

**Opinia Europejskiego Komitetu Ekonomiczno-Społecznego „Wymiana i ochrona danych osobowych w zglobalizowanym świecie”**

[COM(2017) 7 final]

(2018/C 081/29)

Sprawozdawca: **Cristian PÎRVULESCU**

Wniosek o konsultację	Komisja Europejska, 31.5.2017
Podstawa prawna	Art. 304 Traktatu o funkcjonowaniu Unii Europejskiej
Decyzja Zgromadzenia Plenarnego	8.5.2017
Sekcja odpowiedzialna	Sekcja Stosunków Zewnętrznych
Data przyjęcia przez sekcję	28.9.2017
Data przyjęcia na sesji plenarnej	18.10.2017
Sesja plenarna nr	529
Wynik głosowania	175/1/3
(za/przeciw/wstrzymało się)	

## 1. Wnioski i zalecenia

1.1. Zgodnie ze swymi podstawowymi wartościami i dokumentami konstytucyjnymi UE ma obowiązek stać się globalnym podmiotem promującym poszanowanie praw podstawowych i odpowiednią ochronę życia prywatnego i danych osobowych. EKES zachęca zatem Komisję Europejską do proaktywnego propagowania najwyższych standardów ochrony danych osobowych na szczeblu dwustronnym i wielostronnym.

1.2. Komitet jest zdania, że cztery główne kryteria, które Komisja ma uwzględniać przy ocenianiu, z którymi państwami należy prowadzić dialog w kwestii odpowiedniości ochrony, są wyważone i rozsądne. Jednak ważne jest, by interpretować je w świetle rzeczywistego zaangażowania rządów, parlamentów i sądów w tych krajach, by osiągnąć równoważny i funkcjonalny poziom ochrony danych osobowych.

1.3. EKES wzywa do większej przejrzystości i uczestnictwa w procesie wydawania decyzji w sprawie odpowiedniej ochrony danych osobowych. Należy zaangażować w to przedstawicieli sektora biznesu, zwłaszcza MŚP, organizacje ochrony konsumentów, grupy obywatelskie oraz inne organizacje społeczeństwa obywatelskiego i konsultować się z nimi. Komitet gotów jest ułatwić ten proces konsultacji.

1.4. EKES przyjmuje z zadowoleniem rozpoczęty przez Komisję dialog z kluczowymi partnerami handlowymi w Azji Wschodniej i Południowo-Wschodniej, w tym z Japonią i Koreą, a być może także z Indiami, jak również z krajami Ameryki Łacińskiej i państwami objętymi europejską polityką sąsiedztwa, które wyraziły zainteresowanie uzyskaniem „stwierdzenia odpowiedniej ochrony danych”.

1.5. Komitet ma nadzieję, że Komisja, Rada, rządy krajowe i parlamenty państw członkowskich oraz rząd i Kongres USA z zadowoleniem przyjmą propozycje przedstawione w rezolucji Parlamentu Europejskiego z 6 kwietnia 2017 r. w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE–USA. Parlament Europejski wyraził w rezolucji poważne obawy i wielokrotnie wskazał, że zawarte porozumienie oraz obowiązujące w USA ramy prawne w praktyce nie chronią praw obywateli UE.

1.6. Istnieje potrzeba ścisłego nadzoru i monitorowania ze względu na szybki postęp technologiczny i ciągłą rozbudowę infrastruktury ICT. Mimo iż decyzje w sprawie odpowiedniej ochrony danych osobowych są oceniane co cztery lata (zob. art. 45 ust. 3 ogólnego rozporządzenia o ochronie danych), EKES zaleca, by Komisja, organy ochrony danych oraz organy

rządowe państw trzecich były ze sobą w stałym kontakcie w celu identyfikowania nowych wyzwań w tym bardzo dynamicznym środowisku technologicznym i gospodarczym.

1.7. EKES jest zdania, że priorytetem Komisji Europejskiej powinno być promowanie standardów ochrony danych za pośrednictwem instrumentów wielostronnych. Zobowiązanie to powinno być wsparte odpowiednimi środkami, aby zapewnić *a priori* rzeczywistą ochronę praw człowieka oraz dysponować *a posteriori* skutecznym środkiem ochrony prawnej w wypadku szkód.

1.8. Komitet zwraca uwagę na fakt, że Komisja nie rozróżnia w komunikacie różnych rodzajów i zastosowań danych osobowych – z wyjątkiem tych odnoszących się do spraw karnych.

1.9. Konwencja Rady Europy nr 108 z 1981 r. wraz z protokołem dodatkowym do niej z 1999 r., jest jedynym wiążącym narzędziem wielostronnym w dziedzinie ochrony danych. Należy go jeszcze bardziej rozwinąć i zachęcić więcej krajów trzecich do przyłączenia się do niego.

1.10. Istnieje potrzeba zintensyfikowania wielostronnych wysiłków w ramach OECD (Organizacji Współpracy Gospodarczej i Rozwoju), G20 i Współpracy Gospodarczej Azji i Pacyfiku (APEC), z myślą o stworzeniu prawdziwie globalnego wielostronnego systemu ochrony danych. Współpraca ze specjalnym sprawozdawcą ONZ ds. prawa do prywatności powinna mieć solidny i funkcjonalny charakter.

1.11. Jeśli chodzi o wymianę danych osobowych w ramach zapobiegania, dochodzenia i ścigania przestępstw kryminalnych, EKES zdecydowanie popiera tworzenie solidnych zabezpieczeń w zakresie ochrony danych, ale jest także otwarty na możliwość wprowadzenia mechanizmu stwierdzenia odpowiedniej ochrony danych w sektorze egzekwowania przepisów prawa karnego. Ochrona danych oraz zapobieganie, dochodzenie i ściganie przestępstw kryminalnych, w tym cyberprzestępczości i terroryzmu, muszą iść ze sobą w parze.

1.12. EKES przypomina o znaczeniu ochrony danych osobowych oraz danych dotyczących zdrowia i rehabilitacji osób niepełnosprawnych, zgodnie z art. 22 Konwencji ONZ o prawach osób niepełnosprawnych.

## 2. Kontekst/Wprowadzenie

2.1. Ochrona danych osobowych stanowi część wspólnej konstrukcji konstytucyjnej Europy, czego potwierdzenie znaleźć można w art. 8 Karty praw podstawowych Unii Europejskiej. Od ponad 20 lat pełni ona kluczową rolę w prawie Unii – począwszy od dyrektywy o ochronie danych z 1995 r. („dyrektywa z 1995 r.”) aż po przyjęcie ogólnego rozporządzenia o ochronie danych oraz dyrektywy w sprawie policji w 2016 r.

2.2. Reforma unijnych przepisów o ochronie danych przyjęta w kwietniu 2016 r. ustanawia system, który zapewnia wysoki stopień ochrony zarówno wewnątrz UE, jak i w ramach międzynarodowej wymiany danych osobowych do celów egzekwowania prawa oraz do celów handlowych. Nowe przepisy wejdą w życie w maju 2018 r.

2.3. Po zakończeniu prac nad unijnymi regulacjami dotyczącymi ochrony danych Komisja przedstawia obecnie strategię promującą międzynarodowe standardy ochrony danych. W komunikacie określono różne narzędzia służące wymianie danych osobowych na skalę międzynarodową opracowane na podstawie zreformowanych przepisów w zakresie ochrony danych, jak również strategię przyszłej współpracy z wybranymi państwami trzecimi w celu podjęcia decyzji w sprawie odpowiedniej ochrony danych osobowych i promowania standardów ochrony danych osobowych poprzez wykorzystanie wielostronnych narzędzi.

2.4. Ogólne rozporządzenie o ochronie danych z 2016 r. oferuje „zestaw narzędzi” będących mechanizmami przekazywania danych osobowych z UE do państw trzecich – mowa tu o decyzjach w sprawie odpowiedniej ochrony danych osobowych, standardowych klauzulach umownych, wiążących regułach korporacyjnych, mechanizmach certyfikacji i kodeksach postępowania. Głównym celem tego mechanizmu jest zapewnienie, aby przy przekazywaniu danych osobowych Europejczyków utrzymać wysoki stopień ich ochrony. Chociaż konstrukcja międzynarodowego transferu danych osobowych jest podobna do tej z dyrektywy o ochronie danych z 1995 r., reforma upraszcza i rozszerza jego stosowanie oraz wprowadza nowe narzędzia służące do międzynarodowego przekazywania danych (np. kodeksy postępowania i mechanizmy certyfikacji).

### 3. Uwagi ogólne

3.1. EKES pochwała wysiłki UE mające na celu ochronę danych osobowych swych obywateli, przy jednoczesnym dążeniu do otwartości i zintegrowania w coraz bardziej współzależnym świecie.

3.2. Zgodnie ze swymi podstawowymi wartościami i dokumentami konstytutywnymi UE ma obowiązek stać się globalnym podmiotem promującym poszanowanie praw podstawowych i wysoką ochronę życia prywatnego i danych osobowych. W związku z tym EKES zachęca Komisję Europejską do proaktywnego propagowania na szczeblu dwustronnym i wielostronnym najwyższych standardów ochrony danych osobowych dla obywateli unijnych oraz z państw trzecich.

3.3. UE powinna wspierać globalną agendę na rzecz ochrony danych osobowych oraz jej główne zasady: ochrona danych jest prawem podstawowym, zapewnianym poprzez przyjęcie nadrzędnych przepisów w tej dziedzinie, wprowadzanie możliwego do wyegzekwowania prawa do prywatności oraz ustanowienie niezależnego organu nadzorczego.

3.4. Zapewnienie możliwie najwyższego poziomu ochrony danych osobowych jest nie tylko obowiązkiem prawnym, lecz również wielką szansą. Zaufanie obywateli do obowiązujących zabezpieczeń instytucjonalnych i regulacyjnych jest korzystne dla gospodarki cyfrowej, międzynarodowego przepływu towarów i usług oraz administracji elektronicznej. Zarówno ochrona danych, jak i sprawiedliwy handel międzynarodowy są bardzo istotne dla obywateli i nie powinny być postrzegane jako wzajemnie sprzeczne wartości.

3.5. EKES nadal popiera ogólny kierunek polityki UE w zakresie ochrony danych, tak jak to czynił w poprzednich opiniach, ale podkreśla konieczność zapewnienia wyższych poziomów ochrony. W opinii SOC/455 w sprawie ogólnego rozporządzenia o ochronie danych Komitet podał konkretne przykłady dotyczące wielu artykułów w celu lepszego zdefiniowania praw i określenia, na czym polega wzmocnienie ochrony obywateli ogólnie i pracowników w szczególności, a także w celu lepszego zdefiniowania charakteru zgody i zgodności z prawem przetwarzania danych, oraz w szczególności w celu określenia obowiązków inspektorów ochrony danych i przetwarzania danych w kontekście zatrudnienia <sup>(1)</sup>.

3.6. Ponadto EKES podkreślił prawo osób fizycznych lub prawnych do wyrażenia zgody w odniesieniu do przetwarzania swoich danych. W opinii TEN/631 o ochronie danych osobowych EKES stwierdził, że „użytkownicy powinni być poinformowani, wyedukowani i zachować ostrożność, gdyż po wyrażeniu przez nich zgody dostawca będzie mógł w większym stopniu przetwarzać treści i metadane w celu maksymalizacji korzyści i możliwości działania [...]. Edukacja użytkowników do korzystania z ich praw, a także kwestie anonimizacji lub szyfrowania powinny być priorytetami w tym rozporządzeniu” [rozporządzenie w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej] <sup>(2)</sup>.

3.7. EKES popiera utworzenie, począwszy od maja 2018 r., jednego ogólnoeuropejskiego zbioru przepisów, który zastąpi obecne 28 ustawodawstw krajowych. Zgodnie z nowo utworzonym mechanizmem kompleksowej obsługi jeden organ ochrony danych („OOD”) będzie odpowiedzialny za nadzór nad transgranicznymi operacjami przetwarzania danych przeprowadzanymi przez przedsiębiorstwa w UE. Zagwarantowana będzie spójność interpretacji nowych przepisów. Zwłaszcza w przypadku spraw transgranicznych, w które zaangażowanych może być kilka krajowych organów ochrony danych, podejmowana będzie jedna wspólna decyzja gwarantująca wspólne rozwiązanie wspólnych problemów. EKES ma nadzieję, że nowe procedury nie tylko zagwarantują spójność interpretacji, lecz również możliwie najwyższy poziom ochrony danych.

3.8. EKES odnotowuje, że komunikat i przedstawione w nim najważniejsze wnioski zostały przyjęte z zadowoleniem przez Digital Europe, organizację reprezentującą przemysł technologii cyfrowej w Europie <sup>(3)</sup>.

<sup>(1)</sup> Opinia EKES-u w sprawie ogólnego rozporządzenia o ochronie danych, 23 maja 2012 r. Dz.U. C 229 z 31.7.2012, s. 90.

<sup>(2)</sup> Opinia EKES-u w sprawie ochrony danych osobowych, 5 lipca 2017 r. Dz.U. C 345 z 13.10.2017, s. 138.

<sup>(3)</sup> Pismo do Komisji Europejskiej w sprawie niedawno opublikowanego komunikatu dotyczącego międzynarodowego przekazywania danych, DIGITALEUROPE, 12 maja 2017 r., data dostępu: 1 sierpnia: <http://www.digitaleurope.org/Press-Room/Latest-News/News-Story/newsID/623>.

Coraz większe rozpowszechnienie przetwarzania w chmurze stwarza nowe i złożone wyzwania, które będą się nieuchronnie zmieniać ze względu na szybkie tempo przekształceń technologicznych. Prawodawstwo musi być elastyczne, by można je było dostosować do postępu technologicznego i zmian rynkowych.

#### 4. Uwagi szczegółowe

4.1. Podejmowane przez Komisję decyzje w sprawie odpowiedniej ochrony danych osobowych są obecnie właściwym narzędziem do zapewnienia ochrony danych obywateli UE w odniesieniu do innych krajów i podmiotów, zarówno rządowych, jak i prywatnych. Są również przydatnym instrumentem, jeśli chodzi o zachęcanie krajów spoza UE, by dążyły do osiągnięcia podobnego poziomu ochrony dla swoich obywateli i powinny być preferowanym narzędziem ochrony wymiany danych osobowych.

4.2. EKES uważa, że cztery główne kryteria<sup>(4)</sup>, które Komisja ma uwzględniać przy ocenianiu, z którymi państwami należy prowadzić dialog w kwestii odpowiedniości ochrony, są wyważone i rozsądne. Jednak ważne jest, aby interpretować je w świetle rzeczywistego zaangażowania rządów, parlamentów i sądów w tych krajach, by osiągnąć równoważny i funkcjonalny poziom ochrony danych osobowych.

4.3. EKES wzywa do większej przejrzystości i uczestnictwa w procesie wydawania decyzji w sprawie odpowiedniej ochrony danych osobowych. Należy zaangażować w to przedstawicieli sektora biznesu, zwłaszcza MŚP, organizacje ochrony konsumentów, grupy obywatelskie oraz inne organizacje społeczeństwa obywatelskiego i konsultować się z nimi. Komitet gotów jest ułatwić ten proces konsultacji.

4.4. EKES przyjmuje z zadowoleniem rozpoczęty przez Komisję dialog z kluczowymi partnerami handlowymi w Azji Wschodniej i Południowo-Wschodniej, w tym z Japonią i Koreą, a może także z Indiami, jak również z krajami Ameryki Łacińskiej i państwami objętymi europejską polityką sąsiedztwa, które wyraziły zainteresowanie uzyskaniem „stwierdzenia odpowiedniej ochrony danych”.

4.5. EKES uważa, że wprowadzenie statusu częściowej odpowiedniości ochrony danych dla pewnych krajów, w tym dla niektórych obszarów i sektorów, jest problematyczne, ponieważ nie zapewnia wystarczających i spójnych gwarancji konstytucyjnych, proceduralnych i instytucjonalnych w zakresie ochrony danych osobowych. Częściowa odpowiedniość ochrony danych mogłaby stanowić użyteczny etap pośredni, w ramach którego UE i dane kraje mogłyby znaleźć wspólną płaszczyznę porozumienia i koordynować działania. Celem długoterminowym jest osiągnięcie bardziej solidnego i kompleksowego porozumienia na podstawie istniejących ram we wszystkich zainteresowanych krajach<sup>(5)</sup>.

4.6. EKES z zadowoleniem przyjmuje wysiłki na rzecz stworzenia solidnych i funkcjonalnych ram dwustronnych ze Stanami Zjednoczonymi Ameryki. Niedawno przyjęta decyzja w sprawie Tarczy Prywatności UE-USA, która zastępuje ramy prawne „bezpieczna przystań”, jest krokiem we właściwym kierunku. Jednak jej zakres jest ograniczony, gdyż przystąpienie do Tarczy jest dobrowolne, co sprawia, że wiele amerykańskich organizacji pozostaje poza jej zasięgiem.

4.7. Komitet ma nadzieję, że Komisja, Rada, rządy krajowe i parlamenty państw członkowskich oraz rząd i Kongres USA z zadowoleniem przyjmą propozycje przedstawione w rezolucji Parlamentu Europejskiego z 6 kwietnia 2017 r. w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE-USA. Parlament Europejski wyraził w rezolucji poważne obawy i wielokrotnie wskazał, że zawarte porozumienie oraz obowiązujące w USA ramy prawne w praktyce nie chronią praw obywateli UE<sup>(6)</sup>.

<sup>(4)</sup> Najważniejszymi kryteriami są: 1. Zakres (faktycznych lub potencjalnych) stosunków handlowych z danym państwem trzecim, w tym istnienie umowy o wolnym handlu lub trwające negocjacje w tej sprawie; 2. Zakres przepływu danych osobowych z UE, odzwierciedlający powiązania geograficzne lub kulturowe; 3. Wiodąca rola państwa trzeciego w dziedzinie stanowienia przepisów w zakresie ochrony prywatności i danych, a tym samym stanowienie przykładu dla innych państw w regionie; 4. Ogólne stosunki polityczne z danym państwem trzecim, w szczególności w odniesieniu do propagowania wspólnych wartości i wspólnych celów na poziomie międzynarodowym.

<sup>(5)</sup> Komisja zachęca Stany Zjednoczone do kontynuowania starań w kierunku stworzenia kompleksowego systemu ochrony prywatności i danych, dzięki czemu można będzie osiągnąć zbieżność między obydwo systemami w dłuższej perspektywie. Zob. komunikat Komisji do Parlamentu Europejskiego i Rady „Transatlantyckie przepływy danych: odbudowa zaufania dzięki ustanowieniu silniejszych gwarancji”, COM(2016) 117 final, 29 lutego 2016 r.

<sup>(6)</sup> Rezolucja Parlamentu Europejskiego z 6 kwietnia 2017 r. w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności: PE „ubolewa nad faktem, że ani zasady Tarczy Prywatności, ani wyjaśnienia i zapewnienia w pismach administracji USA nie dowodzą istnienia skutecznych mechanizmów ochrony prawnej dla obywateli UE, których dane osobowe przekazywane są do organizacji amerykańskiej w oparciu o zasady Tarczy Prywatności, a następnie do których mają dostęp amerykańskie organy publiczne w celu ich przetwarzania na potrzeby egzekwowania prawa oraz w interesie publicznym, co podkreślił Trybunał Sprawiedliwości Unii Europejskiej w wyroku z dnia 6 października 2015 r. jako istotę prawa podstawowego, o którym mowa w art. 47 Karty”, pkt 26.

4.8. Podobne obawy wyraziło szereg organizacji społeczeństwa obywatelskiego z Unii Europejskiej i Stanów Zjednoczonych<sup>(7)</sup>. EKES zachęca wszystkie instytucje UE do uwzględnienia tych obaw.

4.9. Komitet odnotowuje dążenie Komisji do zbudowania nowej dynamiki, ale zauważa, że jej propozycje utrzymują niepewność prawa w przypadku osób, których prawa zostały naruszone. Istnieje szereg aspektów przyczyniających się do tego:

- nie uściślono charakteru przetwarzanych danych: danych osobowych, metadanych i własności intelektualnej,
- rodzaje zastosowań: jakiego rodzaju dane osobowe można przetwarzać w celach komercyjnych lub w celu egzekwowania prawa?
- charakter zaangażowanych podmiotów: jaką rolę powinny tu odgrywać przedsiębiorstwa prywatne, organy państwa i sądy?
- niejasny jest status prawny i odpowiedzialność przedsiębiorstw mających do czynienia z danymi osobowymi. Kary i odszkodowania za poniesione szkody: jaką rolę powinny tu odgrywać sądy krajowe w państwach członkowskich UE lub inne sądy, w tym w krajach trzecich?

4.10. Po przyjęciu decyzji w sprawie odpowiedniej ochrony danych osobowych bardzo istotne jest dalsze monitorowanie, by zapewnić funkcjonowanie tych umów w praktyce. Istnieje potrzeba ścisłego nadzoru i monitorowania ze względu na szybki postęp technologiczny i ciągłą rozbudowę infrastruktury ICT. Mimo że decyzje w sprawie odpowiedniej ochrony danych osobowych są oceniane co cztery lata (zob. art. 45 ust. 3 ogólnego rozporządzenia o ochronie danych), EKES zaleca, by Komisja, organy ochrony danych oraz organy rządowe państw trzecich były ze sobą w stałym kontakcie w celu identyfikowania nowych wyzwań w tym bardzo dynamicznym środowisku technologicznym i gospodarczym.

4.11. EKES zachęca Komisję do współpracy z zainteresowanymi stronami w celu opracowania alternatywnych mechanizmów przekazywania danych dostosowanych do szczególnych potrzeb lub sytuacji poszczególnych branż, modeli biznesowych lub podmiotów gospodarczych.

4.12. EKES jest zdania, że priorytetem Komisji Europejskiej powinno być promowanie standardów ochrony danych za pośrednictwem instrumentów wielostronnych i że należy wesprzeć to zobowiązanie odpowiednimi środkami.

4.13. Konwencja Rady Europy nr 108 z 1981 r. wraz z protokołem dodatkowym do niej z 1999 r. jest jedynym wiążącym narzędziem wielostronnym w dziedzinie ochrony danych. Należy je jeszcze bardziej rozwinąć i zachęcić więcej krajów trzecich do przyłączenia się do niego.

4.14. Istnieje potrzeba zintensyfikowania wielostronnych wysiłków w ramach OECD, G20 i APEC, z myślą o stworzeniu prawdziwie globalnego wielostronnego systemu ochrony danych. Współpraca ze specjalnym sprawozdawcą ONZ ds. prawa do prywatności powinna mieć solidny i funkcjonalny charakter.

4.15. Priorytetem powinno być zacieśnienie współpracy z właściwymi organami ds. egzekwowania prywatności i organami nadzorczymi w państwach trzecich. Mimo że ustanowiona przez OECD Światowa Sieć na rzecz Prywatności (ang. Global Privacy Enforcement Network, GPEN) nie tworzy prawnie wiążących zobowiązań, to może sprzyjać współpracy w zakresie egzekwowania prawa poprzez dzielenie się najlepszymi praktykami, jeśli chodzi o stawianie czoła wyzwaniom transgranicznym i wspieranie wspólnych inicjatyw w zakresie egzekwowania prawa i kampanii na rzecz podnoszenia świadomości społecznej<sup>(8)</sup>.

4.16. Jeśli chodzi o wymianę danych osobowych w ramach zapobiegania, dochodzenia i ścigania przestępstw kryminalnych, EKES zdecydowanie popiera tworzenie solidnych zabezpieczeń w zakresie ochrony danych, ale jest także otwarty na możliwość wprowadzenia mechanizmu stwierdzenia odpowiedniej ochrony danych w sektorze egzekwowania przepisów prawa karnego. Ochrona danych oraz zapobieganie, dochodzenie i ściganie przestępstw kryminalnych, w tym cyberprzestępczości i terroryzmu, muszą iść ze sobą w parze.

<sup>(7)</sup> Koalicja Organizacji na rzecz Swobód Obywatelskich wzywa unijnych prawodawców do przeprowadzenia reformy nadzoru, by zapewnić ramy poszanowania praw osobom spoza USA, 28 lutego 2017 r., data dostępu: 1 sierpnia: <https://www.accessnow.org/cms/assets/uploads/2017/02/Section702CoalitionLetter1.pdf>.

<sup>(8)</sup> Zob. także ramy OECD w sprawie ochrony prywatności, OECD, 2013 r.

4.17. Zawarta w grudniu 2016 r. umowa ramowa między UE a USA o ochronie danych jest dobrym przykładem uwzględnienia w umowach dwustronnych praw i zobowiązań w zakresie ochrony danych zgodnych z dorobkiem prawnym UE. Te same procedury mogą być również stosowane w różnych obszarach polityki, np. w polityce konkurencji lub ochrony konsumentów. EKES zachęca Komisję do zbadania możliwości zawierania podobnych umów ramowych ze swoimi ważnymi partnerami w dziedzinie egzekwowania prawa.

4.18. Komitet z niecierpliwością oczekuje na wyniki pierwszego corocznego przeglądu funkcjonowania Tarczy Prywatności UE-USA i ma nadzieję, że proces ten będzie miał gruntowny i partycypacyjny charakter. EKES liczy też na to, że zarówno UE, jak i USA będą nadal angażować się we współpracę na rzecz osiągnięcia wyższego poziomu ochrony danych osobowych.

Bruksela, dnia 18 października 2017 r.

Georges DASSIS  
Przewodniczący  
Europejskiego Komitetu Ekonomiczno-Społecznego

---