Opinia Europejskiego Komitetu Ekonomiczno-Społecznego „Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady dotyczącego ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez unijne instytucje, organy i jednostki organizacyjne oraz swobodnego przepływu takich danych i uchylającego rozporządzenie (WE) nr 45/2001 i decyzję nr 1247/2002/WE"

[COM(2017) 8 final – 2017/0002 (COD)]

(2017/C 288/15)

Sprawozdawca: **Jorge PEGADO LIZ**

Wniosek o konsultację	Komisja Europejska, 26.4.2017
Podstawa prawna	Art. 16 ust. 2 TFUE
Sekcja odpowiedzialna	Sekcja Transportu, Energii, Infrastruktury i Społeczeństwa Informacyjnego
Data przyjęcia przez sekcję	16.5.2017
Data przyjęcia na sesji plenarnej	31.5.2017
Sesja plenarna nr	526
Wynik głosowania	161/0/2
(za/przeciw/wstrzymało się)	

1. **Wnioski i zalecenia**

1.1. W omawianym wniosku Komisja dokonuje – w zasadzie poprawnie i w odpowiedni sposób z czysto techniczno-prawnego punktu widzenia – niezbędnego dostosowania obecnego systemu na mocy **rozporządzenia (WE) nr 45/2001 Parlamentu Europejskiego i Rady** ([1]) **i decyzji nr 1247/2002/WE Parlamentu Europejskiego i Rady** ([2]) **dotyczących ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez unijne instytucje, organy i jednostki organizacyjne** do nowego ogólnego rozporządzenia o ochronie danych ([3]), które będzie obowiązywać w całej UE od 25 maja 2018 r.

1.2. EKES przypomina swoje uwagi w sprawie wniosku dotyczącego ogólnego rozporządzenia (przekształconego obecnie w aktualne rozporządzenie) i ubolewa, że nie uwzględniono ich w całości w ostatecznej wersji. Ponadto obawia się, że opóźnienia w przyjęciu i wejściu w życie rozporządzenia, z uwagi na gwałtowne zmiany technologiczne w tym obszarze, zwiększają ryzyko niewłaściwego wykorzystania danych oraz nadużyć w ich przetwarzaniu i udostępnianiu, co z kolei może spowodować, że rozporządzenie zdezaktualizuje się jeszcze przed wejściem w życie. Ponieważ omawiany wniosek stanowi dostosowanie ogólnego rozporządzenia do funkcjonowania instytucji europejskich, uwagi te mają zastosowanie mutatis mutandis do omawianego dokumentu, zwłaszcza jeśli chodzi o brak przejrzystości stosowanego języka, trudnego do zrozumienia dla przeciętnego obywatela.

1.3. Z drugiej strony funkcjonowanie instytucji UE powinno służyć za przykład na poziomie krajowym, dlatego EKES apeluje o zwrócenie szczególnej uwagi na sformułowanie omawianego wniosku.

1.4. W związku z tym Komitet sądziłby, że wyraźnie wspomniano by o takich aspektach jak: powiązanie omawianego wniosku z Regulaminem pracowniczym urzędników Unii Europejskiej, kwestia agresji w internecie, cyberprzemoc, sygnalizowanie nieprawidłowości w instytucjach unijnych, zastosowanie wniosku do internetu rzeczy, duże zbiory danych i korzystanie z wyszukiwarek w celach uzyskania dostępu, tworzenie lub wykorzystanie danych osobowych oraz prywatne informacje publikowane na stronach instytucji w sieciach społecznościowych (Facebook, Twitter, Instagram, Linkedin itp.).

([1]) Dz.U. L 8 z 12.1.2001, s. 1.
([2]) Dz.U. L 183 z 12.7.2002, s. 1.
([3]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (Dz.U. L 119 z 4.5.2016, s. 1).

1.5. Komitet pragnąłby także, by we wniosku zajęto się warunkami bezpieczeństwa systemów informatycznych, które będą wspierać przetwarzanie danych oraz służyć jako zabezpieczenie przed atakami cybernetycznymi i naruszeniem lub ujawnieniem takich danych. Jednocześnie trzeba zapewnić ich neutralność technologiczną, nie ograniczać ich jedynie do wewnętrznych norm poszczególnych działów, a także lepiej wyjaśnić powiązania między ochroną danych a zwalczaniem przestępczości i terroryzmu, co nie może prowadzić do przyjmowania nieproporcjonalnych bądź nadmiernych środków nadzoru i w każdym wypadku musi podlegać kontroli Europejskiego Inspektora Ochrony Danych (EIOD).

1.6. Dobrze byłoby, gdyby we wniosku określono kompetencje, szkolenia i cechy osobowości niezbędne do pełnienia funkcji inspektora ochrony danych, administratora danych oraz podmiotu przetwarzającego przy instytucjach UE, przy czym muszą one zawsze podlegać kontroli i monitorowaniu ze strony EIOD.

1.7. EKES sądzi też, że ze względu na szczególny charakter gromadzonych danych i fakt, że wpływają bezpośrednio na prywatne życie osób, których dotyczą, zwłaszcza w dziedzinie zdrowia, opodatkowania i kwestii społecznych, powinny one zostać ograniczone do minimum niezbędnego dla osiągnięcia wytyczonych celów. Należy również zagwarantować maksymalny poziom ochrony i gwarancji podczas przetwarzania szczególnie wrażliwych danych osobowych, opierając się na międzynarodowych przepisach i bardziej zaawansowanym prawodawstwie krajowym oraz na najlepszych praktykach niektórych państw członkowskich.

1.8. Komitet podkreśla konieczność wyraźnego przewidzenia we wniosku zwiększenia środków EIOD, przydzielenia wystarczających zasobów kadrowych oraz podniesienia umiejętności technicznych i wiedzy na temat ochrony danych.

1.9. EKES ponownie przypomina o tym, że gromadzenie i przetwarzanie danych dotyczących legalnych osób prawnych (przedsiębiorstw, organizacji pozarządowych, spółek handlowych itp.) musi również podlegać ochronie.

1.10. Wreszcie Komitet przedstawia w uwagach szczegółowych szereg zmian do różnych artykułów, mających na celu zwiększenie skuteczności ochrony danych osobowych w instytucjach UE, nie tylko w odniesieniu do urzędników, lecz także tysięcy obywateli europejskich, którzy mają z nimi kontakt. Wzywa Komisję oraz Parlament Europejski i Radę do uwzględnienia tych uwag w końcowej wersji wniosku.

2. **Uzasadnienie i kontekst wniosku**

2.1. Jak wskazuje sama Komisja w uzasadnieniu, celem wniosku jest uchylenie rozporządzenia (WE) nr 45/2001 ([4]) i decyzji nr 1247/2002/WE dotyczących ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez unijne instytucje, organy i jednostki organizacyjne, tak aby:

— chronić podstawowe prawo do ochrony danych,

— zagwarantować swobodny przepływ danych osobowych w UE.

2.2. Po długich i złożonych przygotowaniach Rada i Parlament przyjęły ogólne rozporządzenie o ochronie danych ([5]), które wejdzie w życie w całej UE 25 maja 2018 r. Wiąże się to z dostosowaniem różnych instrumentów ustawodawczych ([6]), wśród których należy wskazać wspomniane już rozporządzenie (WE) nr 45/2001 i decyzję nr 1247/2002/WE.

2.3. Mając na uwadze wyniki badań i konsultacji z zainteresowanymi stronami oraz badanie oceniające stosowanie rozporządzenia (WE) nr 45/2001 na przestrzeni 15 lat, Komisja szeroko omawia to zagadnienie i dochodzi zwłaszcza do następujących wniosków:

— rozporządzenie można by lepiej egzekwować dzięki stosowaniu sankcji przez Europejskiego Inspektora Ochrony Danych (EIOD),

— zwiększone wykorzystanie uprawnień organu nadzorczego mogłoby prowadzić do lepszego wdrożenia przepisów o ochronie danych osobowych,

([4]) Odnośna opinia EKES-u (Dz.U. C 51 z 23.2.2000, s. 48).
([5]) Rozporządzenie (UE) 2016/679 z 27.4.2016 (Dz.U. L 119 z 4.5.2016, s. 1).
([6]) COM (2017) 10 final, COM (2017) 9 final.

— trzeba uprościć system zgłoszeń i kontroli wstępnych, aby zwiększyć efektywność i ograniczyć obciążenie administracyjne,

— administratorzy danych powinni przyjąć zasady zarządzania ryzykiem i przeprowadzać oceny ryzyka przed przystąpieniem do operacji przetwarzania, aby lepiej wdrażać wymogi dotyczące zatrzymywania danych i ich bezpieczeństwa,

— obowiązujące przepisy dotyczące sektora telekomunikacyjnego są nieaktualne i konieczne jest dostosowanie tego rozdziału do dyrektywy o prywatności elektronicznej,

— istnieje również potrzeba doprecyzowania niektórych kluczowych definicji zawartych w rozporządzeniu, dotyczących identyfikacji administratorów danych w unijnych instytucjach, organach i jednostkach organizacyjnych, definicji odbiorcy i objęcia obowiązkiem zachowania poufności również zewnętrzne podmioty przetwarzające.

2.4. Mając na uwadze charakter i zakres zmian, jakie należy wprowadzić we wcześniejszych instrumentach prawnych, Komisja postanowiła uchylić te instrumenty w całości i zastąpić je omawianym rozporządzeniem, spójnym z pozostałymi wspomnianymi przepisami, które wejdą w życie równocześnie z rozporządzeniem (UE) 2016/679 i zgodnie z postanowieniami jego art. 98.

3. **Uwagi ogólne**

3.1. Z czysto techniczno-prawnego punktu widzenia EKES zgadza się ogólnie z:

— koniecznością i aktualnością omawianej inicjatywy,

— wybranym instrumentem prawnym (rozporządzeniem),

— opcją uchylenia w całości istniejących instrumentów,

— wybraną podstawą prawną,

— poszanowaniem zasady pomocniczości, proporcjonalności i rozliczalności,

— jasnym charakterem i strukturą postanowień,

— lepszym zdefiniowaniem niektórych pojęć, np. ważnej zgody,

— spójnością z pozostałymi powiązanymi instrumentami prawnymi, zwłaszcza rozporządzeniem (UE) 2016/679, wnioskiem dotyczącym rozporządzenia COM(2017) 10 final i samym komunikatem Komisji „Budowa europejskiej gospodarki opartej na danych” ([7]),

— uwzględnieniem po raz pierwszy możliwości nałożenia kar administracyjnych za ewentualne naruszenia i nieprzestrzeganie przepisów,

— wzmocnieniem uprawnień EIOD,

— niewłączeniem tej inicjatywy do programu REFIT,

— dążeniem do zgodności z innymi prawami, jak np. zapisaną w Karcie praw podstawowych Unii Europejskiej wolnością wypowiedzi i informacji (art. 11), ochroną własności intelektualnej (art. 17 ust. 2), zakazem dyskryminacji ze względu na rasę, pochodzenie etniczne, cechy genetyczne, religię lub światopogląd, opinie polityczne lub wszelkie inne, niepełnosprawność lub orientację seksualną (art. 21), prawami dziecka (art. 24), wysokim poziomem ochrony zdrowia (art. 35), dostępem do dokumentów (art. 42) oraz skutecznym środkiem prawnym i sprawiedliwym procesem sądowym (art. 47).

([7]) COM(2017) 9 final.

3.2. Nie wyklucza to uwag i zaleceń poczynionych przez Komitet w związku z wnioskiem dotyczącym ogólnego rozporządzenia ([8]) (przekształconym obecnie w aktualne rozporządzenie ([9])), których nie uwzględniono w całości w ostatecznej wersji. Z uwagi na gwałtowne zmiany technologiczne w tym obszarze, opóźnienia w przyjęciu i wejściu w życie rozporządzenia zwiększają ryzyko niewłaściwego wykorzystania danych oraz nadużyć w ich przetwarzaniu i udostępnianiu, co z kolei może spowodować, że rozporządzenie zdezaktualizuje się jeszcze przed wejściem w życie. Ponieważ omawiany wniosek stanowi dostosowanie ogólnego rozporządzenia do funkcjonowania instytucji europejskich, uwagi te mają zastosowanie mutatis mutandis do omawianego dokumentu, zwłaszcza jeśli chodzi o brak przejrzystości stosowanego języka, trudnego do zrozumienia dla przeciętnego obywatela. Lepiej byłoby, gdyby oba wnioski zostały przedłożone i omówione wspólnie.

3.3. Z drugiej strony, mając na uwadze, że funkcjonowanie instytucji UE powinno służyć za przykład na poziomie krajowym, zdaniem EKES-u należałoby zająć się pewnymi zagadnieniami w omawianym wniosku.

3.4. Nie jest jasne, czy wniosek został należycie powiązany z Regulaminem pracowniczym urzędników Unii Europejskiej (rozporządzenie nr 31 EWG ([10])), gdyż zabrakło konkretnych przepisów gwarantujących, że dane osobowe urzędników i osób współpracujących z instytucjami UE będą podlegać skuteczniejszej ochronie w odniesieniu do naboru, kariery, okresu obowiązywania umowy, ewentualnego przedłużenia i oceny.

3.4.1. W tekście ocenianego wniosku należałoby przewidzieć ogólne przepisy dotyczące zdrowia urzędników, ochrony tworzonych lub wykorzystywanych przez urzędników i ich bliskich danych i odnośnych danych genetycznych, przetwarzania i ochrony wiadomości wysyłanych pocztą elektroniczną (przez obywateli do instytucji UE, między urzędnikami czy między urzędnikami a podmiotami zewnętrznymi) oraz ich treści i odwiedzanych stron internetowych ([11]).

3.4.2. Szczególnego traktowania wymagają także przypadki cyberprzemocy i sygnalizowania nieprawidłowości w instytucjach unijnych, niezależnie od postanowień art. 68.

3.4.3. EKES zastanawia się także nad warunkami stosowania omawianego wniosku i rozporządzenia (UE) 2016/679 w odniesieniu do internetu rzeczy, dużych zbiorów danych i korzystania z wyszukiwarek w celach uzyskania dostępu, tworzenia lub wykorzystania danych osobowych oraz prywatnych informacji publikowanych na stronach instytucji w sieciach społecznościowych (Facebook, Twitter, Instagram, Linkedin itp.), bez względu na wyraźną zgodę osoby, której dane dotyczą.

3.5. Komitet pragnąłby także, by we wniosku Komisji, obok nawiązania do poufności łączności elektronicznej wspomnianej w art. 34 wniosku dotyczącego rozporządzenia, zajęto się warunkami bezpieczeństwa systemów informatycznych, które będą wspierać przetwarzanie danych oraz służyć jako zabezpieczenie przed atakami cybernetycznymi i naruszeniem lub ujawnieniem takich danych ([12]). Jednocześnie trzeba zapewnić ich neutralność technologiczną, nie ograniczać ich jedynie do wewnętrznych norm poszczególnych działów, a także lepiej wyjaśnić powiązania między ochroną danych a zwalczaniem przestępczości i terroryzmu, co nie może prowadzić do przyjmowania nieproporcjonalnych bądź nadmiernych środków nadzoru i w każdym wypadku musi podlegać kontroli EIOD.

3.6. Komitet zaznacza, że powiązanie danych osobowych w instytucjach i organach UE nie może opierać się wyłącznie na zasadzie rozliczalności przewidzianej w motywie 16. Wzywa więc Komisję do wprowadzenia konkretnego przepisu, zgodnie z którym powiązanie danych będzie możliwe jedynie po zatwierdzeniu przez EIOD na wniosek administratora danych lub podmiotu przetwarzającego.

3.7. Dobrze byłoby, gdyby, bez uszczerbku dla punktu 51 preambuły i art. 44 ust. 3 wniosku, określono kompetencje, szkolenia i cechy osobowości niezbędne do pełnienia funkcji inspektora ochrony danych, administratora danych oraz podmiotu przetwarzającego przy instytucjach UE ([13]). Ewentualne naruszenia ich zadań muszą podlegać wymienionym we wniosku wystarczająco zniechęcającym karom dyscyplinarnym oraz sankcjom na mocy prawa cywilnego i karnego, co w każdym wypadku musi być przedmiotem kontroli i monitorowania ze strony EIOD.

([8]) Dz.U. C 229 z 31.7 2012, s. 90.
([9]) Rozporządzenie (UE) nr 2016/679.
([10]) Dz.U. 45 z 14.6.1962, s. 1385/62 oraz kolejne zmiany.
([11]) Jak stwierdzono np. w „Avis et Recommandations de la Commission de la Vie privé de la Belgique sur la vie privé sur le lieu de travail", styczeń 2013 [Opinia i zalecenia belgijskiej Komisji ds. Ochrony Życia Prywatnego w sprawie prywatności w miejscu pracy].
([12]) Jak stwierdzono np. w „Recommandation d'initiative relative aux mesures de sécurité à respecter afin de prévenir les fuites de données" [Zalecenie z inicjatywy własnej w sprawie środków bezpieczeństwa w celu uniknięcia przecieku danych], belgijska Komisja ds. Ochrony Życia Prywatnego, 1/2013 z 21 stycznia 2013 r.
([13]) Jak wspomniano w „Guidelines on Data Protection Officers" [Wytyczne dotyczące inspektorów ochrony danych], WP 243, art. 29, 13 grudnia 2016 r.

3.8. EKES uznaje wprawdzie, że omawiany wniosek gwarantuje wyższy poziom ochrony w porównaniu z obecnym rozporządzeniem (WE) nr 45/2001, jednak sądzi, że ze względu na szczególny charakter gromadzonych danych i fakt, że wpływają bezpośrednio na prywatne życie osób, których dotyczą, zwłaszcza w dziedzinie zdrowia, opodatkowania i kwestii społecznych, powinny one zostać ograniczone do minimum niezbędnego dla osiągnięcia wytyczonych celów. Należy również zagwarantować maksymalny poziom ochrony i gwarancji podczas przetwarzania danych osobowych, opierając się na międzynarodowych przepisach i bardziej zaawansowanym prawodawstwie krajowym oraz na najlepszych praktykach niektórych państw członkowskich ([14]).

3.9. Choć Komitet ma świadomość, że zarówno rozporządzenie (UE) 2016/679, jak i omawiany wniosek stosują się jedynie do danych dotyczących osób fizycznych, ponownie przypomina o tym, że gromadzenie i przetwarzanie danych dotyczących legalnych osób prawnych (przedsiębiorstw, organizacji pozarządowych, spółek handlowych itp.) musi również podlegać ochronie.

4. **Uwagi szczegółowe**

4.1. Szczegółowa analiza tekstu budzi pewne wątpliwości i zastrzeżenia w świetle podstawowych zasad dotyczących ochrony życia prywatnego wynikających z Karty praw podstawowych oraz zasad proporcjonalności i ostrożności.

4.2. *Artykuł 3*

W ust. 2 lit. a) definiuje się instytucje i organy unijne jako unijne instytucje, organy i jednostki organizacyjne ustanowione Traktatem o funkcjonowaniu Unii Europejskiej, Traktatem o Unii Europejskiej lub Traktatem Euratom lub na ich podstawie. EKES nie jest pewien, czy definicja ta uwzględnia również grupy robocze, komitety doradcze, komisje, platformy, ewentualne grupy itp., a także międzynarodowe sieci informatyczne, w których uczestniczą instytucje UE, lecz nie są ich współzałożycielami.

4.3. *Artykuł 4*

4.3.1. Biorąc pod uwagę, że omawiane obecnie rozporządzenie ma zastosowanie do danych przetwarzanych w instytucjach unijnych, EKES pragnąłby, aby wyraźnie uwzględniono zasadę niedyskryminacji w odniesieniu do przetwarzanych danych.

4.3.2. Jeśli chodzi o art. 4 ust. 1 lit. b), przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych powinno podlegać procedurze uprzedniego zatwierdzenia przez Europejskiego Inspektora Ochrony Danych, co nie zostało przewidziane w art. 58.

4.3.3. Należy także wprowadzić wyraźny przepis równoważny obecnemu art. 7 rozporządzenia (WE) nr 45/2001 w odniesieniu do przekazywania danych między instytucjami UE.

4.4. *Artykuł 5*

4.4.1. Komitet nie rozumie, dlaczego lit. b) art. 5 ust. 1 wniosku dotyczącego rozporządzenia nie została objęta postanowieniami ust. 2 tego samego artykułu, w przeciwieństwie do lit. c) i e) art. 6, które podlegają postanowieniom art. 3 ogólnego rozporządzenia.

4.4.2. Zdaniem EKES-u w lit. d) należy dodać, że wyrażenie zgody powinno odbywać się na zasadzie dobrej wiary.

4.5. *Artykuł 6*

4.5.1. Stosowanie tego artykułu powinno zawsze podlegać zatwierdzeniu przez EIOD.

4.5.2. W takich przypadkach osoba, której dane dotyczą, powinna zawsze otrzymywać informacje z wyprzedzeniem w odniesieniu do zbierania danych lub gdy podejmowana jest nowa decyzja, by mogła złożyć wniosek o sprostowanie, usunięcie danych lub ograniczenie ich przetwarzania bądź wyrazić sprzeciw.

([14]) Zob. np. ustawa portugalska w sprawie ochrony danych (67/98 z 26 października 1998 r.).

4.6. *Artykuł 8*

4.6.1. Zdaniem Komitetu wyjątek od zasady ważności zgody w wypadku dzieci poniżej 16 lat (od 13 do 16 lat) – już sam w sobie nietypowy – może mieć zastosowanie jedynie do państw członkowskich ze względów kulturowych w prawie wewnętrznym (art. 8 ogólnego rozporządzenia), lecz nie powinien zostać dopuszczony jako zasada ogólna w instytucjach UE (art. 8 ust. 1) ustanawiająca wiek na 13 lat.

4.6.2. Z drugiej strony nie jest jasne, w jaki sposób EIOD miałby zwracać „szczególną uwagę" na dzieci (art. 58 ust. 1 lit. b)), zwłaszcza w wypadku list użytkowników przewidzianych w art. 36, gdy dane są dostępne publiczne.

4.7. *Artykuł 10*

4.7.1. W ustępie 1 należy także uwzględnić przynależność polityczną (która nie jest równoznaczna z przekonaniami politycznymi) oraz życie prywatne.

4.7.2. W ust. 2 lit. b), w celu wypełnienia obowiązków i wykonywania szczególnych praw przez osobę, której dane dotyczą, osoba ta powinna dysponować wcześniej informacjami na ten temat.

4.7.3. W ust. 2 lit. d) przetwarzanie powinno być możliwe jedynie za zgodą osoby, której dane dotyczą.

4.7.4. Lit. e) może stanowić wyjątek jedynie, jeśli można w uzasadniony sposób wywnioskować zgodę na przetwarzanie danych.

4.8. *Artykuł 14*

Instytucje UE nie są uprawnione do pobierania opłat za świadczone usługi, tak więc odmowa podjęcia działań może mieć zastosowanie jedynie w ostateczności.

4.9. *Artykuły 15, 16 i 17*

4.9.1. W wypadku dodatkowych informacji przewidzianych w art. 15 ust. 2, należy uwzględnić jeszcze wymóg, by osoba, której dane dotyczą, została poinformowana o obowiązkowym bądź nieobowiązkowym charakterze odpowiedzi administratora danych oraz o ewentualnych konsekwencjach braku odpowiedzi.

4.9.2. Odnośnie do gromadzenia danych w otwartych sieciach, osoba, której dane dotyczą, musi być informowana zawsze, gdy jej dane osobowe mogłyby znaleźć się w sieci bez zabezpieczenia, gdyż powstałoby ryzyko, że zostaną obejrzane i wykorzystane przez nieupoważnione osoby trzecie.

4.9.3. Prawo przewidziane w art. 17 ust. 1 powinno być realizowane bez przeszkód, w rozsądnym terminie, szybko lub natychmiastowo oraz bezpłatnie.

4.9.4. EKES proponuje, by osoba, której dane dotyczą, otrzymała obowiązkowo potwierdzenie, że dotyczące jej dane są lub nie są przetwarzane.

4.9.5. Informacje zawarte w art. 17 ust. 1 muszą być przekazywane w czytelnej, jasnej i zrozumiałej formie, zwłaszcza w odniesieniu do danych podlegających przetwarzaniu bądź wszelkich informacji na temat pochodzenia takich danych.

4.10. *Artykuł 21*

Wykluczenie z wniosku dotyczącego rozporządzenia identycznych przepisów zawartych w art. 21 ust. 2 i 3 ogólnego rozporządzenia oznacza zdaniem Komitetu, że dane nigdy nie mogą być przetwarzane do celów marketingu bezpośredniego, co byłoby godne pochwały. Niemniej przepis powinien wyraźnie wyjaśnić niepewny charakter tej interpretacji.

4.11. *Artykuł 24*

4.11.1. EKES uważa, że w ust. 2 lit. c) należy dodać, że zgoda ta jest wyrażana jedynie po wyraźnym powiadomieniu osoby, której dane dotyczą, o prawnych skutkach decyzji, gdyż tylko w ten sposób możliwe będzie udzielenie świadomej zgody.

4.11.2. Jeśli chodzi o ust. 3, zdaniem EKES-u właściwe środki powinny zostać określone przez EIOD, a nie administratora danych.

4.12. *Artykuł 25*

4.12.1. Komitet obawia się, że sformułowanie art. 25 wniosku dotyczącego rozporządzenia stanowi zbyt szeroką interpretację postanowień art. 23 ogólnego rozporządzenia w odniesieniu do ograniczenia stosowania przepisów ustanawiających podstawowe prawa osoby, której dane dotyczą. Zaleca więc krytyczny przegląd oparty na dokładnej, a w razie potrzeby ograniczonej analizie niektórych punktów, zwłaszcza jeśli chodzi o ograniczenie prawa do poufności w sieciach łączności elektronicznej na mocy art. 7 Karty praw podstawowych, rozważane obecnie w dyrektywie o prywatności i łączności elektronicznej i utrzymane we wniosku dotyczącym rozporządzenia będącym przedmiotem innej opinii EKES-u.

4.12.2. Komitet całkowicie sprzeciwia się przewidzianej w art. 25 ust. 2 możliwości ograniczenia przez instytucje i organy unijne stosowania ograniczeń praw osób, których dane dotyczą, jeśli nie zostało to przewidziane wyraźnie w akcie prawnym. Ta sama uwaga ma zastosowanie do art. 34.

4.13. *Artykuł 26*

Należy wyjaśnić, że administratorzy danych, podmioty przetwarzające oraz osoby, które przy pełnieniu swoich funkcji mają kontakt z danymi osobowymi, muszą zachować tajemnicę służbową przez rozsądny czas, nawet po zakończeniu pełnienia funkcji.

4.14. *Artykuły 29 i 39*

Artykuł 24 ust. 3, art. 40 i nast. ogólnego rozporządzenia słusznie nie zostały włączone do wniosku dotyczącego rozporządzenia (kodeks postępowania), jak wyraźnie wspomniano w preambule punktu odnoszącego się do art. 26. Nie wydaje się właściwe, że w art. 29 ust. 5 i 39 ust. 7 wniosku stwierdzono, że stosowanie kodeksu postępowania, o którym mowa w art. 40 ogólnego rozporządzenia, można uznać za wystarczającą gwarancję pełnienia funkcji przez podmiot przetwarzający, który nie jest instytucją unijną lub organem unijnym.

4.15. *Artykuł 31*

Zdaniem EKES-u sama „możliwość" wspomniana w art. 31 ust. 5 powinna być „obowiązkiem" zachowania rejestrów czynności przetwarzania w publicznie dostępnym rejestrze centralnym.

4.16. *Artykuł 33*

Ponadto EKES sugeruje, by administrator i podmiot przetwarzający sprawowali kontrolę nośników danych, wprowadzania danych, korzystania z nich oraz ich przekazywania. W tym celu należy:

— uniemożliwić osobom nieuprawnionym dostęp do urządzeń wykorzystywanych do przetwarzania tych danych,

— zapobiec nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu i usuwaniu nośników danych,

— zapobiec nieuprawnionemu wprowadzaniu danych i nieuprawnionej inspekcji, zmienianiu i usuwaniu przechowywanych danych osobowych,

— zapobiec wykorzystywaniu zautomatyzowanych systemów przetwarzania danych przez nieupoważnione osoby z wykorzystaniem sprzętu do przekazywania danych,

— zapewnić możliwość sprawdzenia, jakim organom można przekazywać dane osobowe,

— dopilnować, by jedynie upoważnione osoby miały dostęp do danych objętych procedurą uprzedniego zezwolenia.

4.17. *Artykuł 34*

EKES ma nadzieję, że artykuł będzie zgodny z przepisami dotyczącymi wniosku dotyczącego rozporządzenia w sprawie prywatności, a instytucje i organy unijne będą podlegać kontroli ze strony EIOD odnośnie do poufności łączności elektronicznej.

4.18. *Artykuł 42*

EKES obawia się, że słowo „po" w ust. 1 można by rozumieć jako obowiązek konsultacji dopiero po przyjęciu aktu ustawodawczego, co zniosłoby obecną praktykę choćby nieformalnych konsultacji.

4.19. *Artykuł 44*

Zdaniem EKES-u zasadniczo tylko urzędnicy powinni być mianowani na osobę odpowiedzialną za ochronę danych. Jeśli wyjątkowo nie byłoby to możliwe, osoby takie powinny być zatrudniane na podstawie przepisów dotyczących zamówień publicznych na świadczenie usług oraz podlegać ocenie EIOD.

4.20. *Artykuł 45*

4.20.1. Niezależnie od powyższych uwag, jeśli inspektor ochrony danych nie jest urzędnikiem, jego zwolnienie ze względu na charakter pełnionych przez niego obowiązków powinno być możliwe w każdym momencie. W tym celu wystarczy pozytywna opinia EIOD (art. 45 ust. 8 rozporządzenia).

4.20.2. Czas trwania jego kadencji należy ustalić na 5 lat, z możliwością jednokrotnego odnowienia.

4.21. *Artykuł 56*

Ostatnie, dobrze znane wydarzenia związane z najwyższymi urzędnikami instytucji zachęcają do ustanowienia zasad niezgodności i niemożności wykonywania obowiązków przez rozsądny czas w odniesieniu do niektórych funkcji, zwłaszcza w prywatnych przedsiębiorstwach po wygaśnięciu funkcji.

4.22. *Artykuł 59*

W niektórych wersjach językowych, zwłaszcza angielskiej, słowo „actions" w ust. 5 jest zbyt restryktywne i powinno zostać zastąpione przez „proceedings".

4.23. *Artykuł 63*

W odniesieniu do ust. 3 i z uwagi na delikatny charakter omawianej tu kwestii, zdaniem EKES-u należałoby odwrócić zasadę domniemanego odrzucenia, obligując EIOD do udzielenia wyraźnej odpowiedzi na wszystkie przedłożone mu skargi. Brak reakcji oznaczałby domniemane zaakceptowanie skargi.

4.24. *Artykuł 65*

Jak stwierdzono w opinii EKES-u w sprawie wniosku leżącego u podstaw rozporządzenia (UE) 2016/679, podkreśla się konieczność przewidzenia we wniosku, obok postanowień zawartych w art. 67, możliwości zareagowania na naruszenie danych osobowych w formie roszczeń zbiorowych, bez konieczności pojedynczego mandatu. Trzeba pamiętać, że ogólnie, gdy dochodzi do takich naruszeń, to dotykają one wielu osób.

4.25. Wniosek dotyczący rozporządzenia zawiera wyrażenia lub pojęcia o dwuznacznym i subiektywnym charakterze, które należy przejrzeć i zastąpić, jak np. „w miarę możliwości", „jeżeli jest to możliwe", „bez zbędnej zwłoki", „wysokie ryzyko", „należycie", „w rozsądnym terminie", „szczególne znaczenie".

Bruksela, dnia 31 maja 2017 r.

Georges DASSIS
Przewodniczący
Europejskiego Komitetu Ekonomiczno-Społecznego