RADA UNII EUROPEJSKIEJ

Bruksela, 27 stycznia 2012 r. (13.02)
(OR. en)

5852/12

DATAPROTECT 8
JAI 43
MI 57
DRS 10
DAPIX 11
FREMP 6

PISMO PRZEWODNIE

Od:	Sekretarz Generalny Komisji Europejskiej, podpisał dyrektor Jordi AYET PUIGARNAU
Data otrzymania:	27 stycznia 2012 r.
Do:	Uwe CORSEPIUS, Sekretarz Generalny Rady Unii Europejskiej
Nr dok. Kom.:	COM(2012) 9 final
Dotyczy:	Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów Ochrona prywatności w połączonym świecie – europejskie ramy ochrony danych w XXI wieku

Delegacje otrzymują w załączeniu dokument Komisji COM(2012) 9 final.

Zał.: COM(2012) 9 final

KOMISJA EUROPEJSKA

Bruksela, dnia 25.1.2012 r.
COM(2012) 9 final

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO, RADY, EUROPEJSKIEGO KOMITETU EKONOMICZNO-SPOŁECZNEGO I KOMITETU REGIONÓW

Ochrona prywatności w połączonym świecie – europejskie ramy ochrony danych w XXI wieku

(Tekst mający znaczenie dla EOG)

[…]

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO, RADY, EUROPEJSKIEGO KOMITETU EKONOMICZNO-SPOŁECZNEGO I KOMITETU REGIONÓW

Ochrona prywatności w połączonym świecie – europejskie ramy ochrony danych w XXI wieku

(Tekst mający znaczenie dla EOG)

1. OBECNE WYZWANIA W ZAKRESIE OCHRONY DANYCH

Szybkie tempo zmian technologicznych oraz globalizacja radykalnie zmieniły sposób zbierania stale rosnącej ilości danych, dostępu do nich, ich wykorzystywania i przekazywania. Nowe metody wymiany informacji poprzez sieci społecznościowe oraz zdalne przechowywanie znacznych ilości danych stało się stałym elementem życia dużej części z 250 milionów użytkowników internetu. Równocześnie dane osobowe stały się cennym aktywem dla wielu przedsiębiorstw. Zbieranie, agregacja i analiza danych potencjalnych klientów stanowi często ważną część ich działalności gospodarczej[1].

W tym nowym środowisku cyfrowym **osoby fizyczne mają prawo do skutecznej kontroli swoich danych osobowych**. Ochrona danych jest w Europie prawem podstawowym, zapisanym w art. 8 Karty praw podstawowych Unii Europejskiej oraz w art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), które musi być należycie chronione.

Brak zaufania sprawia, że konsumenci wahają się, czy kupować w internecie i korzystać z nowych usług. Dlatego wysoki poziom ochrony danych osobowych ma również zasadnicze znaczenie dla zwiększenia zaufania do usług internetowych i wykorzystania potencjału gospodarki cyfrowej, a przez to pobudzenia **wzrostu gospodarczego i zwiększania konkurencyjności przemysłu UE**.

Nowoczesne, spójne przepisy w całej UE są konieczne, aby możliwy był swobodny przepływ danych między państwami członkowskimi. Przedsiębiorstwa potrzebują jasnych i jednolitych przepisów gwarantujących pewność prawa i minimalizujących obciążenia administracyjne. Jest to niezbędne, aby jednolity rynek mógł funkcjonować i **stymulować wzrost gospodarczy i tworzenie miejsc pracy , a także wspierać innowacje.**[2]. Modernizacja unijnych przepisów o ochronie danych, umacniająca ich wymiar dotyczący rynku wewnętrznego, zapewnia wysoki stopień ochrony danych osób fizycznych oraz wspiera pewność prawa, przejrzystość i

---

[1] Rynek analizy bardzo dużych zbiorów danych rozwija się w tempie 40% rocznie w skali ogólnoświatowej: http://www.mckinsey.com/mgi/publications/big_data/.

[2] Zob. również konkluzje Rady Europejskiej z dnia 23 października 2011 r., w których podkreślono „kluczową rolę" jednolitego rynku „w zapewnieniu wzrostu gospodarczego i zatrudnienia", a także potrzebę zakończenia do 2015 r. prac nad jednolitym rynkiem internetowym.

spójność, dlatego odgrywa kluczową rolę w planie działań Komisji Europejskiej służącym realizacji programu sztokholmskiego[3], w Europejskiej agendzie cyfrowej[4] i szerzej – w unijnej strategii na rzecz rozwoju „Europa 2020”[5].

Unijna dyrektywa z 1995 r.[6], będąca głównym instrumentem prawnym w zakresie ochrony danych osobowych w Europie, była przełomowym dokumentem w historii ochrony danych. Nadal aktualne są jej cele polegające na zapewnieniu funkcjonowania jednolitego rynku i skutecznej ochrony praw podstawowych i swobód osób fizycznych. Została ona jednak przyjęta 17 lat temu, kiedy internet dopiero raczkował. W dzisiejszym nowym, wymagającym środowisku cyfrowym istniejące przepisy nie zapewniają wymaganego stopnia harmonizacji ani niezbędnej skuteczności gwarantującej prawo do ochrony danych osobowych. Z tego względu Komisja Europejska proponuje gruntowną reformę unijnych ram ochrony danych.

Ponadto traktat lizboński stworzył w art. 16 TFUE nową podstawę prawną zmodernizowanego i spójnego podejścia do ochrony danych i swobodnego przepływu danych osobowych, obejmującą również współpracę policyjną i współpracę wymiarów sprawiedliwości w sprawach karnych[7]. Podejście to zostało odzwierciedlone w komunikatach Komisji Europejskiej dotyczących programu sztokholmskiego i planu działań służącego realizacji programu sztokholmskiego[8], w których podkreśla się, że Unia powinna „przyjąć pełny system ochrony danych osobowych, obejmujący wszystkie obszary, w których przysługuje jej właściwość” oraz „zagwarantować spójne wykonywanie prawa do ochrony danych, będącego jednym z praw podstawowych”.

Aby w sposób przejrzysty przygotować reformę unijnych ram ochrony danych, Komisja od 2009 r. prowadzi konsultacje społeczne w sprawie ochrony danych[9] oraz zaangażowała się w intensywny dialog z zainteresowanymi podmiotami[10]. W dniu 4 listopada 2010 r. Komisja opublikowała komunikat „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej”[11], w którym nakreślono główne obszary reformy. Od września do grudnia 2011 r. Komisja prowadziła rozszerzony dialog z działającymi w UE krajowymi organami ochrony danych i z Europejskim Inspektorem Ochrony Danych w celu przeanalizowania możliwości

---

3 COM(2010) 171 wersja ostateczna.

4 COM(2010) 245 wersja ostateczna.

5 COM(2010) 2020 wersja ostateczna.

6 Dyrektywa 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz.U. L 281 z 23.11.1995, s. 31.

7 Szczegółowe zasady przetwarzania danych przez państwa członkowskie w dziedzinie wspólnej polityki zagranicznej i bezpieczeństwa ustanawia się decyzją Rady na podstawie art. 39 TUE.

8 Odpowiednio COM(2009) 262 i COM(2010) 171.

9 Przeprowadzono dwie rundy konsultacji społecznych w sprawie reformy przepisów dotyczących ochrony danych: jedną od lipca do grudnia 2009 r. (http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm), a drugą od listopada 2010 r. do stycznia 2011 r. (http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm).

10 Specjalistyczne konsultacje odbyły się w 2010 r. z udziałem przedstawicieli organów państw członkowskich i zainteresowanych podmiotów prywatnych. W listopadzie 2010 r. Viviane Reding, komisarz UE ds. sprawiedliwości, zorganizowała wspólną debatę na temat reformy ochrony danych. Przez cały 2011 r. odbywały się również dedykowane warsztaty i seminaria dotyczące konkretnych zagadnień (np. zgłaszania naruszeń ochrony danych).

11 COM(2010) 609.

bardziej spójnego stosowania unijnych przepisów o ochronie danych we wszystkich państwach członkowskich UE[12].

Rozmowy te pokazały, że zarówno obywatele jak i przedsiębiorstwa chciały, by Komisja w kompleksowy sposób zreformowała unijne przepisy o ochronie danych. Po przeprowadzeniu oceny poszczególnych wariantów politycznych[13] Komisja Europejska proponuje obecnie **solidne i spójne ramy prawne dotyczące wszystkich obszarów polityki UE, wzmacniające prawa osób fizycznych, wymiar jednolitego rynku dotyczący ochrony danych oraz ograniczające obciążenia administracyjne dla przedsiębiorstw**[14]. Komisja proponuje, by nowe ramy prawne obejmowały:

– **rozporządzenie** (zastępujące dyrektywę 95/46/WE) ustanawiające ogólne unijne ramy ochrony danych[15];

– oraz **dyrektywa** (zastępująca decyzję ramową 2008/977/WSiSW[16]) określającą przepisy o ochronie danych osobowych przetwarzanych do celów **zapobiegania przestępstwom, wykrywania ich, prowadzenia dochodzeń w ich sprawie i ścigania ich oraz powiązanych działań sądowych**.

Niniejszy komunikat zawiera opis najważniejszych elementów reformy unijnych ram ochrony danych.

2. UMOŻLIWIENIE OSOBOM FIZYCZNYM KONTROLI SWOICH DANYCH OSOBOWYCH

Na podstawie dyrektywy 95/46/WE – będącej obecnie głównym aktem prawnym UE w dziedzinie ochrony danych – sposoby korzystania przez osoby fizyczne z przysługującego im prawa do ochrony danych nie są wystarczająco zharmonizowane we wszystkich państwach członkowskich. Podobnie uprawnienia krajowych organów odpowiedzialnych za ochronę danych nie są wystarczająco zharmonizowane, aby zapewnić spójne i skuteczne stosowanie obowiązujących

---

12 Zob. pismo Viviane Reding, komisarz UE ds. sprawiedliwości z dnia 19 września 2011 r. do członków Grupy Roboczej Art. 29, opublikowane na stronie: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm.

13 Zob. ocena skutków SEC(2012) 72.

14 Będzie to wiązało się z wprowadzeniem na późniejszym etapie zmian w niektórych aktach prawnych w celu dostosowania instrumentów szczególnych i sektorowych, na przykład rozporządzenia (WE) nr 45/2001, Dz.U. L 8 z 12.1.2001, s. 1.

15 Rozporządzenie to wprowadza również ograniczoną liczbę poprawek technicznych do dyrektywy w sprawie e-prywatności (dyrektywy 2002/58/WE ostatnio zmienionej dyrektywą 2009/136/WE – Dz.U. L 337 z 18.12.2009, s. 11) w celu uwzględnienia przekształcenia dyrektywy 95/46/WE w rozporządzenie. Te istotne skutki prawne wprowadzenia nowego rozporządzenia i nowej dyrektywy dla przepisów dyrektywy w sprawie e-prywatności będą w odpowiednim terminie przedmiotem przeglądu Komisji, z uwzględnieniem wyników negocjacji w sprawie bieżących propozycji z Parlamentem Europejskim i Radą.

16 Decyzja ramowa 2008/977/JHA z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych, Dz.U. L 350 z 30.12.2008, s. 60. Sprawozdanie dotyczące wdrażania przez państwa członkowskie decyzji ramowej (COM(2012) 12) jest przyjmowane jako element pakietu reformy ochrony danych.

przepisów. Oznacza to, że rzeczywiste korzystanie z tych praw jest trudniejsze w niektórych państwach członkowskich niż w innych, w szczególności w internecie.

Trudności te wynikają również z samej ogromnej ilości zbieranych obecnie danych oraz z faktu, że użytkownicy często nie są w pełni świadomi, że ich dane są zbierane. Chociaż wielu Europejczyków uważa, że ujawnianie danych osobowych jest w coraz większym stopniu elementem współczesnego stylu życia[17], 72% użytkowników internetu w Europie nadal ma obawy, że żąda się od nich podania zbyt wielu danych osobowych w internecie[18]. Czują oni, że nie mają kontroli nad swoimi danymi. Nie są odpowiednio informowani o tym, co dzieje się z ich danymi osobowymi, komu są przekazywane i do jakich celów. Często nie wiedzą, jak korzystać ze swoich praw w internecie.

„Prawo do bycia zapomnianym"

Europejski student będący członkiem internetowej sieci społecznościowej postanawia zwrócić się o dostęp do wszystkich danych osobowych, jakie sieć przechowuje na jego temat. Czyniąc to, dowiaduje się, że sieć ta zbiera znacznie więcej danych niż przypuszczał, oraz że niektóre dane osobowe, o których myślał, że zostały usunięte, były nadal przechowywane.

Reforma unijnych przepisów o ochronie danych pozwoli zagwarantować, że nie będzie to więcej miało miejsca, poprzez:

– wyraźny wymóg zobowiązujący internetowe sieci społecznościowe (i wszystkich innych administratorów danych) do ograniczenia do minimum ilości danych osobowych użytkowników, które są zbierane i przetwarzane;

– wymóg, by domyślne ustawienia zapewniały, że dane nie są upubliczniane;

– wyraźny wymóg względem administratorów danych, aby usuwali oni dane osobowe osoby fizycznej, jeśli zwróci się ona wyraźnie o ich usunięcie i nie ma innej uzasadnionej prawem przyczyny ich przechowywania.

W tym konkretnym przypadku oznaczałoby to dla właściciela sieci społecznościowej obowiązek natychmiastowego i całkowitego usunięcia danych studenta.

Jak podkreślono w Europejskiej agendzie cyfrowej, obawy dotyczące prywatności są jednymi z najczęstszych przyczyn niedokonywania przez osoby fizyczne zakupu towarów i usług w sieci. Z uwagi na wkład sektora technologii informacyjno-komunikacyjnych (TIK) w ogólny wzrost produktywności w Europie – 20% bezpośrednio z sektora TIK i 30% z inwestycji w sektorze TIK[19] – zaufanie do tych usług jest niezbędne do pobudzania wzrostu gospodarki UE i konkurencyjności przemysłu europejskiego.

Zgłaszanie naruszeń ochrony danych

Hakerzy zaatakowali usługę gier internetowych, z której korzystają użytkownicy w UE. Naruszenie to dotyczyło baz danych zawierających dane osobowe (w tym nazwiska, adresy i potencjalnie dane kart

[17] Zob. specjalna ankieta Eurobarometru nr 359 – „Stosunek do ochrony danych i tożsamości elektronicznej w Unii Europejskiej", czerwiec 2011 r., s. 23.

[18] Ibidem, s. 54.

[19] Zob. Europejska agenda cyfrowa, s. 4.

kredytowych) dziesiątek milionów użytkowników z całego świata. Przedsiębiorstwo czekało tydzień, zanim powiadomiło odnośnych użytkowników.

Reforma unijnych przepisów o ochronie danych pozwoli zagwarantować, że nie będzie to więcej miało miejsca. Nowe przepisy zobowiążą przedsiębiorstwa do:

– wzmocnienia swoich zabezpieczeń, aby zapobiegać naruszeniom i unikać ich;

– zgłaszania naruszeń ochrony danych zarówno krajowym organom ochrony danych – jeśli to możliwe, w terminie 24 godzin od wykrycia naruszenia– jak i zawiadamiania zainteresowanych osób fizycznych bez nieuzasadnionej zwłoki.

Celem nowych aktów prawnych zaproponowanych przez Komisję jest wzmocnienie praw, zapewnienie osobom fizycznym skutecznych i sprawnych środków gwarantujących, że będą oni w pełni informowani o tym, co dzieje się z ich danymi osobowymi i umożliwiających im skuteczniejsze korzystanie z przysługujących im praw.

Aby wzmocnić prawo osób fizycznych do ochrony swoich danych osobowych, Komisja proponuje nowe przepisy, które:

zwiększą możliwości osób fizycznych w zakresie kontroli swoich danych, poprzez:

- dopilnowanie, by w sytuacjach kiedy wymagana jest ich **zgoda**, była ona **udzielana wyraźnie, tzn. na podstawie oświadczenia lub wyraźnego działania potwierdzającego ze strony danej osoby** i w sposób dobrowolny;

- zapewnienie użytkownikom internetu skutecznego **prawa do bycia zapomnianym** w internecie: prawo do usunięcia swoich danych przez osoby fizyczne, jeśli wycofają swoją zgodę i nie ma innych zasadnych podstaw do zachowania tych danych;

- zagwarantowanie **łatwego dostępu do swoich danych** oraz **prawa do przenoszenia danych**: prawo do otrzymania kopii przechowywanych danych od administratora oraz swoboda przenoszenia ich od jednego usługodawcy do innego, bez utrudnień;

- wzmocnienie **prawa do bycia poinformowanym**, tak aby osoby fizyczne w pełni rozumiały, w jaki sposób ich dane osobowe są przetwarzane, w szczególności gdy przetwarzanie to dotyczy **dzieci**.

usprawnią sposoby korzystania przez osoby fizyczne z przysługujących im praw, poprzez:

- wzmocnienie **niezależności i uprawnień krajowych organów ochrony danych**, tak aby posiadały one odpowiednie kompetencje do skutecznego rozpatrywania skarg, uprawnienia do przeprowadzania skutecznych dochodzeń, podejmowania wiążących decyzji i nakładania skutecznych i odstraszających sankcji;

- rozszerzenie **administracyjnych i sądowych środków ochrony prawnej** w przypadku **naruszenia** praw do ochrony danych. W szczególności, specjalistyczne zrzeszenia będą w stanie wnosić sprawy do sądów w imieniu osób fizycznych.

wzmocnią bezpieczeństwo danych, poprzez:

- promowanie korzystania z **technologii zwiększających ochronę prywatności** (technologii, które chronią prywatność informacji poprzez ograniczenie do minimum przechowywania danych osobowych), ustawienia domyślne sprzyjające ochronie prywatności oraz **programy certyfikacji w zakresie ochrony prywatności**;

- wprowadzenie **ogólnego wymogu**[20] względem administratorów danych, aby **bez nieuzasadnionej zwłoki powiadamiali o naruszeniu danych** zarówno organy ochrony danych (w terminie 24 godzin, jeśli to możliwe), jak i zainteresowane osoby fizyczne.

zwiększa odpowiedzialność podmiotów przetwarzających dane, w szczególności poprzez:

- zobowiązanie administratorów danych do wyznaczenia **inspektora ochrony danych** w przedsiębiorstwach zatrudniających ponad 250 osób i firmach uczestniczących w operacjach przetwarzania danych, które ze względu na swój charakter, zakres lub cele stwarzają szczególne ryzyko naruszenia praw i swobód osób fizycznych („ryzykowne przetwarzanie”);

- wprowadzenie **zasady** „**ochrony prywatności już w fazie projektowania**”, aby zagwarantować, że zabezpieczenia ochrony danych będą uwzględniane na etapie planowania procedur i systemów;

- wprowadzenie obowiązku przeprowadzania **ocen skutków w zakresie ochrony danych**.

3. PRZEPISY O OCHRONIE DANYCH DOPASOWANE DO JEDNOLITEGO RYNKU CYFROWEGO

Celem obecnej dyrektywy jest zapewnienie równorzędnego poziomu ochrony danych w UE, jednak w przepisach obowiązujących w państwach członkowskich nadal istnieją istotne rozbieżności. W związku z tym administratorzy danych mogą stawać wobec konieczności uwzględnienia 27 różnych krajowych systemów i wymogów prawnych. Wynikiem tego jest **rozdrobnione środowisko prawne**, w którym występuje **brak pewności prawa** i nierówny poziom ochrony osób fizycznych. Powoduje to **niepotrzebne koszty i obciążenia administracyjne** dla przedsiębiorstw i zniechęca przedsiębiorstwa działające na jednolitym rynku do rozszerzania swojej działalności w wymiarze transgranicznym.

[20] Obecnie jest to obowiązkowe jedynie w sektorze telekomunikacji, na podstawie dyrektywy w sprawie e-prywatności.

Zasoby i uprawnienia krajowych organów odpowiedzialnych za ochronę danych istotnie różnią się między państwami członkowskimi[21]. W niektórych przypadkach nie są one w stanie w zadowalający sposób wykonywać swoich zadań w zakresie egzekwowania przepisów. Współpraca między tymi organami na szczeblu europejskim – za pośrednictwem istniejącej grupy doradczej (tzw. Grupy Roboczej Art. 29)[22] – nie zawsze prowadzi do spójnego egzekwowania przepisów i również wymaga ulepszenia.

Spójne egzekwowanie przepisów o ochronie danych w całej Europie

Międzynarodowe przedsiębiorstwo posiadające szereg oddziałów w UE uruchomiło internetowy system map w całej Europie, który gromadzi zdjęcia wszystkich prywatnych i publicznych budynków i może również robić zdjęcia ludziom na ulicy. W jednym z państw członkowskich umieszczenie w tym systemie nierozmazanych zdjęć osób nieświadomych tego, że są fotografowane, zostało uznane za niezgodne z prawem, natomiast w innych państwach członkowskich nie nastąpiło tego rodzaju naruszenie przepisów o ochronie danych. W rezultacie nie było spójnej reakcji krajowych organów ochrony danych w celu zaradzenia tej sytuacji.

Reforma unijnych przepisów o ochronie danych pozwoli zagwarantować, że nie będzie to miało miejsca w przyszłości, ponieważ:

– w rozporządzeniu UE ustanowione zostaną wymogi w zakresie ochrony danych i zabezpieczenia, które będą miały bezpośrednie zastosowanie w całej Unii;

– jedynie organy ochrony danych w państwie, w którym przedsiębiorstwo ma główną siedzibę, będą odpowiedzialne za stwierdzenie, czy przedsiębiorstwo działa zgodnie z prawem;

sprawna i skuteczna koordynacja między krajowymi organami ochrony danych – w przypadku gdy dana usługa jest skierowana do osób fizycznych w więcej niż jednym państwie członkowskim - pozwoli dopilnować, by nowe przepisy o ochronie danych w UE były stosowane i egzekwowane spójnie we wszystkich państwach członkowskich.

Należy wzmocnić organy krajowe i zacieśnić ich współpracę, aby zagwarantować spójne egzekwowanie przepisów i ostatecznie jednolite stosowanie przepisów w całej UE.

Solidne, jasne i jednolite ramy prawne na szczeblu UE pomogą uwolnić potencjał jednolitego rynku cyfrowego i będą sprzyjać wzrostowi gospodarczemu, innowacjom i tworzeniu miejsc pracy. Rozporządzenie położy kres rozdrobnieniu systemów prawnych w 27 państwach członkowskich oraz usunie bariery wejścia na rynek; czynnik ten jest szczególnie ważny dla mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.

Nowe przepisy zapewnią również przedsiębiorstwom unijnym lepszą pozycję w ogólnoświatowej konkurencji. W ramach zreformowanych ram prawnych będą one w stanie zagwarantować swoim klientom, że ich cenne dane osobowe będą traktowane z niezbędną ostrożnością i starannością. Zaufanie do spójnego systemu

---

21 Więcej informacji na ten temat można znaleźć w ocenie skutków dołączonej do niniejszego wniosku, SEC(2012) 72.

22 Grupa Robocza Art. 29 została ustanowiona w 1996 r. (na podstawie art. 29 dyrektywy 95/46/WE) jako organ o charakterze doradczym, złożony z przedstawicieli krajowych organów nadzorujących ochronę danych, Europejskiego Inspektora Ochrony Danych oraz Komisji. Bliższe informacje dostępne są na następującej stronie: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

prawnego UE będzie kluczowym atutem dla usługodawców oraz zachętą dla inwestorów poszukujących optymalnych warunków przy wyborze lokalizacji swoich usług.

Aby rozszerzyć **wymiar jednolitego rynku dotyczący ochrony danych**, Komisja proponuje:

- ustanowienie przepisów o ochronie danych na szczeblu UE poprzez **rozporządzenie bezpośrednio obowiązujące we wszystkich państwach członkowskich**[23], co położy kres łącznemu i równoczesnemu stosowaniu różnych krajowych przepisów o ochronie danych. Pozwoli to **przedsiębiorstwom** osiągnąć **oszczędności w wysokości około 2,3 mld EUR rocznie w wyniku samego ograniczenia obciążeń administracyjnych**;

- **uproszczenie otoczenia regulacyjnego poprzez drastyczne cięcia obciążeń administracyjnych** i zniesienie **formalności** takich jak ogólne wymogi w zakresie zgłaszania (dające oszczędności w wysokości 130 mln EUR rocznie w wyniku samego ograniczenia obciążeń administracyjnych). Ze względu na duże znaczenie specyficznych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw dla konkurencyjności gospodarki europejskiej, zwraca się na nie szczególną uwagę;

- **dalsze wzmocnienie niezależności i uprawnień krajowych organów ochrony danych**, aby umożliwić im prowadzenie dochodzeń, podejmowanie wiążących decyzji i nakładanie skutecznych i odstraszających sankcji oraz zobowiązać państwa członkowskie do zapewnienia im **odpowiednich zasobów** do realizacji tych celów;

- **ustanowienie systemu „punktu kompleksowej obsługi" w zakresie ochrony danych w UE:** administratorzy danych w UE będą musieli kontaktować się jedynie z **jednym krajowym organem ochrony danych**, mianowicie z krajowym organem ochrony danych w państwie członkowskim, w którym znajduje się główna siedziba przedsiębiorstwa;

- stworzenie warunków do **szybkiej i skutecznej współpracy między krajowymi organami ochrony danych**, przewidujących między innymi wymóg prowadzenia przez te organy dochodzeń i inspekcji na wniosek innego organu oraz wzajemnego uznawania swoich decyzji;

- **ustanowienie mechanizmu spójności** na szczeblu UE, aby zagwarantować, by decyzje krajowych organów ochrony danych niosące szersze skutki w wymiarze europejskim w pełni uwzględniały stanowisko innych odnośnych krajowych organów ochrony danych i były w pełni zgodne z prawem UE;

- nadanie Grupie Roboczej Art. 29 statusu **niezależnej Europejskiej Rady Ochrony Danych**, aby zwiększyć jej wkład w spójne stosowanie przepisów o ochronie danych i stworzyć solidną podstawę do współpracy organów ochrony danych, w tym Europejskiego Inspektora Ochrony Danych, oraz zwiększyć efekt

[23] Proponuje się dyrektywę w celu zdefiniowania przepisów obowiązujących w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych (zob. pkt 4 poniżej), co zapewni większą elastyczność państwom członkowskim w tej konkretnej dziedzinie.

synergii i skuteczność poprzez określenie w przepisach, że obsługę sekretariatu Europejskiej Rady Ochrony Danych zapewni Europejski Inspektor Ochrony Danych.

Nowe rozporządzenie UE zapewni solidną ochronę praw podstawowych w zakresie ochrony danych w całej Unii Europejskiej oraz umocni funkcjonowanie jednolitego rynku. Równocześnie – z uwagi na fakt, że, jak podkreślił Trybunał Sprawiedliwości UE[24], prawo do ochrony danych osobowych nie jest prawem bezwzględnym i musi być rozpatrywane w kontekście funkcji, jaką pełni w społeczeństwie[25] oraz musi być równoważone innymi prawami podstawowymi, zgodnie z zasadą proporcjonalności[26] – rozporządzenie będzie zawierało wyraźne przepisy zapewniające ochronę innych praw podstawowych, takich jak wolność wypowiedzi i informacji, prawo do obrony oraz obowiązek zachowania tajemnicy zawodowej (na przykład w zawodach prawniczych), bez uszczerbku dla statusu kościołów w systemach prawnych państw członkowskich.

4. WYKORZYSTYWANIE DANYCH W RAMACH WSPÓŁPRACY POLICYJNEJ I WSPÓŁPRACY WYMIARÓW SPRAWIEDLIWOŚCI W SPRAWACH KARNYCH

Wejście w życie traktatu lizbońskiego, a w szczególności wprowadzenie nowej podstawy prawnej (art. 16 TFUE) umożliwia ustanowienie kompleksowych ram ochrony danych zapewniających wysoki poziom ochrony danych osób fizycznych przy jednoczesnym poszanowaniu szczególnego charakteru współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych. W szczególności umożliwia to objęcie zrewidowanymi unijnymi ramami ochrony danych zarówno transgranicznego jak i krajowego przetwarzania danych osobowych. Pozwoliłoby to ograniczyć różnice między systemami prawnymi w państwach członkowskich i przypuszczalnie przyniosłoby ogólne korzyści w zakresie ochrony danych osobowych. Mogłoby to również przyczynić się do sprawniejszej wymiany informacji między organami policyjnymi i sądowymi państw członkowskich, a przez to poprawić współpracę w zakresie zwalczania poważnej przestępczości w Europie. Przetwarzanie danych przez organy policyjne i sądowe w sprawach karnych jest obecnie zasadniczo regulowane decyzją ramową 2008/977/WSiSW, która weszła w życie wcześniej niż traktat lizboński. Ponieważ jest to decyzja ramowa, Komisja nie posiada uprawnień do egzekwowania jej przepisów, co przyczyniło się do jej niejednolitego wdrożenia. Ponadto zakres decyzji ramowej jest ograniczony do transgranicznego przetwarzania danych[27]. Oznacza to, że przetwarzanie danych osobowych, które nie było przedmiotem wymiany informacji, nie jest obecnie objęte przepisami UE dotyczącymi takiego przetwarzania i zapewniającymi ochronę praw podstawowego do ochrony danych. W niektórych przypadkach stwarza to praktyczne

---

24 Trybunał Sprawiedliwości UE, wyrok z dnia 9.11.2010 r.; sprawy połączone C-92/09 i C-93/09 Volker und Markus Schecke oraz Eifert [2010], dotychczas nieopublikowany.

25 Zgodnie z art. 52 ust. 1 Karty, można ograniczyć korzystanie z prawa do ochrony danych, o ile takie ograniczenia są przewidziane prawem i respektują istotę praw i wolności, i o ile, z zastrzeżeniem zasady proporcjonalności, są one konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię Europejską lub potrzebom ochrony praw i wolności innych osób.

26 Trybunał Sprawiedliwości UE, wyrok z dnia 6.11.2003 r., C-101/01, Lindqvist [2003] ECR I-12971, pkt 82-90; wyrok z dnia 16.12.2008 r., C-73/07, Satamedia [2008], ECR I-9831, pkt 50-62.

27 Ściślej rzecz biorąc, decyzja ramowa ma zastosowanie do danych osobowych, które zostały przekazane lub są przekazywane lub udostępniane między państwami członkowskimi lub wymieniane między państwami członkowskimi i instytucjami lub organami UE (zob. art. 1 ust. 2).

utrudnienia dla policji i innych organów, dla których może nie być oczywiste, czy przetwarzanie danych będzie czysto krajowe czy transgraniczne; może być im również trudno przewidzieć, czy dane „krajowe" mogą stać się później przedmiotem wymiany transgranicznej[28].

W związku z powyższym celem nowych zreformowanych unijnych ram ochrony danych jest zapewnienie spójnego, wysokiego poziomu ochrony danych, aby **pogłębić wzajemne zaufanie między organami policyjnymi i sądowymi różnych państw członkowskich, a przez to jeszcze bardziej przyczynić się do swobodnego przepływu danych i skutecznej współpracy między organami policyjnymi i sądowymi**.

Aby zapewnić wysoki poziom ochrony danych osobowych w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych oraz ułatwić wymianę danych osobowych między organami policyjnymi i sądowymi państw członkowskich, Komisja proponuje, w ramach pakietu reformy ochrony danych, dyrektywę, w której:

- **zastosowane zostaną ogólne zasady ochrony danych** w ramach współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, przy poszanowaniu specyficznego charakteru tych dziedzin[29];

- przewidziane zostaną **minimalne zharmonizowane kryteria i warunki ewentualnych ograniczeń** stosowania przepisów ogólnych. Dotyczy to w szczególności praw osób fizycznych do bycia poinformowanymi, kiedy policja i organy sądowe przetwarzają ich dane lub uzyskują do nich dostęp. Takie ograniczenia są niezbędne dla zagwarantowania skuteczności zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania;

- ustanowione zostaną **szczegółowe przepisy uwzględniające szczególny charakter działań związanych z egzekwowaniem prawa, w tym wprowadzone zostanie rozróżnienie na różne kategorie podmiotów danych** (takie jak świadkowie i podejrzani), których prawa mogą być zróżnicowane.

5. OCHRONA DANYCH W ZGLOBALIZOWANYM ŚWIECIE

Prawa osób fizycznych muszą być nadal przestrzegane, kiedy dane osobowe są przekazywane z UE do państw trzecich i w każdej sytuacji, kiedy sprawa dotyczy osób fizycznych w państwach członkowskich i ich dane są wykorzystywane lub analizowane przez usługodawców z państwa trzeciego. Oznacza to, że unijne standardy ochrony danych muszą być stosowane niezależnie od lokalizacji geograficznej przedsiębiorstwa lub jego infrastruktury przetwarzającej dane.

---

[28] Zostało to potwierdzone przez niektóre państwa członkowskie w ich odpowiedziach na kwestionariusz Komisji dotyczący sprawozdania z wdrażania decyzji ramowej (COM(2012) 12).

[29] Por. Deklaracja nr 21 w sprawie ochrony danych osobowych w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej, załączona do Aktu końcowego konferencji przedstawicieli państw członkowskich, która przyjęła Traktat z Lizbony.

W dzisiejszym zglobalizowanym świecie dane osobowe są przekazywane przez coraz większą liczbę granic wirtualnych i geograficznych oraz przechowywane na serwerach w wielu krajach. Coraz więcej przedsiębiorstw oferuje usługi przetwarzania w chmurze, które umożliwiają klientom dostęp do danych na odległych serwerach i przechowywanie tam danych. Czynniki te skłaniają do doskonalenia obecnych mechanizmów przekazywania danych do państw trzecich. Dotyczy to między innymi decyzji stwierdzających odpowiedni poziom ochrony danych, tj. decyzji poświadczających „odpowiednie" standardy ochrony danych w państwach trzecich, a także stosownych gwarancji, takich jak standardowe klauzule umowne czy „wiążące reguły korporacyjne"[30], tak aby zagwarantować wysoki poziom ochrony danych w międzynarodowych operacjach przetwarzania danych i ułatwić przepływ danych przez granice.

Wiążące reguły korporacyjne

Grupa korporacyjna musi regularnie przekazywać dane osobowe z oddziałów w UE do innych oddziałów zlokalizowanych w państwach trzecich. Grupa chciałaby wprowadzić zbiór wiążących reguł korporacyjnych, aby przestrzegać prawa UE, a jednocześnie ograniczyć wymogi administracyjne dla każdego indywidualnego przypadku przekazania danych. W praktyce dzięki tym regułom pojedynczy zbiór reguł ma zastosowanie w całej grupie zamiast szeregu różnych umów wewnętrznych.

W ramach obecnej praktyki uzgodnionej na szczeblu Grupy Roboczej Art. 29, stwierdzenie, czy wiążące reguły korporacyjne danego przedsiębiorstwa zapewniają odpowiednie gwarancje, wymaga przeglądu przeprowadzonego przez trzy organy ochrony danych (jeden „główny" i dwa „rewizyjne"), jednak również szereg innych organów może zgłosić swoje uwagi. Ponadto wiele aktów prawnych państw członkowskich wymaga dodatkowego zatwierdzenia na szczeblu krajowym operacji przekazywania danych objętych wiążącymi regułami korporacyjnymi, co sprawia, że ich przyjęcie jest uciążliwe, kosztowne, długotrwałe i skomplikowane.

W wyniku reformy ochrony danych:

– proces ten zostanie uproszczony i usprawniony;

– wiążące reguły korporacyjne będą zatwierdzane wyłącznie przez jeden organ ochrony danych oraz będą istnieć mechanizmy zapewniające szybkie włączenie innych właściwych organów ochrony danych;

– po tym jak jeden organ zatwierdzi wiążące reguły korporacyjne, będą one obowiązywać w całej UE bez konieczności jakiegokolwiek dodatkowego zatwierdzenia na szczeblu krajowym.

Aby **sprostać wyzwaniom globalizacji**, konieczne są elastyczne instrumenty i mechanizmy – zwłaszcza w przypadku przedsiębiorstw działających w skali ogólnoświatowej – przy zagwarantowaniu ochrony danych osób fizycznych bez jakichkolwiek luk prawnych. Komisja proponuje następujące środki:

[30] „Wiążące reguły korporacyjne" to kodeksy postępowania oparte na europejskich normach ochrony danych, zatwierdzone przez co najmniej jeden krajowy organ ochrony danych, sporządzane i przestrzegane dobrowolnie przez organizacje wielonarodowe w celu zapewnienia odpowiednich gwarancji w zakresie kategorii przekazywania danych osobowych między spółkami należącymi do tej samej grupy korporacyjnej i związanymi tymi regułami. Nie są one wyraźnie objęte dyrektywą 95/46/WE, lecz zostały opracowane w wyniku praktycznej współpracy między krajowymi organami ochrony danych, przy wsparciu Grupy Roboczej Art. 29.

- **jasne przepisy** określające, kiedy **prawo UE ma zastosowanie wobec administratorów danych działających w państwach trzecich**, w szczególności poprzez zapis stanowiący, że kiedykolwiek towary i usługi są oferowane osobom fizycznym w UE, lub kiedykolwiek ich zachowanie jest monitorowane, **obowiązują przepisy europejskie**;

- wszelkie **decyzje stwierdzające odpowiedni poziom ochrony danych** będą podejmowane przez Komisję Europejską na podstawie wyraźnych i przejrzystych kryteriów, w tym w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości;

- legalny przepływ danych do państw trzecich będzie łatwiejszy dzięki wzmocnieniu i uproszczeniu **przepisów dotyczących międzynarodowego przekazywania danych** do krajów nieobjętych decyzjami stwierdzającymi odpowiedni poziom ochrony danych, w szczególności poprzez zoptymalizowanie i szersze wykorzystanie instrumentów takich jak **wiążące reguły korporacyjne**, tak aby mogły być one wykorzystywane w celu objęcia nimi **podmiotów przetwarzających dane** i całych **grup przedsiębiorstw**, przez co będą lepiej odzwierciedlały wzrastającą liczbę przedsiębiorstw uczestniczących w operacjach przetwarzania danych, w szczególności przetwarzania w chmurze;

- zaangażowanie się w **dialog**, a w stosownych przypadkach **negocjacje**, z państwami trzecimi – w szczególności ze strategicznymi partnerami UE i państwami objętymi europejską polityką sąsiedztwa – oraz właściwymi organizacjami międzynarodowymi (takimi jak Rada Europy, Organizacja Współpracy Gospodarczej i Rozwoju, ONZ) w celu **promowania** na całym świecie **wysokich, interoperacyjnych standardów ochrony danych**.

6. PODSUMOWANIE

Unijna reforma ochrony danych ma na celu stworzenie **nowoczesnych, solidnych, spójnych i kompleksowych ram ochrony danych w Unii Europejskiej**. Wzmocnione zostanie prawo podstawowe osób fizycznych do ochrony danych. Przestrzegane będą inne prawa, takie jak wolność wypowiedzi i informacji, prawa dziecka, prawo do prowadzenia działalności gospodarczej, prawo do rzetelnego procesu sądowego i obowiązek zachowania tajemnicy zawodowej (na przykład w zawodach prawniczych), a także status kościołów w systemach prawnych państw członkowskich.

Reforma przyniesie korzyści przede wszystkim osobom fizycznym poprzez wzmocnienie ich praw do ochrony danych osobowych oraz zaufania do środowiska cyfrowego. Ponadto reforma w znaczącym stopniu uprości środowisko prawne dla przedsiębiorstw i sektora publicznego. Oczekuje się, że pobudzi to rozwój gospodarki cyfrowej na całym jednolitym rynku UE i poza nim, zgodnie z celami strategii „Europa 2020” i Europejskiej agendy cyfrowej. Wreszcie, reforma zwiększy wzajemne zaufanie organów ścigania, co ułatwi wymianę danych między nimi oraz współpracę w zakresie zwalczania poważnej przestępczości, a przy tym zapewni wysoki poziom ochrony osobom fizycznym.

Komisja Europejska będzie ściśle współpracować z Parlamentem Europejskim i Radą, aby do końca 2012 r. osiągnąć porozumienie w sprawie nowych unijnych ram ochrony danych. W toku prac nad przyjęciem tych ram i poza nimi, zwłaszcza w kontekście wdrażania nowych instrumentów prawnych, Komisja będzie utrzymywać **ścisły i przejrzysty dialog z wszystkimi zainteresowanymi podmiotami,** w tym z przedstawicielami sektora prywatnego i publicznego. Będą to między innymi przedstawiciele policji i sądownictwa, regulatorów łączności elektronicznej, organizacji społeczeństwa obywatelskiego, organów ochrony danych i środowisk akademickich, a także specjalistycznych agencji UE, takich jak Eurojust, Europol, Agencja Praw Podstawowych i Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji.

W związku z ciągłym rozwojem technologii informatycznych i zmianą zachowań społecznych taki dialog ma ogromne znaczenie, aby wykorzystać uzyskane w ten sposób informacje niezbędne w celu zapewnienia wysokiego poziomu ochrony osób fizycznych, wzrostu gospodarczego i konkurencyjności przemysłu UE, skuteczności działania sektora publicznego (w tym policji i sądownictwa) oraz niskiego poziomu obciążeń administracyjnych.