



Bruksela, dnia 22 października 2012 r.

KANCELARIA SENATU

Przedstawiciel Kancelarii Senatu  
przy Unii Europejskiej

**Sprawozdanie nr 79/2012**

**Sprawozdanie ze spotkania polskich eurodeputowanych  
z p. Wojciechem Wiewiórowskim - Generalnym Inspektorem  
Ochrony Danych Osobowych**

W dniu 9 października 2012 roku w ramach tzw. Koła Polskiego odbyło się spotkanie polskich eurodeputowanych z panem **Wojciechem Wiewiórowskim** - Generalnym Inspektorem Ochrony Danych Osobowych. Tematem spotkania była planowana reforma ochrony danych osobowych w Unii Europejskiej.

W ciągu minionych ponad piętnastu lat od wejścia w życie dyrektywy w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, odsetek ludzi korzystających z internetu wzrósł wielokrotnie, podobnie jak pojemność pamięci komputerów, a tym samym - wzrosły możliwości zbierania i przechowywania danych. W konsekwencji tego procesu powstały ogromne zbiory danych osobowych, znajdujące się zarówno w rękach prywatnych, jak i państwowych. Obowiązujące przepisy prawne nie uwzględniły postępu w tej dziedzinie na tak dużą skalę. Są one technicznie przestarzałe i wymagają aktualizacji i dostosowania do obecnych realiów.

Ponadto, w cyfrowym, zglobalizowanym świecie dogłębnie zmienił się sposób gromadzenia, wykorzystywania i przekazywania danych osobowych oraz dostępu do nich, jednocześnie nabrał on bardziej zaawansowanego charakteru. Nowe technologie pozwalają na ciągłe zwiększanie zasobów danych osobowych. Podobnie organy

ścigania znacząco wzmogły przetwarzanie danych osobowych do celów wykonywania swoich zadań.

W tym środowisku pełnym wyzwań ochrona danych osobowych stała się głównym przedmiotem zainteresowania, co do praw jednostki w odniesieniu do ochrony dotyczących jej danych oraz co do koniecznego i proporcjonalnego przetwarzania danych osobowych przez podmioty prywatne i organy publiczne. Ochrona danych jest podstawowym prawem zapisanym w art. 8 Karty praw podstawowych Unii Europejskiej i w art. 16 Traktatu o funkcjonowaniu Unii Europejskiej.

W związku z tym, w oparciu o doświadczenia zdobyte w związku z obecną dyrektywą nr 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. L 281 z 23.11.1995, s. 31) i decyzją ramową Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (Dz.U. L 350 z 30.12.2008, s. 60)<sup>1</sup>, a także na podstawie stanowiska Parlamentu Europejskiego<sup>2</sup>, **Komisja przedstawiła dwa wnioski** – wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych, COM(2012)0011) oraz wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych (dyrektywa o ochronie danych, COM(2012)0010). Początkowo Komisja zamierzała przedstawić jeden horyzontalny akt prawny<sup>3</sup>. Obydwa nowe akty, jeżeli zostaną przyjęte, w znacznym stopniu określą przepisy i zasady ochrony danych w UE na następne dziesięciolecia. Celem obydwu wniosków jest według Komisji stworzenie nowoczesnych, solidnych i

---

<sup>1</sup> Zob. również komunikat Komisji w sprawie ochrony prywatności w połączonym świecie – europejskie ramy ochrony danych w XXI wieku (COM(2012)0009).

<sup>2</sup> Rezolucja Parlamentu Europejskiego z dnia 6 lipca 2011 r. w sprawie całościowego podejścia do kwestii ochrony danych osobowych w Unii Europejskiej (P7\_TA-PROV(2011)0323).

<sup>3</sup> Komunikat Komisji w sprawie całościowego podejścia do kwestii ochrony danych osobowych w Unii Europejskiej (COM(2010)0609).

spójnych ram ochrony danych we wszystkich obszarach polityki Unii, wzmocniających prawa jednostki, pogłębiających wymiar jednolitego rynku dotyczący ochrony danych, ograniczających obciążenia administracyjne dla przedsiębiorstw i obejmujących zagadnienia związane z transnarodowym przepływem danych osobowych.

Komisja 25 stycznia 2012 roku opublikowała ww. projekty rozporządzenia i dyrektywy. Teksty tych wniosków można znaleźć pod adresami:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:PL:PDF> oraz <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:PL:PDF>.

Komisja chce zastąpić wcześniejszą dyrektywę rozporządzeniem, ponieważ fakt, że dyrektywy muszą być implementowane do prawa państw członkowskich, spowodował powstanie bardzo różnorodnych ustaw narodowych w tej dziedzinie. Dyrektywy bowiem w wielu kwestiach pozostawiają krajom członkowskim Unii znaczną swobodę wyboru rozwiązań. W celu stworzenia jednolitego systemu ochrony praw osobowych, Komisja zdecydowała się na skorzystanie z możliwości ustanowienia rozporządzenia, jako aktu prawnego bezpośrednio obowiązującego w każdym państwie członkowskim. Dwadzieścia siedem krajowych systemów prawa ochrony, przetwarzania i przepływu danych osobowych zostałyby zastąpionych przez jednolity w skali całej UE system. Dodatkowo została jednak przedstawiona dyrektywa, która swym zakresem ma objąć ochronę danych osobowych w sektorze publicznym, w pierwszej kolejności policji i służb specjalnych. Motywem wyjęcia tych służb z zakresu rozporządzenia jest fakt, iż przyjmuje się założenie, iż instytucje państwowe będą się czuły bardziej zobowiązane ustawą własnego kraju niż aktem prawnym UE.

W tym aspekcie te dwa akty powinny m.in. położyć kres obecnemu rozdrobnieniu na szczegółowe przepisy krajowe (stąd forma rozporządzenia dla pierwszego wniosku), rozszerzyć wspólne zasady na czysto wewnętrzne przypadki przetwarzania danych, także w obszarze egzekwowania prawa (dotyczy dyrektywy), tak by zapewnić wysoki poziom ochrony podstawowego prawa jednostki do ochrony danych. W rezultacie zwiększy się zaufanie jednostek do gospodarki cyfrowej i zaufanie obywateli do ochrony podstawowych praw przez organy policji i organy sądowe państw

członkowskich, tym samym przyczyniając się do wzrostu gospodarczego i skutecznej pracy organów ścigania.

Co do treści wniosków, Generalny Inspektor Ochrony Danych Osobowych zwracał uwagę na fakt, że Komisja chce sobie zastrzec prawo do wydania wyjątkowo dużej ilości **aktów delegowanych**. Spowodowało to obawy obrońców praw obywateli w zakresie danych osobowych, ponieważ dawałoby to Komisji bardzo daleko idącą możliwość ustanawiania prawa poza kontrolą zarówno Rady, jak i Parlamentu Europejskiego. Szczególne zastrzeżenia budzi możliwość podejmowania decyzji indywidualnych.

Wyjątkowo krytycznie trzeba spojrzeć na **problem ochrony prawnej**. Komisja ma zamiar ułatwić przedsiębiorstwom spełnianie wymogów administracyjnych i proponuje system, w którym podmiot działający w więcej niż jednym kraju Unii musiałby kontaktować się i współpracować tylko z urzędem odpowiedzialnym za ochronę danych osobowych jednego kraju. O ile stanowiłoby to znaczne ułatwienie w kontaktach z administracją dla przedsiębiorstw zarządzających danymi, takie rozwiązanie oznaczałoby, dla osób chcących bronić swoich praw na drodze administracyjnej, brak możliwości zwrócenia się do urzędu we własnym kraju, jeżeli przedsiębiorstwo współpracuje z urzędem innego kraju Unii.

Innym problemem jest wprowadzona we wniosku zasada "**przenoszenia danych**". Jednym z pomysłów była możliwość migracji danych np. z jednego portalu społecznościowego do drugiego. Istnieją jednak obawy, że ułatwiłoby to niekontrolowane przekazywanie danych bez zgody strony zainteresowanej.

Kolejnym aspektem jest tzw. **prawo do zapomnienia**. Ma ono dać osobom zainteresowanym prawo do usunięcia własnych danych umieszczonych na komputerach osób trzecich. Zamysłem było ukrócenie sytuacji, w której dane raz zapisane np. przez przedsiębiorstwo w ramach usług, pozostają w posiadaniu tego przedsiębiorstwa nawet po zakończeniu współdziałania z osobą, której dane zostały zebrane. Dziś niektóre przedsiębiorstwa przetrzymują tzw. wrażliwe dane klienta nawet po zakończeniu umowy. Nowy zapis ma więc dawać prawo do zarządzania własnymi danymi nawet, jeśli powodować by to miało ich usunięcie.

Niemniej powstaje tu problem - powołując się na tę zasadę, niektóre osoby żądały skasowania z publicznie dostępnych źródeł internetowych informacji o ich nielegalnych czynach. Taka forma prywatnej cenzury nie powinna raczej zostać dopuszczona.

Generalny Inspektor zwrócił uwagę na fakt, że po konsultacji Rady, odpowiedzialność za ostateczny kształt rozporządzenia i dyrektywy spoczywa na posłach Parlamentu Europejskiego. Dodał, że w przypadku wyboru formuły rozporządzenia, będą oni jedynymi, bezpośrednio wybranymi przedstawicielami obywateli, mającymi wpływ na przyszłe unijne prawo ochrony danych osobowych.

**Opracowała:**  
**dr Magdalena Skulimowska**