

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Streszczenie opinii Europejskiego Inspektora Ochrony Danych w sprawie komunikatu Komisji do Parlamentu Europejskiego i Rady zatytułowanego „Odbudowa zaufania do przepływów danych między Unią Europejską a Stanami Zjednoczonymi” oraz komunikatu Komisji do Parlamentu Europejskiego i Rady w sprawie funkcjonowania zasad bezpiecznego transferu danych osobowych z punktu widzenia obywateli UE i przedsiębiorstw z siedzibą w UE

(Niniejsza opinia jest dostępna w pełnym brzmieniu w językach angielskim, francuskim i niemieckim na stronie internetowej EIOD (www.edps.europa.eu))

(2014/C 116/04)

I. Wprowadzenie

I.1. Konsultacje z EIOD

1. W dniu 27 listopada 2013 r. Komisja przyjęła komunikat do Parlamentu Europejskiego i Rady zatytułowany „Odbudowa zaufania do przepływów danych między Unią Europejską a Stanami Zjednoczonymi”⁽¹⁾ (zwany dalej „komunikatem w sprawie odbudowy zaufania”). Komunikatowi temu towarzyszyło sprawozdanie zawierające ustalenia dokonane przez współprzewodniczących z ramienia UE w grupie roboczej *ad hoc* UE-USA ds. ochrony danych (zwane dalej odpowiednio „sprawozdaniem” i „grupą roboczą”).
2. W tym samym dniu Komisja przyjęła komunikat do Parlamentu Europejskiego i Rady w sprawie funkcjonowania zasad bezpiecznego transferu danych osobowych z punktu widzenia obywateli UE i przedsiębiorstw z siedzibą w UE⁽²⁾ (zwany dalej „komunikatem w sprawie zasad bezpiecznego transferu danych osobowych”).
3. EIOD z zadowoleniem przyjmuje fakt, że umożliwiono mu przedstawienie Komisji nieformalnych uwag przed przyjęciem powyższych dokumentów. Dokumenty te zostały przyjęte przez Komisję w następstwie doniesień o programach nadzoru prowadzonych przez amerykańskie służby wywiadowcze. EIOD zdecydował się przyjąć obecną opinię z własnej inicjatywy ze względu na wpływ tych programów nadzoru na prawa osób fizycznych do prywatności i ochrony ich danych osobowych w UE.

I.2. I.2. Cel i zakres dokumentów Komisji

a) Komunikat w sprawie odbudowy zaufania i sprawozdanie

4. W komunikacie zaproponowano przyszłe działania w następstwie doniesień o szeroko zakrojonych programach gromadzenia danych przez amerykańskie służby wywiadowcze (zwanym dalej „programami” lub „ujawnionymi programami”) oraz ich wpływu na zaufanie między UE i USA. Nie wspomniano w nim o doniesieniach na temat podobnych działań lub współpracy z USA prowadzonej przez państwa członkowskie UE lub przez inne państwa trzecie.
5. W sprawozdaniu zestawiono ustalenia współprzewodniczących z ramienia UE w grupie roboczej *ad hoc* UE-USA ds. ochrony danych, którą ustanowiono w następstwie posiedzenia Komitetu Stałych Przedstawicieli z dnia 18 lipca 2013 r., aby ustalić fakty dotyczące programów oraz ich wpływu na prawa podstawowe w UE i dane osobowe obywateli UE. Przeanalizowano w nim ramy prawne obowiązujące w USA⁽³⁾, to, w jaki sposób odbywa się gromadzenie i dalsze przetwarzanie danych⁽⁴⁾, oraz istniejące mechanizmy nadzoru i dochodzenia roszczeń.

⁽¹⁾ COM(2013) 846 final.

⁽²⁾ COM(2013) 847 final.

⁽³⁾ W szczególności Konstytucję zgodnie z wykładnią sądu najwyższego; sekcję 702 ustawy o nadzorze nad wywiadem zagranicznym z 1978 r. (FISA) (zmienionej w 2008 r. ustawą zmieniającą FISA, tytuł 50 kodeksu Stanów Zjednoczonych, par. 1881a); oraz sekcję 215 amerykańskiej ustawy Patriot Act z 2001 r. (również zmieniającej FISA, tytuł 50 kodeksu Stanów Zjednoczonych, par. 1861) i rozporządzenie wykonawcze 12333.

⁽⁴⁾ Na podstawie informacji dostarczonych przez USA w ramach grupy roboczej i odtajnionych dokumentów, w tym opinii sądu ds. nadzoru nad wywiadem zagranicznym (zwanego dalej „sądem”), oraz dokumentów dostępnych publicznie, takich jak wytyczne amerykańskiego prokuratora generalnego w sprawie krajowych operacji Federalnego Biura Śledczego.

6. W sprawozdaniu wspomina się o „drugiej ścieżce działania”, którą także omówiono podczas posiedzenia Komitetu Stałych Przedstawicieli w dniu 18 lipca 2013 r. Stwierdza się w nim, że w ramach „drugiej ścieżki działania” instytucje UE mogą zadawać władzom USA zapytania dotyczące zarzucanego nadzoru nad instytucjami i placówkami dyplomatycznymi UE, natomiast państwa członkowskie mogą omawiać z władzami USA w trakcie rozmów dwustronnych zagadnienia związane ze swoim bezpieczeństwem narodowym.
 7. W sprawozdaniu wskazano również, że ten podział nakłada pewne ograniczenia na rozmowy prowadzone i informacje przedstawiane na forum grupy roboczej. EIOD nie otrzymał żadnych informacji dotyczących „drugiej ścieżki działania” ani utworzenia równoległej grupy roboczej w tym zakresie. Zwraca się w związku z tym do Komisji o informacje na temat ustaleń w ramach „drugiej ścieżki działania”, w szczególności w odniesieniu do zarzucanego nadzoru nad instytucjami i placówkami dyplomatycznymi UE.
- b) Komunikat w sprawie zasad bezpiecznego transferu danych osobowych
8. W komunikacie w sprawie zasad bezpiecznego transferu danych osobowych przeanalizowano funkcjonowanie tych zasad, wskazano niedociągnięcia i zaproponowano możliwe udoskonalenia. W dokumencie stwierdza się, że ilość danych przesyłanych między UE i USA rośnie, a zasad bezpiecznego transferu danych osobowych przestrzega coraz większa liczba przedsiębiorstw. Po przypomnieniu struktury i funkcjonowania zasad bezpiecznego transferu danych osobowych Komisja kładzie nacisk na konieczność sprawniejszego egzekwowania zasad wobec przedsiębiorstw uczestniczących w programie oraz ich podwykonawców. Zgodnie z komunikatem będzie to wymagać skuteczniejszego włączenia zasad bezpiecznego transferu danych osobowych do polityki ochrony prywatności uczestniczących przedsiębiorstw i podania ich do publicznej wiadomości. Federalna komisja handlu powinna bardziej aktywnie egzekwować przestrzeganie tych zasad. Ponadto organy ochrony danych powinny uczestniczyć w informowaniu o zasadach bezpiecznego transferu danych osobowych w UE, a w szczególności o istnieniu grupy UE ds. ochrony danych. Komisja przedstawia też rozwiązania służące usprawnieniu alternatywnych metod rozwiązywania sporów.
 9. Jeżeli chodzi o dostęp do danych przesyłanych w ramach systemu zasad bezpiecznego transferu danych osobowych oraz przetwarzanych dalej przez władze USA, Komisja podkreśla, że takie działania powinny ograniczać się do zakresu ściśle koniecznego i proporcjonalnego. Wymaga przy tym ścisłego monitorowania ograniczeń dotyczących zasad polityki prywatności w związku z wymaganiami bezpieczeństwa narodowego, interesu publicznego lub przestrzegania prawa, aby nie osłabiały one ochrony zapewnianej przez te zasady. Zachęca także uczestniczące przedsiębiorstwa do udzielania przejrzystych informacji na temat tych ograniczeń i ich wpływu na poufność komunikacji w celu podnoszenia świadomości obywateli.
- I.3. *Zakres i cel obecnej opinii*
10. W obecnej opinii skoncentrowano się na komunikacie w sprawie odbudowy zaufania, a w tym kontekście także na komunikacie w sprawie zasad bezpiecznego transferu danych osobowych. W związku z tym nie odniesiono się w niej bezpośrednio do doniesień o działaniach państw członkowskich UE podejmowanych we współpracy ze Stanami Zjednoczonymi lub samodzielnie bądź też o nadzorze prowadzonym przez państwa trzecie inne niż Stany Zjednoczone.
 11. Na początku opinii przedstawiono uwagi na temat ogólnego podejścia przyjętego w komunikacie w sprawie odbudowy zaufania. W części II przeanalizowano w skrócie zastosowanie odpowiednich ram prawnych i jego konsekwencje, a także zamieszczono uwagi dotyczące komunikatu w sprawie zasad bezpiecznego transferu danych osobowych. Jako że Grupa Robocza art. 29⁽¹⁾ analizuje obecnie stosowne unijne i międzynarodowe ramy prawne, w niniejszej opinii nie omawiano szczegółowo tych zagadnień. W części III odniesiono się do zaleceń Komisji dotyczących przyszłych działań.
- I.4. *Uwagi na temat podejścia przyjętego w komunikacie w sprawie odbudowy zaufania*
12. W komunikacie skoncentrowano się na negatywnym wpływie doniesień o programach na zaufanie między UE i USA jako partnerami strategicznymi, które należy przywrócić. EIOD z zadowoleniem przyjmuje to stwierdzenie.

(¹) Ustanowiona na mocy dyrektywy 95/46/WE Grupa Robocza ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych jest niezależnym ciałem o charakterze doradczym. W jej skład wchodzi przedstawiciele krajowych organów ochrony danych państw członkowskich UE, EIOD oraz Komisji.

13. Wspomniane programy, których istnienie w niektórych przypadkach wyraźnie potwierdzono w sprawozdaniu⁽¹⁾, mają jednak wpływ nie tylko na zaufanie, ale również na prawa zawarte w prawie pierwotnym i wtórnym UE oraz Rady Europy, w szczególności prawo do prywatności i ochrony danych. Na ich przykładzie widać też, że poza granicami USA dochodzi do szeroko zakrojonego gromadzenia informacji wywiadowczych na mocy amerykańskich ram prawnych⁽²⁾ zgodnie z ich wykładnią przedstawioną przez sąd najwyższy USA⁽³⁾. W sprawozdaniu potwierdzono też, że na mocy amerykańskich ram obywatelom UE nie przysługują zabezpieczenia, ochrona, prawa, możliwość nadzoru ani dochodzenia roszczeń⁽⁴⁾.
14. Jak wielokrotnie podkreślała Komisja, zaufanie obywateli i przedsiębiorców do komunikacji internetowej zależy od dostępności skutecznych technicznych narzędzi ochrony prywatności, a mówiąc dokładniej – poufności komunikacji. Potrzebę tę zauważyła także amerykańska grupa ds. przeglądu technologii wywiadowczych i komunikacyjnych⁽⁵⁾, która przedstawiła pewne zalecenia mające na celu przywrócenie zaufania do narzędzi szyfrujących i oprogramowania komercyjnego, jak też do funkcjonowania mechanizmów szybkiego usuwania luk w oprogramowaniu. Część najbardziej uznanych ekspertów ds. bezpieczeństwa uznaje osłabienie zaufania do tych systemów za jeden z najbardziej szkodliwych efektów niedawnych dyskusji na temat działań w zakresie rozpoznania elektronicznego⁽⁶⁾. Ze względu na znaczenie skutecznych mechanizmów zapewniających bezpieczeństwo cybernetyczne Europy sposób reakcji na to wyzwanie techniczne i polityczne należy określić na poziomie UE, a z inicjatywą taką powinna wyjść Komisja.
15. W sekcji 3 komunikatu Komisja odnosi się do przyszłych działań, które należy podjąć w celu przywrócenia zaufania do przepływów danych między UE a USA. EIOD z zadowoleniem przyjmuje treść tej sekcji, w której skupiono się na doskonaleniu istniejących ram prawnych i zaproponowano nowe instrumenty. Komisja nie zajmuje się wszakże zagadnieniem wpływu programów na stosowne instrumenty na poziomie krajowym, UE i Rady Europy. EIOD uważa, że w komunikacie należało zwrócić większą uwagę na ich skutki z punktu widzenia istniejących instrumentów prawnych.

IV. Uwagi końcowe

79. EIOD z zadowoleniem przyjmuje środki rozważane przez Komisję, ale podkreśla zarazem, że ujawnione działania amerykańskich agencji wywiadowczych w zakresie nadzoru wpływają nie tylko na zaufanie do przepływów danych między UE a USA. Mają one też skutki dla istniejących i możliwych do wyegzekwowania praw obywateli UE do poszanowania prywatności oraz ochrony danych osobowych, zapisanych w prawie pierwotnym i wtórnym zarówno UE, jak i Rady Europy. Dlatego też EIOD ubolewa, że w komunikacie w sprawie odbudowy zaufania nie zwrócono większej uwagi na skutki z punktu widzenia istniejących instrumentów prawnych.
80. W kilku przypadkach EIOD opowiada się za ambitniejszym sposobem określenia przyszłych działań przez Komisję; stwierdza przy tym, że:
- Prawidłowe stosowanie i egzekwowanie obecnych europejskich ram prawnych ochrony danych jest nie tylko wymagane przez prawo, ale także stanowiłoby istotny wkład w przywrócenie zaufania. Dotyczy to też instrumentów regulujących międzynarodowe przepływy danych między UE i USA, w tym obowiązujących zasad bezpiecznego transferu danych osobowych.
 - Należy przypomnieć Komisji, że wyjątki lub ograniczenia stosowania praw podstawowych w związku z celami bezpieczeństwa narodowego są uzasadnione i dopuszczalne tylko wtedy, gdy są bezwzględnie konieczne, proporcjonalne i zgodne z orzecznictwem Europejskiego Trybunału Praw Człowieka oraz Trybunału Sprawiedliwości.

⁽¹⁾ Zob. s. 5, 10 i 26 sprawozdania, w którym na podstawie odtajnionych opinii sądu ds. nadzoru nad wywiadem zagranicznym potwierdzono, że „amerykańskie agencje wywiadowcze stosują na mocy sekcji 702 metody szeroko zakrojonego gromadzenia danych, takie jak gromadzenie w ramach programu PRISM danych od dostawców usług internetowych bądź gromadzenie danych przepływających przez łącza na terytorium USA (ang. *upstream collection*)”.

⁽²⁾ Stany Zjednoczone potwierdziły, że istnieją inne podstawy prawne gromadzenia danych wywiadowczych na temat osób spoza USA, nie przedstawiając jednak szczegółów co do ich umocowania prawnego i obowiązujących procedur. Nie wszystkie stosowne podstawy prawne ujawniono grupie roboczej (zob. s. 13 sprawozdania).

⁽³⁾ Zob. s. 4–12 sprawozdania.

⁽⁴⁾ Zob. s. 26–27 sprawozdania.

⁽⁵⁾ „Liberty and Security in a Changing World” [„Wolność i bezpieczeństwo w zmieniającym się świecie”], sprawozdanie i zalecenia prezydenckiej Grupy ds. Przeglądu Technologii Wywiadowczych i Komunikacyjnych, w szczególności zalecenia 25, 29 i 30. http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

⁽⁶⁾ B. Schaefer, C. Soghoian w raporcie z 6 września 2013 r., <http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>; B. Preneel: przemówienie zamykające konferencję ISSE 2013: „The Cryptographic Year in Review” [„Rok w kryptografii”] http://homes.esat.kuleuven.be/~preneel/preneel_isse13.pdf

- EIOD w pełni zgadza się z poglądem, że konsolidacja oraz usprawnienie unijnych ram ochrony danych wymagają szybkiego przyjęcia wniosków w sprawie reformy ochrony danych, które obejmą odpowiednie zapisy zapewniające ściślejszą, skuteczniejszą i spójniejszą ochronę danych osobowych oraz prywatności w całym prawie UE. Powinny one także zapewnić odpowiednią ochronę danych w przypadku ich dalszego wykorzystania do celów egzekwowania prawa oraz konfliktów jurysdykcji.
- Zasady bezpiecznego transferu danych osobowych należy poddać przeglądowi i doprecyzować zgodnie z kierunkiem wskazanym przez Komisję. EIOD zaleca wyznaczenie ściślejszych terminów podjęcia takich działań, a także stosownych działań następczych w przypadku utrzymujących się uchybień.
- Trzeba wzmocnić zabezpieczenia służące ochronie danych, które mają zastosowanie do współpracy UE-USA w dziedzinie egzekwowania prawa. Toczące się negocjacje w sprawie umowy ramowej nie powinny skutkować legalizacją masowego przekazywania danych, lecz powinny być zgodne z istniejącymi ramami ochrony danych oraz wynikiem trwającego obecnie procesu ich przeglądu. W szczególności wszystkie osoby, których dane dotyczą, powinny mieć bez względu na narodowość dostęp do skutecznych mechanizmów dochodzenia roszczeń. Zasada ta powinna we właściwym czasie znaleźć zastosowanie także do obowiązujących umów międzynarodowych, w razie potrzeby na mocy odpowiednich postanowień przejściowych.
- Komisja powinna wesprzeć działania amerykańskiej administracji i Kongresu Stanów Zjednoczonych zmierzające do wprowadzenia ogólnej ustawy o prywatności, w której zapewnione zostaną ściśle zabezpieczenia i wystarczający nadzór, zwłaszcza w obszarach, gdzie obecnie brakuje jakiegokolwiek skutecznej ochrony prywatności.
- Trwające obecnie negocjacje w sprawie przyjęcia TTIP nie powinny wywierać negatywnego wpływu na ochronę danych osobowych obywateli. Jednocześnie Komisja powinna rozważyć ustanowienie wspólnego celu polegającego na stopniowym zacieśnianiu związków między ramami prawnymi w zakresie prywatności i ochrony danych, w co wkład mogą wnieść – jak wskazano powyżej – Stany Zjednoczone.
- Międzynarodowe działania zmierzające do upowszechniania standardów prywatności powinny objąć:
 - (i) działanie na rzecz pełnej zgodności nowych międzynarodowych aktów prawnych z europejskimi ramami ochrony danych;
 - (ii) zachęcanie państw trzecich, w szczególności USA, do przystąpienia do Konwencji Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (konwencji nr 108);
 - (iii) działanie na rzecz przyjęcia międzynarodowego aktu prawnego ustanawiającego wymóg przestrzegania standardów ochrony danych w działaniach wywiadowczych. Mógłby on zostać przyjęty na szczeblu ONZ na podstawie art. 17 MPPOiP.
- Podmioty prowadzące działania w zakresie nadzoru powinny być w każdym przypadku zobowiązane do przestrzegania zasad praworządności oraz konieczności i proporcjonalności w demokratycznym społeczeństwie. Należy w związku z tym wyjaśnić ramy prawne na wszystkich stosownych poziomach oraz w razie potrzeby je uzupełnić. Ramy takie powinny obejmować odpowiednie i wystarczająco silne mechanizmy nadzorcze.
- Jako administratorzy danych instytucje UE oraz wszelkie stosowne podmioty w państwach członkowskich także ponoszą bezpośrednią odpowiedzialność za wdrożenie skutecznych środków zapewniających bezpieczeństwo informatyczne. Wiąże się to z przeprowadzeniem na odpowiednim poziomie oceny zagrożeń dla bezpieczeństwa danych. Wymaga to także wsparcia badań nad mechanizmami szyfrowania oraz podnoszenia świadomości administratorów danych i obywateli na temat zagrożeń dla prywatności, jakie niosą sprzedawane lub wykorzystywane produkty, a ponadto wprowadzenia wymogu, aby przy opracowywaniu tych produktów stosowano konkretne metody projektowania pozwalające uniknąć tych zagrożeń bądź przynajmniej je zredukować. UE powinna stanąć na czele inicjatyw edukacyjnych dotyczących bezpieczeństwa danych przetwarzanych w internecie.

Sporządzono w Brukseli dnia 20 lutego 2014 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych