do Polityki nie powinny zawierać odmiennych sformułowań oznaczających to samo. Stosujmy uzgodniony format i styl dokumentacji. Dodatkową wskazówką udzieloną przez ICO jest to, aby najstarszy stażem pracownik przeglądał i zatwierdzał wszystkie nowe i istniejące zasady znajdujące się w dokumentacji. Może to wynikać z największej wiedzy o procesach zachodzących w organizacji.

Przegląd Polityki bezpieczeństwa i innych procedur powinien być dokumentowany. Jeżeli istnieje konieczność aktualizacji wytycznych należy tego dokonać bez zbędnej zwłoki, w szczególności jeżeli zmiany są podyktowane decyzją Prezesa UODO, sądu czy zmianą wytycznych uprawnionych organów (np. unijnych organów doradczych). Każdy dokument powinien mieć numer wersji, właściciela, datę przeglądu i historię zmian.

Pracownicy mają świadomość procedur i zasad przetwarzania danych, na pewno?

Wszystkie dokumenty powinny być napisane w sposób klarowny, aby pracownicy rozumieli zasady i procedury oraz mieli świadomość dlaczego ich wdrożenie i stosowanie jest ważne. Pracownicy powinni być informowani o aktualizacji dokumentów i o miejscu, w którym mogą znaleźć wszystkie aktualne wytyczne. Dodatkowe treści również są wskazane (np. plakaty, przypominajki wysyłane na maila), w celu podniesienia świadomości pracowników..

Privacy by design, privacy by default.

Wszelkie dokumenty powinny nie tylko uwzględnić ryzyka i dostosować do nich sposoby zabezpieczenia danych, ale ponadto muszą uwzględniać zasady projektowania domyślnej ochrony danych. Dla firmy oznacza to, że powinna przewidywać ryzyka i zagrożenie dla prywatności przed ich pojawieniem się, uwzględnić ochronę danych już na etapie projektowania jakiegoś procesu i przyjąć wszystkie możliwe założenia dla prywatności jako domyślne. Dokumentacja powinna go w tym wspierać, biorąc pod uwagę przy każdym procesie, którego dana procedura dotyczy (również przy tych planowanych), m. in. zamierzone czynności przetwarzania czy możliwe środki ograniczające ryzyko naruszenia danych osobowych.

Podsumowanie – dlaczego treść i świadomość procedur ma znaczenie?

Polityka bezpieczeństwa (polityka ochrony danych) i inne procedury jej towarzyszące są najważniejszymi dokumentami dotyczącymi ochrony danych osobowych u przedsiębiorcy. Pracownik powinien je znać i rozumieć, aby móc stosować. Jeżeli w sposób przejrzysty i spójny nie zakomunikujemy pracownikom, co powinni robić, jak postępować z danymi osobowymi i dlaczego to jest ważne dla organizacji w której pracują, to według brytyjskiego organu dokumenty te nie będą miały sensu, ponieważ nie będą spełniały swojej podstawowej roli. Poziom szczegółowości dokumentów może być różny, co jest uzależnione od wielkości firmy, ryzyka czy przetwarzanych danych. Jednak należy pamiętać, że nie liczy się grubość segregatora, a dobranie skutecznych zasad i procedur, które w praktyce pozwolą wypełnić obowiązki prawne przedsiębiorcy w zakresie wymogów stawianych mu przez RODO.

BONUS! Checklista od ICO pomagająca wskazać w którym miejscu znajdujesz się w zakresie realizacji zasady rozliczalności przy tworzeniu dokumentów.

Czy potrafisz twierdząco odpowiedzieć na poniższe pytania?

1. Czy pracownicy wiedzą, gdzie znaleźć odpowiednie wytyczne dotyczące przetwarzania danych w Twojej organizacji i czy łatwo je znaleźć?
2. Czy personel w Twojej firmie potrafiłby wyjaśnić swoją rolę i obowiązki w zakresie bezpieczeństwa przetwarzania danych i czy dostarczone wytyczne/procedury im w tym pomagają?
3. Czy dyrektorzy/kierownictwo wyższego szczebla jest świadome konieczności ochrony danych osobowych?
4. Czy proces zatwierdzania dokumentów/sposobu przetwarzania danych jest odpowiedni?
5. Czy treści w procedurach są zrozumiałe dla pracowników?
6. Czy są udostępniane dodatkowe materiały pracownikom podnoszące świadomość w zakresie ochrony danych osobowych i czy są łatwo dostępne?

Przemysław Siarka, Specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.