



**02356/09/EN**  
**WP 168**

**Przyszłość prywatności**

**Wspólny wkład do Konsultacji Komisji Europejskiej w sprawie ram  
prawnych dla podstawowego prawa do ochrony danych osobowych**

**Przyjęty w dniu 1 grudnia 2009 r.**

Niniejsza Grupa Robocza została powołana na mocy artykułu 29 Dyrektywy 95/46/WE. Jest to niezależny europejski organ doradczy w sprawach ochrony danych i prywatności. Jego zadania opisane zostały w artykule 30 Dyrektywy 95/46/WE i artykule 15 Dyrektywy 2002/58/WE.

Obsługę Sekretariatu zapewnia Dyrekcja D (Prawa podstawowe i Obywatelstwo) Komisji Europejskiej, Dyrekcja Generalna ds. Sprawiedliwości, Wolności i Bezpieczeństwa, B-1049 Bruksela, Belgia, Biuro nr LX-46 01/190.

Strona internetowa: [http://ec.europa.eu/justice\\_home/fsj/privacy/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm)

Grupa Robocza ds. Policji i Wymiaru Sprawiedliwości została powołana jako grupa robocza Konferencji Europejskich Organów Ochrony Danych. Do jej zadań należy monitorowanie i badanie wydarzeń w obszarze policji i egzekwowania prawa, aby stawić czoła rosnącym wyzwaniom w zakresie ochrony prywatności osób fizycznych w odniesieniu do przetwarzania danych osobowych.

## Streszczenie

W dniu 9 lipca 2009 r. Komisja zainicjowała Konsultacje w sprawie ram prawnych dla podstawowego prawa do ochrony danych osobowych. W ramach tych konsultacji Komisja pyta o poglądy na temat nowych wyzwań dla ochrony danych osobowych, w szczególności w kontekście nowych technologii i globalizacji. Chce uzyskać odpowiedzi na pytania, czy obecne ramy prawne odpowiadają tym wyzwaniom oraz jakie przyszłe działania będą potrzebne w celu stawienia czoła zidentyfikowanym wyzwaniom. Niniejszy dokument przedstawia wspólną reakcję Grupy Roboczej Artykułu 29 (WP 29) oraz Grupy Roboczej ds. Policji i Wymiaru Sprawiedliwości (WPPJ) na te konsultacje.

Główne przesłanie niniejszego wkładu stanowi stwierdzenie, że najważniejsze zasady ochrony danych wciąż obowiązują w obliczu nowych wyzwań. Poziom ochrony danych w UE może podnieść się dzięki lepszemu zastosowaniu istniejących zasad ochrony danych w praktyce. Nie oznacza to jednak, że nie są potrzebne zmiany legislacyjne. Wręcz przeciwnie, warto wykorzystać tę możliwość, by:

- Wyjaśnić zastosowanie niektórych spośród najważniejszych zasad ochrony danych (np. zgody i przejrzystości).
- Uaktualnić ramy prawne poprzez wprowadzenie dodatkowych zasad (takich jak „prywatność w fazie projektowania” i „rozliczalność”).
- Zwiększyć skuteczność systemu poprzez modernizację założeń dyrektywy 95/46/WE (np. ograniczenie biurokracji).
- Włączyć najważniejsze zasady ochrony danych w jedne kompleksowe ramy prawne, odnoszące się także do współpracy policyjnej i sądowej w sprawach karnych.

Rozdział 1 stanowi wstęp i pokrótce przedstawia historię i kontekst ochrony danych w UE.

Rozdział 2 proponuje wprowadzenie kompleksowych ram prawnych. Potwierdza potrzebę istnienia zasad szczególnych (*leges speciales*), jeśli są one zgodne z ideą kompleksowych ram prawnych i z najważniejszymi zasadami. Najważniejsze zasady i zabezpieczenia związane z ochroną danych winny mieć zastosowanie do przetwarzania danych we wszystkich sektorach.

Rozdziały 3 i 4 omawiają najważniejsze wyzwania stojące przed ochroną danych.

Rozdział 3, dotyczący globalizacji, stwierdza, że na mocy prawa UE, prawo do ochrony danych jest prawem podstawowym. UE i jej państwa członkowskie winny zagwarantować to fundamentalne prawo wszystkim osobom objętym ich jurysdykcją. Obywatele powinni być objęci ochroną również jeżeli ich dane są przetwarzane poza terytorium UE. W związku z powyższym, wzywa się Komisję do podjęcia inicjatyw zmierzających do dalszego rozwoju międzynarodowych globalnych standardów w zakresie ochrony danych osobowych. Ponadto, proces uznawania odpowiedniości wymaga poprawienia. Odpowiednimi instrumentami ochrony danych osobowych w kontekście globalnym mogą być także umowy międzynarodowe, a przyszłe ramy prawne mogą wymieniać warunki zawierania takich umów państwami trzecimi. Przetwarzanie danych poza obszarem UE mogą chronić także Wiążące Reguły Korporacyjne (BCR). Przepisy w sprawie BCR powinny być rozwinięte i włączone w zakres nowych ram

prawnych. Jeśli chodzi o prawo właściwe, Grupa Robocza Art. 29 zamierza doradzać Komisji w tej kwestii w ciągu najbliższego roku.

Rozdział 4 w sprawie rozwoju technologicznego stwierdza, że dyrektywa 95/46/WE zachowała aktualność mimo zmian technologicznych, gdyż zawarte w niej zasady i pojęcia są rozsądne i neutralne technologicznie i pozostają równie ważne i możliwe do zastosowania w dzisiejszym sieciowym świecie. Rozwój technologiczny zwiększył zagrożenia dla danych i prywatności obywateli, a dla ich zrównoważenia, w nowych ramach prawnych należy wprowadzić zasadę „Prywatności w fazie projektowania”: ochrona danych i prywatności powinna być włączona w projekt technologii informacyjnych i komunikacyjnych. Wdrożenie takiej zasady podkreśliłoby konieczność zastosowania technologii wspierających prywatność, domyślnych ustawień prywatności i narzędzi niezbędnych dla umożliwienia użytkownikom lepszej ochrony ich danych. Zasada „Prywatności w fazie projektowania” winna zatem być wiążąca nie tylko dla administratorów, ale także dla projektantów i producentów technologii. Ponadto. W razie potrzeby, powinny być regulowane poszczególne aspekty technologiczne, w które należy zasady ochrony danych i prywatności.

Rozdziały 5, 6 i 7 stwierdzają, że w związku z wyzwaniami stojącymi przed ochroną danych, różne strony zainteresowane winny odgrywać większą rolę.

Zmiany w zachowaniu i roli osób, których dane dotyczą i doświadczenie w stosowaniu dyrektywy 95/46/WE wymagają zwiększenia roli osób, których dane dotyczą w ramach prawnych ochrony danych. Rozdział 5 zawiera propozycję przyznania osobom, których dane dotyczą dodatkowych uprawnień, by umożliwić im odgrywanie bardziej aktywnej roli. Wymaga to, m.in. ulepszenia mechanizmów odszkodowawczych: zwiększenia możliwości wykonywania praw przez osoby, których dane dotyczą, w tym wprowadzenia pozwów zbiorowych i łatwiej dostępnych, skuteczniejszych i tańszych procedur skargowych i polubownych. Ponadto, nowe ramy prawne winny przedstawiać rozwiązania alternatywne w celu zwiększenia przejrzystości i wprowadzenia obowiązku zgłaszania naruszeń prywatności. „Zgoda” stanowi istotną podstawę przetwarzania, co w pewnych okolicznościach zwiększa zakres uprawnień osoby, której dane dotyczą. Jednakże, na chwilę obecną, często niesłusznie przedstawia się ją jako odpowiednią podstawę przetwarzania, gdy warunki jej zastosowania nie są w pełni spełnione. W związku z powyższym nowe ramy prawne winny określać wymogi uzyskania zgody. Ponadto, należy poprawić harmonizację, gdyż obecnie prawa osób, których dane dotyczą osłabia brak harmonizacji pomiędzy przepisami krajowymi wdrażającymi dyrektywę 95/46/WE. Wreszcie, rola osób, których dane dotyczą, w internecie, budzi obawy i powinna zostać wyjaśniona w kontekście nowych ram prawnych. W każdym przypadku każdy podmiot świadczący usługi dla obywateli winien wdrożyć określone środki zapewniające bezpieczeństwo, a w razie potrzeby także poufność, danych wprowadzonych przez użytkowników, niezależnie od tego, czy jego klient jest administratorem.

Rozdział 6 mówi o zwiększeniu odpowiedzialności administratorów. Po pierwsze, zasady ochrony danych należy włączyć w kulturę organizacyjną – powinny one stać się częścią wspólnych wartości i praktyk organizacji, a odpowiedzialność w tym zakresie winna być jasno przypisana. Pomoże to także krajowym organom ochrony danych w pełnieniu ich zadań w zakresie nadzoru i egzekwowania zasad i przez to zwiększy skuteczność ochrony danych. Administratorzy winni podejmować różnego rodzaju środki proaktywne i reaktywne wymienione w tym rozdziale. Ponadto, właściwe byłoby

wprowadzenie w kompleksowych ramach prawnych zasady rozliczalności, by administratorzy byli zobowiązani do wprowadzenia odpowiednich środków w celu zapewnienia zgodności z zasadami i zobowiązaniami przewidzianymi przez dyrektywę w jej obowiązującym kształcie podczas przetwarzania danych osobowych, oraz dysponowania niezbędnymi mechanizmami wewnętrznymi w celu wykazania zgodności zainteresowanym stronom trzecim, w tym organom ochrony danych. Zgłaszanie operacji przetwarzania danych krajowym organom ochrony danych mogłoby ulec uproszczeniu lub zmniejszeniu. Należy zbadać, czy i w jakim zakresie można ograniczyć zgłaszanie do przypadków tworzących szczególne zagrożenie dla prywatności, co pozwoliłoby organom ochrony danych na bardziej selektywne działanie i skupienie wysiłków na takich sprawach, oraz w jaki sposób można usprawnić proces zgłaszania.

Rozdział 7a omawia większą i wyraźniejszą rolę krajowych organów ochrony danych. Na chwilę obecną istnieją znaczące różnice pomiędzy państwami członkowskimi w zakresie, m.in. pozycji, zasobów i uprawnień tych organów. Nowe wyzwania stojące przed ochroną danych wymagają szczegółowego, a przy tym bardziej jednolitego i skutecznego nadzoru organów ochrony danych. Nowe ramy prawne winny zatem gwarantować jednolite i wysokie standardy w zakresie niezależności, uprawnień, roli doradczej w procesach ustawodawczych i możliwości ustalania własnego sposobu działania poprzez, w szczególności, określanie priorytetów w zakresie rozpatrywania skarg.

Rozdział 7b rozważa możliwość zacieśnienia współpracy między organami ochrony danych. Europejskie organy ochrony danych należą do Grupy Roboczej Art. 29. Przede wszystkim należy zapewnić objęcie wszystkich kwestii związanych z przetwarzaniem danych osobowych, w szczególności współpracy policyjnej i sądowej w sprawach karnych, działalnością Grupy Roboczej Art. 29 w jej obecnym kształcie. Ponadto, należy usprawnić metody pracy Grupy, w razie potrzeby wymagając dużego zaangażowania od jej członków podczas wprowadzania jej opinii w praktyce krajowej. Relacje pomiędzy Grupą Roboczą Art. 29 a Komisją zapewniającą jej Sekretariat mogą być poprawione poprzez zawarcie porozumienia opisującego rolę obydwu stron. Grupa Robocza rozpocznie konsultacje z Komisją w tej sprawie w roku 2010.

Wreszcie, Rozdział 8 omawia wyzwania dla ochrony danych w zakresie działalności policyjnej i sądowej, stanowiącej obszar szczególnej wagi. Jego kontekst zmienił się z wejściem w życie Traktatu z Lizbony. Decyzja ramowa 2008/977/WSiSW w sprawie ochrony danych osobowych w ramach współpracy policyjnej i sądowej w sprawach karnych może być traktowana jako pierwszy krok w celu stworzenia kompleksowych ram prawnych dla dawnego III filara, nie kończy ona jednak prac w tym obszarze. W ostatnich latach gwałtownie zwiększyła się częstotliwość przechowywania i przekazywania danych osobowych związanych z działalnością organów policyjnych i sądowych ze względu na wzrastające potrzeby wykorzystania informacji w celu opanowania nowych zagrożeń związanych z terroryzmem i przestępczością zorganizowaną, a wspieranych przez rozwój technologiczny. W tym kontekście, przed ochroną danych osobowych stoją olbrzymie wyzwania, które należy rozważyć w przyszłych ramach prawnych. Rozdział 8 określa warunki tworzenia prawa i polityki w obszarze policji i wymiaru sprawiedliwości: oparcie przekazywania danych na spójnej strategii, okresową ocenę istniejących środków, instrumenty prawne i ich zastosowanie, przejrzystość i kwestię praw dostępu i poprawiania danych w kontekście transgranicznym, przejrzystość i demokratyczną kontrolę procesów ustawodawczych, odpowiednią budowę systemów przechowywania i przekazywania danych osobowych,

jasne ramy dla stosunków z państwami trzecimi, wiążące dla wszystkich stron i oparte na pojęciu odpowiedzialności, poświęcenie szczególnej uwagi dużym systemom informacyjnym działającym w UE, odpowiednie rozwiązanie kwestii niezależnego nadzoru, nadzór sądowy i odpowiednie środki prawne oraz wzmacnianie współpracy pomiędzy organami ochrony danych.

## 1. Wstęp

### *Konsultacje*

1. W dniu 9 lipca 2009 r. Komisja zainicjowała Konsultacje w sprawie ram prawnych dla podstawowego prawa do ochrony danych osobowych. W ramach tych konsultacji Komisja pyta o poglądy na temat nowych wyzwań dla ochrony danych osobowych, w szczególności w kontekście nowych technologii i globalizacji. Chce uzyskać odpowiedzi na pytania, czy obecne ramy prawne odpowiadają tym wyzwaniom oraz jakie przyszłe działania będą potrzebne w celu stawienia czoła zidentyfikowanym wyzwaniom.
2. Niniejszy dokument przedstawia wspólną reakcję Grupy Roboczej Artykułu 29 (WP 29) oraz Grupy Roboczej ds. Policji i Wymiaru Sprawiedliwości (WPPJ) na te konsultacje.

### *Historia i kontekst*

3. Konwencję Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Konwencja 108)<sup>1</sup> można uznać za pierwsze europejskie ramy prawne dla podstawowego prawa do ochrony danych osobowych. Prawo do ochrony danych jest ściśle powiązane z, ale nie identyczne jak prawo do życia prywatnego, zgodnie z artykułem 8 Europejskiej Konwencji Praw Człowieka. Prawo do ochrony danych uznane jest za niezależne prawo podstawowe w Karcie Praw Podstawowych Unii Europejskiej.
4. Zasady Konwencji 108 udoskonalono w dyrektywie 95/46/WE<sup>2</sup>, która stanowi główny element składowy prawa dotyczącego ochrony danych w ramach UE. Skuteczność dyrektywy (w przyszłości) jest głównym przedmiotem konsultacji Komisji. Inne instrumenty legislacyjne UE w zakresie ochrony danych to Rozporządzenie (WE) Nr 45/2001<sup>3</sup>, mające zastosowanie do przetwarzania danych przez instytucje i organy UE, dyrektywa 2002/58/WE<sup>4</sup> o prywatności i łączności elektronicznej oraz Decyzja ramowa 2008/977/WSiSW<sup>5</sup> w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych.
5. Traktat z Lizbony nadał ochronie danych szczególną wagę – nie tylko poprzez wejście w życie Karty Praw Podstawowych, ale także przez wprowadzenie art. 16 Traktatu jako nowej podstawy prawnej dla ochrony danych, mającej zastosowanie do każdego rodzaju przetwarzania w sektorze prywatnym i publicznym, w tym w

---

<sup>1</sup> ETS Nr 108, 28.01.1981.

<sup>2</sup> Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych, Dz. Urzęd. 1995, L 281, str. 31.

<sup>3</sup> Rozporządzenie (WE) Nr 45/2001 Parlamentu Europejskiego i Rady z 18 grudnia 2000 o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych, Dz. Urzęd. 2001, L 8, str. 1.

<sup>4</sup> Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z 12 lipca 2002 dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), OJ 2002 L 201, str. 37; zrewidowana dyrektywą 2009/136/WE Parlamentu Europejskiego i Rady z 25 listopada 2009.

<sup>5</sup> Decyzja ramowa Rady 2008/977/JHA z 27 listopada 2008 w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych Dz. Urzęd. 2008 L 350, str. 60., ma być implementowana w prawie krajowych do dnia 27 listopada 2010.

ramach współpracy policyjnej i sądowej oraz wspólnej polityki zagranicznej i bezpieczeństwa. Art. 16 stanowi bodziec do ochrony danych.

6. W tym kontekście należy wspomnieć także o tzw. „Programie sztokholmskim”. W tym wieloletnim programie UE poświęca się wiele uwagi ochronie danych w obszarze wolności, sprawiedliwości i bezpieczeństwa chroniącym obywateli.<sup>6</sup>

### ***Główne przesłanie***

7. Konsultacje Komisji odbyły się w odpowiednim momencie – po pojawieniu się istotnych nowych wyzwań związanych z nowymi technologiami i globalizacją, również z punktu widzenia Traktatu z Lizbony.
8. Główne przesłanie stanowi fakt, że najważniejsze zasady ochrony danych wciąż obowiązują w obliczu nowych wyzwań. Poziom ochrony danych w UE może podnieść się dzięki lepszemu zastosowaniu istniejących zasad ochrony danych w praktyce. Nie oznacza to jednak, że nie są potrzebne zmiany legislacyjne. Wręcz przeciwnie, warto wykorzystać tę możliwość, by:
- Wyjaśnić zastosowanie niektórych spośród najważniejszych zasad ochrony danych (np. zgody i przejrzystości).
  - Uaktualnić ramy prawne poprzez wprowadzenie dodatkowych zasad (takich jak „prywatność w fazie projektowania” i „rozliczalność”).
  - Zwiększyć skuteczność systemu poprzez modernizację założeń dyrektywy 95/46/WE (np. ograniczenie biurokracji).
  - Włączyć najważniejsze zasady ochrony danych w jedne kompleksowe ramy prawne, odnoszące się także do współpracy policyjnej i sądowej w sprawach karnych.

## **2. Jedne kompleksowe ramy prawne**

### ***Obecne ramy prawne***

9. Ochrona danych została wprowadzona do ram prawnych Unii Europejskiej w związku z rynkiem wewnętrznym. Dyrektywa 95/46/WE opiera się na art. 95 Traktatu o Unii Europejskiej. Cel dyrektywy jest dwojaki: utworzenie i funkcjonowanie rynku wewnętrznego wymaga umożliwienia swobodnego przepływu danych z jednego państwa członkowskiego do drugiego, a jednocześnie należy zachować wysoki poziom ochrony podstawowych praw osób.
10. Dyrektywa 95/46/WE ma stanowić ogólne ramy prawne, które mogłyby być uzupełniane szczególnymi zasadami ochrony danych dla poszczególnych sektorów. Do tej pory przyjęto jedynie jeden zestaw takich zasad, dla prywatności i łączności elektronicznej (obecnie dyrektywa 2002/58/WE). Ponadto, niektóre sektorowe akty ustawodawcze również zawierają szczegółowe zasady odnoszące się do przetwarzania danych osobowych<sup>7</sup> (np. ustawodawstwo w zakresie prania brudnych pieniędzy, ceł, VIS, EURODAC czy SIS II).

<sup>6</sup> Program sztokholmski: Otwarta i bezpieczna Europa w służbie obywateli ma zostać zatwierdzony przez Radę Europejską w grudniu 2009 r.

<sup>7</sup> Np. dyrektywa 2005/60/WE Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy oraz

11. Wykorzystanie art. 95 TUE miało znaczenie dla zakresu zastosowania dyrektywy 95/46/WE. Mimo, że dyrektywa miała stanowić, i w wielu aspektach – stanowi, ogólne ramy prawne dla ochrony danych, nie obejmuje przetwarzania danych przez instytucje UE ani operacji przetwarzania wykraczających poza zakres dawnego I filara (głównie tych z dawnego III filara). Dla przetwarzania przez instytucje UE (prowadzonego w zakresie dawnego I filara) wprowadzono rozporządzenie 45/2001, w znacznym stopniu przypominające dyrektywę 95/46/WE. Obecna sytuację w dawnym III filarze określić można jako mozaikę różnych zasad ochrony danych mających zastosowanie w różnych sytuacjach. Niektóre różnice pomiędzy zasadami mogą wynikać z cech szczególnych danego obszaru, inne stanowią konsekwencję innej historii ustawodawczej. Jako pierwszy krok w kierunku bardziej ogólnych ram prawnych należy traktować decyzję ramową 2008/977/JHA.
12. Sytuacja nie jest satysfakcjonująca, szczególnie w III filarze:
- Ochronę danych coraz częściej uznaje się za ogólny problem UE, niekoniecznie związany z rynkiem wewnętrznym. Znajduje to odzwierciedlenie np. w art. 8 Karty Praw Podstawowych UE.
  - W ostatnich latach, w szczególności po atakach terrorystycznych w USA z 11 września 2001 r., wymiana danych osobowych pomiędzy państwami członkowskimi stała się istotną częścią współpracy policyjnej i sądowej, w ramach której, rzecz jasna, wymaga odpowiedniej ochrony.
  - Dawny podział na filary nie odzwierciedla sytuacji na polu ochrony danych, gdy dane wykorzystywane są w różnych filarach – pokazują to orzeczenia Europejskiego Trybunału Sprawiedliwości w sprawach PNR i zatrzymywania danych, dotyczące wykorzystania w celu egzekwowania prawa danych zebranych w kontekście biznesowym.

### ***Potrzeba nowych ram***

13. Niedociągnięcia obecnego systemu wymagają refleksji na temat „kompleksowych i spójnych ram dla ochrony danych obejmujących wszystkie obszary kompetencji UE”<sup>8</sup>. Traktat z Lizbony przewiduje nowe, horyzontalne podejście do ochrony danych i prywatności i daje niezbędną podstawę prawną dla niego (art. 16)<sup>9</sup>, aby usunąć obecnie istniejące różnice i rozbieżności, które uniemożliwiają sprawną, spójną i skuteczną ochronę wszystkich obywateli.
14. Najważniejsze zasady i zabezpieczenia winny odnosić się do przetwarzania danych w każdym sektorze, zapewniając zintegrowane podejście oraz sprawną, spójną i skuteczną ochronę.

---

finansowania terroryzmu. Dz. U. 2005, L 309, str.. 15 i różne instrumenty prawne odnoszące się do dużych systemów informacyjnych SIS, VIS i EURODAC.

<sup>8</sup> Sformułowanie zastosowane przez Komisję w ostatecznej wersji COM 262.

<sup>9</sup> Art. 16 Traktatu z Lizbony obejmuje nie tylko III, ale również II filar (wspólną politykę zagraniczną i bezpieczeństwa) w zakresie przetwarzania danych przez instytucje UE. Art. 39 TUE przewiduje szczególne ramy prawne dla przetwarzania danych przez państwa członkowskie w ramach II filara. Ma to znaczenie np. w związku z listami terrorystów tworzonymi przez UE i państwa członkowskie, kwestia ta nie będzie jednak szczegółowo omawiana w niniejszym rozdziale.



15. Dyrektywa 95/46/WE winna służyć jako wzorzec dla nowych ram prawnych, których główny cel stanowiłaby skuteczność i skuteczna ochrona obywateli. Istniejące zasady ochrony danych winny być uznane i uzupełnione środkami pozwalającymi wykonywać je w bardziej skuteczny sposób (i zapewnić skuteczniejszą ochronę danych osobowych obywateli).
16. Najważniejsze zasady ochrony danych winny stanowić fundament kompleksowych ram prawnych: winny zostać potwierdzone najważniejsze pojęcia (kto/administrator – co/dane osobowe) i zasady, w tym w szczególności zasada legalności, słuszności, proporcjonalności, ograniczenia celu i przejrzystości, a także prawa osób, których dane dotyczą i niezależny nadzór prowadzony przez organy publiczne. Tworzenie ram stanowi także okazję do wyjaśnienia sposobu stosowania niektórych kluczowych pojęć, np.:
- zgody: należy unikać mylenia zasad opt-in i opt-out oraz stosowania zgody w sytuacjach, w których nie stanowi ona odpowiedniej podstawy prawnej (patrz także Rozdział 5);
  - przejrzystości: jest to warunek konieczny legalnego przetwarzania. Winno być jasne, że przejrzystość nie musi prowadzić do wyrażenia zgody, ale jest warunkiem do uzyskania ważnej zgody i możliwości wykonywania praw osób, których dane dotyczą (patrz także Rozdział 5).

Celem winno być usprawnienie ochrony danych na szczeblu międzynarodowym, zgodnie z prawami i zasadami określonymi w dyrektywie 95/46/WE, przy jednoczesnym zachowaniu dotychczasowego poziomu ochrony (patrz także Rozdział 3).

17. Przyjęcie jednych kompleksowych ram prawnych pozwoliłoby także na wprowadzenie przydatnych innowacji w obecnych zasadach, obejmujących np. Wprowadzenie ogólnej zasady „prywatności w fazie projektowania” jako rozszerzenia obecnie obowiązujących zasad o środkach technicznych i organizacyjnych (patrz także Rozdział 4) oraz ogólnej zasady rozliczalności (patrz także Rozdział 6).

### ***Budowa kompleksowych ram prawnych***

18. Jedne kompleksowe ramy prawne – zgodnie z Traktatem z Lizbony oparte na jednej podstawie prawnej – nie muszą oznaczać braku elastyczności i różnic pomiędzy poszczególnymi sektorami czy państwami członkowskimi w obrębie ogólnych ram. Zasady szczególne (*leges speciales*), wprowadzane dodatkowo, mogłyby wzmacniać ochronę, pod warunkiem, że, jak określono powyżej, byłyby zgodne z ideą kompleksowych ram prawnych i najważniejszymi zasadami.
19. Dodatkowe zasady sektorowe i szczególne można wprowadzić np. w odniesieniu do:
- Poszczególnych sektorów, takich jak zdrowie publiczne, zatrudnienie czy inteligentne systemy transportowe.
  - Narzędzi i usług związanych z prywatnością, takich jak znaki jakości i audyty (patrz także Rozdziały 4 i 6).

- Naruszeń zasad bezpieczeństwa (jako dopełnienie zasady bezpieczeństwa; patrz także Rozdziały 5 i 6).
  - Współpracy policyjnej i sądowej, jak przewidziano w Deklaracji 21 załączonej do Traktatu z Lizbony (patrz także Rozdział 8).
  - Krajowej polityki bezpieczeństwa, jak przewidziano w Deklaracji 20 załączonej do Traktatu z Lizbony.
20. Mogą zostać wprowadzone dodatkowe uregulowania na szczeblu krajowym, uwzględniające różnice kulturowe i organizację wewnętrzną państw członkowskich, o ile nie stanowią przeszkody dla harmonizacji potrzebnej w Unii Europejskiej pozbawionej granic wewnętrznych.
21. Dalsza harmonizacja jest potrzebna i winna stanowić część jednoznacznych, jasnych ram prawnych, nie oznacza to jednak, że wartości pozbawiona jest pewna elastyczność, uznawana obecnie w dyrektywie 95/46/WE, np. jeśli wymagają jej różnice kulturowe. W gestii ustawodawstwa krajowego można pozostawić także określenie podziału obowiązków i ról sektora publicznego i prywatnego.

### **3. Globalizacja**

#### ***Kontekst i obecne ramy prawne***

22. Zgodnie z prawem UE, prawo do ochrony danych osobowych to prawo podstawowe, podlegające ochronie na mocy art. 8 Karty Praw Podstawowych UE (patrz także Rozdział 1). W innych częściach świata potrzeba ochrony danych jest uznawana, niekoniecznie jednak ma status prawa podstawowego.
23. UE i jej państwa członkowskie winny zagwarantować to podstawowe prawo każdej osobie objętej ich jurysdykcją. W zglobalizowanym świecie oznacza to, że obywatele mogą żądać ochrony również jeśli ich dane są przetwarzane poza terytorium UE.
24. Dyrektywa 95/46/WE omawia potrzebę takiej ochrony w art. 4. Dyrektywa ma zastosowanie do przetwarzania danych wszędzie, a zatem również poza UE<sup>10</sup>, jeśli (a) administrator danych ma siedzibę w UE lub (b) administrator ma siedzibę poza UE, ale używa sprzętu znajdującego się na terytorium UE.
25. Ponadto, art. 25 i 26 dyrektywy 95/46/WE określają warunki przekazywania danych osobowych do państw trzecich. Podstawowa zasada zawarta w art. 25 głosi, że możliwe jest przekazywanie jedynie do krajów zapewniających odpowiedni poziom ochrony. Art. 26 przewiduje wyjątki od tej reguły – np. Wiążące Reguły Korporacyjne (BCR) i wzorcowe klauzule umowne.

#### ***Prawo właściwe***

26. Dokładny zakres dyrektywy 95/46/WE nie jest jednak wystarczająco jasny. Nie zawsze wiadomo, czy ma zastosowanie prawo UE, prawo którego państwa członkowskiego jest właściwe i jakie przepisy obowiązywałyby w przypadku firm międzynarodowych mających siedzibę w wielu państwach członkowskich. Art. 4 dyrektywy, określający, kiedy ma ona zastosowanie do przetwarzania, pozostawia pewną dowolność interpretacji.

---

<sup>10</sup> W tym kontekście do UE należy zaliczyć także państwa członkowskie EFTA.

27. Ponadto, istnieją sytuacje wykraczające poza zakres zastosowania dyrektywy – np. jeśli administratorzy niemający siedziby na terytorium UE obejmują swymi działaniami mieszkańców UE, co skutkuje zbieraniem i dalszym przetwarzaniem danych osobowych. Dzieje się tak np. w przypadku sklepów internetowych i innych podmiotów stosujących reklamy spersonalizowane, stron skierowanych bezpośrednio do obywateli UE (np. poprzez zastosowanie lokalnego języka) itp. Jeśli administratorzy nie posługują się przy tym sprzętem znajdującym się na terytorium UE, dyrektywa 95/46/WE nie ma zastosowania.
28. W obecnej chwili trwają prace Grupy Roboczej Art. 29 nad opinią w sprawie pojęcia prawa właściwego. Grupa Robocza zamierza doradzać Komisji Europejskiej w tej sprawie w ciągu najbliższego roku. Poradnictwo to może obejmować dalsze zalecenia związane z przyszłymi ramami prawnymi.

### ***Standardy międzynarodowe i Rezolucja Madrycka***

29. Globalne standardy w zakresie ochrony danych stają się niezbędne. Ułatwiłyby one także transgraniczny przepływ danych, który w wyniku globalizacji staje się regułą, nie wyjątkiem. Dopóki nie powstaną globalne standardy, będzie panować różnorodność. Należy ułatwić transgraniczny przepływ danych, jednocześnie zapewniając wysoki poziom ochrony danych osobowych przekazywanych i przetwarzanych w państwach trzecich.
30. „Rezolucja Madrycka”, Wspólna Propozycja w sprawie Międzynarodowych Standardów Ochrony Prywatności, przyjęta przez Międzynarodową Konferencję Rzeczników Ochrony Danych i Prywatności w dniu 6 listopada 2009 r., zasługuje na poparcie. Propozycja zawiera projekt globalnego standardu i podsumowuje wszystkie możliwe podejścia do ochrony danych osobowych i prywatności, łącząc ustawodawstwo z pięciu kontynentów. Zawiera zestaw zasad, praw i zobowiązań, który powinien stanowić podstawę ochrony danych w każdym systemie prawnym na świecie i wykazuje, że możliwe jest osiągnięcie w odpowiednim czasie globalnych standardów zapewniających odpowiedni poziom ochrony danych.
31. Komisję wzywa się:
- Do podjęcia inicjatyw zmierzających do dalszego rozwoju międzynarodowych globalnych standardów ochrony danych osobowych w celu promowania międzynarodowych ram prawnych dla ochrony danych i ułatwienia transgranicznych przepływów danych przy jednoczesnym zapewnieniu odpowiedniego poziomu ochrony osób, których dane dotyczą. Inicjatywy takie winny obejmować zbadanie możliwości stworzenia wiążącej sieci międzynarodowej.
  - W sytuacji braku standardów globalnych, do promowania rozwoju ustawodawstwa z zakresu ochrony danych i powstawania niezależnych organów ochrony danych w krajach poza UE. Podstawę takiego ustawodawstwa winny stanowić podstawowe zasady ochrony danych określone w Rezolucji Madryckiej.

Niniejsze szczególne zadania Komisji winny być wymienione w przyszłych ramach prawnych.

### ***Ulepszanie decyzji o odpowiedniości***

32. W zglobalizowanym środowisku ma miejsce coraz więcej operacji przetwarzania danych osobowych. Zapewnianie swobodnego przepływu danych przy jednoczesnym zagwarantowaniu wysokiego poziomu ochrony praw osób, których dane dotyczą jest coraz bardziej istotne, w związku z czym konieczna jest zmiana procesu uznawania odpowiedniości poprzez:

- Bardziej precyzyjne określanie kryteriów statusu „odpowiedniości”, z odpowiednim uwzględnieniem podejścia Grupy Roboczej Art. 29<sup>11</sup> i innych sposobów postrzegania ochrony danych osobowych w innych częściach świata, w szczególności praw i zasad określonych w Rezolucji Madryckiej.
- Usprawnienie procedur analizy systemu prawnego państw trzecich w celu wydawania większej liczby decyzji o odpowiednim poziomie ochrony.

Kwestie te winny zostać określone w przyszłych ramach prawnych.

### ***Umowy międzynarodowe***

33. Zauważono działalność Grupy Kontaktowej Wysokiego Szczebla UE-USA w sprawie wymiany informacji i ochrony danych osobowych i prywatności. Działalność ta może doprowadzić do zawarcia międzynarodowej umowy określającej wspólne zasady ochrony danych i prywatności mające zastosowanie do wymiany informacji ze Stanami Zjednoczonymi prowadzonej w ramach walki z terroryzmem i poważną przestępczością międzynarodową.<sup>12</sup>

34. Umowy międzynarodowe są odpowiednimi instrumentami dla ochrony danych osobowych w kontekście globalnym o ile zapewniony przez nie poziom ochrony danych jest co najmniej równy wspomnianym powyżej globalnym standardom, każdemu obywatelowi przysługuje łatwe do wykonania i skuteczne prawo ubiegania się o zadośćuczynienie, również na drodze sądowej, i zostały podjęte odpowiednie zabezpieczenia związane z celem, w jakim będą wykorzystywane dane osobowe.

35. Pod powyższymi warunkami, przewidywana umowa międzynarodowa mogłaby służyć jako wzorzec dla wymiany informacji z innymi państwami trzecimi i dla innych celów. Przyszłe ramy prawne mogłyby określać warunki zawierania umów z państwami trzecimi.

36. Ponadto, UE winna wspierać współpracę pomiędzy międzynarodowymi organami ochrony danych, np. na szczeblu transatlantyckim. Taka współpraca stanowi skuteczny sposób promowania ochrony danych poza UE.

### ***Wiążące Reguły Korporacyjne/Rozliczalność***

37. Przetwarzanie danych poza obszarem UE może być również chronione Wiążącymi Regułami Korporacyjnymi (BCR), międzynarodowymi kodeksami postępowania przyjmowanymi przez firmy międzynarodowe, pozwalającymi na transgraniczne przekazywanie danych w ramach międzynarodowej korporacji. BCR zostały wprowadzone przez Grupę Roboczą Art. 29 w roku 2003. Zarówno organy ochrony danych jak i korporacje są zdania, że BCR stanowią dobry sposób ułatwienia

---

<sup>11</sup> Patrz w szczególności Dokument Roboczy WP 29 nr 12: Przekazywanie danych osobowych do państw trzecich: zastosowanie art. 25 i 26 dyrektywy UE o ochronie danych osobowych, przyjęty w dniu 24 lipca 1998

<sup>12</sup> W tym kontekście pozostaje do rozwiązania transatlantycki problem związany z zadośćuczynieniem.

międzynarodowych przepływów danych, jednocześnie gwarantując ochronę danych osobowych. Dyrektywa 95/46/WE nie wspomina jednak bezpośrednio o wiążących regułach korporacyjnych. W efekcie proces przyjmowania BCR, oparty na art. 26 (2) dyrektywy 95/46/WE, wymaga zatwierdzenia przez wszystkie państwa członkowskie objęte regułami, przez co ocenianie i zatwierdzanie BCR stanowi długotrwały proces. Grupa Robocza Art. 29 poświęciła wiele czasu i wysiłku promowaniu i ułatwianiu wykorzystania i zatwierdzania BCR w kontekście istniejących obecnie ram prawnych. Do tej pory, w celu usprawnienia tego procesu, 19 organów ochrony danych zgodziło się na zastosowanie procedury zatwierdzania BCR zwanej wzajemnym uznawaniem („Mutual Recognition”).

38. W związku z powyższym, w nowych ramach prawnych należy zawrzeć przepis dotyczący BCR, który służyłby kilku celom:

- Uznaniu BCR za narzędzie właściwe do zapewnienia odpowiedniego poziomu ochrony.
- Zdefiniowaniu głównych elementów merytorycznych i proceduralnych tych reguł zgodnie z opinią Grupy Roboczej Art. 29 na ten temat.

39. Ochronę danych poza terytorium UE można promować poprzez wprowadzenie pojęcia „rozliczalności” jako dodatku do postanowień obowiązującej obecnie dyrektywy 95/46/WE, również w odniesieniu do przekazywania danych do państw trzecich. W tym celu w nowych ramach prawnych można wprowadzić nowy przepis, zgodnie z którym administrator byłby rozliczalny i odpowiedzialny za ochronę danych osobowych, których jest administratorem, również w przypadku przekazania takich danych do innych administratorów i przetwarzających poza UE (więcej informacji o „rozliczalności” znajduje się w Rozdziale 6).

#### ***Uwaga końcowa***

40. Niniejszy rozdział omawia globalizację jako taką, jednak wszystkie części niniejszego wkładu dotyczą tej kwestii w taki czy inny sposób. Często myśląc o „globalizacji” rozumie się przez nią biznes, jednak w zglobalizowanym świecie ma miejsce coraz więcej operacji przetwarzania danych osobowych. Choć obywatele zwykle żyją w środowisku lokalnym, coraz częściej korzystają z internetu, gdzie ich dane przetwarza się globalnie. Globalizacja jest więc związana z technologią (Rozdział 4), sytuacją osoby, której dane dotyczą (Rozdział 5), administratorem (Rozdział 6), organami ochrony danych/Grupą Roboczą Art. 29 (Rozdział 7) oraz egzekwowaniem prawa (Rozdział 8).

#### **4. Postęp technologiczny. „Prywatność w fazie projektowania” jako nowa zasada**

41. Podstawowe założenia zawarte w dyrektywie 95/46/WE powstały w latach 70. XX w., kiedy informacje przetwarzano za pomocą indeksów kartkowych, kart perforowanych i komputerów typu mainframe. Obecnie komputery są wszechobecne, globalne i połączone w sieć. Urządzenia technologii informacyjnej są coraz mniejsze i coraz częściej wyposażone w karty sieciowe, WiFi lub inne interfejsy radiowe. W niemal wszystkich biurach i domach użytkownicy komputerów mogą komunikować się globalnie za pośrednictwem Internetu. Usługi Web 2.0 i technologia cloud

computing zacierają granice pomiędzy administratorami, przetwarzającymi i osobami, których dane dotyczą.

42. Dyrektywa 95/46/WE pozostała aktualna mimo rozwoju technologii, ponieważ zawarte w niej zasady i pojęcia są nie tylko rozsądne, ale także neutralne technologicznie, które pozostają istotne i mają zastosowanie również w dzisiejszym, sieciowym świecie.
43. Choć jasne jest, że opisany powyżej rozwój technologii jest zwykle korzystny dla społeczeństwa, zwiększył on również zagrożenia dla danych i prywatności obywateli. Aby zrównoważyć te zagrożenia, należy uzupełnić ramy prawne dla ochrony danych. Po pierwsze, należy do nich wprowadzić zasadę „prywatności w fazie projektowania”, po drugie należy, w miarę potrzeb, regulować poszczególne kwestie technologiczne wymagające wprowadzenia zasad ochrony danych i prywatności.

#### ***Zasada prywatności w fazie projektowania***

44. Pomysł włączania technologicznych zabezpieczeń danych w technologie informacyjno-komunikacyjne („ICT”) nie jest nowy. Już w dyrektywie 95/46/WE zawarto kilka przepisów wzywających administratorów danych do wdrażania zabezpieczeń technologicznych podczas projektowania i wykorzystywania ICT – np. art. 17, który nakłada na administratorów zobowiązanie wprowadzania odpowiednich środków technicznych i organizacyjnych. Motyw 46 wzywa do podjęcia takich środków zarówno podczas projektowania systemu przetwarzającego jak i podczas samego przetwarzania. Art. 16 ustanawia poufność przetwarzania – zasada ta jest odzwierciedlona i uzupełniona w przepisach dotyczących bezpieczeństwa informatycznego. Oprócz powyższych artykułów, zastosowanie mają także zasady związane z jakością danych zawarte w art. 6 (legalność i uczciwość, ograniczenie celu, odpowiedniość, dokładność, ograniczenie czasu przechowywania, odpowiedzialność).
45. Choć wyżej wymienione przepisy dyrektywy pomagają w promowaniu prywatności w fazie projektowania, w praktyce nie okazały się wystarczające, by zapewnić uwzględnienie prywatności w ICT. Użytkownicy usług ICT – przedsiębiorstwa, sektor publiczny, a w szczególności osoby fizyczne – nie są w stanie samodzielnie wprowadzać odpowiednich środków bezpieczeństwa, by chronić własne lub cudze dane osobowe, takie usługi i technologie winny więc być projektowane z myślą o prywatności.
46. Z powyższych powodów nowe ramy prawne powinny zawierać przepisy przekształcające obecne szczegółowe wymogi w szerszą, spójną zasadę prywatności w fazie projektowania, określaną także mianem technologii wspierających prywatność (PET). Zasada ta winna być wiążąca dla projektantów i producentów oraz dla administratorów danych, którzy podejmują decyzję o zakupie i wykorzystaniu ICT. Powinni oni mieć obowiązek uwzględniania technologicznych środków ochrony danych już w fazie planowania procedur i systemów technologii informacyjnej. Dostawcy takich systemów i administratorzy winni wykazać, że podjęli wszelkie środki niezbędne dla zachowania zgodności z powyższymi wymogami.
47. Zasada prywatności w fazie projektowania winna nakładać obowiązek wdrażania zasad ochrony danych w ICT przeznaczonych lub stosowanych do przetwarzania

danych osobowych. Z zasady tej wynikać powinien nie tylko wymóg utrzymania bezpieczeństwa przez ICT, ale także zaprojektowania ich w taki sposób, by unikać przetwarzania danych lub minimalizować ilość przetwarzanych danych. Jest to zgodne z niemieckim prawem precedensowym.<sup>13</sup>

48. Wprowadzenie takiej zasady podkreśliłoby potrzebę zastosowania „prywatności w fazie projektowania” i niezbędnych narzędzi umożliwiających użytkownikom lepszą ochronę danych osobowych (np. kontrola dostępu, szyfrowanie). Zastosowanie zasady winno być wymogiem koniecznym w odniesieniu do produktów i usług zapewnianych stronom trzecim i klientom indywidualnym (np. routerów WiFi, portali społecznościowych i wyszukiwarek), co z kolei dałoby organom ochrony danych większą możliwość egzekwowania skutecznego wdrażania takich środków.
49. Zasadę należy sformułować w sposób *neutralny technologicznie*, aby zachowała aktualność przez długi czas mimo szybko postępujących zmian technologicznych i społecznych. Powinna również być wystarczająco *elastyczna*, by administratorzy i organy ochrony danych byli w stanie w każdym konkretnym przypadku zastosować na jej podstawie konkretne środki ochrony danych.
50. Zasada powinna podkreślać, podobnie jak czyni to obecnie Motyw 46, potrzebę wprowadzania zasady *najwcześniej jak to możliwe*: „Podczas projektowania systemu przetwarzania i w czasie samego przetwarzania”. Zabezpieczenia wdrażane w późniejszych fazach są niespójne i niewystarczające z punktu widzenia wymogów skutecznej ochrony praw i wolności osób, których dane dotyczą.
51. Powinny zostać opracowane standardy technologiczne uwzględniane przez projektantów sprzętu i oprogramowania w celu zminimalizowania trudności w określeniu wymogów wynikających z zasady „prywatności w fazie projektowania”. Standardy takie mogą mieć charakter ogólny lub szczegółowo odnosić się do określonych celów i technologii przetwarzania.
52. Następujące przykłady pokazują, jak zasada „prywatność w fazie projektowania”/technologie wspierające prywatność mogą przyczynić się do lepszej ochrony danych:
  - Identyfikatory biometryczne powinny być przechowywane w urządzeniach znajdujących się pod kontrolą osób, które dane dotyczą (np. smart card), nie w zewnętrznych bazach danych.
  - Wideonadzór w systemach transportu publicznego winien być zaprojektowany w sposób uniemożliwiający rozpoznanie twarzy objętych nim osób (poza wyjątkowymi sytuacjami, np. kiedy dana osoba podejrzewana jest o popełnienie przestępstwa karnego).

---

<sup>13</sup> Wydany niedawno wyrok niemieckiego sądu konstytucyjnego z dnia 27 lutego 2008 r. ([1 BvR 370/07](#); [1 BvR 595/07](#)) stworzył konstytucyjne prawo do poufności i integralności w odniesieniu do systemów informatycznych. Systemy mające zdolność tworzenia, przetwarzania lub przechowywania szczególnie chronionych danych osobowych wymagają szczególnej ochrony. Zakres ochrony zapewnianej przez fundamentalne prawo do poufności i integralności systemów informatycznych obejmuje systemy, które same lub w połączeniu mogą zawierać dane osobowe obywateli w takiej ilości i tak różnorodne, że dostęp do system ułatwia zapoznanie się ze znaczącą częścią życia danej osoby lub wręcz z obrazem jej osobowości. Systemy takie to np. komputery osobiste i laptopy, telefony komórkowe i kalendarze elektroniczne.

- Nazwiska pacjentów i inne dane osobowe przechowywane w systemach informacyjnych szpitali powinny być oddzielone od danych o stanie zdrowia i leczeniu i łączone z nimi jedynie w takim stopniu, w jakim jest to niezbędne dla celów medycznych lub innych, w bezpiecznym środowisku.
- W razie potrzeby należy wprowadzić funkcjonalność ułatwiającą osobom, których dane dotyczą wycofanie zgody, powodujące usunięcie danych ze wszystkich serwerów, na których są przechowywane (w tym proxy i mirror).

53. W praktyce wdrażanie zasady „prywatności w fazie projektowania” winno wymagać oceny kilku konkretnych aspektów lub celów. Podczas podejmowania decyzji dotyczących projektu systemu przetwarzającego, jego zakupu i wykorzystania, należy uwzględnić w szczególności następujące ogólne aspekty/cele:

- Minimalizację ilości przetwarzanych danych: systemy przetwarzania danych powinny być projektowane i wybierane w taki sposób, by zapobiegać zbieraniu, przetwarzaniu lub wykorzystaniu danych osobowych lub maksymalnemu ograniczeniu ilości wykorzystanych danych.
- Możliwość kontroli: system informatyczny winien dawać osobom, których dane dotyczą możliwość skutecznej kontroli swoich danych osobowych. Możliwości wyrażenia zgody lub sprzeciwu powinny towarzyszyć odpowiednie środki technologiczne.
- Przezrzystość: zarówno projektanci jak i użytkownicy systemów informatycznych winni zapewnić odpowiednią informację osób, których dane dotyczą o sposobie działania tych systemów. Należy dać możliwość dostępu i informacji w formie elektronicznej.
- Przyjazność dla użytkownika: związane z prywatnością funkcje powinny być przyjazne dla użytkownika tj. zapewniać odpowiednią pomoc i prosty interfejs, by mogli z nich korzystać również mniej doświadczeni użytkownicy.
- Poufność danych: niezbędne jest projektowanie i zabezpieczanie systemów informatycznych w taki sposób, by jedynie podmioty upoważnione miały dostęp do danych osobowych.
- Jakość danych: administratorzy muszą wspomagać jakość danych środkami technicznymi. Dostęp do istotnych danych powinien zostać udzielony, jeśli są one niezbędne dla prawnie uzasadnionych celów.
- Ograniczenie wykorzystania: systemy informatyczne, które mogą być stosowane do różnych celów lub są stosowane w środowisku mającym wielu użytkowników (np. systemy połączone wirtualnie, takie jak olbrzymie bazy danych, cloud computing czy identyfikatory cyfrowe) muszą zapewnić oddzielenie danych i procesów służących określonej celowi od innych w sposób bezpieczny.

#### ***Uregulowania poszczególnych kwestii technologicznych***

54. Zasada „prywatności w fazie projektowania” może nie wystarczyć do zapewnienia we wszystkich przypadkach odpowiedniego włączenia zasad ochrony danych do ICT. W niektórych przypadkach niezbędne może okazać się bardziej konkretne podejście. Aby ułatwić przyjmowanie takich środków, nowe ramy prawne powinny zawierać przepis umożliwiający przyjmowanie konkretnych uregulowań poszczególnych kwestii technicznych, wymagających ustalenia zasad prywatności.

55. Pojęcie to nie jest nowe: art. 14 (3) dyrektywy o prywatności i łączności elektronicznej zawiera podobny przepis: „W miarę potrzeb, możliwe jest przyjęcie środków w celu zapewnienia, że terminal jest skonstruowany w sposób zgodny z



prawem użytkowników do ochrony i kontroli używania ich danych osobowych, zgodnie z dyrektywą 1999/5/WE i decyzją Rady 87/95/EWG z dnia 22 grudnia 1986 r. w sprawie normalizacji w dziedzinie technologii informatycznych i telekomunikacji”.

56. Wymienione powyżej środki ułatwiłyby przyjęcie, w pewnych przypadkach, szczególnych środków prawnych obejmujących pojęcie „prywatności w fazie projektowania”, zapewniających podanie odpowiednich specyfikacji. Może tak być np. w przypadku technologii RFID, portali społecznościowych, reklam behawioralnych itp.

### ***Uwagi końcowe***

57. Rosnące znaczenie ochrony danych podczas tworzenia i wykorzystywania systemów informatycznych pociąga za sobą nowe zobowiązania dla specjalistów w tej dziedzinie i konieczność wyraźnego włączenia zasad ochrony danych w program szkolenia informatyków.
58. Zasady technologicznej ochrony danych i wynikające z nich konkretne kryteria powinny stanowić podstawę przyznawania znaków jakości (certyfikacji) po przeprowadzeniu audytu w zakresie ochrony danych.<sup>14</sup>

## **5. Nadawanie uprawnień osobom, których dane dotyczą**

59. Potencjał, jaki daje rola osoby, której dane dotyczą określona w dyrektywie 95/46/WE nie został w pełni zrealizowany. Ponadto, zarówno zachowania obywateli jak i rola osób, których dane dotyczą w odniesieniu do ochrony danych zmieniły się, między innymi w wyniku przemian społecznych. Osoby, których dane dotyczą, traktują swoją prywatność nierozważnie, i niekiedy są gotowe z niej zrezygnować w zamian za obiecywane korzyści. Z drugiej strony, wciąż wiele oczekują od podmiotów, z którymi prowadzą interesy. Ponadto same osoby, których dane dotyczą odgrywają coraz bardziej aktywną rolę w przetwarzaniu danych osobowych, w szczególności w internecie.
60. Zmiany w zachowaniu i roli osób, których dane dotyczą i doświadczenie związane z zastosowaniem dyrektywy 95/46/WE wymagają odgrywania przez osoby, których dane dotyczą większej roli w ramach prawnych dla ochrony danych<sup>15</sup>. Nadanie osobom, których dane dotyczą większych uprawnień jest niezbędne, jeśli mają one odgrywać większą rolę.

### ***Poprawa mechanizmów dochodzenia zadośćuczynienia***

61. Przyznanie osobie, której dane dotyczą praw wymaga dania jej większej możliwości dochodzenia swoich praw. Postępowanie sądowe może niekiedy być bardzo trudne i obciążone ryzykiem finansowym, w dyrektywie 95/46/WE należy więc wprowadzić możliwość składania pozwów zbiorowych.<sup>16</sup>

<sup>14</sup> Jest tak np. w przypadku projektu EuroPriSe.

<sup>15</sup> Ma to szczególne znaczenie w przypadku dzieci. Podczas podejmowania decyzji dotyczących ich danych osobowych, interes dzieci musi być uwzględniany w sposób szczególny, jak stanowi Konwencja o Prawach Dziecka ONZ (<http://www2.ohchr.org/english/law/crc.htm>) i inne akty prawa krajowego i instrumenty międzynarodowe.

<sup>16</sup> Pozwy zbiorowe istnieją np. w prawie ochrony środowiska.

62. Administratorzy powinni ponadto wprowadzić łatwiej dostępne, skuteczniejsze i przystępne cenowo procedury rozpatrywania skarg (patrz także Rozdział 6). Jeśli procedury te nie wystarczą do rozpatrzenia sporu pomiędzy osobą, której dane dotyczą a administratorem, osoba, której dane dotyczą powinna mieć możliwość skorzystania z innych sposobów rozstrzygania sporu, zapewnionych głównie przez przedstawicieli branży.<sup>17</sup> Sposoby te należy włączyć w obręb nowych ram prawnych.

### ***Przejrzystość***

63. Kolejnym podstawowym warunkiem koniecznym, gdyż daje osobom, których dane dotyczą, możliwość wypowiedzenia się o przetwarzaniu danych jeszcze przed jego rozpoczęciem. Tworzenie profili, przeszukiwanie olbrzymich ilości danych (data mining) i rozwój technologiczny, które ułatwiają wymienialność danych osobowych sprawiają, że coraz istotniejsze staje się, by osoby, których dane dotyczą, wiedziały kto, gdzie, dla jakich celów i jakimi środkami technicznymi przetwarza ich dane, oraz aby informacje na ten temat były łatwo zrozumiałe. Obowiązek informowania osób, których dane dotyczą (art. 10 i 11 dyrektywy 95/46/WE) rzadko jest właściwie wypełniany w praktyce. Nowe ramy prawne winny zapewnić rozwiązania alternatywne w celu zwiększenia przejrzystości – na przykład nowe sposoby informowania osób, których dane dotyczą, w odniesieniu do reklam behawioralnych.
64. Przejrzystość wymaga powiadamiania zainteresowanych osób o naruszeniu zasad ochrony prywatności, jeśli istnieje ryzyko, że niekorzystnie wpłyną one na ich dane osobowe i prywatność. Pozwala to osobom, których dane dotyczą podjąć próbę opanowania wyrządzonych im szkód (w niektórych przypadkach należy powiadomić także władze – patrz również rozdział 6). W nowych ramach prawnych należy wprowadzić ogólny sposób powiadamiania o zasadach ochrony prywatności (patrz także Rozdział 6).<sup>18</sup>

### ***Zgoda***

65. W dyrektywie zgoda osoby, której dane dotyczą stanowi podstawę prawną dla przetwarzania danych (por. art. 7 i 8 dyrektywy 95/46/WE). Wciąż stanowi ona istotną podstawę przetwarzania i w pewnych okolicznościach może prowadzić do nadania praw osobie, której dane dotyczą. Zgoda musi jednak być dobrowolna, świadoma i szczegółowa (art. 2 (h) dyrektywy 95/46/WE).
66. W wielu przypadkach dobrowolne udzielenie zgody nie jest możliwe, szczególnie jeśli istnieje wyraźna nierównowaga sił pomiędzy osobą, której dane dotyczą a administratorem (np. w kontekście zatrudnienia lub w przypadku konieczności podania danych organom publicznym).
67. Ponadto, wymóg świadomej zgody opiera się na założeniu, że osoba, której dane dotyczą musi w pełni rozumieć, jakie skutki przyniesie jej udzielenia. Złożony charakter praktyk zbierania danych, modeli biznesowych, modeli sprzedaży i aplikacji technologicznych w wielu przypadkach uniemożliwia obywatelom

---

<sup>17</sup> Rzecz jasna nie może to odbierać obywatelowi prawa zwrócenia się o zadośćuczynienie do sądu lub organu ochrony danych.

<sup>18</sup> W opinii 1/2009 w sprawie propozycji poprawienia dyrektywy 2002/58/WE o prywatności i łączności elektronicznej, Grupa Robocza Art. 29 przedstawiła zalecane podejście do kwestii szczególnych sposobów zgłaszania naruszeń przepisów, omówionych w dyrektywie o prywatności i łączności elektronicznej. Te same zalecenia odnoszą się do wprowadzenia ogólnych sposobów zgłaszania naruszeń przepisów.

podejmowanie decyzji pozwalających kontrolować wykorzystanie i przekazywanie ich danych opartych na aktywnym wyborze.<sup>19</sup>

68. W żadnym z powyższych przypadków zgoda nie stanowi odpowiedniej podstawy dla przetwarzania, często jednak niesłusznie twierdzi się, że jest inaczej. Rozwój technologiczny wymaga również innego wykorzystania systemów opt-in i opt-out. Art. 7 dyrektywy 95/46/WE pozostawia możliwość udzielenia zgody poprzez system opt-out w pewnych okolicznościach i możliwość ta jest często wykorzystywana, szczególnie w kontekście Internetu. Danie osobom, których dane dotyczą, możliwości decydowania przed rozpoczęciem przetwarzania ich danych osobowych, wymaga wyraźnej zgody (czyli zastosowania systemu opt-in) dla wszelkiego rodzaju przetwarzania opartego na zgodzie.<sup>20</sup>
69. Nowe ramy prawne winny dokładnie określać wymóg zgody, uwzględniając spostrzeżenia poczynione powyżej.

### ***Harmonizacja***

70. Obecnie prawa osób, których dane dotyczą, są osłabiane przez brak harmonizacji pomiędzy przepisami krajowymi wdrażającymi dyrektywę 95/46. Kilka elementów dyrektywy, które mają wzmacniać pozycję osób, których dane dotyczą, takie jak przepisy o odpowiedzialności i możliwość dochodzenia zadośćuczynienia za straty niematerialne,<sup>21</sup> nie zostały wdrożone we wszystkich państwach członkowskich. Poza różnicami w sposobie wdrażania dyrektywy 95/46/WE występują również niekiedy różnice w jej interpretacji. W miarę postępowania globalizacji, różnice te coraz bardziej osłabiają pozycję osób, których dane dotyczą, bardzo istotne jest więc poprawienie harmonizacji (patrz także Rozdział 7b), w razie potrzeby – poprzez uszczegółowienie przepisów prawa.

### ***Rola osób, których dane dotyczą w internecie***

71. Obywatele coraz częściej wprowadzają swoje dane osobowe do Internetu (poprzez portale społecznościowe, aplikacje typu cloud computing itp.). Dyrektywa 95/46/WE nie ma jednak zastosowania do osób, które wprowadzają dane dla celów „wyłącznie osobistych” lub „w ramach wykonywania czynności życia codziennego”.<sup>22</sup> Można twierdzić, że dyrektywa nie odnosi się także do dostawcy usług tj. podmiotu, który przechowuje i udostępnia informacje wprowadzone przez daną osobę (chyba, że przetwarza on dane dla własnych celów), w związku z czym dostawca usług nie może być uznawany za administratora.<sup>23</sup> Efektem jest brak zabezpieczeń, któremu

<sup>19</sup> Patrz dokument ‘Data Protection Accountability: The essential Elements – A Document for Discussion’, Centre for Information Policy Leadership działające jako sekretariat Galway Project, październik 2009, str. 4.

<sup>20</sup> W kwestii zgody i systemu opt-in/opt-out, patrz także Rozdział 2, w którym wyjaśniono, że należy unikać mylenia zasad opt-in i opt-out oraz wykorzystania zgody w sytuacjach, w których nie stanowi ona odpowiedniej podstawy prawnej.

<sup>21</sup> W większości przypadków, w których osoba, której dane dotyczą poniosła straty, mają one charakter niematerialny i polegają np. na poczuciu niemożności poruszania się w sektorze publicznym i prywatnym nie będąc obserwowanym. Problem ten nasila się we współczesnym „społeczeństwie nadzorowanym”.

<sup>22</sup> Aby upewnić się, czy dane działanie objęte jest „wyłączeniem dla użytku domowego”, patrz [Opinia 5/2009](#) w sprawie portali społecznościowych (WP 163).

<sup>23</sup> Problem ten nie występuje, jeśli organizacje – zarówno z sektora publicznego jak i prywatnego – wykorzystują aplikacje typu cloud computing, gdyż dyrektywa odnosi się do nich i prowadzonych przez nie operacji przetwarzania jako „wykonywanego w ramach działalności oddziału administratora”

należy przeciwdziałać, w szczególności w kontekście coraz częstszego występowania takich sytuacji. W świetle powyższego wszystkie podmioty oferujące usługi osobom fizycznym winny zapewnić określone zabezpieczenia, a w razie potrzeby także zagwarantować poufność informacji wprowadzanych przez użytkowników, niezależnie od tego, czy ich klienci są administratorami danych. Ponadto, należy rozważyć możliwość przyznania osobom, których dane dotyczą dodatkowych środków pozwalających na wykonywanie ich praw w internecie, w tym ochrony praw stron trzecich, których dane mogą podlegać przetwarzaniu (np. w przypadku portali społecznościowych). Z uwagi na fakt, że sprawa ta posiada wiele więcej niewyjaśnionych aspektów<sup>24</sup>, winny one zostać określone w bardziej jasny sposób w kontekście nowych ram prawnych.

## **6. Zwiększenie odpowiedzialności administratorów danych**

72. Na mocy dyrektywy 95/46/WE, administrator danych odgrywa kluczową rolę w zapewnianiu zgodności z zasadami i zobowiązaniami mającymi na celu zagwarantowanie ochrony praw osobowych obywateli. Dyrektywa w sposób dorozumiany, a w wielu przypadkach również wprost, zobowiązuje administratorów do poszanowania zasad ochrony danych i spełnienia określonych wymogów,<sup>25</sup> np. zgłoszenia zbiorów danych do rejestracji i kontroli przez krajowe organy ochrony danych.<sup>26</sup> Ponadto, zapewnienie poszanowania prawa obywateli do ochrony danych wymaga nałożenia na administratora odzwierciedlających je obowiązków, np. obowiązku udzielania informacji.<sup>27</sup>
73. Zobowiązania te mają również zastosowanie – pośrednio lub bezpośrednio – do przetwarzających dane, jeśli administratorzy powierzyli im całość lub część operacji przetwarzania. Aby zapewnić wytyczne w sprawie interpretacji zadań administratora i przetwarzającego, Grupa Robocza Art. 29 pracuje obecnie nad opinią w tej sprawie. Wyżej wymienione wytyczne mogą zawierać dalsze zalecenia dla przyszłych ram prawnych.

### ***Włączanie ochrony danych w kulturę organizacyjną***

74. Odpowiednie przepisy dyrektywy 95/46/WE dają niewątpliwie solidną podstawę dla ochrony danych osobowych i powinny zostać utrzymane, niemniej jednak, na chwilę obecną zgodność z istniejącymi zobowiązaniami prawnymi często nie jest w odpowiedni sposób włączana w zakres wewnętrznych praktyk organizacji. Prywatność często nie stanowi części technologii i systemów przetwarzania danych. Ponadto kadra zarządzająca, również najwyższego szczebla, zwykle nie ma odpowiedniej świadomości, a co za tym idzie – nie podejmuje w sposób aktywny odpowiedzialności za praktyki kierowanego przez siebie podmiotu w zakresie

---

na terytorium UE (patrz art. 4.1.a). W związku z powyższym Rozdział 5 ma zastosowanie niezależnie od tego, czy dostawca usług ma siedzibę na terytorium UE.

<sup>24</sup> Np. w odniesieniu do zgody dzieci lub ich rodziców, żądania dostępu przez organy wymiaru sprawiedliwości, prawa dostępu do kont internetowych dla spadkobierców osób zmarłych i wniosków składanych przez strony trzecie.

<sup>25</sup> Art. 6 (2) wyraźnie stanowi, że „to do administratora należy zachowanie zgodności z ust. 1” (odnoszącym się do głównych zasad związanych z jakością danych).

<sup>26</sup> Patrz art. 18-21 dyrektywy 95/46/WE.

<sup>27</sup> Inne prawa osób, których dane dotyczą, to prawo dostępu, poprawiania, usuwania i blokowania danych oraz sprzeciwu wobec ich przetwarzania (art. 10-12 i 14). Prawa te pociągają za sobą zobowiązanie administratora do umożliwienia ich wykonania.

ochrony danych. Skandale związane z „wyciekami” danych, które miały miejsce w niektórych państwach członkowskich w ciągu ostatnich kilku lat, stanowią dowód tego niepokojącego zjawiska.

75. Jeśli ochrona danych nie zostanie włączona w zakres wspólnych wartości i praktyk organizacji, a związanych z nią zobowiązań nie przypisze się konkretnym osobom, zagrozi to skutecznemu zachowywaniu zgodności z zasadami ochrony danych i wciąż będzie dochodziło do błędów na tym polu. To z kolei może osłabić publiczne zaufanie do przedsiębiorstw i organów administracji publicznej. Ponadto, włączenie ochrony danych w zakres kultury organizacyjnej ułatwi wykonywanie przez organy ochrony danych zadań w zakresie nadzoru i egzekwowania prawa, opisanych szerzej w Rozdziale 7, co zwiększy skuteczność ochrony danych.
76. Zasady i zobowiązania ustanowione w dyrektywie 95/46/WE powinny przenikać strukturę przedsiębiorstw, nie być postrzegane jako zestaw wymogów prawnych, których wypełnienie musi „odhaczyć” departament prawny. Wymogi zawarte w dyrektywie winny prowadzić do konkretnych działań w zakresie ochrony danych podejmowanych w toku codziennej działalności. Możliwość kontroli prywatności powinna być zawarta w projekcie technologii i systemów informacyjnych (patrz także Rozdział 4). Ponadto w obrębie organizacji, zarówno w sektorze publicznym jak i prywatnym, odpowiedzialność za ochronę danych winna być w odpowiedni sposób uznana i przypisana konkretnej osobie.
77. Skuteczność przepisów dyrektywy 95/46/WE zależy od wysiłków podejmowanych przez administratora w celu osiągnięcia założonych w niej celów. Wymaga to podjęcia następujących środków proaktywnych:
- *Przyjęcie przez administratora wewnętrznych polityk i procedur* w celu wdrożenia wymogów dyrektywy w odniesieniu do poszczególnych operacji przetwarzania wykonywanych przez administratora. Takie polityki i procedury winny zostać zatwierdzone na najwyższym szczeblu organizacji i jako takie być wiążące dla wszystkich pracowników.
  - *Wprowadzenie mechanizmów egzekwowania procedur i polityk wewnętrznych, w tym procedur skargowych (patrz także Rozdział 5)*, w celu zapewnienia skuteczności takich polityk w praktyce. Może obejmować podnoszenie świadomości w zakresie ochrony danych oraz szkolenie pracowników.
  - *Tworzenie raportów zgodności i przeprowadzanie audytów, otrzymywanie certyfikatów lub znaków jakości od stron trzecich* w celu monitorowania i oceny, czy wewnętrzne środki przyjęte w celu zapewnienia zgodności pozwalają na skuteczne zarządzanie, ochronę i zabezpieczanie danych osobowych (patrz także Rozdział 4).
  - *Prowadzenie oceny wpływu na prywatność*, w szczególności dla niektórych operacji przetwarzania danych uznanych za szczególnie zagrażające prawom i wolnościom osób, których dane dotyczą, np. przez swój charakter, zakres lub cel.
  - *Przypisanie odpowiedzialności za ochronę danych* wyznaczonym osobom, bezpośrednio odpowiadającym za zgodność działań ich organizacji z ustawodawstwem w zakresie ochrony danych.
  - *Certyfikacja zgodności przez kadrę zarządzającą najwyższego szczebla* potwierdzająca, że wprowadziła ona odpowiednie zabezpieczenia danych osobowych.

- *Przejrzystość przyjętych środków* w odniesieniu do osób, których dane dotyczą i w ogóle. Wymogi w zakresie przejrzystości przyczyniają się do rozliczalności administratorów danych (np. poprzez publikację polityk prywatności w internecie, przejrzystość w odniesieniu do wewnętrznych procedur skargowych i publikację sprawozdań rocznych).

78. Art. 17 (1) dyrektywy 95/46/WE do pewnego stopnia zobowiązuje administratorów do wprowadzenia pewnych środków, zarówno technicznych jak i organizacyjnych (muszą oni „wprowadzić odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych przed (...) nielegalnymi formami przetwarzania”). Środki takie mogą obejmować niektóre z opisanych powyżej. W praktyce jednak, art. 17 (1) nie zdołał wprowadzić odpowiednio skutecznej ochrony danych w organizacjach, m.in. z uwagi na różne podejścia przyjęte podczas wdrażania dyrektywy w prawie krajowym.

### ***Zasada rozliczalności***<sup>28</sup>

79. Właściwą odpowiedzią na ten problem byłoby wprowadzenie w kompleksowych ramach prawnych zasady rozliczalności, zgodnie z którą administratorzy danych byłiby zobowiązani do podjęcia koniecznych środków w celu *zapewnienia przestrzegania* istotnych zasad i zobowiązań przewidzianych w dyrektywie podczas przetwarzania danych osobowych. Przepis taki zwiększyłby potrzebę podjęcia efektywnych działań w kierunku efektywnego wewnętrznego wdrażania istotnych zasad i zobowiązań przewidzianych w dyrektywie. Ponadto, zasada rozliczalności nakładałaby na administratorów wymóg wprowadzenia niezbędnych mechanizmów wewnętrznych w celu *wykazania zgodności* przed zainteresowanymi stronami trzecimi, w tym krajowymi organami ochrony danych. Wynikająca z tego konieczność udowodnienia podjęcia odpowiednich środków w celu zapewnienia zgodności znacznie ułatwiłaby egzekwowanie obowiązujących przepisów.

80. W każdym przypadku, środki, jakich podjęcia wymaga się od administratorów, winny być skalowalne i uwzględniać m.in. rodzaj firmy, jej wielkość, odpowiedzialność oraz rodzaj, charakter i ilość danych osobowych przetwarzanych przez administratora.

### ***Więcej opcji: podejście proaktywne lub reaktywne***

81. Niektóre ze środków opisanych powyżej uznać można za standardowe dobre praktyki, wypełniające wymóg rozliczalności w przypadku ich zastosowania w praktyce. Można przewidzieć w prawie system nagród zachęający organizacje do ich wdrażania.

82. Można też zastosować rozwiązanie bardziej normatywne, np. rozwinięcie art. 17 (1) tak, by wymieniał on dodatkowe środki proaktywne, takie jak wymienione powyżej, które winny zostać zastosowane przez administratorów danych. Środki takie powinny być zorientowane na osiągnięcie konkretnych celów i neutralne technologicznie.

83. Inne środki, mające charakter bardziej reaktywny, mogłyby mieć zastosowanie w przypadku stwierdzenia bezprawnego przetwarzania danych osobowych, i obejmować m.in:

---

<sup>28</sup> Kwestia rozliczalności została omówiona także w ust. 39.

- *Ustanowienie obowiązku zgłaszania naruszeń bezpieczeństwa* (patrz także Rozdziały 2 i 5).
- *Wzmocnienie uprawnień egzekucyjnych organów ochrony danych*, w tym narzucania określonych wymogów w celu zapewnienia skutecznej ochrony (patrz także Rozdział 7a).

### ***Uproszczenie zgłaszania***

84. Obowiązek zgłaszania operacji przetwarzania danych do krajowych organów ochrony danych można uprościć lub zmniejszyć. W tym kontekście należy zbadać związek pomiędzy zgodnością z wymogami wymienionymi powyżej i możliwością dalszego uszczegółowienia wymogów administracyjnych, w szczególności zgłaszania operacji przetwarzania danych do krajowych organów ochrony danych.
85. Zgłaszanie przetwarzania przyczynia się do zwiększenia świadomości operacji przetwarzania danych i praktyk ochrony danych obowiązujących w ramach organizacji.<sup>29</sup> Daje także organom ochrony danych możliwość dokonania przeglądu operacji przetwarzania. Te same cele można jednak osiągnąć za pomocą lepszego zarządzania danymi i większej rozliczalności – takie mechanizmy mogą pomóc wprowadzić środki niezbędne do osiągnięcia istotnych celów i wypełnienia wymogów obecnie wyszczególnionych w dyrektywie, oraz do dowiedzenia takiej zgodności.
86. Należy zbadać czy i w jakim stopniu można by ograniczyć zgłaszanie przetwarzania do przypadków stwarzających szczególne zagrożenie dla prywatności, co umożliwiłoby organom ochrony danych bardziej selektywne działanie i skupienie się na takich przypadkach. Nawet w nich zgłaszanie mogłoby zostać uproszczone, np. poprzez przedstawianie wyników oceny wpływu na prywatność lub przeprowadzonego przez stronę trzecią audytu ochrony danych. Można by połączyć je z systemem rejestracji, w którym wszyscy administratorzy byłiby wpisywani do rejestru prowadzonego przez organ ochrony danych w celu zapewnienia łatwości identyfikacji jednostek organizacyjnych w przypadku konieczności przeprowadzenia skutecznej i efektywnej egzekucji.

## **7. Większa i wyraźniejsza rola organów ochrony danych i ich współpraca w obrębie UE**

### **7a. Organy ochrony danych**

87. Na chwilę obecną, istnieją znaczące różnice pomiędzy pozycją organów ochrony danych w 27 państwach członkowskich, wynikające z różnej historii, precedensów, kultury i organizacji wewnętrznej państw członkowskich, ale także z braku precyzji w kilku aspektach art. 28 dyrektywy 95/46/WE. Ponadto, niektóre aspekty dyrektywy zostały nieodpowiednio wprowadzone w niektórych reżimach prawnych, co

<sup>29</sup> Poglądy te potwierdza raport grupy roboczej w sprawie obowiązku zgłaszania zbiorów do rejestracji przez organy ochrony danych, najlepszego wykorzystania wyjątków i uproszczeń oraz roli administratorów bezpieczeństwa informacji w Unii Europejskiej (WP 106), przyjęty w dniu 18 stycznia 2005 r.

spowodowało znaczące rozbieżności pomiędzy państwami członkowskimi w zakresie, m.in. zasobów i uprawnień, jakimi dysponują organy ochrony danych.

88. Nowe wyzwania stojące przed ochroną danych (globalizacja i rozwój technologiczny – patrz Rozdziały 3 i 4) wymagają szczegółowego, a także bardziej jednolitego i skutecznego nadzoru ze strony organów ochrony danych. W efekcie, nowe ramy prawne winny gwarantować na wysokim poziomie zachowanie jednolitych standardów w zakresie niezależności, uprawnień i roli doradczej w procesie ustawodawczym oraz możliwości ustalania sposobu działania, w szczególności poprzez wyznaczanie priorytetów w zakresie rozpatrywania skarg.
89. Organy ochrony danych muszą być w pełni, prawdziwie niezależne. Art. 28 (1) dyrektywy 95/46/WE w obecnym kształcie jest niejasny, co wykazuje sprawa C-584/07 (Komisja przeciwko Niemcom), tocząca się obecnie przez Europejskim Trybunałem Sprawiedliwości. W kontekście nowych ram prawnych organy ochrony danych powinny posiadać:
- całkowitą niezależność instytucjonalną i nie podlegać żadnym innym organom rządowym.
  - niezależność funkcjonalną i nie podlegać kontroli innych instytucji w kontekście zakresu swojego działania.
  - niezależność materialną. Powinny posiadać infrastrukturę umożliwiającą sprawne wykonywanie ich obowiązków, w szczególności odpowiednie fundusze. Organom ochrony danych należy przyznać odpowiednie zasoby.
90. Rola organów ochrony danych w egzekwowaniu prawa staje się coraz istotniejsza. Organy muszą mieć możliwość zaprezentowania silnego, śmiałego i strategicznego podejścia do interwencji i egzekwowania prawa. Obecny sposób sformułowania art. 29 dyrektywy 95/46/WE zaowocował znaczącymi różnicami w uprawnieniach w zakresie egzekwowania prawa. Nowe ramy prawne powinny wymagać bardziej jednolitego podejścia od państw członkowskich w zakresie przyznawania organom ochrony danych niezbędnych uprawnień i określać je bardziej szczegółowo niż dyrektywa 95/46/WE. Niezbędne uprawnienia powinny obejmować m.in. możliwość nakładania kar finansowych na administratorów i przetwarzających.
91. Rola doradcza organów ochrony danych w procesie ustawodawczym jest niezbędna, zaś wiedza pozyskiwana przez te organy podczas badania i wdrażania jest często konieczna dla ulepszania ustawodawstwa w zakresie ochrony danych. Rola doradcza powinna obejmować wszystkie środki i akty prawne odnoszące się do przetwarzania danych osobowych, nie tylko „środki administracyjne lub przepisy”<sup>30</sup>. Organy ochrony danych winny być proszone o konsultację przed przyjęciem projektu ustawodawczego. Ponadto, nowe ramy prawne winny zapewnić przyznanie organom ochrony danych roli doradczej w odniesieniu do parlamentów krajowych lub innych właściwych instytucji krajowych zaangażowanych w tworzenie nowych przepisów prawa UE.
92. Organy ochrony danych muszą mieć możliwość ustalania swojego sposobu działania i określania priorytetów w odniesieniu, m.in. do rozpatrywania skarg, w tym do

---

<sup>30</sup> Art. 28 (2) dyrektywy 95/46/WE.



sposobu ich rozpatrywania.<sup>31</sup> Organy ochrony danych w każdym przypadku powinny mieć możliwość uwzględnienia fakty, czy rozpatrzenie danej skargi w wystarczający sposób przyczyni się do ochrony danych osobowych.<sup>32</sup> Nowe ramy prawne powinny dać organom ochrony danych możliwość zastosowania „selektywności zapewniającej efektywność”.

93. Z drugiej strony, organy ochrony danych muszą być rozliczane ze sposobu, w jaki wykorzystują większe uprawnienia nadzorcze, i winny zachować w tej kwestii przejrzystość i publicznie zdawać sprawę ze sposobu działania i z ustalonych priorytetów. W kontekście nowych ram prawnych art. 28 (5) dyrektywy 95/46/WE wymaga uszczegółowienia.

## **7b. Współpraca pomiędzy organami ochrony danych**

### ***Obecne ramy prawne***

94. Art. 29 dyrektywy 95/46/WE ustanowił Grupę Roboczą ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych jako organ instytucjonalny dla współpracy pomiędzy krajowymi organami ochrony danych. Grupa Robocza art. 29 ma status doradczy i działa w sposób niezależny. Jej zadania są określone w art. 30 (1) dyrektywy. Należą do nich: badanie każdej kwestii dotyczącej stosowania krajowych środków przyjętych na podstawie niniejszej dyrektywy, aby przyczynić się w ten sposób do jednolitego stosowania tych środków, przekazywanie Komisji opinie na temat stopnia ochrony we Wspólnocie i w krajach trzecich oraz doradzanie (również z własnej inicjatywy) w sprawie wszelkich proponowanych zmian dyrektywy, dodatkowych lub szczegółowych środków mających na celu zabezpieczenie praw i wolności osób fizycznych w zakresie przetwarzania danych osobowych oraz innych proponowanych przez środków wspólnotowych wpływających na prawa i wolności. Komisja jest członkiem Grupy Roboczej Art. 29 i zapewnia jej Sekretariat.
95. Grupa Robocza Art. 29 wypełnia swoje zadania w zakresie przewidzianym w dyrektywie 95/46/WE, określonym w jej art. 3 (2). W roku 2007 europejskie organy ochrony danych ustanowiły w obszarze współpracy policyjnej i sądowej Grupę Roboczą ds. Współpracy Policyjnej i Sądowej, pełniącą rolę podobną jak Grupa Robocza Art. 29, jednak bez podstaw prawnych i Sekretariatu zapewnianego przez instytucję UE. Decyzja ramowa 2008/977/WPiPS, wprowadzająca zasady ochrony danych na tym obszarze, nie ustanawia zinstytucjonalizowanej współpracy pomiędzy organami ochrony danych.

### ***Działanie Grupy Roboczej Art. 29***

---

<sup>31</sup> Możliwość wyboru może być wprowadzona w praktyce na różne sposoby, np. poprzez utworzenie „szybkiej ścieżki” dla rozpatrywania drobnych spraw.

<sup>32</sup> Kryteria mające zastosowanie do oceny, czy należy rozpatrzyć skargę, to np. jej powiązanie z sytuacją obejmującą większą liczbę osób, z naruszeniem zasad ochrony danych, które ma duże znaczenie i prawdopodobnie nie stanowi odosobnionego przypadku oraz ocena, czy rozpatrzenie skargi może być skuteczne i czy nie wymaga nieproporcjonalnego wysiłku.

96. Grupa Robocza Art. 29 działa od ponad 10 lat i znacząco przyczyniła się do osiągnięcia celów nakreślonych w art. 30 dyrektywy 95/46/WE. Wyniki wielu z jej działań można znaleźć na jej stronie internetowej.<sup>33</sup>

97. Grupa Robocza Art. 29 stale pracuje nad poprawą skuteczności swojego działania i powinna w dalszym ciągu rozważać swój sposób funkcjonowania.

Szczególną uwagę należy zwrócić na następujące kwestie:

- w jaki sposób Grupa Robocza Art. 29 może skutecznie przyczynić się do jednolitego wdrażania ustawodawstwa UE w prawie krajowym i do jednolitego stosowania prawa krajowego?
- jak może zwiększyć skuteczność swych działań w odniesieniu do instytucji UE, a w szczególności do Komisji, biorąc pod uwagę dwojaką rolę Komisji, która jest członkiem Grupy, a zarazem adresatem wielu jej opinii?

### ***Konsekwencje dla przyszłości***

98. Przede wszystkim należy zapewnić objęcie wszystkich kwestii związanych z przetwarzaniem danych osobowych, w szczególności w obszarze współpracy policyjnej i sądowej w sprawach karnych, działalnością Grupy Roboczej Art. 29 w jej obecnym kształcie. W kompleksowych ramach prawnych winien znaleźć się kompleksowy organ doradczy. W okresie przejściowym, przed wejściem w życie zmian ustawodawczych, należy opracować odpowiedni sposób bliskiej współpracy Grupy Roboczej Art. 29 z WPPJ.

99. Inne ulepszenia nie wymagają zmian w ustawodawstwie.

- Jednolite stosowanie prawa krajowego wdrażające dyrektywę 95/46 można osiągnąć w kontekście istniejących ram prawnych poprzez dalsze ulepszanie metod pracy Grupy Roboczej i, w razie potrzeby, wymaganie od członków grupy zaangażowania we wdrażanie poglądów Grupy w praktyce krajowej.
- Zgodnie z art. 29 dyrektywy 95/46/WE, Sekretariat Grupy Roboczej zapewniany jest przez Komisję. Sekretariat powinien ściśle współpracować z Przewodnictwem Grupy i jego pracownikami. Zadania Sekretariatu i Przewodnictwa uzupełniają się, powinny więc one ściśle współpracować w celu umożliwienia Grupie Roboczej jak najsprawniejszego wykonywania jej zadań. Sekretariat zajmuje się aspektami logistycznymi pracy Grupy Roboczej i pomaga jej w przygotowaniu opinii i innych dokumentów, natomiast Przewodnictwo (i Wiceprzewodnictwo) skupia się głównie na procesie decyzyjnym i strategii działania Grupy Roboczej Art. 29.
- Relacje z Komisją można dalej poprawić poprzez określenie najważniejszych ról obu stron w porozumieniu pomiędzy Grupą Roboczą Art. 29 a Komisją. Porozumienie winno także określać zasoby udostępniane Grupie Roboczej Art. 29, by umożliwić jej wypełnianie swych zadań z maksymalną wydajnością oraz sposób funkcjonowania Sekretariatu, w celu zapewnienia, że zarówno Grupa Robocza jak i sam Sekretariat posiadają zasoby wystarczające do przygotowania opinii i dokumentów roboczych Grupy Roboczej. Grupa Robocza rozpocznie konsultacje z Komisją w tej sprawie w roku 2010.

<sup>33</sup> [http://ec.europa.eu/justice\\_home/fsj/privacy/workinggroup/index\\_en.htm?refer=true&theme=blue](http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm?refer=true&theme=blue)

## **8. Wyzwania dla ochrony danych w kontekście działalności policji i organów wymiaru sprawiedliwości**

100. Ochrona danych osobowych w kontekście działań policji i organów wymiaru sprawiedliwości to szczególna kwestia wymagająca szczególnej uwagi i uwzględnienia złożoności związku pomiędzy działaniami państw zmierzającymi do zapewnienia bezpieczeństwa a ochroną danych osobowych obywateli. Szczególny charakter tej kwestii wynika nie tylko z podziału na trzy filary na mocy poprzednich traktatów o Unii Europejskiej – jest szeroko uznawana (patrz np. wyjątki od art. 13 dyrektywy 95/46/WE i Deklaracja 21 stanowiąca załącznik do Traktatu z Lizbony).

### ***Zmiana sytuacji w obrębie UE***

101. Po wejściu w życie Traktatu z Lizbony pojawią się nowe perspektywy dla ustawodawstwa w zakresie ochrony danych. Zostanie zniesiony podział na filary, a art. 16 Traktatu stworzy jedną podstawę prawną dla ochrony danych w niemal wszystkich obszarach prawa unijnego (patrz Rozdział 2). Nie oznacza to jednak, że zasady ochrony danych będą wdrażane na polu współpracy policyjnej i sądowej w taki sam sposób jak w innych obszarach społeczeństwa. Deklaracja 21 stanowiąca załącznik do Traktatu z Lizbony stwierdza, że szczególne zasady dla obszaru egzekwowania prawa „mogą okazać się konieczne”.

102. Ochrona danych i ich przekazywanie będą stanowić istotną część Programu Sztokholmskiego. Podejmowanie decyzji oparte będzie na zasadzie zachowania odpowiedniej równowagi pomiędzy potrzebami organów wymiaru sprawiedliwości a wymogami ochrony danych. Nowe środki powinny zostać wdrożone dopiero po przeprowadzeniu odpowiedniej oceny istniejących ram prawnych.

103. Decyzja ramowa 2008/977/WPiPS w sprawie ochrony danych osobowych w kontekście współpracy policyjnej i sądowej w sprawach karnych musi zostać wdrożona przez państwa członkowskie przed dniem 27 października 2010 r. Decyzja ta może być uznawana za pierwszy krok do stworzenia ram prawnych dla ochrony danych w dawnym III filarze, nie zawiera podstawowych elementów i narzędzi pozwalających na skuteczne działanie w obliczu zmian metod pracy w zakresie egzekwowania prawa.

### ***Zmiana sposobu egzekwowania prawa***

104. W ostatnich latach zmieniły się metody pracy policji i organów sądowych w zakresie wykorzystania danych osobowych. Zmiana zaowocowała zwiększoną potrzebą wykorzystania informacji w celu stawienia czoła nowym groźbom związanym z terroryzmem i przestępczością zorganizowaną i została dodatkowo przyspieszona rozwojem technologicznym, jaki miał miejsce w ostatnich latach.

105. Zmiana miała wiele wymiarów:

- Wykorzystanie informacji ma miejsce we wcześniejszym ogniwie łańcucha: poza tradycyjnym wykorzystaniem informacji do śledzenia i wykrywania określonych przestępstw, są one także zbierane i przekazywane w celu zapobiegania ewentualnym działaniom przestępczym („polityka prewencyjna”).
- Wykorzystywane są informacje dotyczące szerszej grupy osób. Zbiera się i przekazuje nie tylko dane osób bezpośrednio powiązanych z przestępcami, np.

podejrzanych czy świadków, ale także większych grup osób nieobjętych dochodzeniem (np. podróżnych, użytkowników usług płatniczych itp.).

- Wykorzystywane informacje są coraz częściej oparte na technologii, mogącej łączyć całkowicie odrębne czynniki w celu przewidzenia przyszłych zachowań obywateli za pomocą zautomatyzowanych narzędzi (data mining, tworzenie profili).
- Wykorzystywane informacje mają inny charakter – korzysta się nie tylko z obiektywnie ustalonych informacji („danych twardych”), ale także z informacji uzyskanych w drodze ocen i analiz prowadzonych w ramach dochodzenia („danych miękkich”), a ponadto rozróżnienie między tymi rodzajami danych może być dokonywane w różny sposób w różnych państwach członkowskich.
- Coraz częściej wykorzystuje się dla celów prewencyjnych dane osobowe pochodzące z sektora prywatnego, np. dane bankowe i finansowe czy dane o pasażerach zbierane przez linie lotnicze i CRS.
- Informacje zbierane w określonym prawnie uzasadnionym celu są coraz częściej wykorzystywane w innych, czasami niezgodnych z nim celach. Interoperacyjność systemów stanowi poważny postęp, nie ogranicza się jednak do kwestii technologicznych – powoduje m.in. ryzyko połączenia baz danych prowadzonych w różnych celach.
- Dane wykorzystuje coraz więcej organów – nie tylko organy policyjne i sądowe *sensu stricto*, ale także inne organy publiczne, np. służby celne i podatkowe, a także krajowe służby bezpieczeństwa.

106. Zmiana sposobu egzekwowania prawa doprowadziła do gwałtownego wzrostu ilości danych przechowywanych i przekazywanych w ramach działalności organów policyjnych i sądowych. Możliwości technologiczne pozwalające na łatwe łączenie informacji mogą mieć poważny wpływ na ochronę danych i prywatności wszystkich obywateli, a nawet na samą możliwość wykonywania przez nich podstawowych praw, w szczególności swobody przemieszczania się, swobody wypowiedzi i swobody wyrażania poglądów.

### **Wyzwania dla ochrony danych**

107. Z przedstawionych powyżej faktów wynika, że przed ochroną danych stoją ogromne wyzwania. Przyszłe ramy prawne powinny w każdym przypadku odnosić się do następujących zjawisk:

- Może pojawić się tendencja do mniej lub bardziej stałego nadzorowania wszystkich obywateli, często określana jako społeczeństwo nadzorowane – np. w przypadku połączonego wykorzystania inteligentnych kamer wideo nadzoru i innych narzędzi, takich jak automatyczne rozpoznawanie tablic rejestracyjnych, rejestrujące wszystkie samochody wjeżdżające na dany teren i wyjeżdżające z niego.
- Bazy danych mogą być wykorzystywane do wyszukiwań na wielką skalę (data mining), a na podstawie utworzonych profili obywateli można oceniać związane z nimi ryzyko, co może doprowadzić do stygmatyzacji osób wywodzących się z określonych środowisk.
- Analizy prowadzone na podstawie ogólnych kryteriów wiążą się z ryzykiem znaczących nieścisłości, prowadzących do dużej liczby wyników fałszywie negatywnych i fałszywie pozytywnych.
- Przetwarzanie danych osobowych osób niebędących podejrzanymi ma miejsce coraz częściej. Konieczne są określone warunki i zabezpieczenia w celu oceny

jego legalności i proporcjonalności oraz uniknięcia dyskryminacji osób, które nie są w sposób aktywny zamieszane w przestępstwo.

- Coraz częściej wykorzystywane są dane biometryczne, w tym DNA, co pociąga za sobą szczególne ryzyko.

### ***Warunki tworzenia prawa i polityki***

108. Rosnąca liczba prowadzonych lub planowanych inicjatyw sektorowych może z łatwością doprowadzić do powstania nakładających się lub sprzecznych środków. Korzystne może się więc okazać oparcie wymiany informacji na spójnej strategii, o ile zasady ochrony danych zostaną w pełni uwzględnione i będą stanowiły integralną część takiej strategii.<sup>34</sup>
109. Potrzeba oceny istniejących instrumentów prawnych i ich zastosowania jest niezwykle istotna i winna uwzględniać koszty z punktu widzenia prywatności. Przed wprowadzeniem nowych środków, należy przeprowadzić ocenę już istniejących, powinien się także odbywać okresowych przegląd istniejących środków.
110. Kluczowym elementem jest przejrzystość. Osoby, których dane dotyczą powinny być w jasny sposób informowane o sposobach wykorzystania zbieranych informacji oraz o celach przetwarzania, a informacje takie należy ograniczać jedynie, jeśli w danym przypadku jest to niezbędne, gdyż ich podanie zagroziłoby prowadzonemu dochodzeniu – a i w takim przypadku ograniczenia winno mieć charakter tymczasowy. Prawo dostępu do danych i ich poprawiania przysługujące osobom, których dane dotyczą, winno obowiązywać w kontekście trans granicznym, by zapobiec utracie kontroli przez te osoby.
111. Szczególnej uwagi wymaga kwestia przejrzystości i demokratycznej kontroli procesu ustawodawczego. Ocena wpływu na prywatność, odpowiednie formy konsultacji z organami ochrony danych oraz efektywna debata parlamentarna na poziomie krajowym i unijnym winny odgrywać w tej kwestii istotną rolę.
112. Budowa wszelkich systemów stosowanych do przechowywania i przekazywania danych powinna być odpowiednio przemyślana. Oto niektóre z kwestii, jakie należy uwzględnić:
  - Architektura systemu powinny determinować założenie „prywatności w fazie projektowania” i technologie wspierające prywatność (program certyfikacji). W obszarze wolności, bezpieczeństwa i sprawiedliwości, gdzie organy publiczne są głównymi twórcami każdej inicjatywy zmierzającej do zwiększenia nadzoru nad obywatelami i ilości zbieranych i wykorzystywanych danych osobowych, która może mieć bezpośredni wpływ na ich prawo do ochrony danych i prywatności, wymóg taki mógłby stanowić warunek konieczny.
  - Istotnymi zasadami powinny pozostać ograniczenie celu i minimalizacja ilości przetwarzanych danych.
  - Dostęp do dużych baz danych musi być skonfigurowany w taki sposób, by uniemożliwić bezpośredni dostęp przez Internet do zebranych w nich danych.

---

<sup>34</sup> Europejska Strategia Zarządzania Informacjami, opracowywana obecnie przez radę, może – jeśli właściwie wykorzystana – okazać się przydatnym instrumentem w tym kontekście.

Preferowany jest system indeksowy lub wskazanie, czy dany element znajduje się w bazie.

- Wybór pomiędzy scentralizowanym (opartym na centralnej bazie danych na szczeblu UE) i zdecentralizowanym przechowywaniem danych winien być dokonywany w oparciu o przejrzyste kryteria i w każdym przypadku zapewniać jasne określenie roli i zobowiązań administratora lub administratorów oraz odpowiedni nadzór prowadzony przez właściwe organy ochrony danych.
- Dane biometryczne powinny być wykorzystywane jedynie jeśli użycie innych, mniej inwazyjnych, materiałów nie pozwala na uzyskanie tego samego efektu.

113. Wymiar zewnętrzny. Należy unikać obchodzenia restrykcyjnych zasad ochrony danych obowiązujących na terenie UE. Relacje z państwami trzecimi winny być oparte na jasno określonych ramach wiążących dla wszystkich stron i na pojęciu odpowiedniości. Ocena odpowiedniości winna odbywać się w oparciu o analizę przeprowadzoną przez krajowe organy ochrony danych, a w razie potrzeby za pomocą wspólnych mechanizmów zapewniających spójne wdrażanie i efektywność.
114. Szczególnej uwagi – a w razie potrzeby specjalnie utworzonych zabezpieczeń danych – wymagają duże systemy informacyjne działające w obrębie UE.
115. Należy zapewnić odpowiedni niezależny nadzór, a także nadzór sądowy i możliwość dochodzenia roszczeń na drodze sądowej, w tym, w każdym przypadku, poprzez zapewnienie odpowiednich zasobów i uprawnień niezależnym organom nadzorczym.
116. Współpraca pomiędzy organami ochrony danych gwarantującymi legalność przetwarzania powinna zostać rozwinięta we wszystkich możliwych aspektach i włączona w zakres tam prawnych, również poprzez opracowanie stałych mechanizmów, podobnych do tych obowiązujących obecnie w kwestiach I filara, w celu wspierania zharmonizowanego podejścia w obrębie UE i poza nią.

*W imieniu Grupy Roboczej Art. 29*

*W imieniu Grupy Roboczej ds. Współpracy  
Policyjnej i Sądowej*

Przewodniczący

Przewodniczący

Alex Türk

Francesco PIZZETTI