Katowice, 24 maja 2017r.

Z praktyki zespołu audytorów – ochrona danych osobowych dziś i po rozpoczęciu obowiązywania Rozporządzenia unijnego

Tytuł niniejszego artykułu nie jest przypadkowy. Jako osoba pasjonująca się tematyką ochrony danych osobowych, stworzyłam zespół doradców złożony z prawników, informatyków i audytorów, z którym wspólnie promujemy procesowe, praktyczne podejście do tematyki ochrony danych osobowych. Dzięki realizowanym od lat projektom z zakresu wdrażania systemów ochrony danych osobowych w organizacjach publicznych i prywatnych oraz dzięki pełnieniu funkcji ABI, audytora oraz doradcy, w swojej pracy zwracamy uwagę na te aspekty ochrony danych osobowych, które bardzo często sprawiają problemy osobom odpowiedzialnym w jednostkach organizacyjnych za obszar ochrony danych osobowych. Propagowana przez nas filozofia podejścia do ochrony danych osobowych wpisuje się w ideę ochrony danych, na której opiera się nowe Rozporządzenie unijne – 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 (dalej: rodo). Aby sprostać jego wymogom, punktem wyjścia musi być przyjęcie przez administratorów danych „podejścia procesowego", tj. orientacji na rzeczywiste dostosowanie do wymogów prawnych poszczególnych procesów dotyczących przetwarzania danych osobowych oraz wdrożenie rozwiązań dopasowanych do specyfiki organizacji, a co za tym idzie, także różnorodnych ryzyk związanych z operacjami wykonywanymi na danych osobowych.

Zmiany wprowadzone przez rodo, w szczególności nowe obowiązki ciążące na administratorach danych; nowe, szersze prawa osób, których dane dotyczą; nowe uprawnienia organów nadzorczych oraz bardzo wysokie administracyjne kary finansowe za naruszenia przepisów prawnych, wymuszą ustanowienie obszaru ochrony danych osobowych jako ważnego elementu funkcjonowania każdej organizacji. Aspekt bezpieczeństwa danych osobowych, który wciąż jeszcze jest przez wiele podmiotów marginalizowany, stanie się istotnym kryterium warunkującym powodzenie przedsięwzięć biznesowych.

PERSONA Magdalena Korga
Chorzów 41-506 | ul. Stefana Batorego 48/412
tel./fax 32 247 000 | tel. kom. 606 199 177 | e-mail: biuro@daneosobowe.co
NIP: 634-226-70-57 | REGON: 242 133 363 | nr rachunku: 10 1050 1243 1000 0090 9027 9895

Aby przygotować się do stosowania przepisów rodo, należy w pierwszej kolejności podsumować to, co w nowych przepisach nie ulega zmianie, a ma znaczenie dla administratora danych, oraz to, co podlega modyfikacji lub jest zupełnie nowym wymogiem. Przepisy rodo muszą się zakorzenić w naszej świadomości, z uwagi na fakt, że już teraz powinny mieć one znaczenie dla wykładni istniejących przepisów prawa ochrony danych. Wraz z wydawanymi w przyszłości przez Komisję Europejską aktami delegowanymi, opiniami Generalnego Inspektora Ochrony Danych Osobowych oraz Grupy Roboczej art. 29 (a później Europejskiej Rady Ochrony Danych Osobowych), przepisy rodo muszą stanowić podstawę modyfikacji procesów i dokumentacji obecnie obowiązujących w podmiotach przetwarzających dane, tak by były one zgodne z nowym stanem prawnym, który zacznie obowiązywać 25 maja 2018 r.

Obszary, które w rodo nie podlegają znacznym modyfikacjom to:

- definicja danych osobowych (za wyjątkiem danych wrażliwych), przetwarzania, zbioru danych (wraz z kryteriami jego identyfikacji);
- zasady uznania za administratora danych (za wyjątkiem zasad dotyczących współadministratorów) oraz za podmiot przetwarzający dane na zlecenie administratora;
- podział obowiązków informacyjnych uzależniony od sposobu zbierania danych: od podmiotu, którego dane dotyczą, oraz z pośrednich źródeł;
- zasady szczególnej staranności służące ochronie interesów osób, których dane dotyczą (celowość, adekwatność, czasowość, merytoryczna poprawność, legalność);
- większość zadań dotyczących obecnego ABI, a w przyszłości inspektora ochrony danych oraz jego statusu;
- większość przepisów związanych z transferem danych do państw trzecich.

Najważniejszymi, znacząco zmodyfikowanymi lub zupełnie nowymi instytucjami i zasadami rodo są:

- pseudonimizacja jako nowy rodzaj postępowania z danymi, będący ich dodatkowym zabezpieczeniem;
- szerszy zakres terytorialny stosowania unijnych przepisów prawa ochrony danych;
- modyfikacja zasad dopuszczalnego profilowania danych osobowych;
- konstrukcja prawna zgody na przetwarzanie danych osobowych wraz z warunkami jej wyrażenia;
- rozszerzenie zakresu obowiązku informacyjnego przekazywanego w przypadku zbierania danych od osoby, której dane dotyczą oraz z pośrednich źródeł;
- dopuszczalność współadministrowania danymi przez co najmniej dwóch administratorów;
- prawa podmiotu danych:

a) do usunięcia danych, inaczej zwane prawem do bycia zapomnianym,
b) do przenoszenia danych;
- dookreślenie relacji między administratorem danych a podmiotem przetwarzającym;
- modyfikacja obowiązku rejestracyjnego;
- modyfikacja obowiązków związanych z bezpieczeństwem przetwarzania danych, w tym obowiązek notyfikacji – zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu, a w wybranych przypadkach także osobie, której dane dotyczą;
- konieczność dokonywania oceny skutków dla ochrony danych;
- obowiązek uprzedniego konsultowania się z organem nadzorczym;
- obowiązek wyznaczenia inspektora ochrony danych w odniesieniu do niektórych podmiotów;
- mechanizmy mające pomóc we właściwym stosowaniu przepisów prawa ochrony danych – kodeksy postępowania oraz certyfikacja;
- uprawnienia organu nadzorczego – naprawcze oraz do nakładania administracyjnych kar pieniężnych;
- prawo do odszkodowania za naruszenie przepisów o ochronie danych osobowych.

Analiza przepisów rodo prowadzi do wniosku, że zmienia się sposób patrzenia na ochronę danych osobowych. Obecnie przewidziane kazuistyczne rozwiązania wskazane w ustawie o ochronie danych osobowych (dalej: uodo), a także, a może przede wszystkim, w rozporządzeniach wykonawczych do uodo (rejestracja zbiorów danych, uprzednia zgoda organu ochrony danych na określone operacje na danych, określona długość, złożoność haseł i częstotliwość ich zmiany), zostają zastąpione ogólnymi założeniami – administratorom zostają postawione ogólne cele, a drogę do ich osiągnięcia muszą wytyczać sami. To na administratorach danych będzie ciążyć odpowiedzialność za właściwą ocenę ryzyka związanego z wykonywaniem operacji na danych oraz za wdrożenie wewnętrznych procedur zapewniających ich zgodność z przepisami prawa. Jednocześnie te podmioty będą zobowiązane wykazać, że właściwie spełniły wymogi przepisów ochrony danych osobowych oraz, że wdrożone przez nie środki są skuteczne (przy czym środki powinny uwzględniać charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych).

Rodo wymusza na administratorach danych ochronę danych osobowych już w fazie projektowania nowego procesu związanego z przetwarzaniem danych osobowych. Administrator danych będzie zobowiązany do przeprowadzenia analizy i oceny, czy planowane operacje na danych osobowych w konkretnym procesie oraz sposoby ich zabezpieczenia będą zgodne z obowiązującymi przepisami prawa, zwłaszcza z przepisami rodo. Administrator danych będzie zobowiązany również do wdrożenia środków technicznych i organizacyjnych zapewniających, że domyślnie będą

przetwarzane jedynie te dane, które są niezbędne. Wdrożone rozwiązania powinny skutkować m.in. zapewnieniem, że dane nie będą przetwarzane dłużej niż jest to niezbędne, a po zrealizowaniu celu przetwarzania zostaną usunięte lub zanonimizowane. Obecnie najczęściej spotykanym przez nas problemem w systemach lub aplikacjach jest brak adekwatności gromadzonych danych osobowych do celu ich przetwarzania oraz przechowywanie danych osobowych w postaci elektronicznej bez żadnego wskazanego okresu archiwizacyjnego, czyli nieskończenie długo. Jako przykład takich złych praktyk można podać kartoteki klienta w systemie lub aplikacji do wystawiania faktur zawierające pola informacyjne takie jak numer PESEL, imię ojca i matki, nazwisko rodowe matki, zdjęcie osoby.

W tym miejscu pragnę podkreślić, że nawet ci administratorzy, którzy już teraz przetwarzają dane zgodnie z zasadami określonymi w uodo, powinni jak najszybciej podjąć stosowne działania, tak by w momencie rozpoczęcia obowiązywania rodo móc przetwarzać dane zgodnie z jego wymaganiami. Podejmując czynności dostosowawcze administratorzy powinni zweryfikować, czy są w stanie zrealizować między innymi poniższe wymagania:

- Prowadzenie analiz wpływu na prywatność (ang. *data protection impact assessment*). Jest to nowy obowiązek administratorów danych – zanim przepisy rodo zaczną obowiązywać, administratorzy powinni posiąść niezbędną wiedzę i umiejętność prowadzenia takiej analizy. Analizę wpływu na prywatność administrator danych musi prowadzić, jeżeli dany rodzaj przetwarzania z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Analiza ma na celu zapewnienie, że administrator danych należycie uwzględni interesy osób, których dane przetwarza, i przeprowadzi analizę obejmującą m.in. ocenę ryzyka naruszenia praw lub wolności osób (której nie należy mylić z analizą ryzyka związaną z doborem zabezpieczeń).

- Powiadomienie organu nadzorczego w przypadku naruszenia ochrony danych osobowych. W określonych sytuacjach będą musiały być powiadomione również osoby, których dotyczy naruszenie danych. Ponieważ organ nadzorczy będzie musiał zostać powiadomiony w ciągu 72 godzin od momentu stwierdzeniu naruszenia, administratorzy powinni opracować, wdrożyć i przetestować procedury zapewniające dotrzymanie tego terminu.

- Systemy informatyczne administratora danych muszą umożliwiać wyeksportowanie danych dotyczących osoby fizycznej w celu umożliwienia jej np. przeniesienia danych do innego administratora. Dane muszą być wyeksportowane w powszechnie używanym formacie - zapewne zwykle będzie to format XML lub CSV. Administrator danych musi umożliwić przeniesienie danych, jeżeli są one przetwarzane na podstawie zgody lub umowy.

- W związku z dużo szerszymi wymaganiami dotyczącymi zawierania umów powierzenia przetwarzania **administratorzy powinni dokonać przeglądu aktualnie obowiązujących umów w tym zakresie.** Powinni zapewnić, że od 25 maja 2018 r., wszystkie umowy powierzenia przetwarzania danych będą zgodne z wymogami rodo.

Należy podkreślić, iż wdrożony w organizacji system ochrony danych osobowych bazujący na założeniach procesowego, kompleksowego podejścia do ochrony danych, w momencie rozpoczęcia obowiązywania przepisów rodo będzie w dużej mierze aktualny i w znacznej części prawidłowy. Konieczne będzie oczywiście dostosowanie wybranych istniejących procesów i procedur do przepisów unijnych oraz uzupełnienie istniejącego systemu o nowe, wymagane przez przepisy prawa elementy – procesy i procedury, jednak podstawowe założenia ochrony danych pozostaną takie same.

Magdalena Korga