EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Streszczenie opinii Europejskiego Inspektora Ochrony Danych w sprawie komunikatu Komisji „Wykorzystanie potencjału chmury obliczeniowej w Europie”

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

(2013/C 253/03)

I. **Wprowadzenie**

I.1. *Cel opinii*

1. Ze względu na znaczenie chmury obliczeniowej dla zmieniającego się społeczeństwa informacyjnego oraz toczącą się w UE debatę na temat przetwarzania w chmurze EIOD zdecydował się przedstawić niniejszą opinię z własnej inicjatywy.

2. Niniejsza opinia stanowi odpowiedź na komunikat Komisji „Wykorzystanie potencjału chmury obliczeniowej w Europie” z dnia 27 września 2012 r. (zwany dalej „komunikatem”) ([1]), określający najważniejsze działania i kroki polityczne, które mają zostać podjęte w celu szybszego rozpowszechnienia usług w chmurze obliczeniowej w Europie. Przed przyjęciem komunikatu przeprowadzono nieformalne konsultacje z EIOD, który przedstawił nieformalne uwagi. EIOD z zadowoleniem przyjmuje fakt uwzględnienia niektórych z jego uwag w komunikacie.

3. Ze względu jednak na zakres i znaczenie trwającej debaty na temat relacji między chmurą obliczeniową a ramami prawnymi ochrony danych niniejsza opinia nie ogranicza się do tematów poruszonych w komunikacie.

4. Skupiono się w niej w szczególności na wyzwaniach, jakie chmura obliczeniowa niesie dla ochrony danych, oraz na sposobie zaradzenia im przez proponowane rozporządzenie o ochronie danych (zwane dalej „proponowanym rozporządzeniem”) ([2]). Zawarto w niej także uwagi na temat obszarów dalszych działań wskazanych w komunikacie.

I.2. *Kontekst*

5. W kontekście toczącej się w UE ogólnej debaty na temat chmury obliczeniowej szczególne znaczenie mają następujące działania i dokumenty:

— po wydaniu w 2010 r. komunikatu w sprawie europejskiej agendy cyfrowej ([3]) Komisja przeprowadziła od dnia 16 maja do dnia 31 sierpnia 2011 r. konsultacje społeczne na temat chmury obliczeniowej w Europie, po czym opublikowała ich wyniki w dniu 5 grudnia 2011 r. ([4]),

— w dniu 1 lipca 2012 r. Grupa Robocza Art. 29 ([5]) przyjęła opinię na temat przetwarzania danych w chmurze obliczeniowej (zwaną dalej „opinią Grupy Roboczej Art. 29”) ([6]), która zawiera analizę zastosowania obecnych zasad ochrony danych określonych w dyrektywie 95/46/WE do dostawców usług w chmurze obliczeniowej działających w Europejskim Obszarze Gospodarczym (EOG) i ich klientów ([7]),

— w dniu 26 października 2012 r. rzecznicy ochrony danych i prywatności przyjęli uchwałę w sprawie chmury obliczeniowej podczas swojej 34. Międzynarodowej Konferencji ([8]).

([1]) COM(2012) 529 final.
([2]) COM(2012) 11 final.
([3]) COM(2010) 245 wersja ostateczna.
([4]) http://ec.europa.eu/information_society/activities/cloudcomputing/docs/ccconsultationfinalreport.pdf
([5]) Grupa Robocza Art. 29 jest ciałem doradczym utworzonym na mocy art. 29 dyrektywy 95/46/WE. Składa się ona z przedstawicieli krajowych organów nadzorczych i EIOD oraz przedstawiciela Komisji.
([6]) Opinia Grupy Roboczej Art. 29 nr 05/2012 na temat przetwarzania danych w chmurze obliczeniowej, dostępna pod adresem: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_pl.pdf
([7]) Ponadto organy ochrony danych w kilku państwach członkowskich, np. we Włoszech, Szwecji, Danii, Niemczech, Francji i Zjednoczonym Królestwie, wydały własne wytyczne w sprawie chmury obliczeniowej na szczeblu krajowym.
([8]) Uchwała w sprawie chmury obliczeniowej przyjęta podczas 34. Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności w Urugwaju w dniu 26 października 2012 r.

I.3. *Komunikat w sprawie chmury obliczeniowej*

6. EIOD przyjmuje komunikat z zadowoleniem. Wskazano w nim trzy konkretne najważniejsze działania na szczeblu UE, które mają towarzyszyć wykorzystaniu chmury obliczeniowej i sprzyjać jej przyjęciu w Europie:

— działanie 1: uporządkowanie dużej ilości różnych norm,

— działanie 2: bezpieczne i uczciwe warunki umowne,

— działanie 3: utworzenie Europejskiego partnerstwa na rzecz chmur obliczeniowych w celu wspierania innowacji i wzrostu przez sektor publiczny.

7. Przewidziano także dodatkowe działania, np. mające stymulować wykorzystanie chmury obliczeniowej poprzez wspieranie badań i rozwoju lub podnoszenie świadomości; stwierdzono też potrzebę zajęcia się najważniejszymi zagadnieniami związanymi z usługami w chmurze obliczeniowej – w tym między innymi ochroną danych, dostępem organów ścigania, bezpieczeństwem i odpowiedzialnością usługodawców będących pośrednikami – za pośrednictwem intensywniejszego międzynarodowego dialogu.

8. W komunikacie wspomina się o ochronie danych jako o czynniku niezbędnym, aby zapewnić pomyślne przyjęcie chmury obliczeniowej w Europie. Stwierdza się też ([1]), że w proponowanym rozporządzeniu podjęto wiele kwestii podniesionych przez dostawców usług w chmurze obliczeniowej i klientów chmury obliczeniowej ([2]).

I.4. *Treść i struktura opinii*

9. Niniejsza opinia ma trzy cele.

10. Pierwszym jest podkreślenie znaczenia ochrony prywatności i danych w trwających dyskusjach na temat chmury obliczeniowej. W szczególności wskazuje się w niej, że poziom ochrony danych w chmurze obliczeniowej nie może być niższy od wymaganego w przypadku przetwarzania danych w jakimkolwiek innym kontekście. Warunkiem zgodnego z prawem rozwoju i wykorzystania chmury obliczeniowej jest zagwarantowanie takiego poziomu ochrony danych (zob. rozdział III.3). W opinii uwzględniono wytyczne przedstawione w opinii Grupy Roboczej Art. 29.

11. Drugim celem jest dalsza analiza najważniejszych wyzwań dla ochrony danych związanych z chmurą obliczeniową w kontekście proponowanego rozporządzenia o ochronie danych, w szczególności trudności z jednoznacznym określeniem zakresu odpowiedzialności poszczególnych podmiotów oraz pojęć administratora i podmiotu przetwarzającego. W opinii (głównie w rozdziale IV) przeanalizowano, w jaki sposób proponowane rozporządzenie w obecnej formie ([3]) pomoże w zapewnieniu wysokiego poziomu ochrony danych w związku z usługami w chmurze obliczeniowej. Dlatego też rozwija się w niej poglądy przedstawione przez EIOD w opinii w sprawie pakietu dotyczącego reform w zakresie ochrony danych (zwanej dalej „opinią EIOD w sprawie pakietu dotyczącego reform w zakresie ochrony danych") ([4]) i uzupełnia tę opinię rozważaniami dotyczącymi konkretnie chmury obliczeniowej. EIOD podkreśla, że jego opinia w sprawie pakietu dotyczącego reform w zakresie ochrony danych ma pełne zastosowanie do usług w chmurze obliczeniowej i należy ją uznać za podstawę niniejszej opinii. Ponadto niektóre spośród poruszonych w niej kwestii – jak np. analiza nowych przepisów dotyczących podmiotów danych ([5]) – zostały przedstawione w sposób wystarczająco jasny i dlatego nie będą one rozwijane w niniejszej opinii.

12. Trzecim celem jest wskazanie obszarów, które wymagają dalszych działań na szczeblu UE z punktu widzenia ochrony danych i prywatności w obliczu strategii w zakresie chmury obliczeniowej przedstawionej w komunikacie przez Komisję. Wśród tych obszarów znajdują się między innymi dostarczenie dalszych wytycznych, działania na rzecz normalizacji, przeprowadzenie dodatkowej oceny ryzyka w konkretnych sektorach (np. w sektorze publicznym), opracowanie standardowych warunków umownych, nawiązanie międzynarodowego dialogu na temat zagadnień związanych z chmurą obliczeniową oraz zapewnienie skutecznych środków w dziedzinie współpracy międzynarodowej (ten temat zostanie rozwinięty w rozdziale V).

([1]) Zob. s. 8 komunikatu, sekcję „Działania w ramach agendy cyfrowej mające na celu zwiększanie zaufania do środowiska cyfrowego".
([2]) Używany w niniejszej opinii termin „klienci chmury obliczeniowej" odnosi się generalnie do klientów będących firmami oraz konsumentów będących użytkownikami indywidualnymi.
([3]) Należy uwzględnić fakt, że wniosek dotyczący rozporządzenia jest obecnie omawiany w Radzie i Parlamencie Europejskim w ramach zwykłej procedury ustawodawczej.
([4]) Opinia ta jest dostępna pod adresem: http://www.edps.europa.eu
([5]) Zob. opinię EIOD, w szczególności pkt 140–158.

13. Opinia ma następującą strukturę: W sekcji II przedstawiono przegląd najważniejszych cech chmury obliczeniowej i związanych z nią wyzwań w dziedzinie ochrony danych. W sekcji III dokonano przeglądu najważniejszych elementów istniejących ram prawnych UE i proponowanego rozporządzenia. W sekcji IV przeanalizowano, w jaki sposób proponowane rozporządzenie pomogłoby w zaradzeniu wyzwaniom w dziedzinie ochrony danych wynikającym z wykorzystania usług w chmurze obliczeniowej. W sekcji V przeanalizowano sugestie Komisji dotyczące dalszej polityki oraz zidentyfikowano obszary, w których konieczne mogą być dodatkowe prace. W sekcji VI zawarto wnioski.

14. Chociaż wiele rozważań zawartych w niniejszej opinii odnosi się do wszystkich środowisk, w których wykorzystywane są usługi w chmurze obliczeniowej, nie dotyczy ona wykorzystania tych usług konkretnie przez instytucje i organy UE podlegające nadzorowi EIOD na mocy rozporządzenia (WE) nr 45/2001. EIOD wyda osobne wytyczne na ten temat skierowane do wspomnianych instytucji i organów.

VI. **Wnioski**

121. Jak stwierdzono w komunikacie, chmura obliczeniowa oferuje firmom, konsumentom i sektorowi publicznemu liczne nowe możliwości zarządzania danymi dzięki wykorzystaniu zdalnych zewnętrznych zasobów informatycznych. Jednocześnie niesie ona wiele wyzwań, zwłaszcza dotyczących odpowiedniego poziomu ochrony przetwarzanych danych.

122. Wykorzystanie usług w chmurze obliczeniowej niesie poważne ryzyko rozmycia odpowiedzialności za czynności przetwarzania wykonywane przez dostawców usług w chmurze obliczeniowej, jeżeli kryteria stosowania unijnych przepisów o ochronie danych nie będą wystarczająco jasne, a rola i odpowiedzialność dostawców usług w chmurze obliczeniowej będą definiowane lub pojmowane zbyt wąsko, bądź przepisy te nie zostaną skutecznie wdrożone. EIOD podkreśla, że wykorzystanie usług w chmurze obliczeniowej nie może usprawiedliwiać obniżenia standardów ochrony danych w porównaniu z obowiązującymi w przypadku konwencjonalnych czynności przetwarzania danych.

123. Pod tym względem proponowane rozporządzenie o ochronie danych w przedstawionym kształcie wyjaśniłoby wiele kwestii i dostarczyłoby narzędzi pomagających w zapewnieniu zadowalającego poziomu ochrony danych przez dostawców oferujących usługi w chmurze obliczeniowej klientom z Europy, w szczególności:

— w art. 3 wyjaśniony zostałby zakres terytorialny unijnych zasad ochrony danych oraz zostałby on poszerzony w celu objęcia nim usług w chmurze obliczeniowej,

— w art. 4 ust. 5 wprowadzony zostałby nowy element pojęcia administratora, a mianowicie „warunki". Byłoby to zgodne z coraz powszechniejszym poglądem, według którego wobec złożoności technologii informatycznych umożliwiających świadczenie usług w chmurze obliczeniowej konieczne jest rozszerzenie katalogu okoliczności, w których dostawcę usług w chmurze obliczeniowej można uznać za administratora. Lepiej odzwierciedlałoby to jego realny wpływ na czynności przetwarzania danych,

— proponowane rozporządzenie zwiększyłoby zakres obowiązków oraz odpowiedzialności administratorów danych i podmiotów przetwarzających, wprowadzając konkretne obowiązki takie jak ochrona danych już w fazie projektowania oraz ochrona danych jako opcja domyślna (art. 23), zgłaszanie naruszeń ochrony danych (art. 31 i 32), jak też ocena skutków w zakresie ochrony danych (art. 33). Ponadto rozporządzenie nałożyłoby na administratorów i podmioty przetwarzające obowiązek wdrożenia mechanizmów wykazujących skuteczność zastosowanych środków ochrony danych (art. 22),

— zapisy art. 42 i 43 proponowanego rozporządzenia umożliwiłyby elastyczniejsze wykorzystanie mechanizmów przekazywania danych za granicę, pomagając klientom chmury obliczeniowej i dostawcom usług w chmurze obliczeniowej we wprowadzeniu odpowiednich zabezpieczeń służących ochronie danych w odniesieniu do przekazywania danych osobowych do centrów przetwarzania danych lub serwerów zlokalizowanych w państwach trzecich,

— zapisy art. 30, 31 i 32 proponowanego rozporządzenia wyjaśniłyby obowiązki administratorów i podmiotów przetwarzających w odniesieniu do bezpieczeństwa przetwarzania danych oraz wymogów informacyjnych w przypadku naruszenia ochrony danych, stanowiąc podstawy kompleksowego i opartego na współpracy podejścia do zarządzania kwestiami bezpieczeństwa przez różne podmioty w chmurze obliczeniowej,

— zapisy art. 55–63 proponowanego rozporządzenia usprawniłyby współpracę między organami nadzorczymi i ich skoordynowany nadzór nad transgranicznymi czynnościami przetwarzania, co jest szczególnie ważne w przypadku chmury obliczeniowej.

124. EIOD sugeruje jednak, że po uwzględnieniu szczególnych cech usług w chmurze obliczeniowej, w proponowanym rozporządzeniu należy dodatkowo wyjaśnić następujące aspekty:

— jeżeli chodzi o zakres terytorialny proponowanego rozporządzenia, zmienić treść art. 3 ust. 2 lit. a) na następującą: „oferowaniem towarów lub usług *związanych z przetwarzaniem danych osobowych* takich podmiotów danych w Unii" bądź dodać nowy motyw wskazujący, że przetwarzanie danych osobowych podmiotów danych w Unii przez administratorów z siedzibą poza UE oferujących usługi osobom prawnym z siedzibą w UE jest również objęte zakresem terytorialnym proponowanego rozporządzenia,

— dodać jasną definicję pojęcia „przekazywania", co EIOD wskazał już w opinii w sprawie pakietu dotyczącego reform w zakresie ochrony danych,

— dodać przepis jasno określający warunki, jakie należy spełnić w celu uzyskania dostępu do danych przechowywanych w chmurze obliczeniowej przez organy ścigania spoza krajów EOG. Przepis taki może również nakładać na adresata takiego żądania obowiązek poinformowania w konkretnych przypadkach właściwych organów nadzorczych w UE oraz skonsultowania się z nimi.

125. EIOD podkreśla też, że niezbędne będą dodatkowe wytyczne ze strony Komisji lub organów nadzorczych (w szczególności za pośrednictwem przyszłej Europejskiej Rady Ochrony Danych) w odniesieniu do następujących aspektów:

— wyjaśnienia, jakie mechanizmy należy ustanowić, aby zapewnić weryfikację skuteczności środków ochrony danych w praktyce,

— pomocy podmiotom przetwarzającym w zakresie stosowania się do wiążących reguł korporacyjnych i spełnienia stosownych wymogów,

— przedstawienia najlepszych praktyk w dziedzinach takich jak odpowiedzialność administratora/podmiotu przetwarzającego, odpowiednie zatrzymywanie danych w chmurze obliczeniowej, przenośność danych i wykonywanie praw przez podmioty danych.

126. Ponadto EIOD przyznaje, że kodeksy postępowania opracowane przez branżę i zatwierdzone przez stosowne organy nadzorcze mogłyby stanowić użyteczne narzędzie służące poprawie przestrzegania przepisów i zwiększaniu zaufania między podmiotami.

127. EIOD popiera opracowanie przez Komisję we współpracy z organami nadzorczymi standardowych warunków umownych świadczenia usług w chmurze obliczeniowej zgodnych z wymogami ochrony danych, w szczególności:

— opracowanie wzorcowych warunków umownych, które byłyby włączane do warunków komercyjnego świadczenia usług w chmurze obliczeniowej,

— opracowanie wspólnych warunków i wymogów dotyczących zamówień dla sektora publicznego, uwzględniających konieczność szczególnej ochrony przetwarzanych danych,

— dalsze dostosowanie mechanizmów przekazywania danych za granicę do chmury obliczeniowej, zwłaszcza przez aktualizację obecnych standardowych warunków umownych oraz opracowanie standardowych warunków umownych dotyczących przekazywania danych przez podmioty przetwarzające z siedzibą w UE podmiotom przetwarzającym z siedzibą poza UE.

128. EIOD podkreśla, że przy opracowywaniu standardów i systemów certyfikacji trzeba odpowiednio uwzględnić wymogi ochrony danych, w szczególności:

— stosowania podczas opracowywania standardów zasady ochrony danych już w fazie projektowania oraz domyślnej ochrony danych,

— uwzględnienia przy projektowaniu standardów wymogów ochrony danych takich jak zasada celowości i ograniczenie przechowywania,

— spoczywający na dostawcach usług obowiązek dostarczenia klientom informacji niezbędnych w celu dokonania należytej oceny ryzyka oraz wdrożonych środków bezpieczeństwa, jak też informowania ich o incydentach związanych z bezpieczeństwem.

129. Wreszcie, EIOD podkreśla potrzebę zmierzenia się z wyzwaniami związanymi z chmurą obliczeniową na szczeblu międzynarodowym. Zachęca przy tym Komisję do podjęcia międzynarodowego dialogu na temat zagadnień związanych z chmurą obliczeniową, w tym jurysdykcji i dostępu organów ścigania; sugeruje też, że wiele spośród tych zagadnień można uregulować w umowach międzynarodowych lub dwustronnych takich jak umowy o wzajemnej pomocy, jak też umowy handlowe. Na szczeblu międzynarodowym należy wypracować ogólnoświatowe standardy określające minimalne warunki i zasady dostępu organów ścigania do danych. EIOD popiera również wypracowanie przez organy nadzorcze skutecznych mechanizmów współpracy międzynarodowej, w szczególności w odniesieniu do zagadnień związanych z chmurą obliczeniową.

Sporządzono w Brukseli dnia 16 listopada 2012 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych