Stowarzyszenie
Administratorów
Bezpieczeństwa
Informacji

Warszawa, 13 stycznia 2011 r.

Stanowisko Stowarzyszenia Administratorów Bezpieczeństwa Informacji w sprawie zmian w dyrektywie 95/46/WE

Stowarzyszenie Administratorów Bezpieczeństwa Informacji jest organizacją pozarządową działającą na podstawie Prawa o stowarzyszeniach obowiązującego w Polsce. Jego członkami są osoby wypełniające funkcje Administratora Bezpieczeństwa Informacji w podmiotach zarówno sektora publicznego jak i sektora prywatnego oraz osoby w inny sposób zajmujące się ochroną danych osobowych. Celem Stowarzyszenia jest upowszechnianie wiedzy o ochronie danych osobowych oraz podnoszenie poziomu umiejętności zawodowych osób zajmujących się ochroną danych osobowych. W Stowarzyszeniu został opracowany, jest stosowany i promowany na zewnątrz Kodeks Etyki Zawodowej Administratorów Bezpieczeństwa Informacji. Stowarzyszenie uczestniczy w pracach legislacyjnych nad krajowymi przepisami o ochronie danych osobowych. Współpracuje z organem ochrony danych osobowych w Polsce – Generalnym Inspektorem Ochrony Danych Osobowych.

Stowarzyszenie Administratorów Bezpieczeństwa Informacji zrzeszające osoby zajmujące się w praktyce stosowaniem prawa ochrony danych osobowych z zadowoleniem przyjmuje inicjatywę Komisji Europejskiej o podjęciu prac zmierzających do zwiększenia skuteczności prawa ochrony danych osobowych. Odpowiadając na apel Komisji o udziale w społecznej konsultacji dotyczącej nowych ram prawnych w zakresie ochrony danych Stowarzyszenie przedstawia stanowisko o potrzebie zmian w dyrektywie 95/46/WE w kwestiach dotyczących urzędnika do spraw ochrony danych osobowych oraz Grupy Roboczej art. 29 dyrektywy.

I. Urzędnik ds. ochrony danych osobowych

I.1 Daleko idącej reformy wymaga dyrektywa 95/46/WE w zakresie urzędnika ds. ochrony danych osobowych. Reforma tej instytucji powinna opierać się na założeniu, że funkcjonowanie urzędnika ma przynieść stosowne korzyści wszystkim podmiotom uczestniczącym w wykonywaniu zadań ochrony danych osobowych:

a) krajowemu organowi państwowemu ds. ochrony danych osobowych, ponieważ wzmocniona będzie kontrola przestrzegania przepisów o ochronie danych osobowych, której ciężar zostaje w części przesunięty z poziomy krajowego organu na poziom wewnętrznego urzędnika,
b) administratorowi danych, ponieważ oprócz ograniczenia formalnych obowiązków względem organu państwowego (tak jak dotychczas), podlega on zmienionym zasadom odpowiedzialności za przestrzeganie przepisów o ochronie danych osobowych, które mogą wpływać na lepsze dla niego dostosowanie się do obowiązków ochrony danych.
c) samemu urzędnikowi, któremu zapewnia się niezależne wykonywanie zadań i gwarantuje się stabilność funkcji (*pracy*),
d) podmiotowi danych, któremu zapewnia się lepsze i skuteczniejsze wykonywanie uprawnień wobec administratora danych.

I.2 W celu realizacji powyższych celów należy wprowadzić do dyrektywy przepisy stanowiące samodzielną podstawę prawną działalności urzędnika. Obecnie urzędnik występuje jedynie w przepisach dotyczących notyfikacji (art. 18-19) i kontroli wstępnej (art. 20), co z punktu widzenia wyzwań nie jest wystarczające. Nowe przepisy powinny zapewnić jednolite wykonywanie funkcji urzędnika we wszystkich państwach członkowskich.

I.3 Istota proponowanego rozwiązania polega na tym, że modyfikacji w dyrektywie ulegają zasady wykonywania obowiązków ochronie danych osobowych w zakresie kontroli administratora danych (processor'a) oraz realizacji praw podmiotu danych. Modyfikacja polega na przejęciu części zadań w tym przedmiocie przez urzędnika, o czym w pkt I.4-I.6.

I.4 Nowe przepisy dyrektywy dotyczące urzędnika powinny określać:

a) jego szczegółowe zadania, które w naszej ocenie winny koncentrować się na:

- wewnętrznej kontroli przestrzegania przepisów o ochronie danych osobowych oraz wewnętrznych procedur organizacji w tym zakresie,
- podnoszeniu świadomości osób przetwarzających dane osobowe w organizacji w zakresie zasad ochrony,
- udzielaniu pomocy osobie, której dane dotyczą w wykonywaniu jej uprawnień wobec administratora danych *i processor*'a (chodzi przede wszystkim o techniczną realizację żądań informacyjnych i korekcyjnych podmiotu danych),

b) zasady współdziałania urzędnika z krajowym organem ochrony danych osobowych,

c) wymogi kwalifikacyjne wobec urzędnika (wiedza, doświadczenie, wykształcenie),

d) konkretne gwarancje niezależnego wykonywania swoich zadań przez urzędnika (np. gwarancje zatrudnienia).

I.5 Krajowe organy ochrony danych osobowych winny wspomagać urzędnika w wykonywaniu jego zadań poprzez udzielanie stosownych wyjaśnień i porad, jak również - co najmniej jednorazowo dla każdego urzędnika - szkoląc go w wykonywaniu jego zadań. Krajowe organy ochrony danych osobowych, jeżeli nie sprzeciwia się temu interes publiczny, przeprowadzają kontrole administratora (*processor*'a) poprzez zlecenie tych czynności urzędnikowi. Urzędnik po przeprowadzeniu kontroli przedstawia organowi raport, w którym – w przypadku zaistnienia nieprawidłowości - rekomenduje działania przywracające stan prawidłowy. Zatwierdzany przez organ krajowy raport obliguje administratora danych do podjęcia stosownych działań. Urzędnik jest również z własnej inicjatywy uprawniony do zawiadamia organu krajowego o nieprawidłowościach.

W przypadku działania urzędnika naruszającego interes publiczny organ krajowy winien zostać wyposażony w kompetencje do usuwania urzędnika z funkcji.

I.6 Osobie, której dane dotyczą i urzędnikowi powinna zostać zagwarantowana możliwość odformalizowanych procedury udzielania informacji i wyjaśniania wątpliwości dotyczących przetwarzania jej danych osobowych. Taka procedura miałaby charakter wstępny wobec formalnych żądań podmiotu danych wobec administratora. W tej procedurze uczestniczyłby urzędnik lub co najmniej organizowałby proces załatwiania spraw w swojej jednostce. Skorzystanie z odformalizowanej procedury zależne byłoby od woli osoby, której dane dotyczą.

W związku z tym dane urzędnika (imię, nazwisko, telefon, e-mail) powinny być jawne i umieszczane w serwisie internetowym administratora. Można się również zastanowić nad prowadzeniem przez organ krajowy jawnej, ogólnokrajowej listy urzędników.

I.7 Warto rozważyć, aby w korporacjach działających w różnych państwach wprowadzić możliwość funkcjonowania dodatkowego urzędnika koordynującego działania „urzędników krajowych".

I.8 W niniejszym stanowisku nie przesądzamy, czy wyznaczenie urzędnika powinno mieć charakter obowiązkowy czy dobrowolny. Jedynie wskazujemy, że w przypadku dobrowolnego wyznaczania urzędnika przepisy prawa winny stwarzać mechanizm „zachęt" dla administratora (processor'a) do takiego wyznaczenia.

II. Grupa Robocza (art. 29 dyrektywy)

Działalność grupy i jej skład powinny być w szerszym niż obecnie stopniu otwarte na czynnik społeczny, w tym organizacje zrzeszające urzędników ds. ochrony danych osobowych oraz branże objęte kodeksami postępowania (art. 27). W naszej opinii wspomniane otwarcie powinno polegać co najmniej na wprowadzeniu uprawnień dla czynnika społecznego do: wiążącego grupę występowania o zajęcie stanowiska oraz przedstawiania swoich opinii w trakcie prac grupy (bez prawa głosu w podejmowaniu decyzji).

Do wiadomości: Generalnego Inspektora Ochrony Danych Osobowych