

Streszczenie opinii Europejskiego Inspektora Ochrony Danych w sprawie wniosku Komisji dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (rozporządzenie o elektronicznych usługach zaufania)

(Pełny tekst niniejszej opinii jest dostępny w wersji angielskiej, francuskiej i niemieckiej na stronie internetowej EIOD: <http://www.edps.europa.eu>)

(2013/C 28/04)

I. Wstęp

I.1. Wniosek

1. W dniu 4 czerwca 2012 r. Komisja przyjęła wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady zmieniającego dyrektywę 1999/93/WE Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym („wniosek”) ⁽¹⁾.

2. Wniosek stanowi część środków przedstawionych przez Komisję w celu wzmocnienia procesu wdrażania transakcji elektronicznych w Unii Europejskiej. Jest on kontynuacją działań przewidzianych w Europejskiej agendzie cyfrowej ⁽²⁾ w zakresie poprawy ustawodawstwa dotyczącego podpisów elektronicznych (Główne działanie 3) oraz zapewnienia spójnych ram wzajemnego uznawania elektronicznej identyfikacji i elektronicznego uwierzytelniania (Główne działanie 16).

3. Wniosek powinien zwiększyć zaufanie do ogólnoeuropejskich transakcji elektronicznych, a także zapewnić transgraniczne uznanie prawne identyfikacji elektronicznej, uwierzytelnienia elektronicznego i podpisu elektronicznego oraz związanych z nimi usług zaufania na rynku wewnętrznym, jednocześnie gwarantując wysoki poziom ochrony danych i wzmocnienie pozycji użytkownika.

4. Wysoki poziom ochrony danych jest warunkiem koniecznym dla funkcjonowania systemów identyfikacji elektronicznej i usług zaufania. Opracowanie i stosowanie takich środków elektronicznych musi opierać się na odpowiednim przetwarzaniu danych osobowych przez dostawców usług zaufania oraz wydawców środków identyfikacji elektronicznej. Ma to tym większe znaczenie, że takie przetwarzanie będzie stanowiło jedną z podstaw wiarygodnej identyfikacji i uwierzytelniania osób fizycznych (lub prawnych).

I.2. Konsultacje z EIOD

5. Przed przyjęciem wniosku EIOD miał możliwość zgłoszenia nieformalnych uwag. Wiele z nich zostało uwzględnionych we wniosku, dzięki czemu wzmocnieniu uległy zawarte w nim gwarancje ochrony danych.

6. EIOD z zadowoleniem przyjmuje fakt, że Komisja przeprowadziła z nim również formalne konsultacje w trybie art. 28 ust. 2 rozporządzenia (WE) nr 45/2001.

I.3. Tło wniosku

7. Wniosek opiera się na art. 114 Traktatu o funkcjonowaniu Unii Europejskiej i określa warunki oraz mechanizmy wzajemnego uznawania i akceptowania identyfikacji elektronicznej oraz usług zaufania pomiędzy państwami członkowskimi. W szczególności ustanawia zasady świadczenia usług identyfikacji i elektronicznych usług zaufania, w tym zasady uznawania i akceptacji. Wprowadza również wymagania w zakresie tworzenia, kontroli, weryfikacji, obsługi i przechowywania podpisów elektronicznych, pieczęci elektronicznych, elektronicznych znaczników czasu, dokumentów elektronicznych, usług przekazu elektronicznego, usług uwierzytelniania witryn internetowych i certyfikatów elektronicznych.

8. Projekt ustanawia ponadto zasady nadzoru nad świadczeniem usług zaufania oraz zobowiązuje państwa członkowskie do powołania w tym celu organów nadzorczych. Do ich zadań będzie należała między innymi ocena zgodności środków technicznych i organizacyjnych wdrożonych przez dostawców elektronicznych usług zaufania.

⁽¹⁾ COM(2012) 238 final.

⁽²⁾ COM(2010) 245 z 19.5.2010.

9. Rozdział II dotyczy usług identyfikacji elektronicznej, natomiast rozdział III poświęcony jest innym rodzajom elektronicznych usług zaufania, takim jak podpisy elektroniczne, pieczęcie elektroniczne, elektroniczne znaczki czasu, dokumenty elektroniczne, usługi przekazu elektronicznego, certyfikaty elektroniczne oraz uwierzytelnianie witryn internetowych. Usługi identyfikacji elektronicznej związane są z krajowymi dokumentami tożsamości i mogą być wykorzystywane w celu uzyskania dostępu do usług cyfrowych, w szczególności usług administracji elektronicznej. Oznacza to, że podmiot wydający środki identyfikacji elektronicznej działa w imieniu państwa członkowskiego, które ponosi odpowiedzialność za poprawne ustalenie korelacji pomiędzy daną osobą a dotyczącymi jej środkami identyfikacji elektronicznej. W przypadku innych elektronicznych usług zaufania dostawca/wydawca jest osobą fizyczną lub prawną, która odpowiada za prawidłowe i bezpieczne świadczenie tych usług.

I.4. *Kwestie dotyczące ochrony danych związane z wnioskiem*

10. Przetwarzanie danych osobowych jest nierozdzielnie związane ze stosowaniem systemów identyfikacji, a w pewnym stopniu również ze świadczeniem innych usług zaufania (np. podpisów elektronicznych). Przetwarzanie danych osobowych będzie wymagane w celu ustalenia wiarygodnego związku pomiędzy elektronicznymi środkami identyfikacji i uwierzytelnienia stosowanymi przez osobę fizyczną (lub prawną) a tą osobą, tak by móc zaświadczyć, że osoba posługująca się certyfikatem elektronicznym jest faktycznie tym, za kogo się podaje. Na przykład środki identyfikacji elektronicznej lub certyfikaty elektroniczne dotyczą osób fizycznych i obejmują zestaw danych jednoznacznie identyfikujących te osoby. Innymi słowy, tworzenie, kontrola, weryfikacja i obsługa środków elektronicznych, o których mowa w art. 3 ust. 12 wniosku, będzie w wielu przypadkach wiązała się z przetwarzaniem danych osobowych, a zatem ochrona danych staje się zasadną kwestią.

11. Z tego względu należy zapewnić, by przetwarzanie danych w kontekście systemów identyfikacji elektronicznej lub elektronicznych usług zaufania odbywało się zgodnie z unijnymi zasadami ochrony danych, a w szczególności krajowymi przepisami wdrażającymi dyrektywę 95/46/WE.

12. EIOD w niniejszej opinii skupia się na analizie trzech głównych kwestii:

- a) potraktowania kwestii ochrony danych we wniosku;
- b) ujęcia kwestii ochrony danych w systemach identyfikacji elektronicznej podlegających uznaniu i akceptacji ponad granicami;
- c) ujęcia kwestii ochrony danych w elektronicznych usługach zaufania podlegających uznaniu i akceptacji ponad granicami.

III. **Wnioski**

50. EIOD z zadowoleniem przyjmuje wniosek, jako że może on przyczynić się do wzajemnego uznawania (i akceptacji) elektronicznych usług zaufania oraz systemów identyfikacji elektronicznej na szczeblu europejskim. Z zadowoleniem odnosi się również do ustanowienia wspólnego zbioru wymagań, jakie muszą być spełnione przez wydawców środków identyfikacji elektronicznej oraz dostawców usług zaufania. Bez względu na ogólne poparcie dla wniosku EIOD pragnie przedstawić następujące ogólne zalecenia:

- zawarte we wniosku przepisy dotyczące ochrony danych nie powinny ograniczać się tylko do dostawców usług zaufania, lecz objąć również przetwarzanie danych osobowych w ramach systemów identyfikacji elektronicznej opisanych w rozdziale II wniosku,
- projektowane rozporządzenie powinno wprowadzić wspólny zbiór wymagań w zakresie bezpieczeństwa w odniesieniu do dostawców usług zaufania i wydawców środków identyfikacji elektronicznej lub ewentualnie powinno umożliwić Komisji określenie w miarę potrzeby – w drodze selektywnego zastosowania aktów delegowanych lub wykonawczych – kryteriów, warunków i wymagań w zakresie bezpieczeństwa elektronicznych usług zaufania i systemów identyfikacji elektronicznej,
- dostawcy elektronicznych usług zaufania i wydawcy środków identyfikacji elektronicznej powinni zostać zobowiązani do zapewnienia osobom korzystającym z ich usług: (i) stosownych informacji na temat gromadzenia, przekazywania i przechowywania ich danych, jak również (ii) możliwości kontroli danych osobowych i wykonywania uprawnień w zakresie ochrony danych,

- EIOD zaleca bardziej selektywne uwzględnienie we wniosku przepisów uprawniających Komisję do określenia lub uszczegółowienia konkretnych przepisów po przyjęciu projektowanego wniosku w drodze aktów delegowanych lub wykonawczych.

51. Wskazana jest również poprawa niektórych konkretnych przepisów dotyczących wzajemnego uznania systemów identyfikacji elektronicznej:

- projektowane rozporządzenie powinno określać dane lub kategorie danych podlegających przetwarzaniu w ramach transgranicznej identyfikacji osób. Takie określenie powinno być co najmniej równie szczegółowe, jak w załącznikach dotyczących innych usług zaufania, oraz powinno uwzględniać poszanowanie zasady proporcjonalności,
- zabezpieczenia wymagane w przypadku systemów identyfikacji powinny być co najmniej zgodne z wymaganiami obowiązującymi dostawców kwalifikowanych usług zaufania,
- we wniosku należy przyjąć odpowiednie mechanizmy dla stworzenia ram interoperacyjności krajowych systemów identyfikacji.

52. EIOD przedstawia wreszcie następujące zalecenia w odniesieniu do wymagań dotyczących świadczenia i uznawania elektronicznych usług zaufania:

- w odniesieniu do wszystkich usług elektronicznych należy określić, czy dane osobowe będą przetwarzane, a jeśli tak, to których danych lub kategorii danych będzie dotyczyło przetwarzanie,
- w rozporządzeniu należy przyjąć odpowiednie zabezpieczenia w celu uniknięcia dublowania się kompetencji organów nadzoru nad elektronicznymi usługami zaufania i organów ochrony danych,
- obowiązki nałożone na dostawców elektronicznych usług zaufania w odniesieniu do naruszenia ochrony danych i incydentów związanych z bezpieczeństwem powinny być zgodne z wymaganiami ustanowionymi w zmienionej dyrektywie o prywatności elektronicznej oraz w projektowanym rozporządzeniu o ochronie danych,
- doprecyzowania wymagają: definicja podmiotów prywatnych lub publicznych, które mogą występować jako strony trzecie uprawnione do prowadzenia audytów w trybie art. 16 i 17 lub mogą weryfikować urzędnicy do składania kwalifikowanego podpisu elektronicznego w trybie art. 23, jak również kryteria oceny niezawisłości tych podmiotów,
- w rozporządzeniu należy doprecyzować termin przechowywania danych, o których mowa w art. 19 ust. 2 i art. 19 ust. 4 ⁽¹⁾.

Sporządzono w Brukseli dnia 27 września 2012 r.

Giovanni BUTTARELLI
Zastępca Europejskiego Inspektora Ochrony Danych

⁽¹⁾ Zgodnie z art. 19 ust. 2 lit. g) dostawcy kwalifikowanych usług zaufania rejestrują przez odpowiedni okres czasu wszelkie informacje dotyczące danych wydanych i otrzymanych przez nich. Zgodnie z art. 19 ust. 4 dostawcy kwalifikowanych usług zaufania dostarczają każdej stronie ufającej informacje o statusie ważności lub cofnięcia wydanych przez siebie kwalifikowanych certyfikatów.