Streszczenie opinii Europejskiego Inspektora Ochrony Danych w sprawie systemów zarządzania danymi osobowymi

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

(2016/C 463/10)

W opinii analizie poddano pojęcie technologii i ekosystemów, mających na celu wzmocnienie pozycji osób fizycznych, aby miały one możliwość sprawowania kontroli nad udostępnianiem swoich danych osobowych („systemy zarządzania danymi osobowymi" lub w skrócie „PIMS").

Nasza wizja zakłada stworzenie nowej rzeczywistości, w której obywatele zarządzają swoją tożsamością w sieci i sprawują nad nią kontrolę. Naszym celem jest przekształcenie obecnego systemu, który w centrum stawia dostawcę, w taki, który koncentruje się na osobie, gdzie obywatele objęci są ochroną przed bezprawnym przetwarzaniem ich danych, a także przed technikami polegającymi na uciążliwym śledzeniu i tworzeniu profili, które mają na celu obchodzenie kluczowych zasad ochrony danych.

Tę nową rzeczywistość będą wspierać nowoczesne ramy prawne UE, jak również możliwości, jakie oferuje dynamiczny system skoordynowanego egzekwowania przez wszystkie odpowiednie organy nadzorcze i regulacyjne.

Przyjęte niedawno ogólne rozporządzenie o ochronie danych wzmacnia i modernizuje ramy regulacyjne, aby zapewnić ich skuteczność w erze dużych zbiorów danych poprzez zwiększenie pewności i zaufania obywateli w środowisku internetowym oraz na jednolitym rynku cyfrowym. Nowe przepisy, w tym dotyczące większej przejrzystości, wzmocnionego prawa dostępu i prawa do przenoszenia danych mogą przyznawać użytkownikom większą kontrolę nad ich danymi, a także mogą przyczynić się do rozwoju bardziej efektywnych rynków danych osobowych, z korzyścią zarówno dla konsumentów, jak i przedsiębiorstw.

Niedawno EIOD wydał opinię w sprawie skutecznego egzekwowania praw podstawowych w dobie dużych zbiorów danych. W opinii podkreśla się obecne warunki rynkowe i praktyki biznesowe, które stoją na przeszkodzie skutecznemu egzekwowaniu praw obywateli do ochrony ich danych osobowych, jak również innych praw podstawowych, a także wzywa się do nadania większego tempa wspólnemu i spójnemu egzekwowaniu praw konkurencji, ochrony konsumentów i ochrony danych. Mamy nadzieję, że to zwiększone egzekwowanie przysłuży się tworzeniu warunków rynkowych, w których mogą rozwijać się usługi sprzyjające ochronie prywatności. Podejście zastosowane w niniejszej opinii ma na celu wzmacnianie praw podstawowych w otaczającym nas świecie cyfrowym przy jednoczesnym kreowaniu nowych możliwości dla przedsiębiorstw w zakresie tworzenia innowacyjnych usług opartych na danych osobowych, których podstawą jest wzajemne zaufanie. Systemy zarządzania danymi osobowymi oferują nie tylko nową strukturę techniczną i organizacyjną zarządzania danymi, lecz także ramy dotyczące zaufania i, w rezultacie, alternatywne modele biznesowe na potrzeby zbierania i przetwarzania danych osobowych w dobie dużych zbiorów danych w sposób bardziej zgodny z europejskim prawem w zakresie ochrony danych.

W niniejszej opinii przedstawimy zwięzłą charakterystykę PIMS, rodzaje problemów, które te systemy mają rozwiązywać, i sposoby ich rozwiązywania. Następnie analizie zostanie poddany sposób, w jaki mogą się one przyczynić do lepszej ochrony danych osobowych, oraz wyzwania, jakim będą musiały sprostać. Ponadto określimy w niej sposoby na wykorzystanie możliwości, jakie te systemy oferują. Aby nowe modele biznesowe w zakresie ochrony danych mogły się rozwijać, konieczne może być wprowadzenie dodatkowych zachęt dla oferujących je dostawców usług. Należy w szczególności zbadać, które inicjatywy w zakresie polityki mogłyby motywować administratorów danych do zaakceptowania tego sposobu dostarczania danych. Ponadto inicjatywa służb publicznych w zakresie akceptacji PIMS jako źródła danych zamiast bezpośredniego gromadzenia danych mogłaby zwiększyć masę krytyczną akceptacji PIMS.

Nowe środowisko PIMS, które ma na celu przywrócenie osobom fizycznym i konsumentom kontroli nad ich danymi osobowymi, zasługuje na uwagę, wsparcie i dalsze badania, aby przyczynić się do wykorzystywania dużych zbiorów danych w sposób zrównoważony i etyczny oraz do skutecznego wdrożenia zasad przyjętego ostatnio ogólnego rozporządzenia o ochronie danych.

I. PIMS: UDOSTĘPNIANIE DANYCH – DZIELENIE SIĘ KORZYŚCIAMI?

1. Obowiązujące obecnie warunki przetwarzania danych osobowych są często niesprawiedliwe względem osób fizycznych, których dane są przetwarzane. Warunki prawne i narzędzia techniczne utrudniają osobom fizycznym korzystanie z ich praw, umożliwiając administratorom ograniczanie ich odpowiedzialności. Brokerzy danych, sieci reklamowe, dostawcy usług portali społecznościowych oraz inne podmioty korporacyjne dysponują coraz pełniejszymi zestawami danych dotyczących osób fizycznych we współczesnym społeczeństwie cyfrowym, a osoby fizyczne tracą kontrolę nad śladami internetowymi, które pozostawiają. Osoby fizyczne będące celem działania podmiotów, podlegające profilowaniu i ocenie przez te podmioty, często w sposób pozostający poza ich kontrolą czy nawet

wiedzą, mogą czuć się bezsilne i należy przyznać im uprawnienia w zakresie kontrolowania ich tożsamości. Nawet mimo formalnego „powiadomienia" o warunkach ogólnych i możliwości ich „akceptacji" osoby fizyczne stają się niejednokrotnie częścią systemu zaprojektowanego tak, aby zapewnić maksymalną monetyzację danych osobowych, w którym nie pozostawiono im żadnego realnego wyboru czy realnej kontroli.

2. Komunikat Komisji Europejskiej dotyczący dużych zbiorów danych ([1]) określa plan działań realizujących wspólny cel, jakim jest ochrona danych osobowych i konsumentów. Zachęca się w nim w szczególności do wykorzystywania „przestrzeni danych osobowych" jako stawiających użytkownika w centrum, bezpiecznych miejsc, w których przechowuje się dane osobowe i potencjalnie umożliwia się innym uzyskanie do nich dostępu. Podzielamy pogląd, zgodnie z którym należy propagować innowacyjne narzędzia cyfrowe i modele biznesowe oparte na wzmacnianiu praw osób fizycznych. Dzięki temu osoby fizyczne mogą zyskać możliwość czerpania korzyści z tego rodzaju udostępniania danych, a więc uczestnictwa w procesie wykorzystywania i rozpowszechniania ich danych osobowych.

3. W naszej opinii pt. „Sprostanie wyzwaniom związanym z dużymi zbiorami danych" ([2]) przedstawiliśmy pogląd, zgodnie z którym prawny obowiązek skutecznej zgody należy uzupełniać rzeczywistą, praktyczną kontrolą nad danymi osobowymi. Stwierdziliśmy, że „zapewnianie praw dostępu może stanowić właściwość usługi świadczonej klientom, a nie obciążenie administracyjne" oraz że organizacje działające w oparciu o wykorzystywanie „dużych zbiorów danych" powinny „być przygotowane do tego, by dzielić się bogactwem wytworzonym dzięki przetwarzaniu danych osobowych z osobami fizycznymi, których dane przetwarzają". W tym kontekście zauważyliśmy, że „zbiory danych osobowych mogłyby pomóc w rozwiązaniu niektórych problemów związanych z utratą osobistej kontroli nad danymi osobowymi". Na mocy przyjętego ostatnio ogólnego rozporządzenia o ochronie danych ([3]) zwiększono wymogi prawne dotyczące zgody ([4]) oraz wprowadzono skuteczne, nowoczesne zasady ochrony danych w fazie projektowania oraz domyślną ochronę danych ([5]), a także nowe prawo do przenoszenia danych ([6]). Aby założenia przedstawione w nowych ramach prawnych w zakresie ochrony danych mogły się urzeczywistnić, niezbędne są praktyczne narzędzia umożliwiające osobom fizycznym korzystanie z ich praw w wygodny i przyjazny dla użytkownika sposób.

4. W niniejszej opinii analizuje się nowe technologie i ekosystemy, które mają na celu przyznawanie kompetencji osobom fizycznym, aby miały one możliwość sprawowania kontroli nad gromadzeniem i udostępnianiem ich danych osobowych. Pojęcie to będzie określane jako „systemy zarządzania danymi osobowymi" (zwane dalej „PIMS") ([7]). Pojęcie PIMS zawiera w sobie nowe podejście, które przewiduje, że osoby fizyczne są posiadaczami swoich danych osobowych. Może ono spowodować zmianę paradygmatu w obszarze zarządzania danymi osobowymi i przetwarzania ich, która niesie ze sobą skutki społeczno-ekonomiczne. Z kolei obecna sytuacja w obszarze usług internetowych charakteryzuje się niewielką liczbą dostawców usług, którzy zajmują dominującą pozycję na rynku dzięki monetyzacji danych osobowych użytkowników w zamian za „bezpłatne" usługi. Do tego stanu rzeczy dochodzi często nierówny układ sił, gdzie klient staje w obliczu podejścia „chcesz to bierz, nie to nie", oraz asymetria informacyjna pomiędzy dostawcami usług a użytkownikami, gdzie osoby fizyczne spotykają się z niewielką lub zerową przejrzystością odnośnie do tego, co dzieje się z ich danymi osobowymi.

5. Pojęcie PIMS opiera się w głównej mierze na przekształceniu obecnego systemu stawiającego w centrum dostawcę usług w taki, który skupia się na osobach fizycznych zdolnych do zarządzania swoją tożsamością w internecie i sprawowania nad nią kontroli ([8]). Co do zasady, osoby fizyczne powinny móc decydować o tym, czy ich dane osobowe mają być udostępniane, komu, w jakim celu i na jak długo, a także powinny mieć możliwość śledzenia tych danych i wtórnego ich przejęcia, wedle życzenia. Warto zbadać, w jaki sposób PIMS mogłyby pomóc odpowiedzieć na niektóre zastrzeżenia związane z utratą osobistej kontroli nad danymi osobowymi, które wskazano jako kluczowe problemy dotyczące dużych zbiorów danych ([9]).

([1]) Komunikat COM(2014)442: Ku gospodarce opartej na danych: http://ec.europa.eu/transparency/regdoc/rep/1/2014/PL/1-2014-442-PL-F1-1.PDF.

([2]) Opinia Europejskiego Inspektora Ochrony Danych 7/2015: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf. Zob. w szczególności sekcję 3.

([3]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

([4]) Zob. między innymi art. 6 ust. 1 lit. a), art. 7 i 8 oraz motywy 42–43 ogólnego rozporządzenia o ochronie danych.

([5]) Artykuł 25 ogólnego rozporządzenia o ochronie danych.

([6]) Artykuł 20 ogólnego rozporządzenia o ochronie danych.

([7]) Pojęcia powiązane to „zbiory danych osobowych", „przestrzenie danych osobowych" czy „skarbce danych osobowych". W niniejszej opinii będziemy stosować termin „PIMS", ponieważ wydaje się, że za jego pomocą najlepiej można opisać to pojęcie w sposób ogólny i zrozumiały. Zastosowany w niniejszej opinii skrót „PIMS" może odnosić się zarówno do liczby pojedynczej, jak i mnogiej: system zarządzania danymi osobowymi lub systemy zarządzania danymi osobowymi.

([8]) Zob. motyw 7 ogólnego rozporządzenia o ochronie danych: „Osoby fizyczne powinny mieć kontrolę nad własnymi danymi osobowymi". Zobacz na przykład Doc Searls, *The Intention Economy: When Customers Take Charge* (Boston: Harvard Business Review Press, 2012).

([9]) Zob. na przykład Ira S. Rubinstein, Big Data: The End of Privacy or a New Beginning? International Data Privacy Law, 2013, tom 3, nr 2.

6. Podejście to ma na celu wzmacnianie praw podstawowych w otaczającym nas świecie cyfrowym przy jednoczesnym kreowaniu nowych możliwości dla przedsiębiorstw w zakresie tworzenia innowacyjnych usług opartych na danych osobowych, których podstawą jest wzajemne zaufanie. PIMS stanowią obietnicę stworzenia nowej struktury technicznej i organizacyjnej zarządzania danymi, dzięki czemu budowane są ramy zaufania. W zamierzeniu mają one umożliwić funkcjonowanie alternatywnych modeli biznesowych na potrzeby gromadzenia i przetwarzania danych osobowych w dobie dużych zbiorów danych, zapewniających realizację tych procesów w sposób bardziej zgodny z europejskim prawem w zakresie ochrony danych.

7. W niniejszej opinii przedstawiamy zwięzłą charakterystykę PIMS, rodzaje problemów, które te systemy mają rozwiązywać i sposoby ich rozwiązywania ([1]). Analizie poddano sposób, w jaki mogą się one przyczynić do lepszej ochrony danych osobowych oraz wyzwania, jakim będą musiały sprostać. Ponadto określamy w niej sposoby na wykorzystanie możliwości, jakie te systemy oferują.

IV. WNIOSKI I KOLEJNE KROKI

4.1. Na drodze do pełnego zastosowania ogólnego rozporządzenia o ochronie danych – możliwości

54. Jak wskazano powyżej, prawodawca Unii przyjął ostatnio pakiet reform w zakresie ochrony danych, wzmacniających i modernizujących ramy regulacyjne, aby zachowały one skuteczność w dobie dużych zbiorów danych.

55. Nowe ogólne rozporządzenie o ochronie danych, w tym przepisy dotyczące większej przejrzystości, wzmocnionego prawa dostępu i prawa do przenoszenia danych powinny pomóc w przyznaniu osobom fizycznym większej kontroli nad ich danymi, a także mogą przyczynić się do rozwoju bardziej efektywnych rynków danych osobowych, z korzyścią zarówno dla konsumentów, jak i przedsiębiorstw.

56. Kodeksy postępowania oraz systemy certyfikacji przewidziane w ogólnym rozporządzeniu o ochronie danych stanowią uprzywilejowane instrumenty, mające na celu zapewnienie szczególnej widoczności i roli technologii i produktów, które – tak jak PIMS – mogą służyć bardziej efektywnemu wdrażaniu przepisów prawa dotyczących ochrony danych na poziomie praktycznym.

57. Jednakże PIMS stają w obliczu nadrzędnej trudności, jaką stanowi penetracja rynku zdominowanego przez usługi internetowe oparte na modelach biznesowych i strukturach technicznych, w których osoby fizyczne pozbawione są kontroli nad swoimi danymi, jak wyjaśniono w sekcji 3.9. Zmiana sytuacji na taką, w której osoby fizyczne zyskują skuteczną możliwość udostępniania dostawcom usług części danych w swoich PIMS zamiast udostępniania danych bezpośrednio dostawcy usług, będzie wymagała dodatkowych zachęt dla dostawców usług. Komisja może wykorzystać ogłoszone już inicjatywy dotyczące przepływów i własności danych ([2]) w celu zbadania, które dodatkowe inicjatywy w zakresie polityki mogłyby motywować administratorów danych do zaakceptowania tego sposobu dostarczania danych. Ponadto inicjatywa służb publicznych administracji elektronicznej w zakresie akceptacji PIMS jako źródła danych zamiast bezpośredniego gromadzenia danych mogłaby zwiększyć masę krytyczną akceptacji PIMS.

58. Uzupełnieniem niniejszej analizy mogłyby być środki mające na celu stworzenie technicznych, społecznych i gospodarczych podstaw, w tym działania normalizacyjne, zachęty ekonomiczne, jak również wspieranie badań i projektów pilotażowych.

59. Organy administracji publicznej w Unii Europejskiej i państwach członkowskich, jak również projekty przez nie współfinansowane, to obszary, w których w pierwszej kolejności ta zmiana perspektywy powinna zostać przetestowana, wspierana i, miejmy nadzieję, zrealizowana.

4.2. Wspieranie PIMS i podstawowej technologii jako droga do skutecznej ochrony danych

60. Dobre regulacje, choć niezbędne, same w sobie nie są wystarczające. Jak wskazaliśmy w naszej opinii pt. „Sprostanie wyzwaniom związanym z dużymi zbiorami danych" ([3]), przedsiębiorstwa i inne organizacje inwestujące dużo wysiłku w poszukiwanie innowacyjnych sposobów wykorzystania danych osobowych powinny zastosować to samo nowoczesne podejście do wdrażania zasad dotyczących ochrony danych.

([1]) Zob. na przykład raport dotyczący zbiorów danych osobowych sporządzony przez Uniwersytet w Cambridge dla Komisji Europejskiej: https://ec.europa.eu/digital-single-market/en/news/study-personal-data-stores-conducted-cambridge-university-judge-business-school.

([2]) Komunikat: Cyfryzacja europejskiego przemysłu – Pełne wykorzystanie możliwości jednolitego rynku cyfrowego https://ec.europa.eu/transparency/regdoc/rep/1/2016/PL/1-2016-180-PL-F1-1.PDF.

([3]) Cytowana wyżej opinia Europejskiego Inspektora Ochrony Danych 7/2015.

61. Wkład technologii w model PIMS jest kwestią fundamentalną. Systemy zarządzania danymi osobowymi mogą służyć do testowania podejść w zakresie ochrony danych w fazie projektowania i wspomagających je technologii. Stosowne tematy badań, wymagające odpowiedniego wsparcia i odpowiednich inwestycji, obejmują: interoperacyjne i chroniące prywatność zarządzanie tożsamością; mechanizmy autoryzacji; interoperacyjność danych; bezpieczeństwo danych; mechanizmy automatycznego egzekwowania „umów" zawartych pomiędzy osobami fizycznymi a innymi podmiotami. Wszystkie te działania realizowane są z wykorzystaniem kryptografii i szyfrowania, czemu sprzyja dostępność mocy obliczeniowej po niskiej cenie. Zdecydowane wsparcie podmiotów kształtujących politykę, takich jak Komisja, dla podstawowych i stosowanych badań w tych dziedzinach technologii, jest konieczne na tym wstępnym etapie, aby nie zaprzepaścić aktualnych możliwości.

62. W celu wspierania badań i rozwoju oraz wprowadzenia na rynek w obszarze PIMS zalecamy, aby Komisja zaplanowała możliwe synergie z innymi obszarami strategii jednolitego rynku cyfrowego, takimi jak przetwarzanie w chmurze i internet rzeczy. W ten sposób możliwe byłoby prowadzenie projektów pilotażowych, mających na celu zaprojektowanie i przetestowanie interakcji usług w zakresie przetwarzania w chmurze i internetu rzeczy z PIMS.

4.3. **Jaki będzie wkład Europejskiego Inspektora Ochrony Danych w tę debatę**

63. Celem EIOD jest wniesienie wkładu w działania sprzyjające realizacji wysiłków sektora prywatnego i publicznego w kierunku wskazanym powyżej. W dalszym ciągu będziemy ułatwiać debatę, między innymi poprzez organizację wydarzeń/warsztatów, w celu wskazania, zachęcenia do stosowania i propagowania dobrych praktyk, aby zwiększyć przejrzystość i kontrolę użytkownika, jak również w celu odkrywania możliwości, jakie oferują PIMS. Nadal będziemy także wspierać prace sieci Internet Privacy Engineering Network („IPEN") jako interdyscyplinarnego ośrodka wiedzy dla inżynierów i ekspertów w dziedzinie prywatności danych. W tym kontekście nadal będziemy oferować platformę dla programistów i propagatorów PIMS, aby czerpać korzyści z wymiany doświadczeń ze specjalistami zajmującymi się innymi technologiami i ochroną danych.

Sporządzono w Marrakeszu dnia 20 października 2016 r.

Giovanni BUTTARELLI

Europejski Inspektor Ochrony Danych