I

(Rezolucje, zalecenia i opinie)

ZALECENIA

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Zalecenia EIOD dotyczące możliwości reformy ochrony danych w UE

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

(2015/C 301/01)

W dniu 24 czerwca 2015 r. trzy główne instytucje UE – Parlament Europejski, Rada i Komisja Europejska – rozpoczęły określone mianem nieformalnych rozmów trójstronnych negocjacje w ramach procedury współdecyzji w sprawie wnioskowanego ogólnego rozporządzenia o ochronie danych ([1]). Podstawą rozmów trójstronnych jest wniosek Komisji ze stycznia 2012 r., rezolucja ustawodawcza Parlamentu z dnia 12 marca 2014 r. oraz podejście ogólne Rady przyjęte w dniu 15 czerwca 2015 r. ([2]). Wszystkie trzy instytucje zobowiązały się do prac nad rozporządzeniem w ramach ogólniejszego pakietu reform w zakresie ochrony danych, który obejmuje wnioskowaną dyrektywę dotyczącą organów policji i wymiaru sprawiedliwości. Proces ten powinien się zakończyć pod koniec 2015 r., a formalne przyjęcie obydwu instrumentów będzie prawdopodobnie możliwe na początku 2016 r., po czym nastąpi dwuletni okres przejściowy ([3]).

Europejski Inspektor Ochrony Danych (EIOD) jest niezależną instytucją UE. Inspektor nie bierze udziału w rozmowach trójstronnych, ale na mocy art. 41 ust. 2 rozporządzenia nr 45/2001 jest odpowiedzialny „za zapewnienie, że podstawowe prawa i wolności osób fizycznych, w szczególności prawo do prywatności są respektowane przez instytucje i organy wspólnotowe w odniesieniu do przetwarzania danych osobowych" oraz „za doradzanie instytucjom i organom wspólnotowym i podmiotom danych we wszystkich kwestiach związanych z przetwarzaniem danych osobowych". Inspektor i jego zastępca zostali powołani w grudniu 2014 r., przy czym wyraźnie wskazano, że mają działać w sposób bardziej konstruktywny i aktywny; w marcu 2015 r. opublikowali pięcioletnią strategię, wskazując, w jaki sposób zamierzają wypełnić tę misję oraz rozliczyć się z tego zadania ([4]).

Niniejsza opinia stanowi pierwszy ważny krok w realizacji strategii EIOD. Przyjmując za punkt wyjścia dyskusje z instytucjami UE, państwami członkowskimi, społeczeństwem obywatelskim, przemysłem oraz innymi zainteresowanymi stronami, udzielamy rad mających pomóc uczestnikom rozmów trójstronnych w osiągnięciu na czas właściwego konsensusu. Opinia dotycząca ogólnego rozporządzenia o ochronie danych składa się z dwóch części:

— przedstawionej przez EIOD wizji przyszłościowych zasad ochrony danych z przykładami ilustrującymi nasze zalecenia, oraz

— załącznika („Załącznik do opinii 3/2015: tabela porównawcza wersji ogólnego rozporządzenia o ochronie danych z zaleceniami EIOD") z czterokolumnową tabelą umożliwiającą porównanie kolejnych artykułów wersji rozporządzenia przyjętych odpowiednio przez Komisję, Parlament i Radę wraz z zaleceniami EIOD.

Opinię opublikowano na naszej stronie internetowej oraz za pośrednictwem aplikacji mobilnej. Jesienią 2015 r. zostanie ona uzupełniona o zalecenia dotyczące zarówno motywów rozporządzenia, jak i – po przyjęciu przez Radę ogólnego stanowiska w sprawie dyrektywy – ochrony danych w związku z działaniami organów policji i wymiaru sprawiedliwości.

Kompleksowa opinia EIOD w sprawie proponowanego przez Komisję pakietu reform z marca 2012 r. pozostaje w mocy. Trzy lata później musieliśmy jednak zaktualizować nasze rady, aby ustosunkować się bezpośrednio do stanowisk współustawodawców, a także przedstawić konkretne zalecenia ([5]). Podobnie jak w przypadku opinii z 2012 r., niniejszy dokument jest spójny z opiniami i stwierdzeniami Grupy Roboczej Art. 29, w tym zawartymi w przyjętym w dniu 17 czerwca dodatku dotyczącym „podstawowych tematów w świetle rozmów trójstronnych", w powstaniu którego EIOD uczestniczył jako pełnoprawny członek Grupy Roboczej ([6]).

Wyjątkowa możliwość: dlaczego reforma jest tak ważna

Wielki wysiłek związany ze zmianą przepisów dotyczących danych osobowych w UE dobiega końca. Ogólne rozporządzenie o ochronie danych będzie potencjalnie dotyczyć przez najbliższe dziesięciolecia wszystkich osób fizycznych w UE i wszystkich organizacji w UE, które przetwarzają dane osobowe, oraz organizacji spoza UE, które przetwarzają dane osobowe osób fizycznych w UE ([7]). Nadszedł czas, aby chronić podstawowe prawa i wolności osób fizycznych w opartym na danych społeczeństwie przyszłości.

Skuteczna ochrona danych daje uprawnienia osobom fizycznym oraz pobudza do działania odpowiedzialne przedsiębiorstwa i organy publiczne. Przepisy prawne w tym obszarze mają złożony i techniczny charakter, a ich interpretacja wymaga zasięgnięcia porady ekspertów, a w szczególności niezależnych organów ochrony danych, które rozumieją wyzwania związane z zapewnieniem zgodności z prawem. Ogólne rozporządzenie o ochronie danych będzie prawdopodobnie jednym z najdłuższych aktów prawnych Unii, więc UE musi obecnie zastosować selektywne podejście, skupiając się na przepisach naprawdę niezbędnych, a zarazem unikając szczegółowych zapisów, które mogłyby w niezamierzony sposób nadmiernie ingerować w technologie przyszłości. W wersjach poszczególnych instytucji nacisk kładzie się na przejrzystość i zrozumiałość przetwarzania danych osobowych, więc zasady tej należy także przestrzegać w samym rozporządzeniu, czyniąc je tak zwięzłym i łatwym do zrozumienia, jak jest to możliwe.

Ustalenie ostatecznej postaci aktu prawnego jest zadaniem Parlamentu Europejskiego i Rady jako współustawodawców, w czym będzie je wspomagać Komisja jako inicjator ustawodawstwa i strażnik traktatów. EIOD nie uczestniczy w rozmowach trójstronnych, lecz jest uprawniony do aktywnego doradztwa zgodnie z zakresem kompetencji określonym przy powołaniu Inspektora i jego zastępcy, a także przyjętą niedawno strategią EIOD. W niniejszej opinii wykorzystano ponad dziesięcioletnie doświadczenie w nadzorze nad przestrzeganiem przepisów dotyczących ochrony danych i doradztwie w kształtowaniu polityki, aby pomóc instytucjom osiągnąć wynik służący interesom osób fizycznych.

Ustawodawstwo jest sztuką rzeczy możliwych. Każda z dostępnych opcji, a więc wersji rozporządzenia proponowanych odpowiednio przez Komisję, Parlament i Radę, zawiera wiele godnych uznania przepisów, ale każdą z nich można też ulepszyć. Efekt nie będzie naszym zdaniem idealny, ale zamierzamy wspierać instytucje w osiągnięciu jak najlepszego wyniku. Dlatego też nasze zalecenia nie wychodzą poza zakres tych trzech wersji. Kierujemy się przy tym trzema nadrzędnymi celami:

— potrzebą wypracowania lepszego rozwiązania dla obywateli,

— potrzebą opracowania zasad skutecznych w praktyce,

— potrzebą opracowania zasad, które pozostaną aktualne przez kilkadziesiąt lat.

Niniejsza opinia służy zapewnieniu przejrzystości i odpowiedzialności – te dwie zasady są być może najważniejszą nowością wprowadzoną w ogólnym rozporządzeniu o ochronie danych. Rozmowy trójstronne są obserwowane uważniej niż kiedykolwiek wcześniej. Nasze zalecenia mają charakter jawny i wzywamy wszystkie instytucje UE do przejęcia inicjatywy oraz dania przykładu, aby ta reforma ustawodawstwa była wynikiem przejrzystego procesu, nie zaś sekretnego kompromisu.

UE potrzebuje nowego porozumienia w sprawie ochrony danych – otwarcia nowego rozdziału. Reszta świata uważnie obserwuje przebieg prac. Pierwszorzędne znaczenie ma jakość nowego prawa oraz jego wzajemne oddziaływanie z globalnymi systemami i tendencjami prawnymi. Swoją opinią EIOD sygnalizuje gotowość do udzielenia pomocy, aby UE w jak największym stopniu skorzystała z tej historycznej szansy.

1. Lepsze rozwiązanie dla obywateli

Celem przepisów unijnych zawsze było ułatwianie przepływu danych zarówno w obrębie UE, jak i w kontaktach z jej partnerami handlowymi, lecz nadrzędną kwestią pozostaje dbałość o prawa i wolności osób fizycznych. Internet umożliwia w bezprecedensowym stopniu łączność, wyrażanie opinii oraz dostarczanie wartościowych informacji firmom i konsumentom. Prywatność jest niemniej dziś dla Europejczyków ważniejsza niż kiedykolwiek. Zgodnie z badaniem Eurobarometru o ochronie danych z czerwca 2015 r. ([8]) ponad sześciu na dziesięciu obywateli nie ufa przedsiębiorstwom internetowym, a dwie trzecie wyraża niepokój wynikający z braku pełnej kontroli nad informacjami, które podaje w internecie.

Po reformie musimy utrzymać, a w miarę możliwości podwyższyć standardy ochrony osób fizycznych. Pakiet reform ochrony danych zaproponowano w pierwszej kolejności jako drogę do „wzmocnienia prawa do prywatności w internecie" dzięki zapewnieniu obywatelom „lepszej informacji o przysługujących im prawach i większej kontroli nad ich danymi" ([9]). Przedstawiciele organizacji społeczeństwa obywatelskiego wystosowali w kwietniu 2015 r. list do Komisji Europejskiej, wzywając zaangażowane instytucje, by pozostały wierne tym celom ([10]).

Obowiązujące zasady zapisane w Karcie praw podstawowych Unii Europejskiej, która stanowi prawo pierwotne UE, powinny być stosowane w sposób konsekwentny, dynamiczny i nowatorski, aby obywatele mogli skutecznie korzystać ze swoich praw w praktyce. Reforma ta musi mieć charakter kompleksowy, stąd niezbędny jest pakiet, ale przetwarzanie danych będzie prawdopodobnie przedmiotem większej liczby aktów prawnych, więc niezbędna jest jasność co do ich dokładnego zakresu i współdziałania, aby wykluczyć wszelkie luki obniżające skuteczność zabezpieczeń ([11]).

Dla EIOD punktem wyjścia jest godność osoby ludzkiej, która wykracza poza kwestie zwykłej zgodności z prawem ([12]). Nasze zalecenia opierają się na ocenie kolejnych artykułów ogólnego rozporządzenia o ochronie danych – czy z osobna i łącznie wzmacniają one pozycję osób fizycznych w porównaniu do obecnych ram prawnych. Punktem odniesienia są zasady leżące u podstaw ochrony danych, czyli art. 8 Karty praw podstawowych Unii Europejskiej ([13]).

1.1. *Definicje: jasne określenie, czym są dane osobowe*

Osoby fizyczne powinny być w stanie skuteczniej wykonywać swoje prawa w odniesieniu do wszelkich informacji, które umożliwiają ich identyfikację lub wskazanie, nawet jeżeli informacje te są uznawane za „spseudonimizowane" ([14]).

1.2. *Wszelkie operacje przetwarzania danych muszą być zarówno zgodne z prawem, jak i uzasadnione*

— Wymagania, aby wszelkie operacje przetwarzania danych ograniczały się do określonych celów i posiadały podstawę prawną, mają charakter łączny, a nie alternatywny. Zalecamy unikanie wszelkiego łączenia, a tym samym osłabiania tych zasad. UE powinna w zamian zachować, uprościć i wprowadzić w życie istniejącą zasadę, że dane osobowe powinny być używane wyłącznie zgodnie z pierwotnymi celami, w których je zebrano ([15]).

— Jedną z możliwych podstaw prawnych przetwarzania danych jest zgoda, trzeba jednak zapobiec stosowaniu przymusowych pól wyboru w przypadkach, gdzie w rzeczywistości tego wyboru nie ma i gdzie w ogóle nie zachodzi potrzeba przetwarzania danych. Zalecamy umożliwienie wyrażenia zgody w szerokim lub wąskim zakresie (np. dotyczącej badań klinicznych), której zasady będą przestrzegane i która może zostać wycofana ([16]).

— EIOD popiera racjonalne, innowacyjne rozwiązania dotyczące międzynarodowego przekazywania danych osobowych, które ułatwiają wymianę danych z poszanowaniem zasad ochrony danych i nadzoru nad nimi. Zdecydowanie odradzamy zezwalanie na przekazywanie danych na podstawie uzasadnionych interesów administratora, gdyż nie zapewnia to dostatecznej ochrony osobom fizycznym. UE nie powinna też umożliwiać organom państw trzecich bezpośredniego dostępu do danych znajdujących się na jej terytorium. Wniosek o przekazanie danych wystosowany przez organ państwa trzeciego powinien zostać uwzględniony jednie wówczas, gdy jest on zgodny z normami ustanowionymi w porozumieniach o wzajemnej pomocy prawnej, umowach międzynarodowych lub w związku z innymi legalnymi kanałami współpracy międzynarodowej ([17]).

1.3. *Bardziej niezależny i posiadający większe uprawnienia nadzór*

— Organy ochrony danych w UE powinny być gotowe do wykonywania swojej roli w chwili, gdy ogólne rozporządzenie o ochronie danych wejdzie w życie, a Europejska Rada Ochrony Danych powinna w pełni funkcjonować, gdy zacznie ono być stosowane ([18]).

— Organy powinny mieć możliwość rozpatrywania oraz badania skarg i roszczeń wnoszonych przez osoby, których dane dotyczą, jak też instytucje, organizacje oraz stowarzyszenia.

— Egzekwowanie praw osób fizycznych wymaga ustanowienia skutecznego systemu odpowiedzialności i odszkodowań za szkody wyrządzone przez niezgodne z prawem przetwarzanie danych. Ze względu na wyraźne przeszkody w dochodzeniu roszczeń w praktyce powinna istnieć możliwość reprezentacji osób fizycznych w postępowaniu sądowym przez instytucje, organizacje i stowarzyszenia ([19]).

2. **Zasady skuteczne w praktyce**

Zabezpieczeń nie należy mylić z formalnościami. Nadmierna szczegółowość lub próby zarządzania procesami gospodarczymi w skali mikro grożą dezaktualizacją przepisów w przyszłości. Można tutaj wziąć przykład z unijnych zasad dotyczących konkurencji, gdzie stosunkowo niewielki korpus prawa wtórnego jest rygorystycznie egzekwowany, sprzyjając budowie kultury odpowiedzialności i świadomości wśród podmiotów gospodarczych ([20]).

W każdej z trzech wersji rozporządzenia zawarto postulat przedstawiania jaśniejszych i prostszych informacji przez podmioty odpowiedzialne za przetwarzanie danych osobowych ([21]). Również obowiązki techniczne trzeba sformułować w zwięzły i łatwo zrozumiały sposób, jeżeli mają one być należycie wypełniane przez administratorów danych ([22]).

Obecne procedury nie są nienaruszalne, a celem naszych zaleceń jest ustalenie sposobów ograniczenia biurokracji oraz zminimalizowania wymogów w zakresie dokumentacji i nieistotnych formalności. Zalecamy działania ustawodawcze tylko w przypadkach, gdy są one naprawdę niezbędne. Daje to pole manewru przedsiębiorstwom, organom publicznym i organom ochrony danych: powstałą przestrzeń trzeba wypełnić dzięki odpowiedzialności oraz wytycznym ze strony organów ochrony danych. Ogólnie rzecz biorąc, przyjęcie naszych zaleceń poskutkowałoby tekstem ogólnego rozporządzenia o ochronie danych niemal o 30 % krótszym niż średnia długość trzech wersji przedstawionych przez instytucje ([23]).

2.1. *Skuteczne zabezpieczenia, a nie procedury*

— Dokumentacja powinna być środkiem zapewnienia zgodności z prawem, a nie celem; reforma musi skupiać się na wynikach. Zalecamy uzależnione od skali podejście ograniczające obowiązki dokumentacyjne administratorów danych do jednolitej polityki zapewnienia zgodności z rozporządzeniem przy uwzględnieniu ryzyka, przy czym zgodność ta powinna być wykazywana w przejrzysty sposób w przypadku zarówno przekazywania danych, jak i umów z podmiotami przetwarzającymi dane oraz zgłaszania naruszeń ochrony danych ([24]).

— Na podstawie wyraźnych kryteriów oceny ryzyka oraz doświadczeń w sprawowaniu nadzoru nad instytucjami UE zalecamy ograniczenie wymogu zgłaszania naruszenia ochrony danych organowi nadzoru oraz dokonywania oceny skutków w zakresie ochrony danych do przypadków, gdy zagrożone są prawa i wolności osób, których dane dotyczą ([25]).

— Należy aktywnie zachęcać przemysł do podejmowania inicjatyw – zarówno dotyczących wiążących reguł korporacyjnych, jak i pieczęci prywatności ([26]).

2.2. *Lepsza równowaga między interesem publicznym a ochroną danych osobowych*

— Zasady ochrony danych osobowych nie powinny utrudniać badań historycznych, statystycznych i naukowych, które rzeczywiście leżą w interesie publicznym. Odpowiedzialne podmioty muszą podjąć niezbędne kroki, aby zapobiec użyciu danych osobowych wbrew interesom osób fizycznych, zwracając szczególną uwagę na zasady odnoszące się np. do danych szczególnie chronionych dotyczących zdrowia ([27]).

— Badacze i archiwiści powinni mieć możliwość przechowywania danych tak długo, jak jest to potrzebne, z zastrzeżeniem tych zabezpieczeń ([28]).

2.3. *Zaufanie do organów nadzoru i przyznanie im uprawnień*

— Zalecamy umożliwienie organom nadzoru wydawanie wytycznych dla administratorów danych oraz opracowywanie własnych regulaminów wewnętrznych w duchu uproszczonego i łatwiejszego stosowania rozporządzenia przez pojedynczy organ nadzoru („kompleksowej obsługi") położony blisko obywatela („bliskość") ([29]).

— Organy powinny mieć możliwość nakładania skutecznych, proporcjonalnych i odstraszających sankcji naprawczych oraz administracyjnych z uwzględnieniem wszystkich istotnych okoliczności ([30]).

3. **Zasady, które pozostaną aktualne przez kilkadziesiąt lat**

Będąca głównym elementem obecnych ram prawnych dyrektywa 95/46/WE stała się wzorem dla późniejszego ustawodawstwa dotyczącego przetwarzania danych w UE i na całym świecie – oparto się na niej nawet, formułując prawo do ochrony danych osobowych określone w art. 8 Karty praw podstawowych Unii Europejskiej. Obecna reforma określi kształt przetwarzania danych dla pokolenia, które nie pamięta życia bez internetu. Dlatego też UE musi w pełni pojmować implikacje tego aktu prawnego dla osób fizycznych i zapewnić jego trwałość w obliczu rozwoju technologii.

W ostatnich latach proces wytwarzania, zbierania, analizy i wymiany danych osobowych gwałtownie przyspieszył wskutek innowacji technicznych, takich jak internet przedmiotów, przetwarzanie w chmurze, duże zbiory danych i otwarte dane, których wykorzystanie UE uznaje za niezbędny warunek swojej konkurencyjności ([31]). Okres obowiązywania dyrektywy 95/46/WE każe oczekiwać, że do kolejnej gruntownej rewizji zasad ochrony danych upłynie podobny czas, czyli może ona nastąpić dopiero pod koniec lat 30. XXI wieku. Na długo przedtem można się spodziewać, że technologie oparte na danych zbiegną się z wykorzystaniem sztucznej inteligencji, przetwarzania języka naturalnego oraz systemów biometrycznych, dając aplikacjom zdolność uczenia maszynowego prowadzącą do wykształcenia zaawansowanej inteligencji.

Technologie te stanowią wyzwanie dla zasad ochrony danych. Zorientowana na przyszłość reforma musi zatem przyjąć za podstawę godność jednostki i czerpać swoje założenia z etyki. Musi ona przywrócić równowagę między innowacjami w zakresie ochrony danych osobowych oraz ich wykorzystywania, zapewniając skuteczne zabezpieczenia w społeczeństwie cyfrowym, w którym żyjemy.

3.1. *Odpowiedzialne praktyki biznesowe i innowacyjna inżynieria*

— Reforma powinna odwrócić występującą ostatnio tendencję do potajemnego monitorowania oraz podejmowania decyzji w oparciu o profile ukryte przed osobą, której dotyczą. Problemem nie są ukierunkowane reklamy ani sama praktyka profilowania, lecz brak konkretnych informacji na temat logiki działania algorytmów tworzących te profile i mających wpływ na osobę, której dane dotyczą ([32]). Zalecamy zapewnienie pełniejszej przejrzystości działań administratorów danych.

— Zdecydowanie popieramy wprowadzenie zasad ochrony danych już w fazie projektowania oraz jako opcji domyślnej, co zapewni zastosowanie rynkowych rozwiązań w gospodarce cyfrowej. Zalecamy prostsze sformułowanie przepisów wymagających uwzględnienia praw i interesów osób fizycznych przy opracowywaniu produktów oraz w ustawieniach domyślnych ([33]).

3.2. *Uprawnienia osób fizycznych*

Przenoszenie danych w środowisku cyfrowym stanowi drogę do uzyskania kontroli przez użytkownika, której brakuje obecnie osobom fizycznym. Zalecamy umożliwienie bezpośredniego przekazywania danych przez jednego administratora innemu na wniosek osoby, której dane dotyczą, oraz przyznania osobom, których dane dotyczą, uprawnień do otrzymania kopii danych; dane te mogą one następnie samodzielnie przekazać innemu administratorowi ([34]).

3.3. *Zasady odporne na upływ czasu*

Zalecamy unikanie sformułowań i praktyk, które mogą stać się nieaktualne lub sporne ([35]).

4. **Niedokończone prace**

Przyjęcie przyszłościowego unijnego pakietu reformy ochrony danych będzie osiągnięciem imponującym, lecz mimo wszystko niepełnym.

Wszystkie instytucje zgadzają się, że zasady ogólnego rozporządzenia o ochronie danych powinny być stosowane w spójny sposób do instytucji UE. Opowiadamy się za pewnością prawa i jednolitością ram prawnych, przyjmując zarazem do wiadomości wyjątkowy charakter sektora publicznego w UE oraz potrzebę uniknięcia wszelkiego ograniczenia obecnego zakresu obowiązków (jak też konieczność zapewnienia podstaw prawnych i organizacyjnych dla działania EIOD). Dlatego też Komisja powinna jak najszybciej po zakończeniu negocjacji dotyczących ogólnego rozporządzenia o ochronie danych przedstawić spójny z tym rozporządzeniem wniosek dotyczący rewizji rozporządzenia nr 45/2001, tak aby obydwa akty mogły zacząć obowiązywać w tym samym czasie ([36]).

Po drugie, oczywiste jest, że zmiany będzie wymagać dyrektywa 2002/58/WE (dyrektywa o prywatności i łączności elektronicznej). Co znacznie ważniejsze, UE potrzebuje jednoznacznych ram dotyczących zapewnienia nieodłącznego elementu prawa do prywatności, czyli poufności komunikacji, w których uregulowane zostaną wszystkie usługi umożliwiające komunikację, a nie tylko działanie dostawców ogólnie dostępnych usług łączności elektronicznej. Trzeba je uregulować dającym pewność prawa harmonizującym rozporządzeniem, w którym zostaną zapisane co najmniej takie same standardy ochrony na mocy dyrektywy o prywatności i łączności elektronicznej przy zapewnieniu równych warunków działania.

W niniejszej opinii zaleca się zatem wezwanie do podjęcia w najkrótszym możliwym terminie zobowiązań dotyczących szybkiego przyjęcia wniosków w tych dwóch dziedzinach.

5. **Przełomowa chwila dla praw cyfrowych w Europie i poza nią**

Po raz pierwszy od kilkudziesięciu lat UE ma szansę zmodernizować i zharmonizować zasady postępowania z danymi osobowymi. Prywatność oraz ochrona danych nie kłócą się z rozwojem gospodarczym i handlem międzynarodowym ani też z opracowywaniem doskonałych usług i produktów – są one częścią ich jakości oraz wartości. Rada Europejska uznała, że zaufanie jest niezbędnym warunkiem powstawania innowacyjnych produktów i usług, które opierają się na przetwarzaniu danych osobowych.

W 1995 r. UE była pionierem w zakresie ochrony danych. Obecnie prawo o ochronie danych obowiązuje w ponad 100 krajach na całym świecie, z których mniej niż połowa leży w Europie ([37]). UE nadal przyciąga jednak szczególną uwagę tych krajów, które rozważają ustanowienie lub rewizję własnych ram prawnych. W czasach, gdy zaufanie obywateli do przedsiębiorstw oraz rządów zostało nadszarpnięte przez doniesienia o masowej inwigilacji i naruszeniach ochrony danych, oznacza to wielką odpowiedzialność spoczywającą na barkach unijnych ustawodawców, których tegoroczne decyzje wywrą zapewne wpływ oddziałujący poza Europę.

W opinii EIOD poszczególne wersje ogólnego rozporządzenia o ochronie danych zmierzają we właściwym kierunku, pozostają jednak wątpliwości, a niektóre z nich są bardzo poważne. Proces współdecyzji zawsze wiąże się z ryzykiem osłabienia pewnych przepisów przez negocjatorów poszukujących w dobrej wierze kompromisu politycznego. W przypadku reformy ochrony danych mamy jednak do czynienia z inną sytuacją – chodzi o prawa podstawowe i sposób ich zabezpieczenia przez najbliższych kilkadziesiąt lat.

W związku z tym, celem niniejszej opinii jest pomoc głównym instytucjom UE w rozwiązaniu problemów. Pragniemy nie tylko wzmocnienia praw poszczególnych osób, których dane dotyczą, oraz większej odpowiedzialności administratorów; chcemy ułatwić innowacje dzięki ramom prawnym neutralnym z punktu widzenia technologii, ale sprzyjającym korzyściom, jakie może ona przynieść społeczeństwu.

Na ostatnim etapie negocjacji mamy nadzieję, że nasze zalecenia pomogą UE ostatecznie wypracować reformę, która pozostanie przydatna przez następne lata i dziesięciolecia: nowy rozdział w zakresie ochrony danych czyniący UE przykładem dla całego świata.

Bruksela, dnia 27 lipca 2015 r.

Giovanni BUTTARELLI

Europejski Inspektor Ochrony Danych

([1]) Wspólna deklaracja Parlamentu Europejskiego, Rady i Komisji w sprawie praktycznych zasad dotyczących stosowania procedury współdecyzji (art. 251 Traktatu WE) (2007/C 145/02), Dz.U. C 145 z 30.6.2007.

([2]) COM(2012)11 final; Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych), P7_TA(2014)0212; Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) – Przygotowanie podejścia ogólnego, dokument Rady 9565/15 z 11.6.2015.

([3]) Pełny tytuł brzmi: Wniosek dotyczący dyrektywy w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych, COM(2012)10 final; Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych, P7_TA(2014)0219. W sprawie terminu i zakresu rozmów trójstronnych zob. konkluzje Rady Europejskiej z 25–26 czerwca 2015 r., EUCO 22/15; plan działania dotyczący rozmów trójstronnych wskazano podczas wspólnej konferencji prasowej Parlamentu, Rady i Komisji http://audiovisual.europarl.europa.eu/AssetDetail.aspx?id=690e8d8d-682d-4755-bfb6-a4c100eda4ed [ostatni dostęp 20.7.2015], ale nie opublikowano go oficjalnie. Ogólne rozporządzenie o ochronie danych wejdzie w życie 20 dni po jego opublikowaniu w Dzienniku Urzędowym i oczekuje się, że zacznie w pełni obowiązywać dwa lata po wejściu w życie (art. 91).

([4]) Ogłoszenie o wakacie na stanowisku Europejskiego Inspektora Ochrony Danych COM/2014/10354 (2014/C 163 A/02), Dz.U. C 163 A/6 z 28.5.2014. W strategii EIOD na lata 2015–2019 znalazła się zapowiedź „poszukiwania praktycznych rozwiązań, które unikają biurokracji, stanowią elastyczne podejście do innowacji technicznych i transgranicznych przepływów danych oraz umożliwiają osobom fizycznym skuteczniejsze egzekwowanie swoich praw w internecie oraz poza nim"; Dawanie przykładu: strategia EIOD na lata 2015–2019, marzec 2015 r.

([5]) Opinia EIOD z dnia 7 marca 2015 r. w sprawie pakietu dotyczącego reform w zakresie ochrony danych.

([6]) Zob. załącznik do listu Grupy Roboczej Art. 29 do komisarz ds. sprawiedliwości, konsumentów i równouprawnienia płci Věry Jourovej z 17.6.2015.

([7]) Trudno jest zwięźle podsumować zakres materialny i terytorialny ogólnego rozporządzenia o ochronie danych. Instytucje wydają się przynajmniej zgodne co do tego, że zakres ten obejmuje organizacje mające siedzibę w UE, które są odpowiedzialne za przetwarzanie danych osobowych zarówno w UE, jak i poza nią, oraz organizacje mające siedzibę poza UE, które przetwarzają dane osobowe osób fizycznych w UE w związku z oferowaniem towarów lub usług osobom fizycznym w UE bądź monitorowaniem tych osób (zob. określenie zakresu materialnego w art. 2 i zakresu terytorialnego w art. 3).

([8]) Inne wyniki wskazują, że siedmiu na dziesięciu respondentów jest zaniepokojonych możliwością wykorzystania ich informacji w celu innym niż ten, dla którego je zebrano, jeden na siedmiu uważa, że w każdym przypadku przed gromadzeniem i przetwarzaniem danych powinna być wymagana wyraźna zgoda, a dwie trzecie uznaje za ważną kwestię możliwość przeniesienia danych osobowych od starego do nowego usługodawcy; specjalny Eurobarometr 431 w sprawie ochrony danych z czerwca 2015 r. Porównywalne wyniki uzyskano w badaniu Pew Research z 2014 r.: 91 % Amerykanów uważa, że stracili kontrolę nad tym, w jaki sposób firmy zbierają i wykorzystują informacje osobiste, 80 % użytkowników serwisów społecznościowych jest zaniepokojonych możliwością dostępu do ich danych podmiotów zewnętrznych, takich jak reklamodawcy lub firmy, a 64 % twierdzi, że rząd powinien podjąć dodatkowe działania w celu uregulowania branży reklamowej; badanie panelowe Pew Research dotyczące prywatności ze stycznia 2014 r.

([9]) Komisja proponuje kompleksową reformę zasad ochrony danych, aby zwiększyć kontrolę użytkowników nad swoimi danymi oraz obniżyć koszty dla przedsiębiorstw.

([10]) List organizacji pozarządowych do przewodniczącego Junckera z 21.4.2015 r. https://edri.org/files/DP_letter_Juncker_20150421.pdf oraz odpowiedź szefa gabinetu wiceprzewodniczącego Timmermansa z 17.7.2015 r. https://edri.org/files/eudatap/Re_EC_EDRi-GDPR.pdf [dostęp 23.7.2015]. EIOD spotkał się z przedstawicielami kilku spośród tych organizacji pozarządowych, aby omówić ich obawy w maju 2015 r.; KOMUNIKAT PRASOWY EDPS/2015/04 z 1.6.2015 r., Reforma ochrony danych w UE: EIOD spotyka się z międzynarodowymi grupami ds. swobód obywatelskich; nagranie całej rozmowy jest dostępne na stronie internetowej EIOD (https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Pressnews/Videos/GDPR_civil_soc).

([11]) Artykuł 2 ust. 2 lit. e).

([12]) Artykuł 1.

([13]) W art. 8 karty stwierdza się [podkreślenie dodano]:

„1. Każdy ma prawo do ochrony danych osobowych, które go dotyczą.

2. Dane te muszą być ***przetwarzane rzetelnie*** *w* ***określonych celach*** *i* ***za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą****. Każdy ma prawo dostępu do zebranych danych, które go dotyczą, i* ***prawo do dokonania ich sprostowania****.*

3. Przestrzeganie tych zasad podlega ***kontroli niezależnego organu****.*"

([14]) Artykuł 10. Do chwili powstania jasnej i prawnie wiążącej definicji „danych spseudonimizowanych" w odróżnieniu od „danych osobowych", ten rodzaj danych musi podlegać zasadom ochrony danych.

([15]) Artykuł 6 ust. 2 i art. 6 ust. 4. Ze względu na fakt, że występują pewne wątpliwości co do znaczenia pojęcia „zgodności", zalecamy – zgodnie z opinią Grupy Roboczej Art. 29 w sprawie celowości – zastosowanie ogólnych kryteriów oceny, czy przetwarzanie danych jest zgodne z celem (zob. art. 5 ust. 2).

([16]) Jednym ze sposobów zapewnienia zgodnego z prawem przetwarzania w przypadku braku zgody jest skuteczny rozdział funkcjonalny, ale uzasadnionego interesu nie należy interpretować zbyt szeroko. Właściwą alternatywą w niektórych sytuacjach może także być bezwarunkowe prawo do odmowy. Ocena, czy zgoda jest dobrowolna, zależy częściowo (a) od tego, czy istnieje znacząca nierównowaga między osobą, której dane dotyczą, a administratorem danych; oraz (b) w przypadku przetwarzania na mocy art. 6 ust. 1 lit. b) od tego, czy wykonanie umowy lub świadczenie usługi jest uzależnione od zgody na przetwarzanie danych, które nie są niezbędne do tych celów (zob. art. 7 ust. 4). Odzwierciedla to brzmienie przepisu zawartego w prawie konsumenckim UE; na mocy art. 3 ust. 1 dyrektywy 93/13/EWG z dnia 5 kwietnia 1993 r. w sprawie nieuczciwych warunków w umowach konsumenckich: „Warunki umowy, które nie były indywidualnie negocjowane, mogą być uznane za nieuczciwe, jeśli stoją w sprzeczności z wymogami dobrej wiary, powodują znaczącą nierównowagę wynikających z umowy, praw i obowiązków stron ze szkodą dla konsumenta".

([17]) Wśród takich reguł należy wymienić decyzje w sprawie odpowiedniej ochrony danych osobowych w określonych sektorach i na określonych terytoriach, okresowe przeglądy takich decyzji oraz wiążące reguły korporacyjne. Zob. art. 40–45.

([18]) Artykuł 73.

([19]) Artykuł 76. Jeżeli chodzi o trudności w dochodzeniu roszczeń związanych z naruszeniami przepisów o ochronie danych, zob. raport Agencji Praw Podstawowych Unii Europejskiej o dostępie do środków prawnych w zakresie ochrony danych osobowych w państwach członkowskich UE z 2013 r.

([20]) W przepisach UE nacisk kładzie się na samoocenę przedsiębiorstw w zakresie zgodności ich działań z art. 101 zakazującym porozumień antykonkurencyjnych, a na podmiotach zajmujących pozycję dominującą na rynku spoczywa „szczególna odpowiedzialność" za unikanie wszelkich działań, które mogłyby ograniczyć skuteczną konkurencję (pkt 9 wytycznych Komisji 2009/C 45/02); zob. wstępną opinię EIOD w sprawie prywatności i konkurencyjności w erze dużych zbiorów danych z 14.3.2014 r.

([21]) We wszystkich trzech wersjach rozporządzenia znajdują się odniesienia do „zrozumiałego sposobu i zrozumiałej formy, jasnego i prostego języka" (motyw 57 PE; art. 19 Komisji i Rady), „jasności i jednoznaczności" (motyw 99 PE; art. 10a PE) oraz dostarczenia „jasnych i łatwo zrozumiałych informacji" (art. 10 PE, art. 11 PE), jak też informacji, które są „zwięzłe, przejrzyste, jasne i łatwo dostępne" (motyw 25 PE, Komisji i Rady; art. 11 PE).

([22]) Z wersji Parlamentu i Rady w dużej mierze usunięto przepisy dotyczące aktów delegowanych. Naszym zdaniem UE mogłaby pójść jeszcze dalej i pozostawić te zagadnienia techniczne niezależnym organom dysponującym wiedzą specjalistyczną.

([23]) Wersja uwzględniająca nasze zalecenia miałaby około 20 000 słów, podczas gdy średnia długość wersji trzech instytucji wynosi około 28 000 słów.

([24]) Artykuł 22.

([25]) Artykuły 31 i 33.

([26]) Artykuł 39.

([27]) Artykuł 83. Badania naukowe i archiwizacja nie stanowią same w sobie podstawy prawnej przetwarzania, dlatego zalecamy skreślenie art. 6 ust. 2.

([28]) Artykuł 83a.

([29]) Grupa Robocza Art. 29 nakreśliła wizję zarządzania, mechanizmu zgodności i kompleksowej obsługi opartą na zaufaniu do niezależnych organów ochrony danych, która obejmuje trzy warstwy:

— poszczególne organy ochrony danych wyposażone w szerokie uprawnienia i zasoby umożliwiające im prowadzenie postępowań w sprawach należących do ich kompetencji,

— skuteczną współpracę między organami ochrony danych z jasnym wskazaniem organu głównego w przypadkach transgranicznych,

— Europejską Radę Ochrony Danych, która musi być autonomiczna, posiadać własną osobowość prawną i dysponować wystarczającymi środkami, a jej członkami muszą być równoprawne organy ochrony danych działające w duchu solidarności, z uprawnieniami do podejmowania wiążących decyzji i wspierane przez podlegający przewodniczącemu Rady sekretariat zapewniający jej obsługę.

([30]) Zalecamy również doprecyzowanie kompetencji organów nadzoru oraz wyznaczenie organu głównego w przypadkach przetwarzania międzynarodowego przy jednoczesnym zachowaniu zdolności organów nadzoru do zajmowania się przypadkami ściśle lokalnymi. Zalecamy wprowadzenie uproszczonej wersji mechanizmu zgodności zapewniającej większą jasność co do sposobu identyfikacji przypadków, w których organy nadzoru muszą skonsultować się z Europejską Radą Ochrony Danych i w których Rada musi wydać wiążącą decyzję w celu zapewnienia spójnego stosowania rozporządzenia.

([31]) Komunikat Komisji w sprawie strategii jednolitego rynku cyfrowego dla Europy, COM(2015)192 final; konkluzje Rady Europejskiej z czerwca 2015 r., EUCO 22/15; konkluzje Rady na temat cyfrowej transformacji europejskiego przemysłu, 8993/15.

([32]) Artykuł 14 lit. h).

([33]) Artykuł 23.

([34]) Artykuł 18. Wskazujemy ponadto, że aby było ono skuteczne, prawo do przenoszenia danych musi mieć zastosowanie w szerokim zakresie, nie zaś tylko do operacji przetwarzania danych wykorzystujących dane dostarczone przez osobę, której one dotyczą.

([35]) Zalecamy na przykład pominięcie takich terminów, jak „w internecie", „w formie pisemnej" i „społeczeństwo informacyjne".

([36]) Preferowaną przez nas opcją byłoby dokonanie tego przepisem zawartym w ogólnym rozporządzeniu o ochronie danych.

([37]) Greenleaf, Graham, Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority (30 stycznia 2015 r.); (2015) 133 Privacy Laws & Business International Report, luty 2015; UNSW Law Research Paper No. 2015–21.