Warszawa, 1.10.2020 r.

Audyt RODO – czy rzeczywiście jest potrzebny i w jaki sposób go przeprowadzić?

Gdy rozmawiam z potencjalnymi klientami, często od nich słyszę, że nie chcą żadnych audytów tylko chcą być zgodni z RODO. Rzeczywiście istnieją w naszej branży podmioty, które oferują gotowe „pakiety" zgodności z RODO w postaci wzorów dokumentacji, klauzul i ogólnych zaleceń. Warto jednak zadać sobie wówczas pytanie czy otrzymując taki pakiet będziecie wiedzieli co z nim zrobić? Poza tym wdrożenie RODO to dużo więcej niż wzory dokumentacji czy klauzul i ogólnych zaleceń. Specjaliści iSecure, mimo że zajmują się ochroną danych osobowych od kilkunastu lat, żeby rzetelnie wdrożyć RODO u Klienta, muszą najpierw go dobrze poznać. Nawet jeżeli klient dysponuje już raportami z wcześniej przeprowadzonych audytów, audytor rozpoczynający dopiero swoją pracę na jego rzecz może się nimi tylko posiłkować, ale żeby móc wziąć odpowiedzialność za zgodność z RODO, musi sam zweryfikować, które obszary wymagają ewentualnych działań naprawczych i/lub aktualizacyjnych.

Odpowiedź na postawione w tytule pytanie brzmi więc:

bez audytu nie da się odpowiednio wdrożyć wymogów wynikających z RODO!

Rozpoczynając audyt należy określić, **do których obszarów i informacji należy stosować przepisy RODO**. Są obszary, które tego nie wymagają, np. działy produkcji zajmujące się wyłącznie produkcją, a nie czynnościami wymagającymi dostępu do danych osobowych, przy czym nie możemy z góry założyć, że w całym ww. dziale nie będą przetwarzane dane osobowe np. na skutek prowadzenia monitoringu wizyjnego mającego na celu kontrolę tejże produkcji. Tego dowiemy się dopiero po rozmowie z przedstawicielami takiego działu.

Gdy już zostaną zidentyfikowane obszary, w których są przetwarzane dane osobowe, należy określić **status organizacji** w stosunku do tych danych. W większości przypadków audytowana firma będzie administratorem danych, ale w stosunku do części z nich może być współadministratorem, podmiotem przetwarzającym (procesorem) czy nawet subprocesorem. Określenie roli ściśle wiąże się również z określeniem legalności przetwarzania tych konkretnych danych. Czy dane są przetwarzane, bo wynika to z przepisu prawa? Czy może musimy je przetwarzać w związku z realizacją jakiejś umowy? A może mamy tzw. uzasadniony interes (np. ewidencjonujemy korespondencję, by w łatwy sposób móc dotrzeć do pisma z konkretnego dnia i dotyczącego konkretnego adresata) na ich przetwarzanie, a jeśli tak, to czy aby na pewno jest on uzasadniony w rozumieniu przepisów RODO? Największe ryzyko generuje przetwarzanie danych na podstawie zgody osoby, której te dane dotyczą. W RODO znajdują się oddzielne artykuły mówiące o warunkach przetwarzania danych na jej podstawie, a do tego mogą dojść wymagania wynikające z przepisów szczególnych, np. ustawy o świadczeniu usług drogą elektroniczną czy ustawy Prawo telekomunikacyjne.

Kolejnym etapem jest weryfikacja czy osoby, których dane organizacja przetwarza, posiadają wiedzę o tym, że taki fakt ma w ogóle miejsce, a także o innych szczegółach z tym powiązanych takich jak np. informacje o przysługujących uprawnieniach (przykładowo: możliwości zażądania usunięcia danych), a jeżeli ją posiadają to czy zostały przekazane w sposób prawidłowy i kompletny. Krótko mówiąc, chodzi o zweryfikowanie, **czy został skutecznie dopełniony obowiązek informacyjny**.

Dopiero po zebraniu takich informacji możemy przejść do sfery organizacyjnej, tj. analizy odpowiednich zapisów w umowach dot. przetwarzania danych, posiadania procedur ochrony danych – tych wymaganych wprost przez RODO jak również takich, które wynikają z powszechnie akceptowanej dobrej praktyki, przestrzegania przez personel organizacji zapisów wynikających z tych procedur (samo ich posiadanie nie wystarczy), systematycznego szkolenia, posiadania aktualnych rejestrów czynności przetwarzania i/lub rejestrów kategorii czynności, i wielu innych, które tak naprawdę możemy określić po przeprowadzeniu pierwszej części audytu. W tym obszarze należy sprawdzić również czy dla poszczególnych procesów została przeprowadzona ocena ryzyka, a jeżeli tak to czy jest ona prowadzona systematycznie, a nade wszystko, czy wynikające z niej rekomendacje są wdrożone.

I na koniec należy **zweryfikować stosowane środki techniczne** (informatyczne, fizyczne), które mają na celu zabezpieczenie przetwarzanych w firmie danych.

Zebrany w ten sposób materiał audytowy pozwoli przede wszystkim dokonać identyfikacji obszarów wymagających poprawy i docelowe wdrożenie środków, które tę poprawę zapewnią. **Wyniki prac audytowych**, dla celów dowodowych, **należy zamieścić w raporcie poaudytowym** prezentując tam opis niezgodności, w tym wykryte naruszenia prawa, dowody potwierdzające te niezgodności oraz rekomendacje, co do sposobu ich likwidacji. Taki raport powinien zostać przedstawiony najwyższemu kierownictwu organizacji, ponieważ to na nim spoczywa pełna odpowiedzialność za przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami. Raport poaudytowy stanowi również potwierdzenie prowadzenia systematycznej kontroli systemu ochrony danych w organizacji.

Maria Lothamer, Wiceprezes Zarządu iSecure Sp. z o.o.