Opinia Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie komunikatu Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej"

COM (2010) 609 wersja ostateczna

(2011/C 248/21)

Sprawozdawca: **Peter MORGAN**

Dnia 4 listopada 2010 r. Komisja Europejska, działając na podstawie art. 304 Traktatu o funkcjonowaniu Unii Europejskiej, postanowiła zasięgnąć opinii Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie

komunikatu Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej"

COM (2010) 609 wersja ostateczna.

Sekcja Zatrudnienia, Spraw Społecznych i Obywatelstwa, której powierzono przygotowanie prac Komitetu w tej sprawie, przyjęła swoją opinię 27 maja 2011 r.

Na 472. sesji plenarnej w dniach 15–16 czerwca 2011 r. (posiedzenie z 16 czerwca) Europejski Komitet Ekonomiczno-Społeczny stosunkiem głosów 155 do 9 – 12 osób wstrzymało się od głosu – przyjął następującą opinię:

1. **Wnioski i zalecenia**

1.1 Unijne przepisy o ochronie danych opierają się na dyrektywie z roku 1995 (95/46 WE). Ich dwa cele wyrażono w sposób następujący:

1) *Państwa członkowskie zobowiązują się chronić podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do prywatności w odniesieniu do przetwarzania danych osobowych.*

2) *Państwa członkowskie nie będą ograniczać ani zakazywać swobodnego przepływu danych osobowych między państwami członkowskimi ze względów związanych z ochroną przewidzianą w ust. 1.*

Konieczne jest zapewnienie równowagi między tymi celami, aby nie były one ze sobą sprzeczne. Najważniejszym celem nowego ustawodawstwa musi być wdrożenie ram prawnych umożliwiających realizację obu tych celów.

1.2 EKES z zadowoleniem przyjmuje komunikat, który przedstawia podejście Komisji do uaktualnienia dyrektywy o ochronie danych nr 95/46 WE. Dynamiczny rozwój nowych technologii prowadzi do gwałtownego wzrostu natężenia przetwarzania danych on-line, co wymaga równoległego zwiększenia ochrony danych osobowych, by uniknąć naruszenia prywatności na dużą skalę. Należy uważnie ograniczyć gromadzenie i łączenie danych z różnych źródeł, jak również zarządzanie tymi danymi. Sektor publiczny przechowuje wiele różnych dokumentów dotyczących rozmaitych aspektów stosunku obywatel-państwo. Należy zbierać minimum danych wymaganych dla każdego celu oraz zakazać gromadzenia tych danych w bazie typu „wielki brat".

1.3 Równocześnie EKES nawołuje do zachowania ostrożności. Ustawodawstwo regulujące działalność gospodarczą musi pozostać stabilne i przewidywalne. EKES popiera zatem stosowny przegląd dyrektywy o ochronie danych.

1.4 W komunikacie stwierdzono, że jednym z głównych problemów stale wskazywanych przez zainteresowane podmioty, w szczególności wielonarodowe spółki, jest brak dostatecznej harmonizacji obowiązujących w poszczególnych państwach członkowskich przepisów o ochronie danych, mimo wspólnych unijnych ram prawnych. EKES proponuje, by nowe ustawodawstwo bardziej konsekwentnie chroniło dane osobowe pracowników w całej UE i zawierało europejskie ramy służące zwiększeniu jasności i pewności prawnej. W związku z tym EKES ze szczególnym zadowoleniem przyjmuje wprowadzenie obowiązku powołania w przedsiębiorstwach niezależnych inspektorów ochrony danych oraz harmonizację przepisów dotyczących ich zadań i kompetencji.

1.5 Uwzględniając możliwy konflikt między prywatnością osoby fizycznej a wykorzystywaniem danych o osobie fizycznej do celów handlowych, jak również stawkę o jaką idzie w tej kwestii, należy w większym stopniu informować te osoby, w jakich celach ich dane są gromadzone i jakie mają uprawnienia do ich kontrolowania po zgromadzeniu. EKES wierzy zatem, że skuteczne mechanizmy egzekwowania i dochodzenia roszczeń są warunkiem *sine qua non*, jeśli projekt ten ma być prawdziwie „całościowy". Należy również uwzględnić wymiar transgraniczny.

1.6 Jeśli chodzi o obywateli UE, odpowiednim prawem w ramach Unii Europejskiej powinno być prawo obowiązujące w państwie członkowskim administratora danych, bez względu na miejsce przechowywania danych. W odniesieniu do osób uprawnionych do ochrony danych, w szczególności pracowników i konsumentów, powinno mieć zastosowanie prawo do ochrony danych obowiązujące w miejscu ich zamieszkania.

1.7 Odniesienie do dzieci jest pobieżne. Należy konkretnie skupić się na kwestiach prywatności w stosunku do dzieci. Prawo do bycia zapomnianym mogłoby korygować ślady dziecięcej głupoty czy wykroczeń osób nieletnich, lecz może ono być niemożliwe do zrealizowania w rzeczywistości.

1.8 Należy sprecyzować obecną definicję danych szczególnie chronionych, ponieważ wciąż wzrasta liczba kategorii danych elektronicznych dotyczących osób fizycznych. Niepokój EKES-u budzi rozpowszechnione i bezkrytyczne korzystanie z kamer monitorujących. Konieczne jest wprowadzenie prawa ograniczającego nadużywanie tych obrazów. Inną kontrowersyjną kwestią jest wykorzystywanie danych GPRS do ustalania położenia osoby fizycznej. Coraz więcej gromadzonych jest danych biometrycznych. Definicja powinna obejmować powyższe nowe technologie i metodologie, powinna ona również uwzględniać dalszy rozwój technologiczny. Być może konieczne będzie ustalenie zasad zależnych od kontekstu. EKES popiera odpowiednie stosowanie tych nowych technologii.

1.9 Uwzględniając szczególny charakter międzypaństwowej współpracy policyjnej, EKES uważa, że w każdej sytuacji najważniejsze jest przestrzeganie praw podstawowych, w tym ochrona danych osobowych.

1.10 EKES wspiera ogólne dążenie Komisji, by zagwarantować bardziej spójne stosowanie unijnych przepisów o ochronie danych we wszystkich państwach członkowskich. EKES obawia się, że nie wszystkich dwanaście nowych państw członkowskich zakończyło pełne i skuteczne wprowadzanie w życie dyrektywy 95/46.

1.11 Zdaniem EKES-u krajowe organy ochrony danych są najczęściej nieskuteczne i przepracowane, a zatem należy zwiększyć ich niezależność. Zgodnie z postanowieniami jakiejkolwiek nowej dyrektywy, organy krajowe powinny mieć status, uprawnienia i zasoby do wypełniania swojej roli.

1.12 Uwzględniając dotychczasowy wkład grupy roboczej art. 29 w ochronę przetwarzania danych osobowych osób fizycznych, EKES uważa, że grupa ta wciąż ma cenną rolę do odegrania.

1.13 W kontekście agendy cyfrowej UE EKES wzywa Komisję do rozważenie utworzenia organu UE w celu rozpatrzenia szerszych ram społecznych internetu w perspektywie 10–20 lat. Obecne przepisy dotyczące ochrony danych osobowych i ogólnego cyberbezpieczeństwa są coraz bardziej nieadekwatne. Społeczeństwo próbuje za tym nadążyć. W kontekście ochrony danych EKES zaleca wyznaczenie ogólnounijnego inspektora ochrony danych. Obecny inspektor ochrony danych UE zajmuje się tylko instytucjami UE. Konieczny jest inspektor odpowiedzialny za koordynację państw członkowskich i standardy operacyjne. Odzwierciedlałoby to jednak tylko część uprawnień władzy nadrzędnej sugerowanej przez Komitet.

2. **Wstęp**

2.1 EKES nadal wspiera zasady, na których opiera się dyrektywa z roku 1995. Poniżej przedstawiono uproszczone i bezwarunkowe fragmenty tekstu dyrektyw. Jasno wyrażają one obowiązujące zasady:

— Artykuł 6

Państwa członkowskie zapewniają, aby dane osobowe były:

a) przetwarzane w sposób rzetelny i zgodny z prawem;

b) gromadzone do określonych, jednoznacznych i legalnych celów;

c) prawidłowe, istotne oraz nienadmierne w stosunku do celów, dla których zostały zgromadzone i/lub dalej przetworzone;

d) dokładne oraz, w razie konieczności, aktualizowane;

e) przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez czas nie dłuższy niż jest to konieczne do celów, dla których dane zostały zgromadzone.

— Artykuł 7

Państwa członkowskie zapewniają, że dane osobowe mogą być przetwarzane tylko wówczas gdy:

a) osoba, której dane dotyczą, jednoznacznie wyraziła na to zgodę;

b) przetwarzanie danych jest konieczne dla realizacji umowy, której stroną jest osoba, której dane dotyczą; lub

c) przetwarzanie danych jest konieczne dla wykonania zobowiązania prawnego, któremu administrator danych podlega; lub

d) przetwarzanie danych jest konieczne dla ochrony żywotnych interesów osób, których dane dotyczą, lub

e) przetwarzanie danych jest konieczne dla realizacji zadania wykonywanego w interesie publicznym; lub

f) przetwarzanie danych jest konieczne dla potrzeb wynikających z uzasadnionych interesów administratora danych.

— Artykuł 8

Państwa członkowskie zabraniają przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych, jak również danych dotyczących zdrowia lub życia seksualnego.

2.2 W ostatnim dziesięcioleciu sytuacja zmieniła się znacząco w związku z nowymi postanowieniami w art. 16 traktatu lizbońskiego oraz art. 8 Karty praw podstawowych.

2.3 W niniejszym komunikacie zamierza się określić podejście Komisji do kwestii modernizacji unijnego systemu prawnego w zakresie ochrony danych osobowych we wszystkich obszarach działalności Unii, biorąc pod uwagę w szczególności wyzwania wynikające z globalizacji oraz nowych technologii, by w dalszym ciągu gwarantować wysoki poziom ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych we wszystkich obszarach działalności Unii.

2.4 W dzisiejszych czasach wymiana informacji na całym świecie jest łatwiejsza i szybsza. Dane osobowe osoby fizycznej – pocztę elektroniczną, zdjęcia lub agendy elektroniczne – można stworzyć w Wielkiej Brytanii przy użyciu oprogramowania umieszczonego na serwerze w Niemczech, przetwarzać je w Indiach, przechowywać w Polsce, a obywatel Włoch może mieć do nich dostęp z Hiszpanii. Ten szybki przepływ informacji na całym świecie stanowi ogromne wyzwanie, jeśli chodzi o prawa osoby fizycznej do ochrony własnych danych osobowych. Kwestie ochrony danych, w tym ich wymiar transgraniczny, codziennie wpływają na życie ludzi – w pracy, w kontaktach z władzami publicznymi, przy zakupie dóbr i usług, czy też w trakcie podróży lub surfowania po internecie.

2.5 Komisja zaproponuje w 2011 r. przepisy zmierzające do przeglądu prawnych ram ochrony danych w celu wzmocnienia stanowiska UE w zakresie ochrony danych osób fizycznych w kontekście wszystkich polityk UE, w tym egzekwowania prawa i zapobiegania przestępczości, przy uwzględnieniu specyfiki tych obszarów. Równolegle wprowadzane będą środki nielegislacyjne, takie jak zachęcanie do samoregulacji oraz badanie możliwości wprowadzenia unijnych certyfikatów prywatności.

2.6 Komisja będzie również w dalszym ciągu zapewniać odpowiednie monitorowanie prawidłowego wdrażania unijnych przepisów w tym obszarze, prowadząc aktywną politykę ścigania naruszeń w przypadkach, w których unijne przepisy o ochronie danych nie są prawidłowo wprowadzane w życie i stosowane.

2.7 Całościowe podejście do kwestii ochrony danych jest ukierunkowane na następujące kluczowe cele:

— wzmocnienie praw osób fizycznych;

— poprawa wymiaru związanego z rynkiem wewnętrznym;

— przegląd przepisów o ochronie danych w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych;

— globalny wymiar ochrony danych;

— zapewnienie lepszych rozwiązań instytucjonalnych w celu skuteczniejszego egzekwowania przepisów o ochronie danych.

W sekcjach 3–7 poniżej podsumowano te cele i przedstawiono poglądy EKES-u w sprawie tych propozycji. Nagłówki zaznaczone **wytłuszczoną czcionką** mają taką samą strukturę jak komunikat. Tekst *kursywą* jest streszczeniem tego tekstu.

3. **Wzmocnienie praw osób fizycznych**

3.1 *Zagwarantowanie odpowiedniej ochrony osobom fizycznym we wszystkich okolicznościach*

W Karcie praw podstawowych zapisane są prawa do ochrony danych osobowych. Definicja „danych osobowych" ma na celu objęcie zakresem tego pojęcia wszystkich informacji dotyczących, bezpośrednio lub pośrednio, zidentyfikowanych lub możliwych do zidentyfikowania osób. Zostanie rozważone, w jaki sposób zagwarantować spójne stosowanie przepisów o ochronie danych, biorąc pod uwagę wpływ nowych technologii na prawa i wolności osób fizycznych oraz cel dotyczący zagwarantowania swobodnego obiegu danych osobowych w obrębie rynku wewnętrznego.

3.1.1 Swobodny obieg danych osobowych w obrębie rynku wewnętrznego jest konieczny do pełnego funkcjonowania tego rynku, lecz stanowi potencjalne zagrożenie dla prywatności danych przechowywanych przez firmy i dotyczących ich pracowników. Potrzebne są konkretne gwarancje, takie jak odpowiedzialność administratorów danych w przypadku międzynarodowej wymiany danych oraz kodowanie danych szczególnie chronionych.

3.1.2 EKES pragnąłby podkreślić, że sektor zatrudnienia jest prawie całkowicie wykluczony nie tylko z niniejszego komunikatu, ale również z niemal całej debaty dotyczącej ochrony danych w Europie. Jako punkt wyjścia należy wykorzystać prace, które już wykonano na szczeblu europejskim, w szczególności propozycje przedstawione przez Grupę Roboczą ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych (Grupę Roboczą Art. 29).

3.2 *Zwiększenie przejrzystości wobec osób, których dane dotyczą*

Przejrzystość stanowi jeden z podstawowych warunków sprawowania przez osoby fizyczne kontroli nad ich danymi i zagwarantowania skutecznej ochrony danych osobowych. Zostaną rozważone: ogólna zasada przejrzystego przetwarzania, szczególne obowiązki administratorów danych, w szczególności w stosunku do dzieci, standardowe oświadczenia o prawie do prywatności oraz obowiązek zawiadamiania o naruszeniach dotyczących danych osobowych.

3.2.1 Standardowe oświadczenia są preferowane, ponieważ zlikwidowałyby konflikty interesu. Ich stosowanie powinno być dobrowolne.

3.2.2 Przejrzystość nie zawsze rozwiązuje kwestię stronniczych warunków umowy. Konieczne jest opracowanie bardziej rygorystycznych przepisów, aby zapewnić większą ochronę przed niesprawiedliwymi warunkami.

3.2.3 Odniesienie do dzieci jest pobieżne. Należy konkretnie skupić się na kwestiach prywatności w stosunku do dzieci. Prawo do bycia zapomnianym mogłoby korygować ślady dziecięcej głupoty czy wykroczeń osób nieletnich, lecz może ono być niemożliwe do zrealizowania w rzeczywistości. (punkt 3.3.2 poniżej).

3.2.4 Nowe ustawodawstwo musi wyjaśnić rolę osoby odpowiedzialnej za przetwarzanie danych i osoby odpowiedzialnej za ich zapisywanie, tak by nie było żadnych wątpliwości co do ich tożsamości oraz praw i obowiązków każdej z nich.

3.2.5 EKES popiera propozycję wprowadzenia obowiązku zawiadamiania o naruszeniach, jednak uważa, że może on nie mieć zastosowania do wszystkich sytuacji we wszystkich sektorach we wszystkich okolicznościach.

3.3 *Zwiększenie kontroli nad własnymi danymi*

Istotne warunki wstępne są ograniczeniami do przetwarzania danych stosownie do celu przetwarzania (zasada minimalizacji danych) oraz do zachowania przez osoby, których dane dotyczą, skutecznej kontroli nad ich własnymi danymi. Zostaną rozważone: wzmocnienie zasady minimalizacji danych, poprawa metod faktycznego korzystania z prawa do dostępu do danych, ich poprawiania, usuwania lub blokowania, wyjaśnienie prawa do bycia zapomnianym oraz zapewnienie jasno sformułowanego prawa do przenoszalności danych.

3.3.1 Ogólnie EKES wspiera każdy krok zmierzający do zwiększenia prywatności. Osoby fizyczne powinny mieć prawo swobodnego dostępu do gromadzonych danych, które ich dotyczą. Można tu przytoczyć jako przykład swobodny dostęp do danych dotyczących zdolności kredytowej. Wycofanie zgody bez podania powodu i skuteczne prawo do bycia zapomnianym są prawami zasadniczymi, ale prywatność byłaby bardziej chroniona, gdyby od początku gromadzona była mniejsza liczba danych. EKES wzywa zatem Komisję, by nadała rzeczywiste znaczenie propozycji wzmocnienia zasady minimalizacji danych.

3.3.2 Prawo do bycia zapomnianym jest atrakcyjną koncepcją, lecz będzie je trudno zrealizować ze względu na „wirusową" naturę danych w internecie i technologii, które usuwają dane, lecz ich nie zapominają.

3.4 *Pogłębianie świadomości społeczeństwa*

Należy zatem zachęcać do działań służących pogłębianiu świadomości, w tym dostarczanie informacji na stronach internetowych, wyraźne określenie praw przysługujących osobom, których dotyczą dane oraz odpowiedzialności administratorów danych. Szczególne zaniepokojenie budzi brak świadomości wśród młodzieży.

3.4.1 Trudno będzie osiągnąć konieczne zmiany zachowań, szczególnie w obliczu faktu, że szybkiemu rozwojowi sieci społecznych nie towarzyszy wzrost świadomości użytkowników na temat skutków ilości podawanych przez nich danych. Podczas gdy w zasadzie dobre byłoby wprowadzenie obowiązkowych powiadomień służących pogłębianiu świadomości w każdym serwisie internetowym, krok ten może rodzić problemy dla przedsiębiorstw. Należy rozważyć wprowadzenie protokołów służących pogłębianiu świadomości w zależności od kategorii usługi – handel internetowy, dostawcy usług internetowych, wyszukiwarki, portale społecznościowe itd.

3.4.2 EKES z zadowoleniem przyjmuje fakt, że Komisja ma zamiar przeznaczyć fundusze UE na wsparcie działań służących pogłębianiu świadomości. EKES pragnąłby, by do współfinansowania działań służących pogłębianiu świadomości przyłączyli się partnerzy społeczni i organizacje społeczeństwa obywatelskiego na szczeblu europejskim i krajowym.

3.5 *Zapewnienie świadomej i dobrowolnej zgody*

Komisja rozważy sposoby wyjaśnienia i wzmocnienia zasad udzielania zgody.

3.5.1 Rodzaj wymaganej zgody powinien nadal być powiązany z typem przetwarzanych danych, a nie z typem stosowanej technologii. Jednak EKES wyraża zaniepokojenie, że w większości przypadków, gdy zgoda udzielana jest przez internet, aplikacja nie dostarcza żadnego potwierdzenia zgody, nie ma też skutecznych mechanizmów, by rejestrować wycofanie zgody. Ponadto, zgoda może pociągać za sobą kliknięcie przycisku, aby zatwierdzić mnóstwo zasad i warunków, wśród których zgoda może stanowić niewielki element. Sensowne byłoby, by zgoda odnosząca się do kontroli danych była prostym i oddzielnym dokumentem, aby była ona istotna, przemyślana i konkretna.

3.5.2 Dla organizacji i przedsiębiorstw prowadzących swoją działalność w internecie przetwarzanie danych osobowych jest niezbędne. Opcja domyślna jest wyraźnie korzystna dla operatora, lecz jeśli nie jest używana uczciwie, może być niekorzystna dla klienta. Należy ograniczyć jej stosowanie, tak by wszyscy operatorzy byli zobowiązani do oferowania domyślnie opcji prywatności swoim klientom na ich życzenie.

3.5.3 Dobrowolne udzielenie zgody wymaga również sprawiedliwej umowy. Należy ustalić zasady, tak by uniknąć nieuczciwych praktyk handlowych.

3.6 *Ochrona danych szczególnie chronionych*

Zostanie rozważone rozszerzenie zakresu definicji „danych szczególnie chronionych", aby obejmowała ona np. dane genetyczne oraz dalszą harmonizację warunków przetwarzania danych szczególnie chronionych.

3.6.1 Należy sprecyzować obecną definicję danych szczególnie chronionych, ponieważ wciąż rozbudowywane są wzrasta liczba kategorii danych elektronicznych dotyczących osób fizycznych. Niepokój EKES-u budzi rozpowszechnione i bezkrytyczne korzystanie z kamer monitorujących. Konieczne jest wprowadzenie prawa ograniczającego nadużywanie tych obrazów. Inną kontrowersyjną kwestią są dane GPRS służące do ustalania położenia osoby fizycznej. Coraz więcej gromadzonych jest danych biometrycznych. Definicja powinna obejmować powyższe nowe technologie i metodologie, powinna ona również uwzględniać dalszy rozwój technologiczny. Być może konieczne będzie ustalenie zasad zależnych od kontekstu. EKES popiera odpowiednie stosowanie tych nowych technologii.

3.6.2 Należy również zapewnić wzmocnioną ochronę danych szczególnie chronionych. Kodowanie powinno być obowiązkowe w przypadku pewnych kategorii danych szczególnie chronionych. Należy stosować najlepsze dostępne technologie. Kontrolerzy powinni być odpowiedzialni za naruszenie bezpieczeństwa.

3.7 *Zapewnienie większej skuteczności sankcji i środków zaradczych*

Zostanie rozważone rozszerzenie uprawnień do wnoszenia spraw na forum sądów krajowych oraz ewentualne przewidzenie sankcji karnych za poważne naruszenia.

3.7.1 Uwzględniając możliwy konflikt między prywatnością osoby fizycznej a wykorzystywaniem danych o osobie fizycznej do celów handlowych, jak również stawkę, o jaką idzie w tej kwestii, należy w większym stopniu informować te osoby, w jakich celach ich dane są gromadzone i jakie mają uprawnienia do ich kontrolowania po zgromadzeniu. EKES wierzy zatem, że skuteczne egzekwowanie i dochodzenie roszczeń są warunkiem *sine qua non*, jeśli projekt ten ma być prawdziwie „całościowy". Należy również uwzględnić wymiar transgraniczny.

3.7.2 Należy przeanalizować przypadek odszkodowania zbiorowego jako środka zaradczego na wyjątkowe niedociągnięcia w zakresie ochrony danych. Trzeba uwzględnić przypadek organizacji przedsiębiorstw i zawodów oraz związków zawodowych, aby reprezentować osoby fizyczne i wnosić sprawy do sądów.

4. **Poprawa wymiaru związanego z rynkiem wewnętrznym**

4.1 *Zwiększenie pewności prawnej oraz zapewnienie równych szans administratorom danych*

Ochrona danych w UE ma silny wymiar związany z rynkiem wewnętrznym. Zostaną rozważone środki służące osiągnięciu dalszej harmonizacji przepisów w zakresie ochrony danych na poziomie UE.

4.1.1 EKES zaniepokojony jest tym, że z zakresu podejmowania decyzji przez państwa członkowskie, o którym mowa w dyrektywie, wynikł problem związany z wprowadzaniem w życie. W tym kontekście rozporządzenie mogłoby dać więcej pewności. Należy dokonać harmonizacji wokół zestawu norm wystarczających do zaspokojenia wymogów przedmiotowej dyrektywy.

4.1.2 W całym komunikacie nie ma odniesienia do pracowników oraz dostępu do ich danych osobowych, przechowywanych przez pracodawców. W przypadku firm międzynarodowych, które mogą centralizować spisy na terytorium UE, a nawet poza nim, jasno zdefiniowane prawa dostępu stanowiące część nowego ustawodawstwa są nieodzowne dla pracowników.

4.2 *Zmniejszenie obciążeń administracyjnych dla administratorów*

Zostaną rozważone różne możliwości uproszczenia i harmonizacji obecnego systemu zawiadamiania, w tym ewentualność sporządzenia jednolitego, ogólnounijnego formularza rejestracyjnego. Zawiadomienia można by publikować w internecie.

4.2.1 EKES zdecydowanie wspierałby te inicjatywy.

4.3 *Wyjaśnienie przepisów dotyczących prawa właściwego oraz odpowiedzialności państw członkowskich*

W przypadkach dotyczących kilku państw członkowskich administratorzy danych oraz organy nadzorujące ochronę danych nie zawsze wiedzą, które państwo członkowskie ponosi odpowiedzialność, oraz które prawo jest prawem właściwym. Sytuację komplikuje dodatkowo globalizacja i postęp techniczny. Zostanie rozważone zrewidowanie i wyjaśnienie obowiązujących przepisów o prawie właściwym, aby zwiększyć pewność prawną i wyjaśnić zakres odpowiedzialności państw członkowskich.

4.3.1 Jeśli chodzi o obywateli UE, odpowiednim prawem w ramach Unii Europejskiej powinno być prawo obowiązujące w państwie członkowskim administratora danych, bez względu na miejsce przechowywania danych. W odniesieniu do osób uczestniczących w przepływie danych, które są uprawnione do ich ochrony, w szczególności pracowników i konsumentów w UE, powinno mieć zastosowanie prawo do ochrony danych wynikające z przepisów i procedur obowiązujących w miejscu zamieszkania pracowników lub konsumentów.

4.4 *Zwiększenie odpowiedzialności administratorów danych*

Komisja zbada sposoby zagwarantowania, by administratorzy danych wdrożyli skuteczne polityki i mechanizmy mające zapewnić zgodność z przepisami o ochronie danych. Zostanie rozważone wprowadzenie obowiązku powołania inspektorów ochrony danych oraz harmonizacja zasad ich zaangażowania, aby wprowadzić obowiązek dokonywania oceny skutków regulacji w zakresie ochrony danych. Komisja będzie też nadal propagować technologie służące wzmocnieniu ochrony prywatności (PET) oraz realizację koncepcji „uwzględniania ochrony prywatności w fazie projektowania".

4.4.1 PET oraz koncepcja „uwzględniania ochrony prywatności w fazie projektowania" mogą potencjalnie zabrać prawo do decydowania administratorom danych, którzy mogą być w konflikcie z priorytetami handlowymi swoich organizacji. EKES wzywa Komisję, by zapoczątkowała dalsze analizy i opracowanie tych narzędzi, ponieważ dają one możliwość zwiększenia ochrony danych przy jednoczesnej eliminacji konfliktów interesów. Najlepiej byłoby, gdyby stosowanie tych narzędzi mogło stać się obowiązkowe.

4.4.2 Aby zapobiec wszelkim wątpliwościom, administratorzy danych powinni podlegać rozliczeniom za wszystkie aspekty przetwarzania danych, za które są odpowiedzialni. Również w przypadkach, gdy w grę wchodzą podwykonawcy lub operacje w innych krajach, obowiązki w zakresie prywatności danych osobowych powinny być w pełni zapisane w kontrakcie.

4.4.3 EKES uważa, że każde państwo członkowskie powinno powołać profesjonalny organ, który odpowiadałby za poziom umiejętności i certyfikację inspektorów ochrony danych.

4.4.4 Wprowadzenie w życie przepisów w tej dziedzinie powinno być zgodne z celem, o którym mowa w pkt. 4.2, polegającym na zmniejszeniu obciążeń administracyjnych doświadczanych przez administratorów danych.

4.5 *Zachęcanie do inicjatyw w dziedzinie samoregulacji oraz analiza unijnych systemów certyfikacji*

Komisja głębiej przeanalizuje środki sprzyjające rozwojowi inicjatyw samoregulacyjnych, takie jak kodeksy postępowania, i przeanalizuje wykonalność unijnych systemów certyfikacji.

4.5.1 Zob. pkt. 3.7.1 powyżej: egzekwowanie i dochodzenie roszczeń są przedmiotem największej troski EKES-u. Propozycje te są atrakcyjne na tyle, na ile przyczyniają się one do zmniejszenia ogromnego obciążenia regulacyjnego doświadczanego przez przedsiębiorstwa. Każde państwo członkowskie powinno sfinansować wydanie poradnika lub przewodnika po najlepszych praktykach.

5. **Przegląd przepisów o ochronie danych w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych**

Unijnym instrumentem ochrony danych osobowych w obszarze współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych jest decyzja ramowa 2008/977/WSiSW. Ma ona wiele niedociągnięć, które mogą negatywnie wpłynąć na zdolność osób fizycznych do dochodzenia swoich praw dotyczących ochrony danych w następującym zakresie: świadomość, jakie dane osobowe podlegają przetwarzaniu i przekazywaniu, kto to robi i w jakim celu oraz jak dochodzić swoich praw, takich jak prawo dostępu do własnych danych.

Zostanie rozważone rozszerzenie stosowania ogólnych przepisów o ochronie danych na obszar współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych, obejmujące wprowadzenie nowych przepisów w takich dziedzinach jak przetwarzanie danych genetycznych, zapoczątkowanie konsultacji w sprawie zmiany systemów nadzoru w tym obszarze i ocena potrzeby długookresowego dostosowania konkretnych przepisów obowiązujących w różnych sektorach do nowych, ogólnych ram prawnych w zakresie ochrony danych.

5.1 Uwzględniając szczególny charakter międzypaństwowej współpracy policyjnej, EKES uważa, że w każdej sytuacji najważniejsze jest przestrzeganie praw podstawowych, w tym ochrona danych osobowych. EKES obawia się, że względy bezpieczeństwa, choć nieuzasadnione, często przyczyniają się do naruszenia praw podstawowych. Osoby fizyczne powinny być lepiej informowane o metodach i celach wykorzystywanych przez organy do gromadzenia danych osobowych z bilingów telefonicznych, kont bankowych, kontroli na lotniskach itd.

6. **Globalny wymiar ochrony danych**

6.1 *Wyjaśnienie i uproszczenie przepisów dotyczących międzynarodowych transferów danych*

Komisja zamierza przeanalizować, w jaki sposób:

— *ulepszyć i usprawnić obecne procedury transferów danych na poziomie międzynarodowym, aby zagwarantować bardziej jednolite i spójne podejście UE do państw trzecich i organizacji międzynarodowych;*

— *lepiej określić kryteria i wymogi dotyczące oszacowania poziomu ochrony danych w państwach trzecich lub organizacjach międzynarodowych;*

— *zdefiniować podstawowe elementy ochrony danych UE do wykorzystania w umowach międzynarodowych.*

6.1.1 EKES wspiera te pożyteczne inicjatywy i ma nadzieję, że Komisja osiągnie szerokie porozumienie międzynarodowe, bez którego propozycje te mogą być nieskuteczne.

6.2 *Propagowanie uniwersalnych zasad*

Unia Europejska musi pozostać motorem rozwoju i promocji międzynarodowych norm prawnych i technicznych w dziedzinie ochrony danych osobowych. W tym celu Komisja będzie aktywnie działać w obszarze norm międzynarodowych i współpracować z państwami trzecimi i z organizacjami międzynarodowymi, takimi jak OECD.

6.2.1 EKES popiera również tę inicjatywę. Zważywszy na globalny charakter internetu konieczne jest, by przepisy i wytyczne były kompatybilne między kontynentami. Dane osobowe muszą być chronione ponad granicami. Należy zauważyć, ze już istnieją wytyczne OECD, jak również konwencja nr 108 Rady Europy. Konwencja ta jest obecnie poddawana przeglądowi. Komisja powinna zapewnić spójność konwencji i nowej dyrektywy.

7. **Zapewnienie lepszych rozwiązań instytucjonalnych w celu skuteczniejszego egzekwowania przepisów o ochronie danych**

Komisja przeanalizuje:

— *w jaki sposób wzmocnić, wyjaśnić i zharmonizować status i kompetencje krajowych organów ochrony danych;*

— *sposoby poprawy współpracy i koordynacji między organami ochrony danych;*

— *w jaki sposób zapewnić bardziej spójne stosowanie unijnych przepisów o ochronie danych w obrębie całego rynku wewnętrznego. Środki mogłyby obejmować:*

  — *wzmocnienie roli krajowych inspektorów ochrony danych;*

  — *lepszą koordynację ich pracy za pośrednictwem Grupy Roboczej Art. 29;*

  — *stworzenie mechanizmu zapewniającego spójność na rynku wewnętrznym, podlegającego Komisji Europejskiej.*

7.1 Uwzględniając obawy EKES-u związane z egzekwowaniem i zadośćuczynieniem, propozycje te są dla Komitetu kwestiami kluczowymi. Z zadowoleniem przyjmujemy wyrażenia „wzmocnić, wyjaśnić i zharmonizować" oraz „współpraca i koordynacja" i wspieramy ogólne dążenie Komisji, by zagwarantować bardziej spójne stosowanie unijnych przepisów o ochronie danych we wszystkich państwach członkowskich. EKES obawia się, że nie wszystkich dwanaście nowych państw członkowskich zakończyło pełne i skuteczne wprowadzanie w życie dyrektywy 95/46.

7.2 Zdaniem EKES-u krajowe organy ochrony danych są najczęściej nieskuteczne i przepracowane, a zatem należy zwiększyć ich niezależność. Zgodnie z postanowieniami jakiejkolwiek nowej dyrektywy, organy krajowe powinny mieć status, uprawnienia i zasoby do wypełniania swojej roli. Ich zadania oraz zasoby powinny być określane w wymiarze ogólnoeuropejskim. Należy rozważyć wyznaczenie Inspektora Ochrony Danych UE.

7.3 Uwzględniając dotychczasowy wkład Grupy Roboczej Art. 29 w ochronę przetwarzania danych osobowych osób fizycznych, EKES uważa, że grupa ta wciąż ma cenną rolę do odegrania.

Bruksela, 16 czerwca 2011 r.

Przewodniczący
Europejskiego Komitetu Ekonomiczno-Społecznego
Staffan NILSSON

ZAŁĄCZNIK

do opinii Europejskiego Komitetu Ekonomiczno-Społecznego

Następujące fragmenty opinii sekcji, które uzyskały poparcie co najmniej jednej czwartej oddanych głosów, zostały odrzucone na rzecz poprawek przyjętych w trakcie debaty:

Punkt 1.6

Jeśli chodzi o obywateli i pracowników UE, odpowiednim prawem w ramach Unii Europejskiej powinno być prawo obowiązujące w państwie członkowskim administratora danych, bez względu na miejsce przechowywania danych.

Punkt 4.3.1

Jeśli chodzi o obywateli i pracowników UE, odpowiednim prawem w ramach Unii Europejskiej powinno być prawo obowiązujące w państwie członkowskim administratora danych, bez względu na miejsce przechowywania danych.

Wynik głosowania

Za:	86 głosów oddanych za zmianą powyższych punktów
Przeciw:	72
Wstrzymało się:	19