KOMISJA EUROPEJSKA

Bruksela, dnia 4.11.2010
KOM(2010) 609 wersja ostateczna

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

## „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej”

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

**„Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej"**

## 1. NOWE WYZWANIA W ZAKRESIE OCHRONY DANYCH OSOBOWYCH

Dyrektywa w sprawie ochrony danych z 1995 r.[1] stanowiła kamień milowy w historii ochrony danych osobowych w Unii Europejskiej. W dyrektywie zapisano dwa z najstarszych i równie istotnych dążeń w procesie integracji europejskiej: z jednej strony jest to ochrona praw podstawowych i podstawowych wolności jednostek, w szczególności podstawowego prawa do ochrony danych, z drugiej zaś strony – realizacja rynku wewnętrznego – w tym przypadku swobodnego przepływu danych osobowych.

Piętnaście lat później ten podwójny cel nadal obowiązuje, podobnie jak aktualne są zasady zapisane w dyrektywie. **Jednakże szybki rozwój technologiczny i globalizacja doprowadziły go głębokich przemian w otaczającym nas świecie, przynosząc nowe wyzwania w zakresie ochrony danych osobowych.**

Dzisiejsze technologie umożliwiają jednostkom łatwe dzielenie się informacjami na temat ich zachowania i preferencji oraz publiczne udostępnianie tych informacji w skali globalnej na nie mającą precedensu skalę. Sieci społecznościowe z setkami milionów członków rozsianych po całym świecie stanowią chyba najbardziej ewidentny, choć nie jedyny, przykład tego zjawiska. Również „przetwarzanie w chmurze" (ang. *cloud computing*) – tzn. przetwarzanie dokonywane w Internecie przy pomocy oprogramowania, dzielonych zasobów i informacji znajdujących się na zewnętrznych serwerach („w chmurze") stanowi wyzwanie dla ochrony danych, ponieważ wiąże się z utratą przez jednostki kontroli nad ich potencjalnie poufnymi informacjami w sytuacji, w której przechowują one te dane korzystając z programów zainstalowanych na urządzeniach osób trzecich. Niedawno przeprowadzona analiza potwierdziła, że zarówno organy ochrony danych, zrzeszenia przedsiębiorców, jak i organizacje konsumentów są zgodne co do tego, że wzrasta zagrożenie dla prywatności i ochrony danych osobowych w związku z działalnością w Internecie[2].

Równocześnie **metody gromadzenia danych osobowych stały się coraz bardziej wyrafinowane i trudniej wykrywalne**. Przykładowo użycie zaawansowanych narzędzi umożliwia podmiotom gospodarczym lepsze dobranie strategii przyjmowanej wobec poszczególnych jednostek dzięki monitorowaniu ich zachowania. Z kolei coraz intensywniejsze korzystanie z procedur umożliwiających automatyczne gromadzenie danych, takich jak elektroniczne pobieranie opłat za przejazd w transporcie, pobieranie opłat za

---

[1] Dyrektywa 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 (Dz.U. L 281 z 23.11.1995, s. 31).

[2] Zob. analizę dotyczącą korzyści gospodarczych związanych z technologiami służącymi wzmocnieniu ochrony prywatności – *Study on the economic benefits of privacy enhancing technologies,* London Economics, lipiec 2010 r. (http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf), s.14.

przejazd pojazdów oraz stosowanie urządzeń do geolokalizacji ułatwia ustalenie miejsca przebywania osób fizycznych – wystarczy, że mają one przy sobie urządzenie przenośne. Także organy publiczne wykorzystują coraz większą ilość danych osobowych do różnych celów, takich jak ustalanie miejsca pobytu osób fizycznych w przypadku epidemii choroby zakaźnej, zapobieganie terroryzmowi i przestępczości oraz zwalczanie tych zjawisk, zarządzanie systemami zabezpieczenia społecznego, do celów podatkowych, posługując się aplikacjami używanymi do administracji elektronicznej itd.

Wszystko to nieuchronnie zmusza do odpowiedzi na pytanie, czy obowiązujące unijne przepisy w dziedzinie ochrony danych mogą w dalszym ciągu stanowić pełną i skuteczną odpowiedź na te wyzwania.

W związku z powyższym Komisja zainicjowała przegląd obecnych ram prawnych, rozpoczynając od konferencji na wysokim szczeblu w maju 2009 r., po której nastąpiły konsultacje publiczne prowadzone do końca 2009 r.[3]. Zainicjowano również szereg analiz[4].

Dokonanie w nich ustalenie potwierdziły, ze podstawowe zasady dyrektywy są nadal aktualne i że ta technologiczna neutralność powinna być zachowana. Równocześnie jednak zidentyfikowano szereg kwestii problematycznych, wiążących się z konkretnymi wyzwaniami. Obejmują one:

- *reakcję na oddziaływanie nowych technologii*

Odpowiedzi udzielone w ramach konsultacji przez osoby prywatne i organizacje potwierdziły potrzebę wyjaśnienia i sprecyzowania kwestii stosowania zasad ochrony danych do nowych technologii w celu zagwarantowania, by dane osobowe osób fizycznych były faktycznie skutecznie chronione, niezależnie od tego, jaka technologia zostanie wykorzystana do przetwarzania ich danych, oraz by administratorzy danych byli w pełni świadomi wpływu, jaki nowe technologie mają na ochronę danych. Częściowa odpowiedź na te problemy stanowiła dyrektywa 2002/58/WE (tzw. „dyrektywa o prywatności elektronicznej")[5], zawierająca szczególne rozwiązania uzupełniające ogólną dyrektywę o ochronie danych w sektorze łączności elektronicznej[6].

---

3 Zob. odpowiedzi na konsultacje publiczne Komisji: http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm. Ściślej ukierunkowane konsultacje z zainteresowanymi podmiotami przeprowadzono w trakcie 2010 r. Wiceprzewodnicząca Viviane Reding przewodniczyła również spotkaniu na wysokim szczeblu z zainteresowanymi podmiotami w dniu 5 października 2010 r. w Brukseli. Komisja zasięgnęła również opinii Grupy Roboczej Art. 29, która wniosła kompleksowy wkład do konsultacji w 2009 r. (WP 168) oraz przyjęła w lipcu 2010 r. specjalną opinię w sprawie pojęcia rozliczalności (WP 173).

4 Obok analizy dotyczącej korzyści gospodarczych z technologii zwiększających ochronę prywatności (zob. przyp. 2), zob. także analizę porównawczą różnych strategii w zakresie nowych wyzwań w ochronie prywatności, w szczególności w świetle postępu technologicznego, ze stycznia 2010 r. (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf) . Trwa również przygotowanie analizy dotyczącej oceny skutków przyszłych unijnych ram prawnych w dziedzinie ochrony danych osobowych.

5 Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. L 201 z 31.7.2002, s. 37).

6 Dyrektywa 95/46/WE o ochronie danych określa standardy ochrony danych dla wszystkich aktów legislacyjnych UE, w tym dyrektywy w sprawie prywatności elektronicznej (zmienionej dyrektywą 2009/136/WE, Dz.U. L 337 z 18.12.2009, s. 11). Dyrektywę w sprawie prywatności elektronicznej stosuje się w odniesieniu do przetwarzania danych osobowych w związku z dostarczaniem publicznie

- *poprawa sytuacji w zakresie aspektów ochrony danych związanych z rynkiem wewnętrznym*

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. Podkreślały one potrzebę zwiększenia pewności prawnej, zmniejszenia obciążeń administracyjnych oraz zagwarantowania równych szans dla podmiotów gospodarczych i innych administratorów danych.

- *reakcja na globalizację oraz poprawa międzynarodowego przekazywania danych*

Wiele zainteresowanych podmiotów podkreślało, że coraz powszechniejsze powierzanie przetwarzania danych podmiotom zewnętrznym, bardzo często spoza UE, stwarza szereg problemów w odniesieniu do prawa mającego zastosowanie do przetwarzania oraz ustalania związanej z tym odpowiedzialności. Jeżeli chodzi zaś o międzynarodowe przekazywanie danych, wiele organizacji stwierdziło, że obecnie obowiązujące systemy nie są w pełni zadowalające, oraz że muszą zostać zweryfikowane i uproszczone, by uczynić proces międzynarodowego przekazywania danych łatwiejszym i mniej uciążliwym.

- *zapewnienie lepszych rozwiązań instytucjonalnych w celu skutecznego egzekwowania przepisów o ochronie danych*

Zainteresowane podmioty są zgodne co do tego, że należy zwiększyć rolę organów ochrony danych, by zagwarantować lepsze egzekwowanie przepisów o ochronie danych. Niektóre organizacje zaapelowały również o większą przejrzystość prac Grupy Roboczej Art. 29 (*zob. pkt 2.5 poniżej*) oraz jaśniejsze określenie jej zadań i kompetencji.

- *zwiększenie spójności ram prawnych w zakresie ochrony danych*

W toku publicznych konsultacji wszystkie zainteresowane podmioty podkreślały potrzebę nadrzędnego instrumentu mającego zastosowanie do operacji przetwarzania danych we wszystkich sektorach oraz w odniesieniu do wszystkich polityk Unii, gwarantującego zintegrowane podejście, jak również nieprzerwaną, spójną i skuteczną ochronę[7].

Powyższe wyzwania **wymagają od UE wypracowania kompleksowego i spójnego podejścia** gwarantującego **pełne poszanowanie podstawowego prawa osób fizycznych do ochrony ich danych osobowych w UE i poza nią**. Traktat lizboński zapewnił UE dodatkowe środki umożliwiające osiągnięcie tego celu: Kartę praw podstawowych UE, w art. 8 której uznano niezależne prawo do ochrony danych osobowych, stała się prawnie wiążąca, wprowadzono również nową podstawę prawną[8] umożliwiającą ustanowienie całościowych i spójnych unijnych przepisów o ochronie osób fizycznych w odniesieniu do przetwarzania ich

---

dostępnych usług łączności elektronicznej w publicznych sieciach łączności. Stanowi ona przekształcenie zasad określonych w dyrektywie o ochronie danych w szczegółowe przepisy dla sektora łączności elektronicznej. Dyrektywa 95/46/WE ma zastosowanie między innymi do niepublicznych usług łączności.

7 W osobnych komentarzach przedłożonych po zakończeniu publicznych konsultacji Europol i Eurojust zwróciły się o uwzględnienie mimo wszystko specyfiki ich pracy w odniesieniu do koordynacji egzekwowania prawa i zapobiegania przestępczości.

8 Zob. art. 16 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE).

danych osobowych oraz swobodnego przepływu takich danych. W szczególności nowa podstawa prawna umożliwia UE wprowadzenie jednego instrumentu prawnego regulującego ochronę danych, w tym w obszarze współpracy policji i wymiarów sprawiedliwości w sprawach karnych. Artykuł 16 TFUE tylko częściowo obejmuje obszar wspólnej polityki zagranicznej i bezpieczeństwa, ponieważ szczegółowe przepisy dotyczące przetwarzania danych przez państwo członkowskie muszą zostać ustanowione decyzją Rady w oparciu o inną podstawę prawną[9].

Na bazie tych nowych możliwości prawnych Komisja przyzna najwyższy priorytet kwestii zagwarantowania poszanowania podstawowego prawa do ochrony danych na terytorium całej Unii i we wszystkich swoich politykach, równocześnie poprawiając wymiar rynku wewnętrznego oraz ułatwiając swobodny przepływ danych osobowych. W tym kontekście inne właściwe prawa podstawowe zapisane w karcie oraz inne cele zagwarantowane w Traktatach muszą być w pełni uwzględnione w działaniach na rzecz zagwarantowania podstawowego prawa do ochrony danych.

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. Pozwoli to UE utrzymać pozycję podmiotu aktywnie promującego wysokie standardy ochrony danych na całym świecie.

## 2. ZASADNICZE CELE CAŁOŚCIOWEGO PODEJŚCIA DO OCHRONY DANYCH

### 2.1. Wzmocnienie praw osób fizycznych

#### *2.1.1. Zagwarantowanie odpowiedniej ochrony osobom fizycznym we wszystkich okolicznościach*

Przepisy zapisane w obowiązujących instrumentach UE w zakresie ochrony danych mają na **celu ochronę podstawowych praw osób fizycznych, a w szczególności ich prawa do ochrony danych osobowych**, zgodnie z Kartą praw podstawowych UE[10].

Pojęcie „danych osobowych" należy do pojęć o kluczowym znaczeniu dla ochrony osób fizycznych przez obowiązujące instrumenty UE w dziedzinie ochrony danych, które pociąga za sobą konieczność wypełniania przez administratorów danych i przetwarzających dane obowiązków związanych z tymi funkcjami[11]. Definicja „danych osobowych" ma na celu objęcie zakresem tego pojęcia wszystkich informacji dotyczących, bezpośrednio lub pośrednio, zidentyfikowanych lub możliwych do zidentyfikowania osób. Aby ustalić, czy osoba może być zidentyfikowana, należy wziąć pod uwagę „wszystkie sposoby, jakimi może

---

9 Zob. ostatni akapit art. 16 ust. 2 TFUE oraz art. 39 Traktatu o Unii Europejskiej (TUE).

10 Zob. Europejski Trybunał Sprawiedliwości, sprawa C-101/01, „Bodil Lindqvist", ECR [2003], I-1297, 96, 97 ETS, oraz C-275/06, Productores de Música de España (Promusicae) przeciwko Telefónica de España SAU, Zb.Orz. [2008] I-271. Zob. także orzecznictwo Europejskiego Trybunału Spraw Człowieka, np. w sprawach S. i Marper przeciwko Zjednoczonemu Królestwu, 4.12.2008 (skargi nr 30562/04 i 30566/044) oraz Rotaru przeciwko Rumunii, 4.5.2000, nr 28341/95, § 55, ECHR 2000-V.

11 Zob. definicję „administratora danych" i „przetwarzającego" w art. 2 lit. d) i e) dyrektywy 95/46/WE.

posłużyć się administrator danych lub inna osoba w celu zidentyfikowania owej osoby"[12]. Zaletą tego zamierzonego podejścia wybranego przez prawodawcę jest elastyczność, umożliwiająca stosowanie dyrektywy do różnych sytuacji i zdarzeń wpływających na prawa podstawowe, w tym takich, których nie dało się przewidzieć w momencie przyjmowania tego aktu. Jednakże konsekwencją takiego szeroko zakrojonego i elastycznego podejścia są liczne przypadki, w których na etapie wykonywania dyrektywy nie zawsze jest jasne, jakie podejście należy przyjąć, czy osobom fizycznym przysługuje prawo do ochrony danych oraz czy na administratorach danych ciążą obowiązki przewidziane w dyrektywie[13].

Są sytuacje, w których dochodzi do przetwarzania szczególnych informacji, gdzie konieczne byłyby dodatkowe środki w prawie Unii. Takie środki istnieją już w niektórych przypadkach. Przykładowo przechowywanie informacji w urządzeniach końcowych (np. telefonach komórkowych) dozwolone jest wyłącznie w przypadku uzyskania zgody osoby fizycznej. Także ta kwestia może wymagać działań na szczeblu UE, dotyczących np. zakodowanych danych, danych lokalizacyjnych, technologii eksploracji danych umożliwiających połączenie danych z różnych źródeł, lub przypadków gdy konieczne jest zagwarantowanie poufności i integralności systemów informacyjno-komunikacyjnych[14].

Wszystkie powyższe kwestie wymagają zatem dokładnej analizy.

Komisja rozważy, **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**.

### *2.1.2. 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. Dlatego zasadnicze znaczenie ma, by administratorzy danych **odpowiednio i wyraźnie oraz w przejrzysty sposób** informowali osoby fizyczne o tym, w jaki sposób i przez kogo ich dane są gromadzone i przetwarzane, z jakiego powodu oraz na jak długo, jak również jakie przysługują im prawa, gdyby chcieli uzyskać dostęp do swoich danych, poprawić je lub usunąć. Właściwe przepisy dotyczące informacji, których należy udzielić osobom, których dane dotyczą[15], są niewystarczające.

Podstawowymi elementami przejrzystości są wymogi, by **informacje były łatwo dostępne i zrozumiałe, oraz by napisano je jasnym i prostym językiem.** Ma to szczególne znaczenie w środowisku internetowym, gdzie często oświadczenia o ochronie prywatności są niejasne, trudno dostępne, nieprzejrzyste[16] i nie zawsze pozostają w pełnej zgodności z

---

12 Zob. motyw 26 dyrektywy 95/46/WE.

13 Zob. przykładowo przypadek adresów IP przeanalizowany przez Grupę Roboczą art. 29 w opinii 4/2007 w sprawie pojęcia danych osobowych (WP 136).

14 Zob. przykładowo wyrok niemieckiego Federalnego Trybunału Konstytucyjnego (*Bundesverfassungsgericht*) z dnia 27 lutego 2008 r., 1 BvR 370/07.

15 Zob. art. 10 i 11 dyrektywy 95/46/WE.

16 Badanie Eurobarometru przeprowadzone w 2009 r. wykazało, że około połowa respondentów uznała zawiadomienia o prywatności na stronach internetowych za „bardzo" lub „dość" niejasne (zob. Flash Eurobarometer nr 282 : http://ec.europa.eu/public_opinion/flash/fl_282_en.pdf).

obowiązującymi przepisami. Jednym z przykładów mogą być internetowe reklamy behawioralne – ze względu na dużą ilość podmiotów zaangażowanych w dostarczanie reklam behawioralnych oraz złożoność technologiczną tych praktyk osoba fizyczna ma trudności z uzyskaniem wiedzy o tym, czy dane osobowe są gromadzone, przez kogo i w jakim celu oraz ze zrozumieniem całego procesu.

W tym kontekście na szczególną ochronę zasługują **dzieci**, które mogą być w mniejszym stopniu świadome zagrożeń, konsekwencji, gwarancji i praw w związku z przetwarzaniem danych osobowych[17].

Komisja rozważy:

– wprowadzenie **ogólnej zasady przejrzystego przetwarzania** danych osobowych w obrębie ram prawnych;

– wprowadzenie **szczególnych obowiązków** dla administratorów danych dotyczących rodzajów informacji, których należy udzielić oraz **trybów** ich udzielenia, w tym w stosunku do **dzieci**;

– opracowanie jednego lub większej liczy **standardowych formularzy UE („oświadczenia o prawie do prywatności”**), które miałyby być wykorzystywane przez administratorów danych.

Istotne znaczenie ma również informowanie osób fizycznych w przypadku, gdy ich dane zostały przypadkowo lub w sposób bezprawny zniszczone, utracone, zmienione albo gdy osoby nieupoważnione uzyskały dostęp do takich danych lub zostały im one ujawnione. W ramach niedawnej rewizji dyrektywy o prywatności elektronicznej wprowadzono **obowiązek zawiadamiania o naruszeniach dotyczących danych osobowych**, dotyczący jednak jedynie sektora telekomunikacyjnego. Mając na uwadze, że do naruszeń takich dochodzi również w innych sektorach (np. w sektorze finansowym), Komisja zbada możliwości rozciągnięcia tego obowiązku na inne sektory, zgodnie z deklaracją Komisji w sprawie powiadomień o naruszeniu ochrony danych osobowych złożoną przed Parlamentem Europejskim w 2009 r. w kontekście reformy ram regulacyjnych komunikacji elektronicznej[18]. Analiza ta nie wpłynie na przepisy dyrektywy o prywatności elektronicznej, która musi zostać przeniesiona do przepisów krajowych do dnia 25 maja 2011 r.[19]. Konieczne będzie zapewnienie spójnego i konsekwentnego podejścia w tej sprawie.

---

17 Zob. jakościowe badanie „Bezpieczniejszy Internet dla dzieci” dotyczące dzieci w wieku 9-10 oraz 12-14 lat, które pokazało, że dzieci zazwyczaj nie doceniają zagrożeń związanych z wykorzystaniem Internetu i bagatelizują konsekwencje swoich ryzykownych zachowań (dostępne na stronie: http://ec.europa.eu/information_society/activities/sip/surveys/qualitative/index_en.htm).

18 „Komisja przyjmuje do wiadomości wolę Parlamentu Europejskiego, aby obowiązek powiadamiania o naruszeniu danych osobowych nie ograniczał się do sektora komunikacji elektronicznej, ale miał również zastosowanie do takich podmiotów, jak dostawcy usług społeczeństwa informacyjnego. Tak więc Komisja niezwłocznie zainicjuje stosowne prace przygotowawcze, w tym konsultacje z zainteresowanymi stronami, w celu przedstawienia propozycji w tym zakresie do 2011 roku. […]”. Deklaracja dostępna na stronie: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0360+0+DOC+XML+V0//PL. Zob. także motyw 59 dyrektywy 2009/136/WE zmieniającej dyrektywę 2002/58/WE w sprawie prywatności elektronicznej: Ten interes użytkowników w zakresie ich powiadamiania nie ogranicza się oczywiście do sektora łączności elektronicznej, zatem na poziomie Wspólnoty jako sprawę priorytetową należy wprowadzić wyraźne obowiązkowe wymogi powiadamiania mające zastosowanie do wszystkich sektorów.

19 Artykuł 4 dyrektywy 2009/136/WE.

Komisja:

– zbada możliwości wprowadzenia do generalnych ram prawnych **ogólnego obowiązku zawiadamiania o naruszeniu ochrony danych osobowych**, w tym adresatów takich zawiadomień oraz kryteriów powstania obowiązku zawiadomienia.

*2.1.3. Poprawa kontroli nad własnymi danymi*

Dwa istotne warunki wstępne korzystania przez jednostki z wysokiego poziomu ochrony danych to: **ograniczenie przetwarzania danych przez administratorów danych stosownie do celu przetwarzania (zasada minimalizacji danych)** oraz zachowanie przez osoby, których dane dotyczą, **skutecznej kontroli nad ich własnymi danymi**. Artykuł 8 ust. 2 karty stanowi, że „Każda osoba ma prawo dostępu do zebranych danych, które jej dotyczą, i prawo do dokonania ich sprostowania". Osoby fizyczne powinny mieć zawsze możliwość dostępu do danych, poprawiania ich, usuwania lub blokowania, chyba że istnieją słuszne powody, przewidziane prawem, by im tego odmówić. Prawo to istnieje już w obecnych ramach prawnych. Jednakże metody korzystania z tego prawa nie zostały zharmonizowane, dlatego w niektórych państwach członkowskich ich wykonywanie jest w rzeczywistości łatwiejsze niż w innych. Dodatkowo stało się to szczególnie trudne w środowisku internetowym, gdzie dane są często zatrzymywane bez wiedzy lub bez zgody osoby zainteresowanej.

Dobrym przykładem są tutaj zwłaszcza funkcjonujące w Internecie sieci społecznościowe, w których sprawowanie przez osoby fizyczne skutecznej kontroli nad swoimi danymi osobowymi wiąże się ze szczególnymi wyzwaniami. Komisja otrzymała szereg zapytań ze strony osób fizycznych, które nie zawsze były w stanie odzyskać swoje dane osobowe, takie jak zdjęcia, od dostawców usług internetowych, i w związku z tym nie mogły skorzystać z przysługującego im prawa do dostępu, poprawienia i usunięcia.

Prawa te należy zatem zapisać wyraźniej i jaśniej oraz ewentualnie zwiększyć.

Dlatego też Komisja zbada sposoby:

– wzmocnienia **zasady minimalizacji danych**;

– **poprawy metod** faktycznego **korzystania z prawa do dostępu do danych, ich poprawiania, usuwania lub blokowania** (np. poprzez wprowadzenie terminów na odpowiedź na wnioski osób fizycznych, umożliwienie korzystania z praw za pomocą środków elektronicznych lub zapewnienie, że korzystanie z praw do dostępu powinno być zasadniczo zapewnione bezpłatnie);

– wyjaśnienia tzw. **„prawa do bycia zapomnianym"** tzn. prawa osób fizycznych do spowodowania usunięcia ich danych oraz zaprzestania ich przetwarzania, jeżeli przestały być potrzebne do zgodnych z prawem celów. Przykładem jest tutaj sytuacja, w której przetwarzanie odbywa się na podstawie zgody danej osoby, jeśli ta wycofała swoją zgodę lub też skończył się okres przechowywania, na który wyraziła zgodę;

– uzupełnienie praw osób, których dane dotyczą przez zapewnienie „**przenoszalności danych**" tzn. wyraźne przewidzenie prawa osób fizycznych do wycofania swoich danych (np. zdjęć lub listy przyjaciół) z jednej aplikacji lub usługi, tak by można je było przenieść do innej, w zakresie, w jakim jest to technicznie możliwe, bez przeszkód ze strony administratorów danych.

### *2.1.4. Pogłębianie świadomości społeczeństwa*

Chociaż przejrzystość ma zasadnicze znacznie, zachodzi również potrzeba pogłębienia świadomości ogółu społeczeństwa, w szczególności ludzi młodych, w zakresie zagrożeń związanych z przetwarzaniem danych osobowych i przysługujących im praw. Badanie Eurobarometru z 2008 r. pokazało, że znaczna większość osób w państwach członkowskich UE uznaje, że w ich kraju świadomość w zakresie ochrony danych osobowych jest niska[20]. Należy zatem zachęcać do działań służących pogłębianiu świadomości i promować takie działania przy wsparciu szerokiego kręgu podmiotów, tzn. organów państw członkowskich, w szczególności organów ochrony danych oraz instytucji edukacyjnych, jak również administratorów danych oraz organizacji społeczeństwa obywatelskiego. Działania te powinny obejmować środki nielegislacyjne, takie jak kampanie uświadamiające w mediach drukowanych i elektronicznych oraz dostarczanie jasnych informacji na stronach internetowych, wyraźne określenie praw przysługujących osobom, których dotyczą dane oraz odpowiedzialności administratorów danych.

Komisja zbada:

– możliwość **współfinansowania działań służących pogłębianiu świadomości w zakresie ochrony danych** z budżetu Unii;

– potrzeby i możliwości w zakresie włączenia do ram prawnych **obowiązku prowadzenia działań uświadamiających** w tej dziedzinie.

### *2.1.5. Zapewnienie świadomej i dobrowolnej zgody*

Zgodnie z obowiązującymi przepisami, jeżeli wymagane jest świadome wyrażenie zgody przez osobę fizyczną na przetwarzanie jej danych osobowych, zgoda ta powinna stanowić „konkretne i świadome, dobrowolne wskazanie" woli tej osoby, za pośrednictwem którego zgadza się ona na przetwarzanie tych danych[21]. Jednakże poszczególne państwa członkowskie różnie interpretują te warunki, poczynając od ustanowienia ogólnego wymogu pisemnej zgody po akceptowanie zgody dorozumianej.

Ponadto w środowisku internetowym – ze względu na niejasne reguły dotyczące prywatności – osoby fizyczne mają większe trudności z uzyskaniem informacji o przysługujących im prawach oraz wyrażaniem świadomej zgody. Sytuację komplikuje dodatkowo fakt, że w niektórych przypadkach nie jest nawet jasne, co stanowiłoby konkretną i świadomą, dobrowolną zgodę na przetwarzanie danych, tak jak w przypadku reklamy behawioralnej, kiedy to, według stanowiska niektórych podmiotów, użytkownik wyraża zgodę przez same ustawienia przeglądarki internetowej.

Dlatego należy wyjaśnić warunki uzyskania zgody osoby, której dane dotyczą , by zagwarantować, by zgoda była zawsze wyrażana świadomie oraz zapewnić, by osoba fizyczna była zawsze w pełni świadoma wyrażania zgody oraz tego, jakiego przetwarzania danych ona dotyczy, zgodnie z art. 8 Karty praw podstawowych UE. Jasność w zakresie zasadniczych pojęć może również sprzyjać rozwojowi inicjatyw samoregulacyjnych służących opracowaniu praktycznych rozwiązań zgodnych z prawem UE.

---

[20] Zob. Flash Eurobarometer N° 225 – Ochrona danych w Unii Europejskiej: http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

[21] Zob. art. 2 lit. h) dyrektywy 95/46/WE.

Komisja zbada możliwości **wyjaśnienia i udoskonalenia przepisów dotyczących zgody**.

*2.1.6. Ochrona danych szczególnie chronionych*

Przetwarzanie danych szczególnie chronionych, tzn. danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe albo przynależność do związków zawodowych, a także przetwarzanie danych dotyczących zdrowia lub życia seksualnego jest już obecnie ogólnie zakazane, z ograniczonymi wyjątkami, które zastosować można na pewnych warunkach, przy zapewnieniu określonych gwarancji[22]. Jednakże w świetle postępu technologicznego i innych przemian społecznych zachodzi potrzeba ponownego rozważenia obowiązujących przepisów o danych szczególnie chronionych w celu zbadania, czy należy do nich zaliczyć dodatkowe rodzaje danych, oraz dalszego sprecyzowania warunków przetwarzania tych danych. Dotyczy to przykładowo danych genetycznych, które obecnie nie są wyraźnie zaliczane do kategorii danych szczególnie chronionych.

Komisja rozważy:

- czy należy uznać inne kategorie danych, przykładowo dane **genetyczne**, za „**dane szczególnie chronione**";

– dalszą **harmonizację warunków** umożliwiających przetwarzanie kategorii danych szczególnie chronionych.

*2.1.7. Zapewnienie większej skuteczności sankcji i środków zaradczych*

Aby zagwarantować egzekwowanie norm dotyczących ochrony danych konieczne są **skuteczne przepisy o sankcjach i środkach zaradczych**. W licznych przypadkach, kiedy osoby fizyczne padają ofiarą naruszenia przepisów o ochronie danych, dotyka to równocześnie znacznej liczby innych osób w podobnej sytuacji.

W związku z powyższym Komisja:

– rozważy możliwość **rozszerzenia katalogu podmiotów wyposażonych w legitymację czynną przed sądami krajowymi** na organy ochrony danych oraz organizacje społeczeństwa obywatelskiego, jak również na **pozostałe organizacje reprezentujące interesy osób, których dane dotyczą**;

– oceni potrzebę **udoskonalenia obowiązujących przepisów o sankcjach**, np. przez wyraźne przewidzenie kar kryminalnych za poważne naruszenia ochrony danych, aby uczynić je bardziej skutecznymi.

## 2.2. Poprawa wymiaru związanego z rynkiem wewnętrznym

*2.2.1. Zwiększenie pewności prawnej oraz zapewnienie równych szans administratorom danych*

Ochrona danych w UE ma **silny wymiar związany z rynkiem wewnętrznym**, tzn. istnieje potrzeba zapewnienia swobodnego przepływu danych osobowych między państwami członkowskimi w obrębie rynku wewnętrznego. W konsekwencji harmonizacja krajowych

[22] Zob. art. 8 dyrektywy 95/46/WE.

przepisów o ochronie danych w dyrektywie nie ogranicza się do harmonizacji minimalnej, lecz zalicza się do harmonizacji, która jest ogólnie kompletna[23].

Równocześnie dyrektywa daje państwom członkowskim pole do manewru w pewnych dziedzinach oraz upoważnia je do utrzymania lub wprowadzenia szczególnych reguł dotyczących specyficznych sytuacji[24]. Kwestia ta, jak również fakt, że dyrektywa była niekiedy nieprawidłowo wdrażana przez państwa członkowskie, doprowadziły do **zróżnicowania w przepisach krajowych wdrażających dyrektywę, które stoją w sprzeczności z jednym z jej głównych celów, tj. zapewnieniem swobodnego przepływu danych osobowych na rynku wewnętrznym**. Problem ten dotyczy znacznej liczby sektorów i sytuacji, np. przetwarzania danych osobowych w kontekście zatrudnienia lub do celów zdrowia publicznego. Brak harmonizacji jest istotnie jednym z powracających i głównych problemów podnoszonych przez zainteresowane podmioty reprezentujące sektor prywatny, w szczególności przez podmioty gospodarcze, ponieważ oznacza dla nich dodatkowe koszty i obciążenia administracyjne. Dotyczy to w szczególności administratorów danych prowadzących działalność w kilku państwach członkowskich i zmuszonych do postępowania zgodnie z wymogami i praktykami obowiązującymi w każdym z tych państw. Ponadto różnice we wdrażaniu dyrektywy przez państwa członkowskie prowadzą do braku pewności prawnej, nie tylko wśród administratorów danych, lecz także osób, których dane dotyczą, zagrażając realizacji celu dyrektywy, jakim jest zapewnienie równorzędnego poziomu ochrony.

Komisja zbada sposoby osiągnięcia **dalszej harmonizacji przepisów o ochronie danych na szczeblu UE**.

*2.2.2. Zmniejszenie obciążeń administracyjnych*

Zapewnienie równych szans ograniczy potrzebę sprostania zróżnicowanym krajowym wymogom, a tym samym znacząco zmniejszy obciążenia administracyjne ponoszone przez administratorów. Kolejnym konkretnym działaniem służącym zmniejszeniu obciążeń administracyjnych oraz ograniczeniu kosztów ponoszonych przez administratorów danych byłaby **rewizja i uproszczenie obecnego systemu zawiadamiania**[25]. Wśród administratorów danych panuje ogólny konsensus co do tego, że obecny powszechny obowiązek zawiadamiania organów ochrony danych o wszelkich operacjach przetwarzania danych jest raczej uciążliwym obowiązkiem, który sam w sobie nie stanowi realnej wartości dodanej w zakresie ochrony danych osobowych osób fizycznych. Ponadto jest to jeden z tych przypadków, w których dyrektywa zostawia pewne pole manewru państwom członkowskim, które mogą zdecydować o ewentualnych wyłączeniach i uproszczeniach, jak również procedurach, które należy zrealizować.

Zharmonizowany i uproszczony system doprowadziłby do ograniczenia kosztów, jak również obciążeń administracyjnych, w szczególności dla przedsiębiorstw wielonarodowych prowadzących działalność w wielu państwach członkowskich.

---

23 Europejski Trybunał Sprawiedliwości, C-101/01, „Bodil Lindqvist", ECR [2003], I-1297, 96, 97.

24 Tamże pkt 97: Zob. także motyw 9 dyrektywy 95/46/WE.

25 Zob. art. 18 dyrektywy 95/46/WE.

Komisja zbada różne możliwości **uproszczenia i harmonizacji obecnego systemu zawiadamiania**, w tym ewentualność sporządzenia **jednolitego, ogólnounijnego formularza rejestracyjnego**.

### *2.2.3. Wyjaśnienie przepisów dotyczących prawa właściwego oraz odpowiedzialności państw członkowskich*

W pierwszym sprawozdaniu Komisji z wdrażania dyrektywy o ochronie danych przedstawionym jeszcze w 2003 r.[26] podkreślono fakt, że przepisy dotyczące prawa właściwego[27] są „w wielu wypadkach niedoskonałe, prowadząc do powstania takich rodzajów kolizji praw, których uniknięciu omawiany artykuł służy". Sytuacja nie uległa od tamtej pory poprawie, w związku z czym 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. Dotyczy to w szczególności sytuacji, w których administrator danych podlega różnym wymogom w poszczególnych państwach członkowskich, gdy przedsiębiorstwo międzynarodowe prowadzi działalność w więcej niż jednym państwie członkowskim lub gdy administrator danych nie ma siedziby w UE, ale świadczy usługi na rzecz rezydentów UE.

**Sytuację komplikuje dodatkowo globalizacja i postęp techniczny**: zakres działalności administratorów danych obejmuje coraz więcej państw członkowskich i jurysdykcji – świadczą oni usługi i udzielają wsparcia przez 24 godziny na dobę. Rynek internetowy bardzo ułatwia administratorom danych mającym siedzibę poza Europejskim Obszarem Gospodarczym (EOG)[28] świadczenie usług na odległość oraz przetwarzanie danych osobowych w środowisku internetowym, i często trudno jest ustalić lokalizację danych osobowych oraz wyposażenia używanego w danym czasie (np. w aplikacjach i usługach służących do „przetwarzania w chmurze".

Komisja przyjmuje jednak stanowisko, że fakt, iż dane osobowe przetwarzane są przez administratora danych mającego siedzibę w państwie trzecim, nie powinien pozbawiać osób fizycznych ochrony, do której osoby te uprawnione są na mocy Karty praw podstawowych UE oraz unijnych przepisów o ochronie danych.

Komisja zbada, w jaki sposób **zrewidować i wyjaśnić obowiązujące przepisy o prawie właściwym**, w tym obecne kryteria ustalania tego prawa, aby zwiększyć pewność prawną, wyjaśnić zakres odpowiedzialności państw członkowskich za stosowanie przepisów o ochronie danych oraz ostatecznie zapewnić unijnym osobom, których dane dotyczą, ten sam stopień ochrony, niezależnie od lokalizacji geograficznej administratora danych.

### *2.2.4. Wzmocnienie odpowiedzialności administratorów danych*

Uproszczenia administracyjne **nie powinny prowadzić do ogólnego zmniejszenia zakresu odpowiedzialności administratorów danych za zapewnienie skutecznej ochrony danych.** Wręcz przeciwnie, Komisja uważa, że ich obowiązki powinny zostać wyraźniej określone w ramach prawnych, w tym w odniesieniu do mechanizmów kontroli wewnętrznej oraz

---

[26] Sprawozdanie Komisji – Pierwsze sprawozdanie z wdrażania dyrektywy o ochronie danych (95/46/WE) – COM(2003) 265.

[27] Zob. art. 4 dyrektywy 95/46/WE.

[28] Europejski Obszar Gospodarczy obejmuje Norwegię, Liechtenstein i Islandię.

współpracy z organami nadzorującymi ochronę danych. Poza tym należy zagwarantować, by taka odpowiedzialność spoczywała również na administratorach, na których ciąży obowiązek zachowania tajemnicy zawodowej (np. adwokatach), jak również na tych, którzy, co jest coraz powszechniejszym zjawiskiem, przekazują przetwarzanie danych innym podmiotom (np. podmiotom przetwarzającym).

Dlatego też Komisja zbada sposoby **zagwarantowania, by administratorzy danych wdrożyli skuteczne polityki i mechanizmy mające zapewnić zgodność z przepisami o ochronie danych.** Weźmie przy tym pod uwagę obecną dyskusję na temat ewentualnego wprowadzenia tzw. zasady „accountability"[29]. Nie miałoby to na celu zwiększenia obciążeń administracyjnych dla administratorów danych, ponieważ środki te skoncentrowane byłyby raczej na ustanowieniu gwarancji i mechanizmów zapewniających skuteczniejsze przestrzeganie norm ochrony danych, równocześnie ograniczając i upraszczając niektóre formalności administracyjne, takie jak zawiadomienia (*zob. pkt 2.2.2 powyżej*).

Propagowanie wykorzystania technologii podnoszących poziom ochrony prywatności (tzw. PETs), jak już wskazano w komunikacie Komisji z 2007 r. poświęconym tej kwestii, jak również zasady „uwzględniania ochrony prywatności w fazie projektowania", mogłyby tutaj odegrać istotną rolę, także w zapewnieniu bezpieczeństwa danych[30].

Komisja zbada następujące elementy w celu wzmocnienia odpowiedzialności administratorów danych:

- wprowadzenie obowiązku powołania niezależnych **inspektorów ochrony danych** oraz harmonizacja przepisów dotyczących ich zadań i kompetencji[31], przy równoczesnym rozważeniu możliwości ustanowienia odpowiedniego progu, w celu zapobieżenia nadmiernym obciążeniom administracyjnym, w szczególności dla małych i średnich przedsiębiorstw;
- zawarcie w ramach prawnych obowiązku przeprowadzania przez administratorów danych **oceny skutków dotyczącej ochrony danych** w określonych przypadkach, przykładowo gdy przetwarzane są dane szczególnie chronione lub gdy dany rodzaj przetwarzania wiąże się ze szczególnymi zagrożeniami, w szczególności gdy wykorzystywane są określone technologie, mechanizmy lub procedury, w tym profilowanie lub nadzór wideo;
- dalsze promowanie wykorzystania technologii podnoszących poziom ochrony prywatności w celu faktycznej realizacji koncepcji **„uwzględniania ochrony prywatności w fazie projektowania".**

29 Zob. w szczególności opinię przyjętą przez Grupę Roboczą Art. 29 w dniu 13 lipca, 3/2010.

30 W sprawie tych technologii zob. Komunikat Komisji dla Parlamentu Europejskiego i Rady w sprawie lepszej ochrony danych z wykorzystaniem technologii na rzecz ochrony prywatności - COM(2007) 228. Zasada „uwzględniania ochrony prywatności w fazie projektowania" oznacza, że kwestie prywatności i ochrony danych uwzględniane są w całym cyklu technologicznym, poczynając od etapu wczesnego projektowania technologii, po ich wdrożenie, wykorzystanie i ostateczne usunięcie. Zasadę tę wymieniono między innymi w komunikacie Komisji w sprawie „Europejskiej agendy cyfrowej", COM(2010)245.

31 W szeregu państw członkowskich wykorzystano już obecną możliwość powołania przez administratora danych inspektora ochrony danych w celu zapewnienia, w sposób niezależny, zgodności z unijnymi i krajowymi przepisami o ochronie danych oraz wspierania osób fizycznych (zob. np. „Beauftragter für den Datenschutz" w Niemczech oraz „correspondant informatique et libertés (CIL)" we Francji).

### *2.2.5. Zachęcanie do inicjatyw w dziedzinie samoregulacji oraz analiza unijnych systemów certyfikacji*

Komisja podtrzymuje stanowisko, że **inicjatywy samoregulacyjne** ze strony administratorów danych mogą **przyczynić się do lepszego egzekwowania przepisów o ochronie danych**. Obecne przepisy dotyczące samoregulacji w dyrektywie o ochronie danych, tzn. przewidujące możliwość sporządzania kodeksów postępowania[32], były jak dotąd rzadko wykorzystywane i zainteresowane podmioty z sektora prywatnego nie uznają ich za zadowalające.

Ponadto Komisja zbada możliwość stworzenia unijnych **systemów certyfikacji** (**np. „certyfikatów ochrony prywatności")** dla procesów, technologii, produktów i usług odpowiadających wymogom ochrony prywatności[33]. Dzięki temu z jednej strony osoby fizyczne zyskałyby orientację jako użytkownicy takich technologii, produktów oraz usług, z drugiej zaś strony miałoby to także znaczenie dla kwestii odpowiedzialności administratorów danych: administrator mógłby powołać się na wybór certyfikowanych technologii, produktów lub usług na dowód wypełnienia ciążących na nim obowiązków (zob. pkt 2.2.4 powyżej). Oczywiście konieczne byłoby **zapewnienie wiarygodności takich certyfikatów** oraz sprawdzenie ich zgodności ze zobowiązaniami prawnymi i międzynarodowymi normami technicznymi.

Komisja:

– zbada sposoby **dalszego zachęcania do inicjatyw samoregulacyjnych**, w tym aktywnego propagowania kodeksów postępowania.

– zbada realne możliwości ustanowienia **unijnego systemu certyfikacji** w obszarze prywatności i ochrony danych.

## 2.3. Rewizja przepisów o ochronie danych w obszarze współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych

Dyrektywa o ochronie danych dotyczy wszystkich działań związanych z ochroną danych prowadzonych w państwach członkowskich, zarówno w sektorze publicznym, jak i prywatnym. Nie ma ona jednak zastosowania do przetwarzania danych osobowych „w ramach działalności wykraczającej poza zakres prawa Wspólnoty", takiej jak działalność prowadzona w ramach współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych[34]. Traktat lizboński zniósł jednak uprzednią „strukturę filarów" UE oraz wprowadził nową, wszechstronną podstawę prawną dla ochrony danych osobowych we wszystkich politykach UE[35]. W tym kontekście oraz w świetle Karty praw podstawowych UE, w komunikatach Komisji w sprawie programu sztokholmskiego oraz sztokholmskiego planu działania[36] podkreślono potrzebę zapewnienia „systemu pełnej ochrony" oraz „wzmocnienia stanowiska UE dotyczącego ochrony danych osobowych w kontekście wszystkich obszarów polityki UE, w tym w dziedzinie egzekwowania prawa i zapobiegania przestępstwom"

---

32 Zob. art. 27 dyrektywy 95/46/WE.

33 W odniesieniu do tej kwestii zob. również komunikat Komisji o technologiach podnoszących poziom ochrony prywatności, przypis 30.

34 Zob. art. 3 ust. 2 tiret pierwsze dyrektywy 95/46/WE.

35 Zob. art. 16 TFUE.

36 Zob. COM(2009) 262 z 10.6.2009 oraz COM(2010) 171 z 20.4.2010.

Unijnym instrumentem ochrony danych osobowych w obszarze współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych jest **decyzja ramowa 2008/977/WSiSW** [37]. Decyzja ramowa stanowi istotny krok naprzód w dziedzinie, w której bardzo potrzebne są wspólne standardy ochrony danych. Konieczne są jednak dalsze prace.

**Decyzja ramowa dotyczy wyłącznie transgranicznej wymiany danych osobowych w granicach UE** i nie ma zastosowania do wewnętrznych operacji przetwarzania w państwach członkowskich. W praktyce bardzo trudno jest odróżnić obie sytuacje, co może utrudniać faktyczne wprowadzenie w życie i stosowanie decyzji ramowej[38].

**Decyzja ramowa zawiera** również **zbyt szerokie wyłączenie zasady celowości**. Pozostałe niedociągnięcia to: brak przepisów stanowiących, że należy wyodrębnić różne kategorie danych odpowiednio do ich stopnia poprawności i wiarygodności, że dane oparte na faktach należy odróżnić od danych opartych na opiniach i osobistych ocenach[39] oraz że należy wprowadzić rozróżnienie między różnymi kategoriami osób, których dane dotyczą (przestępcy, podejrzani, pokrzywdzeni, świadkowie itd.), i ustanowić specjalne gwarancje dotyczące danych odnoszących się do osób spoza kręgu podejrzanych[40].

Co więcej, **decyzja ramowa nie zastępuje różnych sektorowych aktów legislacyjnych dotyczących współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych przyjętych na szczeblu UE**[41], w szczególności tych, które regulują funkcjonowanie Europolu, Eurojustu, systemu informacyjnego Schengen (SIS) oraz systemu informacji celnej (CIS)[42], i które przewidują szczególne systemy ochrony danych, lub które zazwyczaj odsyłają do instrumentów ochrony danych Rady Europy. W odniesieniu do działalności w obszarze współpracy policji i wymiarów sprawiedliwości wszystkie państwa członkowskie zaakceptowały rekomendację Rady Europy R (87) 15 określającą zasady konwencji 108 w sektorze policji. Nie jest to jednak wiążący instrument prawny.

**Sytuacja ta może wpływać bezpośrednio na możliwość wykonywania przez osoby fizyczne ich prawa do ochrony danych w tym obszarze** (to znaczy uzyskania wiedzy o tym, jakie dane osobowe ich dotyczące są przedmiotem przetwarzania i wymiany, przez kogo i w jakim celu oraz w jaki sposób osoby te mogą korzystać ze swoich praw, np. z prawa dostępu do danych na ich temat).

Cel, jakim jest ustanowienie całościowego i spójnego systemu w UE i wobec państw trzecich pociąga za sobą **potrzebę rozważenia rewizji obecnych przepisów o ochronie danych w obszarze współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych**.

---

37 Decyzja ramowa 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 (Dz.U. L 350 z 30.12.2008, s. 60). Decyzja ta przewiduje jedynie minimalną harmonizację norm ochrony danych.

38 Rozróżnienie takie nie występuje we właściwych instrumentach Rady Europy, takich jak: Konwencja o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, CETS nr 108) oraz jej Protokół dodatkowy dotyczący organów nadzorczych oraz transgranicznych przepływów danych (ETS nr 181) oraz Rekomendacja Rady Europy R(87) 15 dotycząca ochrony danych osobowych wykorzystywanych w sektorze policji, przyjęta dnia 17 września 1987 r.

39 Tak jak wymaga tego zasada 3.2 rekomendacji nr R(87) 15.

40 Wbrew zasadzie 2 rekomendacji nr R (87) 15 i związanym z nią sprawozdaniom z oceny.

41 Zob. przegląd takich instrumentów w komunikacie Komisji „Przegląd zarządzania informacjami w przestrzeni wolności, bezpieczeństwa i sprawiedliwości", COM (2010) 385.

42 Na mocy właściwych instrumentów ustanowiono wspólne organy nadzorcze w celu zagwarantowania nadzoru nad ochroną danych, obok ogólnych kompetencji nadzorczych Europejskiego Inspektora Ochrony Danych, nad instytucjami, organami, urzędami i agencjami Unii, w oparciu o rozporządzenie (WE) nr 45/2001.

Komisja podkreśla, że pojęcie całościowego systemu ochrony danych nie wyklucza szczególnych przepisów o ochronie danych w sektorze policyjnym i sądowym funkcjonujących w obrębie ogólnych ram, przy należytym uwzględnieniu specyfiki tych obszarów, jak zaznaczono w deklaracji 21 dołączonej do traktatu lizbońskiego. Oznacza to przykładowo konieczność rozważenia, w jakim zakresie korzystanie przez osoby fizyczne z niektórych praw do ochrony danych zagroziłoby zapobieganiu, dochodzeniu, wykrywaniu lub ściganiu przestępstw lub wykonywaniu kar kryminalnych w konkretnej sprawie.

Komisja w szczególności:

– rozważy **rozszerzenie stosowania ogólnych przepisów o ochronie danych na obszar współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych**, w tym na przetwarzanie na szczeblu krajowym, zapewniając równocześnie, w razie potrzeby, zharmonizowane **ograniczenia** niektórych praw do ochrony danych przysługujących osobom fizycznym, np. prawa do dostępu lub zasady przejrzystości;

– zbada potrzebę wprowadzenia **szczególnych, zharmonizowanych przepisów** w obrębie nowych ram ochrony danych, przykładowo dotyczących ochrony danych przy przetwarzaniu **danych genetycznych** na potrzeby prawa karnego oraz rozróżnienia poszczególnych kategorii osób, których dane dotyczą (świadków; podejrzanych itd.) w obszarze współpracy policji i wymiarów sprawiedliwości w sprawach karnych;

– zainicjuje w 2011 r. **konsultacje** z wszystkimi zainteresowanymi podmiotami na temat najlepszych metod **zmiany obecnych systemów nadzoru w obszarze współpracy policji i wymiarów sprawiedliwości w sprawach karnych**, aby zagwarantować skuteczny i spójny nadzór nad ochroną danych we wszystkich unijnych instytucjach, organach, urzędach i agencjach;

– oceni potrzebę **uzgodnienia**, w perspektywie długoterminowej, **różnych obowiązujących szczegółowych przepisów sektorowych przyjętych w poszczególnych instrumentach na szczeblu UE na potrzeby współpracy policji i wymiarów sprawiedliwości w sprawach karnych** z nowymi ogólnymi ramami ochrony danych.

## 2.4. Globalny wymiar ochrony danych

### *2.4.1. Wyjaśnienie i uproszczenie przepisów dotyczących międzynarodowych transferów danych*

Jednym ze środków umożliwiających transfer danych osobowych poza obszar UE i EOG jest tzw. **„ocena adekwatności”**. Obecnie adekwatność państwa trzeciego, tzn. czy zapewnia ono poziom ochrony uznawany przez UE za adekwatny, może zostać ustalona przez Komisję oraz państwa członkowskie.

Skutkiem ustalenia adekwatności przez Komisję jest to, że dane osobowe mogą być swobodnie przekazywane z 27 państw członkowskich UE oraz trzech państw członkowskich EOG do tego państwa trzeciego bez konieczności stosowania żadnych dalszych gwarancji. Jednakże dokładne wymogi uznania adekwatności przez Komisję nie są obecnie w zadowalającym stopniu sprecyzowane w dyrektywie o ochronie danych. Co więcej decyzja ramowa nie przewiduje podejmowania takiej decyzji przez Komisję.

W niektórych państwach członkowskich adekwatność ocenia w pierwszym rzędzie administrator danych, który sam przekazuje dane osobowe do państwa trzeciego, czasem działając pod nadzorem następczym organu nadzorującego ochronę danych. Sytuacja ta może

prowadzić do przyjmowania różnych strategii oceny poziomu adekwatności państw trzecich lub organizacji międzynarodowych oraz **wiąże się z niebezpieczeństwem, że poziom ochrony osób, których dane dotyczą, przewidziany w państwie trzecim zostanie różnie oceniony przez poszczególne państwa**. Podobnie, obecne instrumenty prawne nie zawierają szczegółowych, zharmonizowanych wymogów odnośnie do tego, jakie transfery można uznać za zgodne z prawem. Prowadzi to do zróżnicowanych praktyk w poszczególnych państwach członkowskich.

Co więcej, w odniesieniu do transferów danych do państw trzecich niezapewniających adekwatnego poziomu ochrony, stosowane przez Komisję obecnie standardowe klauzule o transferze danych osobowych do administratorów[43] i przetwarzającym[44] nie zostały opracowane na potrzeby sytuacji wykraczających poza ramy umowne i, przykładowo, nie mogą być wykorzystane w przypadku transferów między organami administracji publicznej.

Ponadto umowy międzynarodowe zawarte przez UE lub jej państwa członkowskie wymagają często włączenia przepisów ochrony danych oraz przepisów szczególnych. Może to prowadzić do powstania zróżnicowanych tekstów zawierających niespójne przepisy i prawa, a tym samym otwartych na zróżnicowaną interpretację, ze szkodą dla osoby, której dane dotyczą . W związku z tym Komisja ogłosiła, że będzie pracować nad zasadniczymi elementami ochrony danych osobowych w umowach między Unią i państwami trzecimi zawieranych na potrzeby egzekwowania prawa[45].

Również inne środki, które zostały opracowane w formie samoregulacji, takie jak wewnętrzne kodeksy postępowania zwane „wewnętrznymi regułami korporacyjnymi”[46], mogą stanowić użyteczne narzędzie zgodnego z prawem przekazywania danych między spółkami należącymi do tej samej grupy korporacyjnej. Zainteresowane podmioty zasugerowały jednak, że mechanizm ten mógłby być dalej udoskonalony, a jego wdrażanie ułatwione.

Aby zaradzić zidentyfikowanym problemom zachodzi **ogólna potrzeba poprawy obecnych mechanizmów umożliwiających międzynarodowe transfery danych osobowych**, przy równoczesnym zapewnieniu odpowiedniej ochrony danych przekazywanych i przetwarzanych poza UE i EOG.

---

43 Decyzja Komisji 2001/497/WE z dnia 15 czerwca 2001 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich, na mocy dyrektywy 95/46/WE (Dz.U. L 181 z 4.7.2001, s. 19); decyzja Komisji 2002/16/WE z dnia 27 grudnia 2001 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych przetwarzającym dane mającym siedzibę w państwach trzecich, na mocy dyrektywy 95/46/WE (Dz.U. L 6 z 10.1.2002, s. 52); decyzja Komisji 2004/915/WE z dnia 27 grudnia 2004 r. zmieniająca decyzję 2001/497/WE w zakresie wprowadzenia alternatywnego zestawu standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich (Dz.U. L 385 z 29.12.2004, s. 74).

44 Decyzja Komisji z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach trzecich na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady (Dz.U. L 39 z 12.2.2010, s. 5).

45 Sztokholmski plan działania, zob. przypis 36.

46 „Wiążące reguły korporacyjne” to kodeksy postępowania oparte na europejskich normach ochrony danych sporządzane i realizowane dobrowolnie przez organizacje wielonarodowe w celu zapewnienia odpowiednich gwarancji w zakresie przekazywania lub kategorii przekazywania danych osobowych między spółkami należącymi do tej samej grupy korporacyjnej i związanymi tymi regułami korporacyjnymi. Zob. http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf.

Komisja zamierza zbadać, w jaki sposób:

– **poprawić i uprościć obecne procedury** międzynarodowego przekazywania danych, w tym prawnie wiążące instrumenty oraz „wiążące reguły korporacyjne" w celu zagwarantowania **bardziej jednolitego i spójnego unijnego podejścia** wobec państw trzecich i organizacji międzynarodowych;

– **wyjaśnić procedurę badania adekwatności przez Komisję** oraz sprecyzować **kryteria i wymogi** w zakresie oceny poziomu ochrony danych w państwie trzecim lub organizacji międzynarodowej;

– zdefiniować **zasadnicze elementy unijnej ochrony danych**, które mogą być wykorzystywane we wszystkich rodzajach umów międzynarodowych.

*2.4.2. Propagowanie uniwersalnych zasad*

Przetwarzanie danych jest zglobalizowane i wymaga stworzenia uniwersalnych zasad ochrony osób fizycznych w zakresie przetwarzania danych osobowych.

Unijne ramy prawne w obszarze ochrony danych służyły często jako **punkt odniesienia dla państw trzecich przy regulowaniu kwestii ochrony danych**. Ich skutki i oddziaływanie, na terytorium Unii i poza nim, miały niezwykle istotną wagę. **Dlatego Unia Europejska musi pozostać motorem rozwoju i promocji międzynarodowych norm prawnych i technicznych w dziedzinie ochrony danych osobowych**, w oparciu o właściwe akty unijne oraz inne europejskie instrumenty dotyczące ochrony danych. Ma to szczególnie istotne znaczenie w ramach unijnej polityki rozszerzenia.

Jeżeli chodzi o międzynarodowe normy techniczne opracowane przez organizacje normalizacyjne, Komisja uważa, że spójność przyszłych ram prawnych i takich norm jest bardzo istotna dla zapewnienia jednolitego i praktycznego wdrażania norm ochrony danych przez administratorów danych.

Komisja:

– będzie w dalszym ciągu **wspierać opracowywanie wysokich norm prawnych i technicznych w obszarze ochrony danych** w państwach trzecich i na szczeblu międzynarodowym;

– dążyć do zagwarantowania **zasady wzajemności ochrony** w międzynarodowych działaniach Unii, w szczególności w odniesieniu do osób, których dane dotyczą, których dane są eksportowane z UE do państw trzecich;

– **zacieśni w tym celu swoją współprace z państwami trzecimi oraz organizacjami międzynarodowymi**, takimi jak OECD, Rada Europy, Organizacja Narodów Zjednoczonych i innymi regionalnymi organizacjami;

– **będzie uważnie śledzić proces opracowywania międzynarodowych norm technicznych przez organizacje normalizacyjne** takie jak CEN i ISO, by zapewnić użyteczne uzupełnianie nimi przepisów prawnych oraz zagwarantować operacyjną, skuteczną realizację kluczowych wymogów w dziedzinie ochrony danych.

## 2.5. Zapewnienie lepszych rozwiązań instytucjonalnych w celu skuteczniejszego egzekwowania przepisów o ochronie danych

Wprowadzanie w życie i realizacja zasad i reguł ochrony danych ma zasadnicze znaczenie dla zagwarantowania przestrzegania praw osób fizycznych.

W tym kontekście **kluczową rolę** w egzekwowaniu przepisów o ochronie danych pełnią **organy ochrony danych**. Są one niezależnymi strażnikami podstawowych praw i wolności w odniesieniu do ochrony danych osobowych. Osoby fizyczne oczekują od nich, że będą chronić ich dane osobowe oraz dopilnują, by przetwarzanie danych odbywało się zgodnie z prawem. Z tej przyczyny Komisja uważa, że należy wzmocnić ich rolę, w szczególności mając na względzie niedawne orzeczenie ETS w sprawie ich niezależności[47], oraz że należy im zapewnić kompetencje niezbędne do prawidłowego wykonywania powierzonych im zadań zarówno na szczeblu krajowym, jak i w toku wzajemnej współpracy.

Komisja uznaje równocześnie, że **organy ochrony danych powinny zacieśnić wzajemną współpracę i lepiej koordynować swoje działania**, w szczególności mierząc się z problemami, które mają, ze swej natury, wymiar transgraniczny. Dotyczy to w szczególności przypadku, w którym przedsiębiorstwa wielonarodowe mają siedzibę w kilku państwach członkowskich i prowadzą w każdym z nich swoją działalność, lub gdy niezbędny jest skoordynowany nadzór ze strony Europejskiego Inspektora Ochrony Danych[48].

W tym kontekście **istotną rolę odegrać może Grupa Robocza Art. 29**[49], która już teraz ma za zadanie, obok swoich funkcji doradczych[50], przyczyniać się do jednolitego stosowania unijnych przepisów o ochronie danych na szczeblu krajowym. Jednakże dalsze zróżnicowane – niezależnie od tego, że wyzwania w zakresie ochrony danych są jednakowe w całej UE – stosowanie i interpretowanie przepisów UE przez organy ochrony danych nakazywałoby wzmocnić rolę tej grupy roboczej na etapie koordynacji stanowisk organów ochrony danych oraz zapewnić bardziej jednolite stosowanie na szczeblu krajowym, a tym samym równorzędny poziom ochrony danych.

---

47 Wyrok ETS z 9.3.2010, Komisja przeciwko Niemcom, sprawa C-518/07.

48 Dotyczy to obecnie dużych systemów informatycznych, np. SIS (zob. art. 46 rozporządzenia (WE) nr 1987/2006 – Dz.U. L 318 z 28.12.2006, s. 4) oraz VIS (zob. art. 43 rozporządzenia (WE) nr 767/2008 – Dz.U. L 218 z 13.8.2006, s. 60).

49 Grupa Robocza Art. 29 to organ doradczy, w którym zasiadają: po jednym przedstawicielu każdego państwa członkowskiego, organy ochrony danych, Europejski Inspektor Ochrony Danych oraz przedstawiciel Komisji (bez prawa głosu), która zapewnia również obsługę sekretarską. Zob. http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm .

50 Grupa Robocza Art. 29 ma za zadanie doradzać Komisji w sprawie poziomu ochrony w UE oraz w państwach trzecich, jak również w kwestii wszelkich innych środków dotyczących przetwarzania danych osobowych.

Komisja zbada:

– w jaki sposób **wzmocnić, wyjaśnić i zharmonizować status i kompetencje krajowych organów ochrony danych** w obrębie nowych ram prawnych, włączając pełną realizację koncepcji „całkowitej niezależności”[51];

– 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. Może to obejmować **wzmocnienie roli krajowych organów nadzorujących ochronę danych, lepszą koordynację ich pracy za pośrednictwem Grupy Roboczej Art. 29 (która powinna stać się bardziej przejrzystym organem) lub stworzenie mechanizmu zapewniającego spójność na rynku wewnętrznym, podlegającego Komisji Europejskiej.**

## 3. WNIOSEK: PERSPEKTYWY

Podobnie jak technologie, sposoby korzystania z naszych danych osobowych i ich obiegu w naszym społeczeństwie podlegają stałym zmianom. Prawodawcy stoją w związku z tym przed wyzwaniem, jakim jest ustanowienie ram prawnych, które przejdą próbę czasu. Po zakończeniu procesu reform europejskie przepisy o ochronie danych powinny w dalszym ciągu, przez kolejne pokolenia gwarantować wysoki poziom ochrony oraz pewność prawną – w równym stopniu – osobom fizycznym, administracji publicznej oraz przedsiębiorstwom na rynku wewnętrznym. Niezależnie od tego, jak skomplikowana będzie sytuacja lub jak zaawansowane będą technologie, musi panować jasność co do obowiązujących przepisów i norm, które organy krajowe muszą egzekwować, i których przedsiębiorstwa oraz twórcy technologii muszą przestrzegać. Osoby fizyczne powinny mieć również jasny obraz przysługujących im praw.

**Całościowe podejście Komisji** mające stanowić odpowiedź na problemy zaznaczone w niniejszym komunikacie i służące realizacji wymienionych w nim celów, będzie podstawą dalszych dyskusji z innymi instytucjami europejskimi oraz zainteresowanymi podmiotami oraz zostanie na dalszym etapie przekute na konkretne propozycje i wnioski, zarówno o charakterze legislacyjnym, jak i nielegislacyjnym. W tym celu Komisja z zadowoleniem przyjmie komentarze na temat problemów poruszonych w niniejszym komunikacie.

Na tej podstawie, po przeprowadzaniu oceny skutków i przy uwzględnieniu Karty praw podstawowych UE, Komisja **zaproponuje w 2011 r. przepisy** zmierzające do rewizji 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 realizowane będą środki nielegislacyjne, takie jak zachęcanie do samoregulacji oraz badanie możliwości wprowadzenia unijnych certyfikatów prywatności.

Drugim krokiem Komisji będzie **ocena potrzeby dostosowania innych instrumentów prawnych** do nowych ogólnych ram ochrony danych. Dotyczy to w pierwszym rzędzie rozporządzenia (WE) nr 45/2001, którego przepisy trzeba będzie dostosować do nowych

[51] Zob. wyrok ETS z 9.3.2010, Komisja przeciwko Niemcom, sprawa C-518/07.

ogólnych ram prawnych. Na dalszym etapie trzeba będzie również uważnie zbadać wpływ na inne instrumenty sektorowe.

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. Obecny przegląd instrumentów ochrony danych nie wpływa na obowiązek państw członkowskich w zakresie wprowadzenia w życie oraz zapewnienia prawidłowego stosowania obowiązujących instrumentów prawnych dotyczących ochrony danych osobowych[52].

Wysoki i jednolity poziom ochrony danych w UE będzie najlepszą metodą zapewnienia powszechnej akceptacji dla unijnych norm ochrony danych oraz ich promowania na świecie.

[52] Dotyczy to również decyzji ramowej Rady 2008/977/WSiSW. Państwa członkowskie muszą podjąć niezbędne środki, by dopełnić wymogów zapisanych w przepisach decyzji ramowej przed dniem 27 listopada 2010 r.