P7_TA(2011)0323

Ochrona danych osobowych w Unii Europejskiej

Rezolucja Parlamentu Europejskiego z dnia 6 lipca 2011 r. w sprawie całościowego podejścia do kwestii ochrony danych osobowych w Unii Europejskiej (2011/2025(INI))

Parlament Europejski,

– uwzględniając Traktat o funkcjonowaniu UE, a w szczególności jego art. 16,

– uwzględniając Kartę praw podstawowych Unii Europejskiej, zwłaszcza jej art. 7 i 8, oraz europejską Konwencję o ochronie praw człowieka i podstawowych wolności (EKPC), zwłaszcza jej art. 8 dotyczący poszanowania życia prywatnego i rodzinnego oraz art. 13 dotyczący skutecznego środka odwoławczego,

– uwzględniając dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[1],

– uwzględniając decyzję ramową Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych[2],

– uwzględniając rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych[3],

– uwzględniając dyrektywę 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)[4],

– uwzględniając Konwencję nr 108 Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, której rozwinięciem jest dyrektywa nr 95/46/WE, jak i jej Protokół dodatkowy z dnia 8 listopada 2001 r. dotyczący organów nadzorczych oraz transgranicznych przepływów danych, uwzględniając też rekomendacje Komitetu Ministrów dla państw członkowskich, w szczególności rekomendację nr R(87) 15 dotyczącą ochrony danych osobowych wykorzystywanych w sektorze policji oraz rekomendację CM/Rec(2010)13 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych w kontekście profilowania,

– uwzględniając wytyczne dotyczące regulacji odnoszących się do elektronicznych banków danych ogłoszone przez Zgromadzenie Ogólne ONZ w 1990 r.,

– uwzględniając komunikat Komisji dla Parlamentu, Rady, Europejskiego Komitetu

---

[1] Dz.U. L 281 z 23.11.1995, s. 31.
[2] Dz.U. L 350 z 30.12.2008, s. 60.
[3] Dz.U. L 8 z 12.1.2001, s. 1.
[4] Dz.U. L 201 z 31.7.2002, s. 37.

Ekonomiczno-Społecznego i Komitetu Regionów pod tytułem „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej” (COM(2010)0609),

– uwzględniając konkluzje Rady dotyczące komunikatu Komisji zatytułowanego „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej”[1],

– uwzględniając opinię Europejskiego Inspektora Ochrony Danych (EIOD) z dnia 14 stycznia 2011 r. dotyczącą komunikatu Komisji zatytułowanego „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej”,

– uwzględniając wspólny wkład grupy roboczej art. 29 ds. ochrony danych oraz grupy roboczej ds. policji i wymiaru sprawiedliwości dotyczący konsultacji Komisji Europejskiej w sprawie ram prawnych odnoszących się do podstawowego prawa ochrony danych osobowych, zatytułowany „Przyszłość prywatności”[2],

– uwzględniając opinię nr 8/2010 grupy roboczej art. 29 ds. ochrony danych, odnoszącą się do stosowanego prawa[3],

– uwzględniając swoje poprzednie rezolucje w sprawie ochrony danych, a także rezolucję w sprawie programu sztokholmskiego[4],

– uwzględniając art. 48 Regulaminu,

– uwzględniając sprawozdanie Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych oraz opinie Komisji Przemysłu, Badań Naukowych i Energii, Komisji Rynku Wewnętrznego i Ochrony Konsumentów, Komisji Kultury i Edukacji oraz Komisji Prawnej (A7-0244/2011),

A. mając na uwadze, że dyrektywa w sprawie ochrony danych 95/46/WE i dyrektywa pakietu telekomunikacyjnego UE 2009/140/WE umożliwiają swobodny przepływ danych osobowych na rynku wewnętrznym,

B. mając na uwadze, że przepisy o ochronie danych stały się w UE, państwach członkowskich i poza ich granicami tradycją prawną, którą należy podtrzymywać i dalej rozwijać,

C. mając na uwadze, że choć podstawowe założenia dyrektywy 95/46/WE są nadal aktualne, widać różne podejścia przyjmowane przy ich wdrażaniu i egzekwowaniu w państwach

---

[1] Posiedzenie nr 3071 Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych w Brukseli w dniach 24 i 25 lutego 2011 r., dokument dostępny pod linkiem http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/119461.pdf.

[2] 02356/09/EN WP 168.

[3] 0836/10/EN WP 179.

[4] Na przykład: stanowisko Parlamentu Europejskiego z dnia 23 września 2008 r. w sprawie projektu wniosku dotyczącego decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (Dz.U. C 8 E z 14.1.2010, s. 138); zalecenie Parlamentu Europejskiego z dnia 26 marca 2009 r. dla Rady w sprawie utrwalenia bezpieczeństwa i podstawowych wolności w Internecie (Dz.U. C 117 E z 6.5.2010, s. 206); rezolucja Parlamentu Europejskiego z dnia 25 listopada 2009 r. w sprawie komunikatu Komisji do Parlamentu Europejskiego i Rady: „Przestrzeń wolności, bezpieczeństwa i sprawiedliwości w służbie obywateli – program sztokholmski” (Dz.U. C 285 E z 21.10.2010, s. 12).

członkowskich; mając na uwadze, że UE musi posiadać – po kompleksowej ocenie oddziaływania – całościowe, spójne, nowoczesne i wysokiego szczebla ramy regulacyjne umożliwiające skuteczną ochronę podstawowych praw obywateli, w szczególności ich prywatności, w odniesieniu do jakiegokolwiek przetwarzania danych osobowych jednostek w UE i poza jej granicami w każdych okolicznościach, w celu sprostania licznym wyzwaniom w zakresie ochrony danych, na przykład wyzwaniom spowodowanym globalizacją, rozwojem technologicznym, coraz popularniejszą aktywnością online, zastosowaniami związanymi z coraz szerszymi rodzajami działalności i obawami związanymi z bezpieczeństwem (tj. walką z terroryzmem); mając na uwadze, że takie ramy ochrony danych osobowych mogą zwiększyć pewność prawną, zredukować do minimum obciążenie administracyjne, zagwarantować równe szanse wszystkim podmiotom gospodarczym, stymulować wspólny rynek cyfrowy oraz zwiększyć bezpieczeństwo i zaufanie do zachowania administratorów danych i organów wykonawczych,

D. mając na uwadze, że naruszanie przepisów o ochronie danych może spowodować poważne zagrożenie praw podstawowych przysługujących jednostkom i wartości państw członkowskich, do tego stopnia, że Unia i państwa członkowskie będą zobowiązane do podjęcia skutecznych działań przeciwko takim naruszeniom; mając na uwadze, że takie naruszanie prowadzi do braku zaufania obywateli, co z kolei osłabia celowe wykorzystywanie nowych technologii; mając też na uwadze, że niewłaściwe wykorzystanie i nadużywanie danych osobowych powinno w związku z tym podlegać właściwym, surowym i odstraszającym sankcjom, w tym sankcjom karnym,

E. mając na uwadze, że inne właściwe prawa podstawowe zapisane w Karcie praw podstawowych oraz inne cele wyznaczone w Traktatach, takie jak prawo do wolności wypowiedzi i informacji oraz zasada przejrzystości, muszą zostać w pełni uwzględnione w działaniach na rzecz zagwarantowania podstawowego prawa do ochrony danych osobowych,

F. mając na uwadze, że nowa podstawa prawna z art. 16 TFUE, a także uznanie prawa do ochrony danych osobowych z art. 8 Karty praw podstawowych oraz prawa do poszanowania życia prywatnego i rodzinnego z art. 7 Karty praw podstawowych za prawa autonomiczne koniecznie wymaga całościowego podejścia do ochrony danych we wszystkich obszarach, w których przetwarzane są dane osobowe, w tym w dziedzinie współpracy policyjnej i sądowej w sprawach karnych, w dziedzinie wspólnej polityki zagranicznej i bezpieczeństwa (WPZiB) – bez uszczerbku dla konkretnych przepisów określonych w art. 39 TUE – oraz w dziedzinie przetwarzania danych przez instytucje i organy UE,

G. mając na uwadze, że podczas rozpatrywania rozwiązań legislacyjnych należy koniecznie uwzględnić szereg istotnych elementów, takich jak skuteczna i efektywna ochrona, udzielana w każdych okolicznościach i niezależnie od preferencji politycznych w określonym przedziale czasu; mając na uwadze, że ramy regulacyjne muszą charakteryzować się długookresową stabilnością, a wprowadzanie ograniczeń w wykonywaniu prawa do ochrony – jeżeli okaże się konieczne – musi być sporadyczne, zgodne z prawem, ściśle konieczne i proporcjonalne i nigdy nie może wpływać na zasadnicze elementy samego prawa,

H. mając na uwadze, że gromadzenie, analiza, wymiana, niewłaściwe wykorzystanie danych oraz niebezpieczeństwo „profilowania”, możliwe dzięki rozwojowi technologicznemu,

osiągnęły bezprecedensowe rozmiary i w związku z tym wymagają surowych przepisów chroniących dane, takich jak określenie prawa właściwego i zdefiniowanie obowiązków wszystkich zainteresowanych stron jeśli chodzi o stosowanie unijnego prawodawstwa w zakresie ochrony danych; mając na uwadze, że przedsiębiorstwa i sektor handlowy coraz częściej wykorzystują karty stałego klienta (karty do klubów, karty rabatowe, lojalnościowe itp.), które służą lub mogą służyć do tworzenia profili klientów,

I. mając na uwadze, że obywatele nie dokonują zakupów w internecie tak samo bezpiecznie jak poza nim, z powodu obaw o kradzież tożsamości i braku przejrzystości co do sposobu, w jaki ich dane osobowe są przetwarzane i wykorzystywane,

J. mając na uwadze, że technologia umożliwia w coraz większym stopniu, niezależnie od miejsca i czasu, tworzenie, przesyłanie, przetwarzanie i magazynowanie danych osobowych w wielu różnych formach, oraz mając na uwadze, że w tym kontekście sprawą najwyższej wagi jest, by osoby, których dane dotyczą, miały rzeczywistą kontrolę nad własnymi danymi,

K. mając na uwadze, że podstawowe prawo do ochrony danych oraz prywatności obejmuje ochronę osób przed ewentualną inwigilacją oraz nadużywaniem ich danych przez same państwo, a także podmioty prywatne,

L. mając na uwadze, że zapewnienie prywatności i bezpieczeństwa jest możliwe i że obydwie kwestie mają dla obywateli kluczowe znaczenie, co oznacza, że nie trzeba wybierać pomiędzy prywatnością a bezpieczeństwem,

M. mając na uwadze, że na szczególną ochronę zasługują dzieci, które mogą być w mniejszym stopniu świadome zagrożeń, konsekwencji, gwarancji i praw w związku z przetwarzaniem danych osobowych; mając na uwadze, że młodzi ludzie ujawniają swoje dane osobowe w różnego rodzaju sieciach społecznych, które mnożą się coraz szybciej w internecie,

N. mając na uwadze, że skuteczna kontrola przez osoby, których dane dotyczą, oraz krajowe organy ochrony danych wymaga przejrzystego zachowania administratorów danych,

O. mając na uwadze, że nie wszyscy administratorzy danych prowadzą działalność internetową i że w związku z tym nowe przepisy o ochronie danych muszą obejmować środowisko zarówno internetowe, jak i pozainternetowe, z jednoczesnym uwzględnieniem ewentualnych różnic pomiędzy tymi środowiskami,

P. mając na uwadze, że krajowe organy ochrony danych podlegają przepisom, które znacznie różnią się w 27 państwach członkowskich, w szczególności w odniesieniu do ich statusu, zasobów i kompetencji,

Q. mając na uwadze, że silny europejski i międzynarodowy system ochrony danych jest niezbędną podstawą dla transgranicznego przepływu danych osobowych, mając też na uwadze, że obecne różnice w prawodawstwach z zakresu ochrony danych oraz ich egzekwowania oddziałują na ochronę praw podstawowych i wolności obywatelskich, pewność prawną i przejrzystość w stosunkach umownych, rozwój handlu elektronicznego i e-biznesu, zaufanie konsumentów do systemu, transakcje ponadgraniczne, globalną gospodarkę oraz jednolity rynek europejski; mając w tym kontekście na uwadze, że wymiana danych jest istotna z perspektywy umożliwienia i zapewnienia bezpieczeństwa publicznego na szczeblu lokalnym i międzynarodowym; mając na uwadze, że konieczność,

proporcjonalność, celowość, nadzór i adekwatność są warunkami wstępnymi takiej wymiany,

R. mając na uwadze, że obecne przepisy i warunki regulujące przekazywanie danych z UE do państw trzecich doprowadziły do stosowania różnych podejść i praktyk w różnych państwach członkowskich; mając na uwadze, że konieczne jest, by prawa podmiotów, których dane dotyczą, były w pełni szanowane w krajach trzecich, do których dane osobowe są przekazywane i w których się je przetwarza,

Pełne zaangażowanie charakteryzujące się całościowym podejściem

1. bardzo przychylnie odnosi się do komunikatu Komisji zatytułowanego „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej" oraz przyjętego w nim podejścia, skupiającego się na wzmocnieniu istniejących rozwiązań, przedstawieniu nowych zasad i mechanizmów oraz zapewnieniu spójności i wysokich standardów ochrony danych w kontekście zapewnionym wejściem w życie Traktatu z Lizbony (art. 16 TFUE), a obecnie także prawnie wiążącą Karta praw podstawowych, w szczególności jej art. 8;

2. podkreśla, że normy i zasady określone w dyrektywie 95/46/WE stanowią idealny punkt wyjścia i należy dalej nad nimi pracować, rozszerzać je i wdrażać, czyniąc z nich element nowoczesnego prawa ochrony danych;

3. podkreśla znaczenie art. 9 dyrektywy 95/46/WE, która zobowiązuje państwa członkowskie do przedstawienia odstępstw od przepisów o ochronie danych w sytuacjach, w których dane osobowe są wykorzystywane wyłącznie do celów dziennikarskich lub w celu uzyskania wyrazu artystycznego lub literackiego; wzywa w tym kontekście Komisję do zagwarantowania, że odstępstwa te zostaną zachowane i że podjęte zostaną wszelkie starania w celu oceny potrzeby zwiększenia zakresu tych odstępstw w świetle wszelkich nowych przepisów, tak by chronić wolność prasy;

4. podkreśla, że podejście neutralne technologicznie, określone w dyrektywie 95/46/WE, należy zachować jako zasadę opracowywania nowych ram;

5. uznaje, że rozwój technologiczny z jednej strony przyczynił się do wystąpienia nowych zagrożeń dla ochrony danych osobowych, zaś z drugiej strony doprowadził do znacznego wzrostu wykorzystania technologii informacyjnych w celach związanych z codziennością i zazwyczaj nieszkodliwych oraz że rozwój ten oznacza, że konieczne jest przeprowadzenie szczegółowej oceny obecnie obowiązujących przepisów o ochronie danych w celu zapewnienia, że przepisy te (i) nadal będą gwarantowały wysoki poziom ochrony, (ii) nadal będą sprzyjały osiągnięciu równowagi pomiędzy prawem do ochrony danych osobowych a prawem do wolności wypowiedzi i informacji oraz (iii) nie będą niepotrzebnie utrudniać codziennego przetwarzania danych osobowych, które zazwyczaj jest nieszkodliwe;

6. uważa, że niezbędne jest rozszerzenie stosowania ogólnych przepisów o ochronie danych na obszar współpracy policyjnej i wymiarów sprawiedliwości, w tym przetwarzanie danych na szczeblu krajowym, ze szczególnym uwzględnieniem tendencji systematycznego ponownego wykorzystywania danych osobowych w sektorze prywatnym na potrzeby egzekwowania prawa, zapewniając równocześnie, w razie absolutnej konieczności oraz tam, gdzie to stosowne w społeczeństwie demokratycznym, ściśle dostosowane i zharmonizowane ograniczenia dotyczące niektórych praw do ochrony danych obywateli;

7. podkreśla potrzebę ujęcia przetwarzania danych przez instytucje i organy Unii Europejskiej, uregulowanego na mocy rozporządzenia (WE) nr 45/2001, w zakresie nowych ram;

8. uznaje, że może zaistnieć potrzeba zastosowania dodatkowych i ulepszonych środków w celu określenia, w jaki sposób ogólne zasady określone wszechstronnymi ramami mają zastosowanie do działań i przetwarzania danych w konkretnych sektorach, tak jak miało to już miejsce w przypadku dyrektywy o prywatności elektronicznej, lecz nalega, by takie przepisy sektorowe w żadnym wypadku nie zmniejszały poziomu ochrony przewidzianej w prawodawstwie ramowym, lecz by określały szczegółowo wyjątkowe, konieczne, uzasadnione i ściśle dostosowane odstępstwa od ogólnych zasad dotyczących ochrony danych;

9. wzywa Komisję do zapewnienia, że obecny przegląd prawodawstwa UE z zakresu ochrony danych umożliwi:

   – pełną harmonizację na najwyższym szczeblu zapewniającą pewność prawa oraz jednolity i wysoki standard ochrony jednostek w każdych okolicznościach,

   – dalsze doprecyzowanie zasad dotyczących prawa właściwego w celu zapewnienia jednolitego poziomu ochrony jednostkom niezależnie od geograficznej lokalizacji administratora danych, również wtedy, gdy konieczne jest egzekwowanie zasad ochrony danych przez władze bądź na drodze sądowej;

10. jest zdania, że zmieniony system ochrony danych, przy jednoczesnym pełnym egzekwowaniu praw do prywatności i ochrony danych, powinien ograniczyć do minimum obciążenie biurokratyczne i finansowe oraz zaoferować instrumenty, które umożliwiają funkcjonowanie jako przedsiębiorców w związkach postrzeganych jako całość, a nie jako różnego rodzaju przedsiębiorstwa jednoosobowe; zachęca Komisję do przeprowadzenia ocen wpływu i dokonania szczegółowej oceny kosztów związanych z przedsięwzięciem nowych środków;

Wzmocnienie praw jednostki

11. wzywa Komisję do wzmocnienia obowiązujących zasad i założeń, takich jak przejrzystość, minimalizacja danych i celowość, świadoma, uprzednia i wyraźna zgoda, zawiadamianie o naruszeniu ochrony danych oraz prawa przysługujące osobom, których dane dotyczą, jak określono w dyrektywie 95/46/WE, przez co poprawi się ich wprowadzenie w życie w państwach członkowskich, w szczególności w odniesieniu do „globalnego środowiska internetowego”;

12. podkreśla fakt, że zgodę należy uznać za ważną wyłącznie wówczas, gdy jest jednoznaczna, świadoma, udzielona dobrowolnie, konkretna i wyraźna, oraz to, że należy wprowadzić w życie odpowiednie mechanizmy rejestracji zgody użytkowników lub jej cofnięcia;

13. zwraca uwagę na to, że dobrowolna zgoda nie może być wydawana w odniesieniu do umów o pracę;

14. wyraża zaniepokojenie w odniesieniu do nadużyć związanych z internetową reklamą behawioralną i przypomina, że dyrektywa w sprawie prywatności i łączności elektronicznej

nakłada obowiązek wyraźnego i uprzedniego przyzwolenia osoby, której to dotyczy, na przesyłanie jej plików typu cookie oraz obserwowanie jej późniejszego zachowania w sieci w celu przesyłania jej spersonalizowanych ogłoszeń;

15. całkowicie popiera wprowadzenie w życie ogólnej zasady przejrzystości, a także wykorzystywanie technologii zwiększających przejrzystość oraz opracowywanie standardowych oświadczeń o ochronie prywatności, umożliwiających jednostkom sprawowanie kontroli nad danymi, które ich dotyczą; podkreśla, że informacja dotycząca przetwarzania danych musi być dostępna w jasnym i prostym języku oraz w sposób łatwo zrozumiały i dostępny.

16. podkreśla też znaczenie poprawy środków egzekwowania i świadomości prawa dostępu do danych, ich prostowania, likwidacji oraz zablokowania, a także znaczenie szczegółowego wyjaśnienia i skodyfikowania „prawa do zostania zapomnianym”[1] oraz umożliwienia przenoszalności danych[2], przy jednoczesnym zapewnieniu pełnego rozwoju i wdrożenia możliwości technicznych i organizacyjnych na potrzeby wykonania tych praw; podkreśla, że jednostki muszą mieć wystarczającą kontrolę nad swymi danymi online, by móc w odpowiedzialny sposób korzystać z internetu;

17. podkreśla, że obywatele muszą być w stanie bezpłatnie korzystać ze swych praw do danych; wzywa przedsiębiorstwa do powstrzymania się od wszelkich prób stawiania zbytecznych przeszkód w korzystaniu z prawa do dostępu, zmiany lub usuwania danych osobowych; podkreśla, że osoba, której dane dotyczą, musi w każdym momencie móc dowiedzieć się, które dane są przechowywane przez kogo, kiedy, w jakim celu, na jaki okres oraz w jaki sposób są one przetwarzane; podkreśla, że osoby, których dane dotyczą, muszą mieć możliwość likwidacji danych, ich zmiany lub zablokowania w sposób niebiurokratyczny oraz że muszą być poinformowane o każdym przypadku niewłaściwego wykorzystania danych lub ich naruszenia; domaga się również, aby dane musiały być ujawniane na żądanie zainteresowanej osoby oraz usuwane najpóźniej z chwilą, gdy osoba ta o to wystąpi; podkreśla konieczność jasnego komunikowania osobom, których dotyczą dane, poziomu ochrony danych w krajach trzecich; podkreśla, że prawo dostępu obejmuje nie tylko pełny dostęp do przetworzonych danych dotyczących własnej osoby, łącznie ze źródłem tych danych i ich odbiorcami, lecz również zrozumiałe informacje na temat logicznego udziału we wszelkich procesach automatycznego przetwarzania danych; podkreśla, że przetwarzanie automatyczne będzie stawało się coraz to ważniejsze w związku z profilowaniem i eksploracją danych;

18. zwraca uwagę, że tworzenie profili to jedna z głównych tendencji w świecie cyfrowym, ze względu na rosnące znaczenie sieci społecznościowych oraz zintegrowanych modeli przedsiębiorstw internetowych; wzywa zatem Komisję do włączenia przepisów dotyczących tworzenia profili, a także do jasnego zdefiniowania pojęć „profilu” i „tworzenia profilu”;

19. podkreśla potrzebę zwiększenia obowiązków administratorów danych związanych

---

[1] Należy w sposób jasny i precyzyjny określić wszystkie istotne elementy tego prawa.

[2] Przenoszenie danych osobowych ułatwi sprawne funkcjonowanie zarówno rynku wewnętrznego, jak i internetu i jego charakterystycznej otwartości i interoperacyjności.

z udzielaniem informacji osobom, których dane dotyczą, i przychylnie odnosi się do faktu, że w komunikacie skupiono się na działaniach uświadamiających skierowanych do ogółu społeczeństwa, a konkretniej do młodych ludzi; podkreśla konieczność szczególnego traktowania osób podatnych na zagrożenia, zwłaszcza dzieci i osób starszych; zachęca różne strony do podejmowania takich działań uświadamiających i popiera wniosek Komisji dotyczący współfinansowania z budżetu Unii środków uświadamiających dotyczących ochrony danych; proponuje skuteczne rozpowszechnianie na szczeblu państw członkowskich informacji na temat praw i obowiązków osób fizycznych i przedsiębiorstw w zakresie zbierania, przetwarzania, przechowywania i przesyłania danych osobowych;

20. przypomina o konieczności zapewnienia specjalnej ochrony osobom znajdującym się w trudnej sytuacji, a w szczególności dzieciom, między innymi poprzez zapewnienie wysokiego poziomu ochrony danych jako standardowego wymogu oraz wprowadzenie właściwych dostosowanych środków w celu ochrony ich danych osobowych;

21. podkreśla potrzebę opracowania takiego prawodawstwa z zakresu ochrony danych, które uwzględniałoby szczególną potrzebę ochrony dzieci i małoletnich oraz podkreśla, że umiejętność korzystania z mediów musi stać się elementem edukacji formalnej, tak aby nauczyć dzieci i małoletnich odpowiedzialnego funkcjonowania w środowisku internetowym; w tym celu należy zwrócić szczególną uwagę na przepisy odnoszące się do gromadzenia i dalszego przetwarzania danych dzieci, wzmocnienie zasady celowości w odniesieniu do danych dzieci oraz sposobów pozyskiwania zgody dzieci, a także na ochronę przed reklamą behawioralną[1];

22. popiera dalsze wyjaśnienia i wzmocnienie gwarancji dotyczących przetwarzania danych szczególnie chronionych i wzywa do zastanowienia się nad potrzebą uwzględnienia nowych kategorii, takich jak dane genetyczne i biometryczne, zwłaszcza w kontekście zmian technologicznych (np. „przetwarzanie w chmurze”) i społecznych;

23. podkreśla, że dane osobowe dotyczące sytuacji zawodowej użytkownika, w których posiadaniu jest pracodawca, nie mogą być ujawniane ani przekazywane osobom trzecim bez uprzedniej zgody zainteresowanego;

Zwiększenie wymiaru związanego z rynkiem wewnętrznym oraz skuteczniejsze egzekwowanie przepisów o ochronie danych

24. zauważa, że ochrona danych na rynku wewnętrznym powinna odgrywać coraz większą rolę i podkreśla, że skuteczna ochrona prawa do prywatności ma podstawowe znaczenie dla pozyskania zaufania konsumentów, które jest konieczne, by został uwolniony pełen potencjał wzrostu jednolitego rynku cyfrowego; przypomina Komisji, że warunkiem wstępnym osiągnięcia jednolitego rynku cyfrowego jest konieczność przyjęcia wspólnych zasad i przepisów tak dla towarów, jak i usług, gdyż usługi stanowią ważny składnik rynku cyfrowego;

25. ponownie wzywa Komisję do wyjaśnienia przepisów dotyczących prawa właściwego

[1] Można rozważyć kwestię limitu wiekowego dla dzieci, poniżej którego konieczne jest uzyskanie zgody rodzica, oraz mechanizmy sprawdzania wieku.

w dziedzinie ochrony danych osobowych;

26. uważa, że podstawową sprawą jest wzmocnienie obowiązków administratorów danych w celu zapewnienia zgodności z prawodawstwem w dziedzinie ochrony danych poprzez zastosowanie między innymi proaktywnych mechanizmów i procedur, i z zadowoleniem przyjmuje inne wytyczne zasugerowane w komunikacie Komisji;

27. przypomina, że w tym kontekście szczególną uwagę należy poświęcić administratorom danych, na których ciąży obowiązek zachowania tajemnicy zawodowej, oraz że w ich przypadku należy zastanowić się nad opracowaniem specjalnych struktur służących kontroli ochrony danych;

28. z zadowoleniem przyjmuje i popiera rozważania Komisji dotyczące wprowadzenia zasady odpowiedzialności, ponieważ ma ona kluczowe znaczenie dla zapewnienia odpowiedzialnego postępowania administratorów danych; jednocześnie wzywa Komisję do szczegółowego zbadania sposobów praktycznego wdrożenia tego typu zasady i oceny jej skutków;

29. przychylnie odnosi się do możliwości obowiązkowego mianowania inspektora ochrony danych w każdej organizacji, ponieważ z doświadczeń tych państw członkowskich UE, które już wyznaczyły inspektora ochrony danych, wynika, że koncepcja ta sprawdza się w praktyce; wskazuje jednak, że musi to podlegać ostrożnej ocenie w przypadku małych przedsiębiorstw i mikroprzedsiębiorstw w celu uniknięcia nakładania na te przedsiębiorstwa nadmiernych kosztów bądź obciążeń;

30. w tym kontekście również przychylnie odnosi się do starań na rzecz uproszczenia i ujednolicenia obecnego systemu powiadamiania;

31. za bardzo istotne uważa wprowadzenie obowiązku dokonywania ocen wpływu na prywatność w celu zidentyfikowania zagrożeń prywatności, przewidywania problemów i znajdowania proaktywnych rozwiązań;

32. uważa, że kwestią najwyższej wagi jest egzekwowalność praw przysługujących osobom, których dane dotyczą; odnotowuje, że można by wprowadzić procesy z powództwa zbiorowego jako narzędzia, dzięki którym osoby prywatne broniłyby zbiorowo swych praw w zakresie danych i dochodziły zwrotu odszkodowań z tytułu naruszenia ochrony danych osobowych; zauważa jednak, że wszelkie takie wprowadzenie zawsze musi podlegać ograniczeniom uniemożliwiającym ich nadużywanie; wzywa Komisję do sprecyzowania związku między wspomnianym komunikatem o ochronie danych a obecnie prowadzonymi publicznymi konsultacjami w sprawie roszczeń zbiorowych; wzywa w tym kontekście do opracowania mechanizmu dochodzenia roszczeń zbiorowych w związku z naruszaniem przepisów o ochronie danych w celu umożliwienia osobom, których dane dotyczą, uzyskania odszkodowania za poniesione szkody;

33. podkreśla konieczność właściwego i jednolitego stosowania przepisów w całej UE; wzywa Komisję do przewidzenia w swoim wniosku ustawodawczym surowych i odstraszających sankcji za niewłaściwe wykorzystanie i nadużywanie danych osobowych, w tym sankcji karnych;

34. zachęca Komisję do wprowadzenia ogólnego systemu obowiązkowego zawiadamiania o naruszeniu ochrony danych osobowych oraz objęcia nim, oprócz sektora

telekomunikacyjnego, również innych sektorów, przy jednoczesnym zapewnieniu, że (a) system ten nie stanie się rutynowym ostrzeżeniem przed wszelkiego rodzaju naruszeniami, lecz dotyczyć będzie przede wszystkich takich naruszeń, które mogą wywrzeć negatywny wpływ na jednostki, oraz że (b) wszystkie naruszenia – bez wyjątku – będą rejestrowane i udostępniane organom ochrony danych lub innym właściwym organom na potrzeby i kontroli i oceny, przez co zapewnione zostaną równe szanse i jednolita ochrona dla wszystkich obywateli;

35. jest zdania, że koncepcje poszanowania prywatności od samego początku (ang. „privacy by design") oraz prywatności jako opcji domyślnej (ang. „privacy by default") stanowią wzmocnienie systemu ochrony danych oraz ich praktyczne zastosowanie i dalszy rozwój, jak i konieczność wspierania stosowania technologii podnoszących poziom ochrony prywatności; podkreśla, jak konieczne jest, by każde wdrożenie prywatności od samego początku („privacy by design") opierało się na porządnym i konkretnym kryterium oraz definicjach w celu ochrony prawa użytkowników do prywatności i ochrony danych oraz zapewnienia pewności prawnej, przejrzystości, równych szans i swobodnego przepływu; uważa, że „poszanowanie prywatności od etapu koncepcji" powinno się opierać na zasadzie minimalizacji danych, rozumiejąc przez to, że wszystkie produkty, usługi i systemy powinny być tworzone w taki sposób, by gromadzono, wykorzystywano i przekazywano wyłącznie dane osobowe absolutnie konieczne do ich funkcjonowania;

36. zauważa, że rozwój i szersze stosowanie obliczania rozproszonego (ang. „cloud computing") stawia przed nami nowe wyzwania w zakresie prywatności i ochrony danych osobowych; w związku z tym apeluje o jasne przedstawienie możliwości administratorów danych i przetwarzających dane oraz hostów, aby lepiej podzielić między nich spoczywające na nich zobowiązania prawne oraz aby zapewnić, że osoby, których dotyczą dane, wiedziały gdzie są one przechowywane, kto ma do nich dostęp, kto decyduje o sposobie ich wykorzystania oraz o istniejących systemach tworzenia zapasowych kopii danych i ich odzyskiwania;

37. wzywa zatem Komisję, aby podczas przeglądu dyrektywy 95/46/WE należycie uwzględniła kwestie ochrony prywatności dotyczące obliczania rozproszonego oraz zapewniła, że przepisy dotyczące ochrony danych będą miały zastosowanie do wszystkich zainteresowanych stron, w tym operatorów sieci telekomunikacji i nie tylko;

38. apeluje do Komisji, by zagwarantowała większe poczucie odpowiedzialności użytkowników internetu za kwestię danych osobowych i nalega w szczególności, aby agencje reklamowe i wydawcy wyraźnie informowali internautów, przed gromadzeniem dotyczących ich danych, o zamiarze zgromadzenia tych informacji;

39. z zadowoleniem przyjmuje nowo podpisane porozumienie w sprawie ram oceny oddziaływania ochrony prywatności i danych dla zastosowań związanych z identyfikacją radiową (RFID), które dąży do zapewnienia konsumentom prywatności, zanim na rynku zostaną wprowadzone identyfikatory RFID;

40. popiera starania na rzecz dalszego rozwijania inicjatyw samoregulacyjnych – takich jak kodeksy postępowania – i opowiada się za zastanowieniem się nad ustanowieniem dobrowolnych systemów certyfikacji na szczeblu UE jako działań uzupełniających środki legislacyjne, przy jednoczesnym zapewnieniu, że system ochrony danych na szczeblu UE nadal będzie opierał się na przepisach określających gwarancje na wysokim poziomie; zwraca się do Komisji, aby przeprowadziła ocenę wpływu inicjatyw samoregulacyjnych

jako narzędzi umożliwiających lepsze egzekwowanie przepisów o ochronie danych;

41. uważa, że wszelka certyfikacja czy też program stosowania marki ochrony musi być spójny i wiarygodny, neutralny pod względem technologicznym, uznawany na całym świecie i przystępny cenowo, aby nie tworzyć barier blokujących udział;

42. popiera dalsze wyjaśnienie, wzmocnienie i ujednolicenie statusu i uprawnień krajowych organów ochrony danych, jak i badanie sposobów zapewnienia bardziej jednolitego stosowania unijnych zasad ochrony danych na całym rynku wewnętrznym; podkreśla też znaczenie zapewnienia spójności między uprawnieniami EIOD, krajowych organów odpowiedzialnych za ochronę danych oraz grupy roboczej utworzonej na mocy art. 29;

43. podkreśla, że w tym kontekście należy wzmocnić rolę i kompetencje grupy roboczej art. 29 w celu poprawy koordynacji i współpracy pomiędzy organami ochrony danych funkcjonującymi w państwach członkowskich, zwłaszcza w odniesieniu do potrzeby zapewnienia jednolitego stosowania przepisów o ochronie danych;

44. wzywa Komisję do wyjaśnienia w nowych ramach prawnych kluczowego pojęcia niezależności krajowych organów ochrony danych w kontekście braku jakichkolwiek wpływów zewnętrznych[1]; podkreśla, że krajowym organom ochrony danych należy dać konieczne zasoby oraz nadać im jednolite kompetencje do prowadzenia dochodzeń i nakładania sankcji;

Wzmocnienie całościowego podejścia do ochrony danych

45. wzywa Komisję do udoskonalenia i wzmocnienia bieżących procedur międzynarodowego przekazywania danych – prawnie wiążących umów i wiążących reguł korporacyjnych – oraz określenia, na podstawie wyżej wymienionych zasad ochrony danych osobowych, zasadniczych ambitnych aspektów unijnej ochrony danych, do wykorzystania w umowach międzynarodowych; podkreśla, że porozumienia UE z państwami trzecimi w zakresie wymiany danych osobowych muszą zapewniać obywatelom Unii Europejskiej taki sam poziom ochrony danych osobowych jak w Unii Europejskiej;

46. jest zdania, że procedura badania adekwatności przez Komisję zyskałaby na dalszym uszczegółowieniu, ściślejszym wdrożeniu, egzekwowaniu i monitorowaniu oraz że należy lepiej sprecyzować kryteria i wymogi w zakresie oceny poziomu ochrony danych w kraju trzecim lub organizacji międzynarodowej z uwzględnieniem nowych zagrożeń prywatności i danych osobowych;

47. wzywa Komisję do dokonania szczegółowej oceny skuteczności i prawidłowego stosowania zasad bezpiecznego transferu danych osobowych;

48. z zadowoleniem przyjmuje stanowisko Komisji w sprawie wzajemności w poziomie ochrony danych osób, których dane są eksportowane do krajów trzecich lub w nich przechowywane; wzywa Komisję do podjęcia decydujących kroków w kierunku zacieśnienia współpracy regulacyjnej z krajami trzecimi z myślą o wyjaśnieniu prawa właściwego i spójności ustawodawstwa UE i krajów trzecich w zakresie ochrony danych; wzywa Komisję do priorytetowego potraktowania tego zagadnienia w ramach ponownie wznowionej Transatlantyckiej Rady Gospodarczej;

[1] Zgodnie z art. 16 TFUE i art. 8 Karty.

49. popiera starania Komisji dotyczące zacieśnienia współpracy z krajami trzecimi i organizacjami międzynarodowymi, w tym ONZ, Radą Europy i OECD, jak i innymi organizacjami normalizacyjnymi, takimi jak Europejski Komitet Normalizacyjny (CEN), Międzynarodowa Organizacja Normalizacyjna (ISO), konsorcjum World Wide Web (W3C) i grupa zadaniowa ds. inżynierii internetowej (IETF); zachęca do rozwijania międzynarodowych standardów[1] przy jednoczesnym zapewnieniu spójności między inicjatywami na rzecz standardów międzynarodowych a obecnymi przeglądami w UE, OECD i Radzie Europy;

o

o o

50. zobowiązuje swojego przewodniczącego do przekazania niniejszej rezolucji Radzie i Komisji.

[1] Por. deklaracja madrycka: ogólnoświatowe standardy w globalnym świecie, październik 2009 r. oraz rezolucja w sprawie standardów międzynarodowych przyjęta przez XXXII Międzynarodową Konferencję Rzeczników Ochrony Danych Osobowych i Prywatności, Jerozolima, 27-29 października 2010 r.