GRUPA ROBOCZA ART. 29

01008/2011/PL
WP 186

Opinia 14/2011
dotycząca kwestii ochrony danych w odniesieniu do zapobiegania zjawiskom prania pieniędzy i finansowania terroryzmu

Przyjęta w dniu 13 czerwca 2011 r.

Grupa robocza powołana na podstawie art. 29 dyrektywy 95/46/WE stanowi niezawisłe europejskie ciało doradcze w dziedzinie ochrony prywatności i danych osobowych. Jej zadania określono w art. 30 dyrektywy 95/46/WE oraz art. 15 dyrektywy 2002/58/WE.

Sekretariat Grupy mieści się w DG ds. Sprawiedliwości Komisji Europejskiej, Dyrekcja C (prawa podstawowe i obywatelstwo Unii Europejskiej), B-1049 Brussels, Belgia, biuro nr MO-59 02/013.

Strona internetowa: http://ec.europa.eu/justice/data-protection/index_pl.htm

GRUPA ROBOCZA DS. OCHRONY OSÓB FIZYCZNYCH W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

powołana dyrektywą 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.,

uwzględniając art. 29, art. 30 ust. 1 lit. c) oraz art. 30 ust. 3 wyżej wymienionej dyrektywy,

uwzględniając swój regulamin wewnętrzny, w szczególności jego art. 12 i 14,

1. WPROWADZENIE

Podczas dzisiejszego posiedzenia plenarnego Grupa Robocza Art. 29 („Grupa Robocza") wydała 44 zalecenia dotyczące ochrony prywatności i ochrony danych w związku z zapobieganiem zjawiskom prania pieniędzy i finansowania terroryzmu („AML/CFT"), które zostały wymienione w załączniku do niniejszej opinii.

2. KONTEKST I CEL 44 ZALECEŃ AML/CFT

Przed przyjęciem powyższych zaleceń Grupa Robocza zasięgnęła opinii różnych zainteresowanych stron, wśród których znaleźli się między innymi Komisja Europejska, przedstawiciele podmiotów sprawozdawczych, jednostek wywiadu finansowego, banków narodowych oraz Grupy Specjalnej ds. Przeciwdziałania Praniu Pieniędzy. W ten sposób Grupa Robocza pragnęła zapewnić przeanalizowanie wszystkich istotnych kwestii związanych z ochroną danych i prywatnością, poruszonych przez wymienione powyżej podmioty, w świetle istniejących ram prawnych w obszarze prywatności i ochrony danych.
Celem zaleceń jest przedstawienie stanowiska i udostępnienie praktycznych wskazówek ustawodawcom, podmiotom sprawozdawczym, organom regulacyjnym, jednostkom wywiadu finansowego, organom nadzorczym i innym zainteresowanym stronom, które mają za zadanie stosowanie zasad i przepisów w obydwu obszarach – w odniesieniu do zapobiegania zjawiskom prania pieniędzy i finansowania terroryzmu oraz w odniesieniu do prywatności i ochrony danych – zarówno na szczeblu unijnym, jak i na szczeblu poszczególnych państw członkowskich.

Zalecenia te stanowią odpowiedź na istniejące zapotrzebowanie na praktyczne, obszerne wskazówki na poziomie Unii Europejskiej w obszarze łączącym problematykę zapobiegania

zjawiskom prania pieniędzy oraz finansowania terroryzmu, a także prywatności i ochrony danych (wyjaśniono w pkt 1.4 załącznika).

3. NAJWAŻNIEJSZE PROBLEMY

W zaleceniach uwzględniono różne problemy (pkt 1.5 załącznika). Najważniejsze elementy, które poruszono w zaleceniach, są następujące:

* ***Zgodnie z obowiązującym prawem (art. 8 EKPC)*** prywatność i ochrona danych są uznawane na terytorium UE za prawa człowieka będące elementem demokratycznego społeczeństwa i powinny być zawsze stosowane jako takie, a nie w oparciu o uzasadniony interes lub zgodę osoby, której dane dotyczą (zal. 1). W związku z powyższym środki stosowane jako środki konieczne w celu zapobiegania zjawiskom prania pieniędzy i finansowania terroryzmu powinny zawsze mieć wyraźną podstawę prawną i być niezbędne oraz proporcjonalne do charakteru danych. Grupa Robocza zaleca między innymi, aby dokonać przeglądu obowiązujących obecnie oraz proponowanych przepisów AML/CFT na szczeblu UE oraz na szczeblu poszczególnych państw członkowskich (zal. 3), a także dokonać większego ujednolicenia na szczeblu UE (zal. 5); wprowadzić czytelną politykę publiczną w obszarze ochrony danych (zal. 12), rozpowszechniać zrozumiałe informacje odnośnie do widocznych środków AML/CFT takich jak kwestionariusze i ograniczanie usług (zal. 13) oraz ściśle i wyraźnie stosować zasadę celowości w przepisach AML/CFT (zal. 15-16).

* Zasady i zobowiązania w tym obszarze powinny być realizowane ***w sposób zrównoważony***, przy uwzględnieniu różnych opinii, interesów oraz ram prawnych – zarówno w UE jak i poza jej terytorium. Przykłady obejmują sformułowanie przepisów AML/CFT i wytycznych (zal. 2), zastosowanie wcześniejszych ocen dotyczących ochrony danych (zal. 7-9), wyważone wykorzystanie informacji zwrotnych (zal. 22), unikanie nakładania nadmiernie restrykcyjnych przepisów przez władze krajowe (ang. *gold-plated regulations*) w obszarze AML/CFT (zal. 23), wyważone systemy wymiany danych (zal. 26), wyważony pogląd na mechanizmy zatrzymywania danych (zal. 28), wyważony

pogląd na zakaz przekazywania wskazówek dotyczących poufnych informacji, przy jednoczesnym poszanowaniu praw ochrony danych (zal.12-13).

* Prawa i obowiązki w obszarze prywatności i ochrony danych powinny zawsze być podejmowane i opracowywane ***w sposób pozytywny***, nie zaś przy negatywnym odniesieniu do kwestii prywatności i ochrony danych. Przykład podejścia negatywnego zakłada, że ochrona danych i poszanowanie prywatności przedstawiane są jako przeszkoda, którą można lub powinno się obejść, zaś podejście jest ograniczone do ogólnego stosowania wyjątków od przepisów o ochronie danych, przy czym uwarunkowania umożliwiające stosowanie takich wyjątków zostają pominięte, zaś w zamian nie oferuje się rzeczywistej treści i materii ochrony danych w kontekście przetwarzania AML/CFT. Pojęcie podejścia pozytywnego ilustrują między innymi zalecenia dotyczące konkretnych działań, takich jak przyjęcie przez podmioty sprawozdawcze, jednostki analityki finansowej i organy nadzoru finansowego publicznej i udokumentowanej polityki w celu zachowania zgodności z przepisami dotyczącymi prywatności i ochrony danych (zal. 11), wewnętrzna polityka ochrony poufnych danych (zal. 14), zapobieganie kradzieży tożsamości (zal. 38), wykorzystanie wyłączeń jednostek analityki finansowej dla zastosowania typologii (zal. 19) oraz mechanizm informacji zwrotnych (zal. 21), zapewnienie odpowiednich zabezpieczeń dla wszystkich operacji profilowania (zal.20), nieustanne oceny dokładności danych (zal. 29), przechowywanie informacji o źródłach danych i datach w odniesieniu do wszystkich danych i ocen AML/CFT (zal. 30), dostęp i nadzór za pośrednictwem organów ochrony danych (zal. 34) i ochrona danych szczególnie chronionych (zal. 37).

* ***Grupa Robocza zaleca, aby w celu zapewnienia prawdziwej i skutecznej ochrony*** oraz zgodności z zasadami prywatności i ochrony danych w tym obszarze rozpoczęto stosowanie różnych form wstępnej oceny przepisów, procedur i projektów AML/CFT. Takie formy obejmują ocenę wpływu na sferę prywatności, techniki kontrolne, pracę urzędników ds. ochrony danych (zal. 7-10). Zaleca się również dokonywanie ocen jakości takich jak test warunków skrajnych na podstawie wiążących reguł korporacyjnych (BCR) dla instytucji, które zamierzają przyjąć BCR (zal. 39), wprowadzenie wymaganych poziomów odniesienia dla ustaleń dotyczących stosowności w przypadków transferów międzynarodowych (zal. 40), a także zastosowanie przez jednostki analityki finansowej protokołów ustaleń jako narzędzi ochrony danych (zal.43).

* Dla zagwarantowania pewności prawa na szczeblu UE wymaga się ***stałej, coraz lepszej współpracy*** zainteresowanych stron, w tym różnych organów nadzoru, takich jak organy ds. ochrony danych, jednostki analityki finansowej i organy odpowiedzialne za regulację (zal. 17).

4. PODSUMOWANIE

Grupa Robocza Art. 29 będzie dalej śledzić załączone zalecenia oraz odpowiedni rozwój sytuacji w odniesieniu do przepisów i stosowanych praktyk w obszarze łączącym problematykę zapobiegania zjawiskom prania pieniędzy oraz finansowania terroryzmu, a także prywatności i ochrony danych.

Sporządzono w Brukseli dnia 13 czerwca 2011 r.

W imieniu grupy roboczej
Przewodniczący
Jacob KOHNSTAMM