I

(Rezolucje, zalecenia i opinie)

OPINIE

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych dotycząca komunikatu Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej"

(2011/C 181/01)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 16,

uwzględniając Kartę praw podstawowych Unii Europejskiej, w szczególności jej art. 7 i 8,

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

uwzględniając rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych ([2]), w szczególności jego art. 41,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

A. **CZĘŚĆ OGÓLNA**

1. **Wprowadzenie**

1.1. *Pierwsza ocena ogólna*

1. Dnia 4 listopada 2010 r. Komisja przyjęła komunikat zatytułowany „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej" (zwany dalej „komunikatem") ([3]). Został on przekazany do EIOD do konsultacji. EIOD z zadowoleniem przyjął fakt, że Komisja skonsultowała się z nim zgodnie z art. 41 rozporządzenia (WE) nr 45/2001. Jeszcze przed przyjęciem komunikatu EIOD miał możliwość udzielania nieformalnych uwag. Niektóre z tych uwag zostały uwzględnione w ostatecznej wersji dokumentu.

2. Celem komunikatu jest przedstawienie podejścia Komisji do przeglądu systemu prawnego UE w zakresie ochrony danych osobowych we wszystkich obszarach działalności Unii, zwłaszcza z uwzględnieniem wyzwań wynikających z globalizacji i powstawania nowych technologii ([4]).

3. Generalnie EIOD z zadowoleniem przyjmuje komunikat, gdyż stoi na stanowisku, iż przegląd obecnie obowiązujących ram prawnych ochrony danych w UE jest niezbędny, aby zagwarantować skuteczną ochronę w ciągle rozwijającym się społeczeństwie informacyjnym. Już w opinii z dnia 25 lipca 2007 r. dotyczącej wdrożenia dyrektywy o ochronie danych ([5]) stwierdza on, że w dłuższej perspektywie zmian dyrektywy 95/46/WE nie da się uniknąć.

4. Komunikat stanowi istotny krok w kierunku zmiany ustawodawczej, która z kolei stanowić będzie najważniejszą reformę w dziedzinie ochrony danych w UE od czasu przyjęcia dyrektywy 95/46/WE, która uważana jest powszechnie za kamień węgielny ochrony danych w Unii Europejskiej (oraz szerzej w Europejskim Obszarze Gospodarczym).

5. Komunikat gwarantuje odpowiednie ramy dla dobrze ukierunkowanego przeglądu również dlatego, że określa – generalnie rzecz ujmując – najważniejsze problemy i wyzwania. EIOD podziela pogląd Komisji, że silny system ochrony danych potrzebny będzie nadal w przyszłości w oparciu o założenie, że istniejące ogólne zasady ochrony danych będą nadal aktualne w społeczeństwie, które podlega fundamentalnym zmianom wskutek szybkiego postępu technologicznego i globalizacji. Wymaga to przeglądu istniejących ustaleń prawnych.

([1]) Dz.U. L 281 z 23.11.1995, s. 31.
([2]) Dz.U. L 8 z 12.1.2001, s. 1.
([3]) COM(2010) 609 wersja ostateczna.
([4]) Zob. s. 5 komunikatu, pierwszy akapit.
([5]) Opinia EIOD z dnia 25 lipca 2007 r. w sprawie komunikatu Komisji dla Parlamentu Europejskiego i Rady w sprawie kontynuacji programu prac na rzecz skuteczniejszego wdrażania dyrektywy o ochronie danych, (Dz.U. C 255 z 27.10.2007, s. 1).

6. W komunikacie słusznie podkreśla się, że wyzwania są olbrzymie. EIOD w pełni podziela tę opinię i podkreśla, że proponowane rozwiązania powinny być w związku z tym odpowiednio ambitne i wpływać na wzmocnienie skuteczności ochrony.

1.2. *Cel opinii*

7. Niniejsza opinia jest próbą oceny rozwiązań proponowanych w komunikacie na podstawie dwóch kryteriów: ambicji i skuteczności. Ocena jest ogólnie rzecz biorąc pozytywna. EIOD popiera komunikat, lecz jednocześnie krytycznie podchodzi do tych jego aspektów, gdzie w jego przekonaniu bardziej ambitne podejście wpłynęłoby na stworzenie bardziej skutecznego systemu.

8. Dzięki niniejszej opinii EIOD pragnie wnieść wkład w dalszy rozwój ram prawnych ochrony danych. Oczekuje on z niecierpliwością na wniosek Komisji, którego publikacja planowana jest na połowę 2011 r., mając nadzieję, że jego zalecenia zostaną wzięte pod uwagę i zawarte w treści wniosku. EIOD pragnie również zauważyć, że Komisja wyłączyła pewne obszary, takie jak przetwarzanie danych przez instytucje i organy UE, z zakresu ogólnego instrumentu. Jeżeli Komisja rzeczywiście zdecyduje się pominąć na tym etapie pewne obszary, co EIOD uznaje za niekorzystne, to zdaniem Inspektora powinna zobowiązać się do realizacji kompleksowej architektury systemu w krótkim, dokładnie określonym czasie.

1.3. *Podstawy opinii*

9. Niniejsza opinia nie jest pierwszą opinią tego typu. Oparto ją na wcześniejszych stanowiskach EIOD i europejskich organów ochrony danych, wydawanych w rozmaitych okolicznościach. Należy zwłaszcza podkreślić, że we wspomnianej opinii EIOD z dnia 25 lipca 2007 r. określono i szczegółowo omówiono już niektóre elementy przyszłych zmian ([6]). Opinię tę wydano w oparciu o dyskusje z innymi zainteresowanymi podmiotami z dziedziny prywatności i ochrony danych. Ich wkład stanowi bardzo przydatne tło komunikatu i niniejszej opinii. W tym kontekście stwierdzić należy, że istnieje zgoda, co do sposobu poprawy skuteczności ochrony danych.

10. Innym istotnym elementem niniejszej opinii jest dokument zatytułowany „Przyszłość prywatności" – efekt wspólnych prac grupy roboczej art. 29 ds. ochrony danych oraz grupy roboczej ds. policji i wymiaru sprawiedliwości utworzonej przez Komisję w 2009 r. („dokument grupy roboczej dotyczący przyszłości prywatności") ([7]).

11. Podczas niedawnej konferencji prasowej, która odbyła się dnia 15 listopada 2010 r., EIOD przedstawił pierwsze spostrzeżenia na temat komunikatu. Niniejsza opinia zawiera rozszerzenie bardziej ogólnych poglądów wygłoszonych podczas konferencji prasowej ([8]).

12. Niniejsza opinia opiera się również na wielu wcześniejszych opiniach EIOD oraz dokumentach grupy roboczej art. 29 ds. ochrony danych. Odwołania do wspomnianych opinii i dokumentów znaleźć można w stosownych miejscach w tekście niniejszej opinii.

2. **Kontekst**

13. Przegląd zasad ochrony danych ma miejsce w przełomowym historycznie momencie. Komunikat szeroko i przekonywująco opisuje jego kontekst. Na podstawie tego opisu EIOD zidentyfikował cztery główne czynniki determinujące środowisko, w którym odbywa się proces przeglądu.

14. Pierwszym z nich jest postęp technologiczny. Dzisiejsza technologia nie jest tą samą, która używana była w momencie opracowania i przyjęcia dyrektywy 95/46/WE. Zjawiska technologiczne, takie jak przetwarzanie w chmurze, reklama behawioralna, portale społecznościowe, pobór opłat na drogach czy urządzenia z funkcją geolokalizacji dogłębnie zmieniły sposób przetwarzania danych, stanowią również ogromne wyzwanie z punktu widzenia ochrony danych. Przegląd europejskich zasad ochrony danych będzie musiał skutecznie odnieść się to tych wyzwań.

15. Drugim czynnikiem jest globalizacja. Stopniowe znoszenie barier w handlu umożliwiło przedsiębiorstwom ekspansję na rynki światowe. Transgraniczne przetwarzanie danych i transfery międzynarodowe znacznie wzrosły w ciągu ostatnich lat. Przetwarzanie danych stało się ponadto wszechobecne dzięki technologiom informacyjno-komunikacyjnym – internet i przetwarzanie w chmurze pozwalają na zdelokalizowane przetwarzanie znacznej ilości danych na skalę światową. W ciągu ostatniego dziesięciolecia rozszerzeniu uległa także międzynarodowa działalność

([6]) Zwłaszcza (zob. pkt 77 opinii): nie ma potrzeby zmieniania obowiązujących zasad, istnieje natomiast potrzeba dokonania innych ustaleń administracyjnych; szeroki wachlarz przepisów o ochronie danych mających zastosowanie do wszelkich przypadków wykorzystywania danych osobowych nie powinien ulec zmianie; przepisy o ochronie danych powinny w konkretnych przypadkach pozwalać na zastosowanie zrównoważonego podejścia, a także umożliwiać organom ds. ochrony danych wyznaczanie priorytetów; system powinien w pełni stosować się do wykorzystywania danych osobowych dla celów organów ścigania, choć dla specyficznych problemów w tej dziedzinie powinno się stworzyć odpowiednie środki dodatkowe.

([7]) Dokument WP 168 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf). Jego głównym przesłaniem jest, że zmiany legislacyjne stanowią znakomitą okazję objaśnienia pewnych kluczowych zasad i reguł (takich jak np. zgoda czy przejrzystość), wdrożenia pewnych nowych zasad (np. uwzględniania ochrony prywatności w fazie projektowania, rozliczalności), wzmocnienia skuteczności poprzez modernizację ustaleń (np. poprzez ograniczenie obowiązujących wymogów co do notyfikacji) oraz objęcia wszystkich kwestii wspólnymi kompleksowymi ramami prawnymi (łącznie ze współpracą policji i wymiarów sprawiedliwości).

([8]) Problemy do omówienia podczas konferencji prasowej dostępne są na stronie internetowej EIOD: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-11-15_Press_conf_speaking_points_PHBG_EN.pdf

policji i sądów w zakresie zwalczania terroryzmu i innych form międzynarodowej przestępczości zorganizowanej, wspierana przez wymianę znacznych ilości informacji pomiędzy organami ścigania. W związku z powyższym należy poważnie zastanowić się nad tym, jak skutecznie zagwarantować ochronę danych osobowych w zglobalizowanym świecie bez znaczących utrudnień w zakresie działalności związanej z przetwarzaniem międzynarodowym.

16. Trzecim czynnikiem jest traktat lizboński. Jego wejście w życie oznacza początek nowej ery w dziedzinie ochrony danych. Art. 16 TFUE ustanawia nie tylko prawo indywidualne podmiotu danych, lecz także bezpośrednią podstawę prawną silnego prawa ochrony danych obowiązującego w całej UE. Ponadto rezygnacja ze struktury filarów zobowiązuje Parlament Europejski i Radę do objęcia ochrony danych wszystkimi obszarami prawodawstwa UE. Innymi słowy, umożliwia to stworzenie kompleksowych ram prawnych w zakresie ochrony danych obowiązujących sektor prywatny, sektor publiczny państw członkowskich oraz instytucje i organy UE. Program sztokholmski ([9]) stanowi w tej kwestii konsekwentnie, że Unia musi stworzyć kompleksową strategię ochrony danych w samej UE oraz w ramach relacji z państwami trzecimi.

17. Czwarty czynnik jest reprezentowany przez jednoczesny rozwój w kontekście organizacji międzynarodowych. Mają obecnie miejsce liczne debaty poświęcone modernizacji obowiązujących prawnych instrumentów ochrony danych. Należy w tym miejscu wspomnieć o najnowszych refleksjach dotyczących planowanej rewizji konwencji nr 108 Rady Europy ([10]) i Wytycznych OECD w sprawie ochrony prywatności ([11]). Inny istotny problem dotyczy przyjęcia międzynarodowych standardów ochrony danych osobowych i prywatności, co mogłoby doprowadzić do przyjęcia wiążącego globalnego instrumentu ochrony danych. Wszystkie te inicjatywy zasługują na pełne poparcie, a ich wspólnym celem powinno być zagwarantowanie skutecznej i konsekwentnej ochrony w zdominowanym przez technologię i zglobalizowanym środowisku.

3. **Najważniejsze zagadnienia**

3.1. *Ochrona danych sprzyja zaufaniu, musi też wspierać inne interesy (publiczne)*

18. Silne ramy ochrony danych są nieodzowną konsekwencją wagi, jaką przykłada się do kwestii ochrony danych w kontekście traktatu lizbońskiego, zwłaszcza art. 8 Karty praw podstawowych Unii Europejskiej i art. 16 TFUE, oraz silnych powiązań z art. 7 Karty ([12]).

19. Silne ramy ochrony danych służą jednak szerszym interesom publicznym i prywatnym w społeczeństwie informacyjnym w sytuacji wszechobecnego przetwarzania danych. Ochrona danych buduje zaufanie, które jest najistotniejszym warunkiem dobrego funkcjonowania naszego społeczeństwa. Ważne jest, aby ustalenia co do ochrony danych konstruowane były w taki sposób, by w jak największym stopniu aktywnie wspierały, a nie utrudniały, realizację innych uzasadnionych praw i interesów.

20. Ważnymi przykładami innych uzasadnionych interesów są np. silna gospodarka europejska, bezpieczeństwo obywateli czy rozliczalność rządów.

21. Rozwój gospodarczy UE idzie w parze z wprowadzaniem i marketingiem nowych technologii i usług. W społeczeństwie informacyjnym powstawanie i skuteczne wprowadzanie technologii i usług informacyjno-komunikacyjnych zależy od zaufania. Jeżeli ludzie nie ufają technologiom ICT, prawdopodobnie nie odniosą one sukcesu ([13]). Obywatele zaufają ICT jedynie wówczas, gdy ich dane będą skutecznie chronione. Dlatego też ochrona danych powinna stanowić integralną część technologii i usług. Silne ramy ochrony danych wpływają pozytywnie na europejską gospodarkę, pod warunkiem jednak, że ramy te są nie tylko silne, lecz także dobrze dopasowane. Z tej perspektywy najważniejsza jest dalsza harmonizacja w ramach UE oraz minimalizacja obciążeń administracyjnych (zob. rozdział 5 opinii).

22. Wiele się w ostatnich latach mówiło o potrzebie zrównoważenia prywatności i bezpieczeństwa, zwłaszcza w zakresie instrumentów przetwarzania danych i wymiany na potrzeby policji i współpracy organów ścigania ([14]). Ochrona danych była często niewłaściwie definiowana jako przeszkoda na drodze do pełnej ochrony fizycznego bezpieczeństwa obywateli ([15]) lub co najmniej jako nieunikniony warunek, który szanować muszą organy ścigania. Nie jest to jednak pełna charakterystyka. Silne ramy ochrony danych mogą wpłynąć na zaostrzenie i wzmocnienie bezpieczeństwa. Na podstawie odpowiednio stosowanych zasad ochrony danych administratorzy danych mają obowiązek gwarantować, że informacje są dokładne i aktualne oraz że niepotrzebne dane osobowe, które nie są niezbędne dla potrzeb organów ścigania, będą eliminowane z systemu. Można również wskazać obowiązki wdrażania technologicznych

([9]) Program sztokholmski – Otwarta i bezpieczna Europa dla dobra i ochrony obywateli (Dz.U. C 115 z 4.5.2010, s. 1), na s. 10.

([10]) Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, ETS nr 108, 28 stycznia 1981 r.

([11]) Wytyczne OECD w sprawie ochrony prywatności i transgranicznego przepływu danych osobowych opublikowane na stronie internetowej http://www.oecd.org

([12]) Trybunał Sprawiedliwości podkreślił wagę ochrony danych w powiązania z prywatnością w ramach Karty w wyroku z dnia 9 listopada 2010 r., sprawy połączone C-92/09 i C-93/09, *Schecke*, jeszcze nieopublikowane w Zb. Orz.

([13]) Zob. opinia EIOD z dnia 18 marca 2010 r. w sprawie wspierania zaufania w społeczeństwie informacyjnym poprzez działanie na rzecz ochrony danych i prywatności, (Dz.U. C 280 z 16.10.2010, s. 1), par. 113.

([14]) Zob. np. opinia EIOD z dnia 10 lipca 2009 r. w sprawie komunikatu Komisji do Parlamentu Europejskiego i Rady dotyczącego przestrzeni wolności, bezpieczeństwa i sprawiedliwości w służbie obywateli, (Dz.U. C 276 z 17.9.2009, s. 8).

([15]) Pojęcie bezpieczeństwa jest szersze niż pojęcie bezpieczeństwa fizycznego, lecz dla zilustrowania przytoczonych tu argumentów jest ono używane w tekście opinii w bardziej ograniczonym znaczeniu.

i organizacyjnych środków gwarantujących bezpieczeństwo systemów, takich jak ochrona systemów przed nieuprawnionym ujawnieniem czy dostępem, jakie stosowane są w obszarze ochrony danych.

23. Poszanowanie zasad ochrony danych może ponadto zagwarantować, że organy ścigania działają w sposób praworządny, co pozwala mieć zaufanie do ich działalności, a w szerszej skali budzi zaufanie do społeczeństw. Prawo precedensowe powstałe na mocy art. 8 Europejskiej Konwencji o Ochronie Praw Człowieka gwarantuje, że policja i organy sądowe mogą przetwarzać wszystkie istotne z punktu widzenia ich działalności dane, lecz nie w sposób nieograniczony. Ochrona danych wymaga mechanizmów służących zachowaniu równowagi (zob. rozdział 9 opinii w sprawie policji i wymiaru sprawiedliwości).

24. W społeczeństwach demokratycznych rządy odpowiadają za swoje działania, także za wykorzystywanie danych osobowych dla rozmaitych interesów publicznych, którym służą. Zakres tych działań rozciąga się od publikacji danych w internecie dla celów przejrzystości, poprzez wykorzystywanie danych celem wspierania polityki w dziedzinach, takich jak zdrowie publiczne, transport czy opodatkowanie, do nadzoru nad poszczególnymi obywatelami celem egzekwowania prawa. Dzięki silnym ramom ochrony danych rządy mogą szanować swoje obowiązki i być rozliczane w ramach dobrego sprawowania władzy.

3.2. *Konsekwencje ram prawnych ochrony danych*

3.2.1. Potrzeba dalszej harmonizacji

25. W komunikacie słusznie stwierdzono, że jedną z głównych wad obecnych ram jest to, iż pozostawiają państwom członkowskim zbyt wiele pola manewru co do implementacji przepisów europejskich do prawa krajowego. Brak harmonizacji niesie za sobą wiele negatywnych konsekwencji, zwłaszcza w społeczeństwie informacyjnym, gdy granice fizyczne pomiędzy państwami członkowskimi stają się coraz mniej istotne (zob. rozdział 5 niniejszej opinii).

3.2.2. Ogólne zasady ochrony danych nadal obowiązują

26. Pierwszy, formalny powód, dla którego ogólne zasady ochrony danych powinny, lecz nie mogą być zmienione, ma charakter prawny. Zostały one zawarte w konwencji nr 108 Rady Europy, która jest wiążąca dla wszystkich państw członkowskich. Konwencja ta stanowi podstawę ochrony danych w UE. Niektóre główne zasady wymieniono również w art. 8 Karty praw podstawowych Unii Europejskiej. Wprowadzenie zmian do tych reguł wymagałoby poprawek do wspomnianych traktatów.

27. Nie jest to jednak pełna charakterystyka. Istnieją również powody merytoryczne, dla których nie powinno się zmieniać zasad ogólnych. EIOD jest przekonany, że społeczeństwo informacyjne nie może i nie powinno funkcjonować bez odpowiedniego poziomu ochrony prywatności i danych osobowych obywateli. Gdy przetwarza się więcej informacji, wymagana jest lepsza jakość ich ochrony. Społeczeństwo informacyjne, w ramach którego przetwarzane są znaczące ilości informacji o wszystkich, musi być zbudowane na bazie pojęcia kontroli sprawowanej przez jednostkę, aby mogła ona działać jak jednostka i korzystać z różnych rodzajów wolności w społeczeństwie demokratycznym, takich jak wolność wypowiedzi i słowa.

28. Ponadto trudno wyobrazić sobie kontrolę jednostki bez zobowiązań ze strony administratorów danych, aby ograniczali przetwarzanie danych zgodnie z zasadą niezbędności, proporcjonalności i celowości. Równie trudno jest wyobrazić sobie kontrolę jednostki w sytuacji braku uznanych praw osoby, której dane dotyczą, takich jak prawo do dostępu, korekty, usunięcia czy zablokowania danych.

3.2.3. Z perspektywy praw podstawowych

29. EIOD pragnie podkreślić, że ochrona danych uznawana jest za prawo podstawowe. Nie oznacza to, że ochrona danych powinna zawsze *przeważać* nad innymi istotnymi prawami i interesami w społeczeństwie demokratycznym, lecz że ma to konsekwencje z punktu widzenia charakteru i zakresu ochrony, którą należy zapewnić w unijnych ramach prawnych, aby zagwarantować, że wymogi co do ochrony danych uwzględniane są *w adekwatny sposób*.

30. Najważniejsze konsekwencje są następujące:

— ochrona musi być skuteczna. Ramy prawne muszą zawierać narzędzia umożliwiające jednostkom korzystanie w praktyce z przysługujących im praw,

— ramy muszą być stabilne w długim horyzoncie czasowym,

— ochronę należy gwarantować w każdych okolicznościach, nie w zależności od preferencji politycznych w danych ramach czasowych,

— konieczne mogą być ograniczenia co do korzystania z prawa do ochrony danych, lecz muszą mieć one charakter wyjątkowy, być odpowiednio uzasadnione i w żadnym wypadku nie wpływać na fundamentalne elementy tego prawa ([16]).

EIOD zaleca Komisji, aby uwzględniła powyższe konsekwencje w proponowanych rozwiązaniach prawnych.

3.2.4. Potrzeba nowych ustaleń prawnych

31. W komunikacie słusznie skoncentrowano się na potrzebie wzmocnienia ustaleń prawnych w zakresie ochrony danych. W tym kontekście zasadnym byłoby, aby w dokumencie grupy roboczej zatytułowanym „Przyszłość prywatności” ([17]) organy ochrony danych podkreśliły

([16]) Zob. także opinia EIOD z dnia 25 lipca 2007 r. w sprawie komunikatu Komisji dla Parlamentu Europejskiego i Rady w sprawie kontynuacji programu prac na rzecz skuteczniejszego wdrażania dyrektywy o ochronie danych, ust. 17, która dotyczy prawa precedensowego Europejskiego Trybunału Praw Człowieka i Trybunału Sprawiedliwości.

([17]) Porównaj: przypis 7.

potrzebę silniejszych ról poszczególnych podmiotów działających w dziedzinie ochrony danych, zwłaszcza osób, których dane dotyczą, administratorów danych i samych organów nadzoru.

32. Zainteresowane strony wydają się zgodne co do faktu, że silniejsze ustalenia prawne – z uwzględnieniem zmian technologicznych i globalizacji – są kluczowe z punktu widzenia ambitnej i skutecznej ochrony danych również w przyszłości. Jak już wspomniano w punkcie 7, są to kryteria, według których EIOD ocenia wszystkie proponowane rozwiązania.

3.2.5. Kompleksowość jako *conditio sine qua non*

33. Jak wspominano w komunikacie, dyrektywa 95/46/WE ma zastosowanie do wszystkich działań związanych z przetwarzaniem danych osobowych w państwach członkowskich, zarówno w sektorze państwowym, jak i prywatnym, za wyjątkiem działalności nieobjętej zakresem wcześniejszego prawa wspólnotowego ([18]). Wyjątek ten był potrzebny w czasie obowiązywania poprzedniego traktatu, lecz przestał być konieczny od momentu wejścia w życie traktatu lizbońskiego. Jest on ponadto sprzeczny z treścią i duchem art. 16 TFUE.

34. Według EIOD kompleksowy instrument prawny ochrony danych, obejmujący współpracę policji i wymiarów sprawiedliwości w sprawach karnych, musi być postrzegany jako jedno z najważniejszych ulepszeń, które mogą wprowadzić nowe ramy prawne. Jest to *conditio sine qua non* skutecznej ochrony danych w przyszłości.

35. EIOD pragnie podkreślić następujące argumenty na poparcie tego twierdzenia:

— rozróżnienie na działalność sektora prywatnego i sektora organów ścigania zaciera się. Podmioty sektora prywatnego mogą przetwarzać dane, które wykorzystywane są przez organy ścigania (np. dane dotyczące przelotu pasażera (PNR) ([19])), natomiast w innych przypadkach wymaga się od nich przechowywania danych dla potrzeb organów ścigania (np. dyrektywa w sprawie zatrzymywania danych ([20])),

— na mocy dyrektywy 95/46/WE nie ma zasadniczej różnicy pomiędzy policją i organami sądowymi a innymi organami ścigania (w zakresie podatków, cła, zapobiegania oszustwom czy imigracji),

— jak trafnie stwierdzono w komunikacie narzędzie prawne ochrony danych mające obecnie zastosowanie do policji i organów sądowych (decyzja ramowa 2008/977/WSiSW ([21])) jest nieadekwatne,

— większość państw członkowskich przeprowadziła już implementację dyrektywy 95/46/WE i konwencji nr 108 do prawodawstwa krajowego, dzięki czemu mają one zastosowanie również do ich policji i organów sądowych.

36. Objęcie policji i wymiaru sprawiedliwości zakresem ogólnego instrumentu prawnego stworzyłoby więcej gwarancji dla obywateli, ułatwiłoby też pracę policji. Stosowanie różnych zestawów zasad jest kłopotliwe, czasochłonne i utrudnia współpracę międzynarodową (zob. rozdział 9 niniejszej opinii). Jest to również argument za włączeniem działalności związanej z przetwarzaniem danych przez krajowe służby ds. bezpieczeństwa w zakresie, w jakim jest to możliwe w obecnym stanie prawnym w UE.

3.2.6. Neutralność technologiczna

37. Czas, który upłynął od momentu przyjęcia dyrektywy 95/46/WE w 1995 r., można określić jako burzliwy pod względem technologicznym. Nowinki technologiczne i nowe urządzenia pojawiają się obecnie bardzo często. W wielu przypadkach doprowadziło to do fundamentalnych zmian w sposobie przetwarzania danych osobowych osób fizycznych. Społeczeństwo informacyjne nie może być już uważane za środowisko równoległe, w którym można uczestniczyć na zasadzie dobrowolności, gdyż stało się ono integralną częścią życia codziennego. Jako przykład wymienić tu można tzw. Internet przedmiotów ([22]), który tworzy powiązania pomiędzy przedmiotami fizycznymi a związanymi z nimi informacjami dostępnymi w Internecie.

38. Technologia będzie rozwijać się nadal. Ma to swoje konsekwencje dla nowych ram prawnych, które muszą obowiązywać przez wiele lat, lecz nie stawać na drodze dalszego postępu technologicznego. Dlatego też ustalenia prawne muszą być neutralne pod względem technologicznym. Ramy muszą jednak gwarantować także więcej pewności przedsiębiorstwom i osobom fizycznym, które muszą rozumieć czego się od nich wymaga i sprawnie korzystać ze swoich praw. W związku z tym ustalenia prawne muszą być precyzyjne.

39. Według EIOD ogólne narzędzie prawne ochrony danych należy sformułować w sposób jak najbardziej neutralny z technologicznego punktu widzenia. Oznacza to, że prawa i obowiązki rozmaitych podmiotów należy sformułować w sposób ogólny i neutralny, aby mogły one pozostać co do zasady słuszne i egzekwowalne bez względu na rodzaj technologii zastosowanej do przetwarzania danych osobowych. Nie mamy innego wyjścia

([18]) Opinia ta koncentrować się będzie głównie na dawnym 3. filarze (współpraca policji i wymiarów sprawiedliwości w sprawach karnych), gdyż dawny 2. filar jest nie tylko bardziej skomplikowanym obszarem prawa UE (jak mówi art. 16 TFUE i art. 39 UE), lecz także mniej istotnym z punktu widzenia przetwarzania danych.

([19]) Zob. np. komunikat Komisji w sprawie globalnego podejścia do przekazywania danych dotyczących przelotu pasażera (PNR) państwom trzecim, COM(2010) 492 wersja ostateczna.

([20]) Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE, (Dz.U. L 105 z 13.4.2006, s. 54).

([21]) 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).

([22]) Jak zdefiniowano w dokumencie „Internet przedmiotów – plan działań dla Europy" COM(2009) 278 wersja ostateczna.

z uwagi na szybkie tempo, w jakim odbywa się obecnie postęp technologiczny. EIOD sugeruje wprowadzenie, obok istniejących zasad ochrony danych, nowych „neutralnych pod względem technologicznym" praw, które miałyby konkretne znaczenie w szybko zmieniającym się otoczeniu elektronicznym (zob. zwłaszcza rozdział 6 i 7).

3.2.7. Długi horyzont czasowy – pewność prawa na dłużej

40. Dyrektywa 95/46/WE stanowi środek ciężkości ochrony danych w UE od 15 lat. Została ona wdrożona przez państwa członkowskie, jej postanowienia stosują rozmaite podmioty. Na przestrzeni lat stosowanie dyrektywy wiązało się z coraz większym doświadczeniem w tej dziedzinie, dalsze wytyczne tworzyła też Komisja, organy ochrony danych (na szczeblu krajowym i w ramach prac grupy roboczej art. 29) oraz sądy krajowe i europejskie.

41. Należy podkreślić, że zmiany te wymagają czasu, a w świetle faktu, że mamy do czynienia z ogólnymi ramami wprowadzającymi w życie prawo podstawowe, czas ten potrzebny jest na stworzenie pewności i stabilności prawa. Nowe ogólne narzędzie prawne musi zostać zaprojektowane w sposób gwarantujący pewność i stabilność prawa na dłuższy czas, przy założeniu, że trudno jest przewidzieć dalszy rozwój w dziedzinie technologii i globalizacji. EIOD popiera cel, jakim jest zagwarantowanie pewności prawa na dłuższy czas, porównywalny do horyzontu czasowego dyrektywy 95/46/WE. Krótko mówiąc, gdy technologia rozwija się w szybkim tempie, prawo musi być stałe.

3.2.8. Krótki horyzont czasowy – lepsze stosowanie istniejących instrumentów

42. W krótkim horyzoncie czasowym ważne jest zagwarantowanie skuteczności istniejących ustaleń prawnych, zwłaszcza poprzez koncentrację na egzekwowaniu prawa na szczeblu krajowym i unijnym (zob. rozdział 11 niniejszej opinii).

B. **ELEMENTY NOWYCH RAM**

4. **Podejście całościowe**

43. EIOD w pełni popiera całościowe podejście do ochrony danych, które stanowi nie tylko tytuł, lecz również punkt wyjścia komunikatu, a także obejmuje rozszerzenie ogólnych zasad ochrony danych o współpracę policyjną i sądową w sprawach karnych ([23]).

44. EIOD pragnie również zwrócić uwagę na to, że Komisja nie zamierza objąć wszystkich działań związanych z przetwarzaniem danych zakresem ogólnego narzędzia prawnego. Pominięte zostanie zwłaszcza przetwarzanie danych przez instytucje, organy, urzędy i agencje Unii. Komisja oświadczyła jedynie, że „podda ocenie potrzebę dostosowania innych narzędzi prawnych do nowych ogólnych ram ochrony danych".

45. EIOD pragnąłby oczywiście, by przetwarzanie danych na szczeblu UE objęte zostało ogólnymi ramami prawnymi. EIOD przypomina, że było to pierwotną intencją dawnego art. 286 WE, który po raz pierwszy poruszał kwestię ochrony danych na szczeblu traktatu. Art. 286 WE stanowił, że narzędzia prawne w zakresie przetwarzania danych osobowych mają także zastosowanie do instytucji. Co istotniejsze, jeden tekst prawny pozwala uniknąć ryzyka rozbieżności pomiędzy zapisami, byłby też najlepszy z punktu widzenia wymiany danych pomiędzy podmiotami na szczeblu UE oraz podmiotami publicznymi i prywatnymi w państwach członkowskich. Pozwalałby on również na uniknięcie ryzyka, że po wprowadzeniu modyfikacji do dyrektywy 95/46/WE nie byłoby już politycznego zainteresowania zmianą rozporządzenia (WE) nr 45/2001 czy też nadaniem tej modyfikacji wystarczającego priorytetu celem uniknięcia rozbieżności, co do dat wejścia w życie.

46. EIOD wzywa Komisję – jeżeli stwierdzi ona, że włączenie przetwarzania danych na szczeblu UE do ogólnego narzędzia prawnego nie jest możliwe – aby zobowiązała się do zaproponowania sposobu adaptacji rozporządzenia (WE) nr 45/2001 (a nie do „ocenienia potrzeby") w jak najkrótszym czasie, najlepiej do końca 2011 r.

47. Równie ważne jest, aby Komisja zagwarantowała, że inne obszary nie pozostaną w tyle, zwłaszcza:

— ochrona danych w ramach wspólnej polityki zagranicznej i bezpieczeństwa na mocy art. 39 TFUE ([24]),

— systemy ochrony danych właściwe dla konkretnych sektorów funkcjonujące w ramach takich organów UE, jak Europol, Eurojust i wielkoskalowe systemy informatyczne w zakresie, w jakim należy je dostosować do nowego narzędzia prawnego,

— dyrektywa 2002/58/WE o prywatności i łączności elektronicznej w zakresie, w jakim należy ją dostosować do nowego narzędzia prawnego.

48. Ogólne narzędzie prawne ochrony danych może, i prawdopodobnie musi, zostać uzupełnione dodatkowymi przepisami sektorowymi i szczególnymi, na przykład w dziedzinie współpracy policyjnej i sądowej, lecz również w innych obszarach ([25]). Gdy jest to potrzebne i zgodne z zasadą pomocniczości, dodatkowe przepisy powinny zostać przyjęte na szczeblu UE. W uzasadnionych przypadkach państwa członkowskie powinny ustanowić dodatkowe zasady w obszarach szczególnych (zob. punkt 5.2).

([23]) Zob. s. 14 komunikatu i sekcja 3.2.5 niniejszej opinii.

([24]) Zob. także: opinia Europejskiego Inspektora Ochrony Danych z dnia 24 listopada 2010 r. w sprawie Komunikatu Komisji do Parlamentu Europejskiego i Rady – „Unijna polityka przeciwdziałania terroryzmowi: najważniejsze osiągnięcia i nadchodzące wyzwania", punkt 31.

([25]) Zob. także dokument grupy roboczej dotyczący „Przyszłości prywatności" (przypis 7), punkty 18–21.

5. **Dalsza harmonizacja i uproszczenie**

5.1. *Potrzeba harmonizacji*

49. Harmonizacja ma kapitalne znaczenie dla unijnych przepisów ochrony danych. W komunikacie słusznie podkreśla się, że ochrona danych ma silny wpływ na rynek wewnętrzny, gdyż musi gwarantować swobodny przepływ danych osobowych pomiędzy państwami członkowskimi w ramach tego rynku. Poziom harmonizacji w czasie obowiązywania obecnej dyrektywy oceniono jednak jako niewystarczający. Jego autorzy uznali, że jest to jedna z głównych obaw zainteresowanych stron. Zainteresowane strony podkreślają zwłaszcza potrzebę poprawy pewności prawa, ograniczenia obciążenia administracyjnego i zagwarantowania równego traktowania podmiotów gospodarczych. Jak słusznie zauważyła Komisja, jest to szczególnie ważne w przypadku administratorów danych ustanowionych w kilku państwach członkowskich, którzy mają obowiązek stosowania się do wymogów krajowych przepisów ochrony danych (które mogą być rozbieżne) ([26]).

50. Harmonizacja jest ważna nie tylko z punktu widzenia rynku wewnętrznego, lecz również gwarantowania adekwatnego poziomu ochrony danych. Art. 16 TFUE stanowi, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących. Aby prawo to było skutecznie przestrzegane, w całej UE należy zagwarantować odpowiedni poziom ochrony danych. W dokumencie grupy roboczej dotyczącym „Przyszłości prywatności" podkreśla się, że kilka przepisów związanych z pozycją osób, których dotyczą dane, nie zostało jednolicie implementowanych lub zinterpretowanych we wszystkich państwach członkowskich ([27]). W zglobalizowanym i połączonym świecie rozbieżności te mogą podkopać lub ograniczyć ochronę obywateli.

51. EIOD uważa, że dalsza i lepsza harmonizacja stanowi jeden z głównych celów procesu przeglądu. EIOD z zadowoleniem przyjmuje zobowiązanie Komisji do przeanalizowania środków do osiągnięcia dalszej harmonizacji ochrony danych na szczeblu UE, jest jednak zaskoczony, iż komunikat nie zawiera obecnie żadnych konkretnych propozycji. EIOD pragnąłby więc sam wskazać kilka obszarów, gdzie potrzeba konwergencji jest najpilniejsza (zob. punkt 5.3). Dalsza harmonizacja w tych obszarach powinna zostać osiągnięta nie tylko poprzez ograniczenie pola manewru prawa krajowego, lecz również w drodze zapobiegania nieprawidłowej implementacji przez państwa członkowskie (zob. też rozdział 11) i gwarantowania bardziej spójnej i skoordynowanego egzekwowania prawa (zob. także rozdział 10).

([26]) Komunikat, s. 10.

([27]) Zob. dokument grupy roboczej dotyczący „Przyszłości prywatności" (przypis 7), punkt 70. Dokument dotyczy zwłaszcza przepisów w zakresie odpowiedzialności i możliwości dochodzenia zadośćuczynienia z tytułu szkód niematerialnych.

5.2. *Ograniczanie pola manewru w zakresie implementacji dyrektywy*

52. Dyrektywa zawiera wiele postanowień, które są tak ogólnie sformułowane, że pozostawiają szerokie pole manewru dla rozbieżnej implementacji. Motyw 9 dyrektywy potwierdza wyraźnie, że państwa członkowskie mają pewne pole manewru oraz że z tego powodu powstawać mogą rozbieżności w zakresie jej implementacji. Kilka postanowień zostało rozbieżnie zaimplementowanych przez państwa członkowskie, nawet niektóre postanowienia kluczowe ([28]). Sytuacja ta nie powinna mieć miejsca, należy więc starać się osiągnąć wyższy stopień konwergencji.

53. Nie oznacza to jednak, że z założenia należy wykluczyć różnorodność. W niektórych dziedzinach elastyczność może być potrzebna, aby zachować uzasadnioną specyfikę istotnych interesów publicznych lub instytucjonalną autonomię państwa członkowskiego. Według EIOD możliwości potencjalnych rozbieżności pomiędzy państwami członkowskimi należy ograniczyć zwłaszcza do następujących sytuacji szczególnych:

— wolność wypowiedzi: w obecnych ramach (art. 9) państwa członkowskie mogą wprowadzać zwolnienia i derogacje w zakresie przetwarzania danych w celach dziennikarskich lub w celu uzyskania wyrazu artystycznego lub literackiego. Tego typu elastyczność wydaje się na miejscu, oczywiście jeżeli podlega ograniczeniom zawartym w Karcie i EKPC, oraz przy założeniu, że pomiędzy państwami członkowskimi istnieją różnice tradycji i kulturowe. Nie powinno to jednak stawać na drodze potencjalnego uaktualnienia obecnego brzmienia art. 9 w świetle zmian, jakie pociąga za sobą Internet,

— szczególny interes publiczny: w obecnych ramach (art. 13) państwo członkowskie może przyjąć środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków, kiedy ograniczenie takie stanowi środek konieczny dla zabezpieczenia ważnego interesu publicznego, takiego jak bezpieczeństwo narodowe, obronność, bezpieczeństwo publiczne itp. Tego typu kompetencje państw członkowskich są uzasadnione, lecz gdy to możliwe, należałoby bardziej zharmonizować interpretację wyjątków (zob. punkt 9.1). Obecny zakres wyjątków od art. 6 ust. 1 wydaje się ponadto zbyt szeroki,

— środki odwoławcze, sankcje i procedury administracyjne: europejskie ramy powinny definiować główne warunki, lecz w obecnym stanie prawa UE określanie sankcji, środków odwoławczych, reguł proceduralnych i warunków inspekcji obowiązujących na szczeblu krajowym musi pozostać w gestii państw członkowskich.

([28]) Istnieją również rozbieżne podejścia, co do danych wprowadzanych ręcznie.

5.3. *Obszary dalszej harmonizacji*

54. *Definicje* (art. 2 dyrektywy 95/46/WE). Definicje stanowią kamień węgielny systemu prawnego, w związku z czym powinny być interpretowane tak samo we wszystkich państwach członkowskich, bez pola manewru w zakresie implementacji. W obecnych ramach istnieje wiele rozbieżności, na przykład co do pojęcia administratora danych ([29]). EIOD sugeruje dodanie kolejnych pozycji do obecnej listy zawartej w art. 2 celem uzyskania większej pewności prawa, takich jak np. dane anonimowe, dane pseudoanonimowe, dane sądowe, przekazywanie danych i inspektor ochrony danych.

55. *Legalność przetwarzania danych osobowych* (art. 5). Nowe narzędzie prawne powinno być jak najbardziej precyzyjne w zakresie kluczowych elementów decydujących o legalności przetwarzania danych. Art. 5 dyrektywy (a także motyw 9), który upoważnia państwa członkowskie do bardziej precyzyjnego definiowania warunków legalności przetwarzania danych, może nie być już potrzebny w przyszłych ramach.

56. *Podstawy przetwarzania danych* (art. 7 i 8). Definicja warunków przetwarzania danych stanowi kluczowy element wszelkich przepisów prawa dotyczących ochrony danych. Państwa członkowskie nie powinny mieć możliwości wprowadzania dodatkowych czy zmodyfikowanych podstaw przetwarzania danych, ani też wykluczania ich. Należałoby znieść lub ograniczyć możliwość wprowadzania derogacji (zwłaszcza w przypadku danych wrażliwych ([30])). W ramach nowego narzędzia prawnego należy jasno określić podstawy przetwarzania danych, dzięki czemu ograniczony zostanie margines uznaniowości we wdrażaniu czy egzekwowaniu przepisów. Doprecyzowania wymaga zwłaszcza pojęcie zgody (zob. punkt 6.5). Ponadto podstawa opierająca się na uzasadnionym interesie administratora danych (art. 7 lit. f) umożliwia rozbieżne interpretacje z uwagi na jej elastyczność. Kwestia ta wymaga doprecyzowania. Innym postanowieniem, które powinno zostać doprecyzowane, jest art. 8 ust. 2 lit. b, które zezwala na przetwarzanie danych wrażliwych, gdy jest to konieczne do wypełniania obowiązków i szczególnych uprawnień administratora danych w dziedzinie prawa pracy ([31]).

57. *Prawa osoby, której dane dotyczą* (art. 10–15). Jest to jeden z obszarów, w którym nie wszystkie elementy dyrektywy zostały spójnie wdrożone i zinterpretowane przez państwa członkowskie. Prawa osoby, której dane dotyczą, stanowią centralny element skutecznej ochrony danych, dlatego też należy znacznie ograniczyć pole manewru w tej dziedzinie. EIOD zaleca, aby informacje udostępniane osobom, których dane dotyczą, przez administratora danych były w całej UE takie same.

58. *Międzynarodowe przekazywanie danych osobowych* (art. 25–26). Jest to obszar, który był bardzo często krytykowany z powodu braku jednolitej praktyki w całej UE. Zainteresowane strony negatywnie odnoszą się do faktu, że decyzje Komisji dotyczące adekwatności są rozbieżnie interpretowane i wdrażane przez państwa członkowskie. Wiążące Reguły Korporacyjne (BCR) to kolejny obszar, w którym EIOD zaleca dalszą harmonizację (zob. rozdział 9).

59. *Krajowe organy ochrony danych* (art. 28). Krajowe organy ochrony danych podlegają w 27 państwach członkowskich bardzo rozbieżnym regułom, zwłaszcza w zakresie statusu, zasobów i uprawnień. Rozbieżności te powstały częściowo z winy art. 28, któremu brak precyzji ([32]). Powinien on zostać doprecyzowany zgodnie z wyrokiem Europejskiego Trybunału Sprawiedliwości w sprawie C-518/07 ([33]) (zob. także rozdział 10).

5.4. *Uproszczenie systemu zawiadamiania*

60. Wymogi w zakresie zawiadamiania (art. 18–21 dyrektywy 95/46/WE) to kolejna dziedzina, w której państwa członkowskie cieszą się znaczną dowolnością. W komunikacie słusznie stwierdzono, że zharmonizowany system pozwoliłby ograniczyć koszty działalności, jak i obciążenie administracyjne administratorów danych ([34]).

61. Jest to obszar, w którym uproszczenie powinno być najważniejszym z celów. Przegląd ram ochrony danych stanowi unikalną okazję do dalszego uproszczenia lub ograniczenia zakresu obowiązujących obecnie wymogów zawiadamiania. W komunikacie stwierdzono, że istnieje pomiędzy zainteresowanymi stronami zgoda, co do faktu, iż obecnie obowiązujący system zawiadamiania jest kłopotliwy i sam w sobie nie kreuje wartości dodanej w zakresie ochrony danych osobowych osób fizycznych ([35]). EIOD z zadowoleniem przyjmuje więc zobowiązanie Komisji do przyjrzenia się różnym możliwościom uproszczenia obecnie obowiązującego systemu zawiadamiania.

62. Jego zdaniem punktem wyjścia uproszczenia powinno być przejście od systemu, w którym zawiadamianie jest zasadą, chyba że stanowi się inaczej (tj. „system zwolnień"), do systemu lepiej ukierunkowanego. System zwolnień okazał się nieskuteczny, gdyż poszczególne państwa członkowskie wdrożyły go w rozbieżny sposób ([36]). EIOD sugeruje rozważenie następujących alternatyw:

([29]) Zob. grupa robocza art. 29: Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający" (WP 169).

([30]) Obecnie na mocy art. 8 ust. 4 i ust. 5 państwa członkowskie mogą w pewnych warunkach ustalić dodatkowe wyłączenia w zakresie danych wrażliwych.

([31]) Zob. Pierwsze sprawozdanie Komisji z implementacji dyrektywy o ochronie danych, op. cit., s. 14.

([32]) Dokument grupy roboczej dotyczący „Przyszłości prywatności", punkt 87.

([33]) Sprawa C-518/07, *Komisja przeciwko Republice Federalnej Niemiec*, nieopublikowana w Zb. Orz.

([34]) Porównaj: przypis 26.

([35]) Porównaj: przypis 26.

([36]) Sprawozdanie grupy roboczej art. 29 dotyczące obowiązku zawiadamiania krajowych organów nadzoru, najlepszego wykorzystania wyjątków i uproszczeń oraz roli inspektorów ochrony danych w Unii Europejskiej, WP 106, 2005, s. 7.

— ograniczenia obowiązku zawiadamiania o szczególnych rodzajach operacji przetwarzania wiążących się z określonym ryzykiem (zawiadomienia te mogłyby wpływać na podjęcie dalszych kroków, takich jak wcześniejsze sprawdzenie przetwarzania),

— prosty obowiązek rejestracji dotyczący administratorów danych (w przeciwieństwie do szerokiego zakresu rejestracji wszystkich operacji przetwarzania danych).

Ponadto można by wprowadzić standardowy ogólnoeuropejski formularz zawiadamiania, aby zagwarantować zharmonizowane podejście do potrzebnych informacji.

63. Przegląd obecnie obowiązującego systemu zawiadamiania powinien zostać przeprowadzony bez uszczerbku dla poprawy jakości obowiązków w zakresie uprzedniego sprawdzania wobec niektórych obowiązków związanych z przetwarzaniem danych, które mogłyby wiązać się z określonym ryzykiem (takich jak np. wielkoskalowe systemy informatyczne). EIOD popiera włączenie do nowego narzędzia prawnego otwartej listy przypadków, gdy uprzedniego sprawdzanie jest wymagane. Przydatnym wzorem mogłoby okazać się tu rozporządzenie (WE) nr 45/2001 o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe ([37]).

5.5. *Rozporządzenie, nie dyrektywa*

64. EIOD stoi na stanowisku, że proces przeglądu jest również okazją do ponownego zastanowienia się nad rodzajem narzędzia prawnego ochrony danych. Rozporządzenie, jednolite narzędzie mające bezpośrednie zastosowanie w państwach członkowskich, stanowi najskuteczniejszy środek ochrony prawa podstawowego do ochrony danych, a także stworzenia prawdziwego rynku wewnętrznego, w ramach którego dane osobowe mogłyby się swobodnie przemieszczać i gdzie poziom ochrony jest taki sam, bez względu na kraj czy sektor, w którym przetwarzane są dane.

65. Dzięki rozporządzeniu można by ograniczyć możliwości sprzecznej interpretacji i nieuzasadnionych różnic w zakresie wdrażania i stosowania prawa. Pomogłoby to również ograniczyć istotność zdefiniowania przepisów mających zastosowanie do operacji przetwarzania w ramach UE, co stanowi najbardziej kontrowersyjny aspekt obecnego systemu (zob. rozdział 9).

66. Wydanie rozporządzenia w dziedzinie ochrony danych jest tym bardziej uzasadnione, gdyż:

— art. 16 TFUE rozszerza prawo do ochrony danych osobowych do poziomu zawartego w traktacie i przewiduje – czy też wprowadza – jednorodny poziom ochrony jednostek w całej UE,

— przetwarzanie danych odbywa się w środowisku elektronicznym, gdzie granice wewnętrzne pomiędzy państwami członkowskimi straciły na istotności.

67. Wybór rozporządzenia jako narzędzia ogólnego pozwala na wprowadzenie, gdy jest to konieczne, postanowień skierowanych bezpośrednio do państw członkowskich tam, gdzie wymagana jest elastyczność, nie wpływa on natomiast na ich kompetencje w zakresie wprowadzania – w razie potrzeby – dodatkowych zasad ochrony danych, zgodnych w prawem UE.

6. **Wzmocnienie praw osób fizycznych**

6.1. *Potrzeba wzmocnienia praw*

68. EIOD w pełni popiera zapisy komunikatu, które proponują wzmocnienie praw osób fizycznych, gdyż obecnie obowiązujące narzędzia prawne nie gwarantują skutecznej ochrony wymaganej w coraz bardziej złożonym, zdigitalizowanym świecie.

69. Z jednej strony, rozwój zdigitalizowanego świata pociąga za sobą znaczny wzrost w zakresie gromadzenia, wykorzystywania i dalszego przekazywania danych osobowych w bardzo złożony i nieprzejrzysty sposób. Zazwyczaj nie wiemy albo nie rozumiemy jak to się odbywa, kto gromadzi nasze dane ani jak ten proces kontrolować. Przykładem tego zjawiska może być monitorowanie przez dostawców reklam stron przeglądanych przez danego użytkownika (pliki typu cookie lub podobne) dla celów reklamy ukierunkowanej. Gdy internauci odwiedzają strony internetowe, nie spodziewają się raczej, że niewidoczna dla nich osoba trzecia notuje te wizyty i zbiera dane o użytkownikach, które zawierają informacje na temat ich stylu życia czy preferencji.

70. Z drugiej strony, rozwój umożliwia nam aktywne dzielenie się informacjami natury osobistej, na przykład na portalach społecznościowych. Młodzi ludzie w coraz większym stopniu angażują się w działalność portali społecznościowych, gdzie mają możliwość kontaktu ze znajomymi. Nie mają oni raczej świadomości, jak wiele informacji o sobie ujawniają, nie zdają sobie też sprawy z długofalowych konsekwencji swoich działań.

6.2. *Poprawa przejrzystości*

71. Przejrzystość ma kapitalne znaczenie w każdym systemie ochrony danych, nie tylko ze względu na tkwiącą w jej istocie wartość, lecz także dlatego, iż umożliwia realizację innych zasad ochrony danych. Osoby fizyczne będą mogły korzystać ze swoich praw jedynie wówczas, gdy posiądą wiedzę o przetwarzaniu danych.

72. Przejrzystości dotyczy kilka zapisów dyrektywy 95/46/WE. Zgodnie z art. 10 i 11 podmioty gromadzące dane zobowiązane są poinformować o tym fakcie osoby, których dane dotyczą. Art. 12 mówi również o prawie do otrzymania kopii własnych danych wyrażonych w zrozumiałej formie (prawo dostępu). Art. 15 uznaje prawo dostępu do logiki, według której podejmowane są zautomatyzowane decyzje wywołujące skutki prawne. Art. 6 ust. 1 lit. a) wymaga, aby przetwarzane było rzetelne i przejrzyste. Dane osobowe nie mogą być przetwarzane w sposób nieujawniony ani ukryty.

([37]) Zob. art. 27 rozporządzenia, (Dz.U. L 8 z 12.1.2001, s. 1).

73. W komunikacie sugeruje się, aby dodać ogólną zasadę przejrzystości. W związku z tą propozycją EIOD pragnie podkreślić, że pojęcie przejrzystości stanowi już nieodłączną część obecnie obowiązujących ram prawnych ochrony danych, choć w sposób dorozumiany. Jak wspomniano w poprzednim paragrafie, można to wywnioskować z rozmaitych zapisów dotyczących przejrzystości. Według EIOD wartość dodaną można by wygenerować dodając *jasno sprecyzowaną* zasadę przejrzystości, która mogłaby być powiązana z istniejącym zapisem dotyczącym rzetelnego przetwarzania danych. Wpłynęłoby to na poprawę pewności prawa i potwierdziło, że administrator danych powinien w każdych okolicznościach przetwarzać dane osobowe w sposób przejrzysty, nie tylko na wyraźną prośbę czy wtedy, gdy zobowiązuje go do tego szczególny przepis prawa.

74. Jednak jeszcze ważniejsze jest, by wzmacniać istniejące przepisy dotyczące przejrzystości, takie jak obowiązujący art. 10 i 11 dyrektywy 95/46/WE. Ich zapisy określają zakres informacji, jakie muszą zostać udzielone, lecz nie precyzują procedur. EIOD konkretniej sugeruje, aby wzmocnić obecnie obowiązujące przepisy w drodze:

— wymogu dla administratorów danych, aby udostępniali informacje dotyczące przetwarzania danych w sposób łatwo dostępny i zrozumiały, sformułowane przejrzystym i prostym językiem ([38]). Informacje powinny być jasne, wyraźne i łatwo dostępne. Przepis ten mógłby również obejmować obowiązek zagwarantowania łatwego zrozumienia informacji. Dzięki niemu nieprzejrzysta lub niezrozumiała polityka prywatności stawałby się niezgodna z prawem,

— wymogu, aby informacje przekazywane były osobom, których dane dotyczą, w sposób łatwy i bezpośredni. Informacje powinny być również dostępne zawsze, a nie znikać z medium elektronicznego po krótkim czasie. Pozwoliłoby to użytkownikom na przechowywanie i odtwarzanie informacji w przyszłości, umożliwiając dalszy dostęp.

6.3. *Poparcie dla obowiązku zgłaszania przypadków naruszenia bezpieczeństwa*

75. EIOD popiera wprowadzenie zapisu dotyczącego zawiadamiania o naruszeniu przepisów dotyczących danych osobowych do ogólnego narzędzia prawnego, który rozszerzałby obowiązek niektórych dostawców, o którym mowa w zrewidowanej dyrektywie o prywatności i łączności elektronicznej, o wszystkich administratorów danych, jak zaproponowano w komunikacie. W myśl zrewidowanej dyrektywie o prywatności i łączności elektronicznej obowiązek ten stosuje się wyłącznie do dostawców usług komunikacji elektronicznej (dostawców usług telefonicznych (łącznie z VoIP) i internetu). Innych administratorów danych obowiązek ten nie obejmuje. Powody uzasadniające ten obowiązek mają pełne zastosowanie do kontrolerów danych innych niż dostawcy usług komunikacji elektronicznej.

76. Zawiadamianie o naruszeniu bezpieczeństwa służy zgoła inny celom. Najbardziej oczywistym z nich, podkreślonym przez Komisję, jest fakt, że służy to jako narzędzie informowania obywateli celem uświadomienia im ryzyka, na jakie są narażeni, gdy naruszone zostanie bezpieczeństwo ich danych osobowych. Może to pomóc im podjąć niezbędne kroki w celu ograniczenia tego typu ryzyka. Gdy osoba fizyczna otrzyma zawiadomienie o naruszeniu bezpieczeństwa jej danych, może m.in. zmienić hasła lub usunąć swoje konto. Ponadto zawiadomienia o naruszeniu bezpieczeństwa przyczyniają się do skutecznego stosowania innych zasad i obowiązków zawartych w dyrektywie. Wymogi, co do zawiadamiania o naruszeniu bezpieczeństwa zachęcają na przykład administratorów danych do wprowadzania bardziej rygorystycznych zabezpieczeń. Naruszenie bezpieczeństwa jest również narzędziem służącym wzmocnieniu odpowiedzialności administratorów danych, a zwłaszcza poprawie rozliczalności (zob. rozdział 7). Służy ono również jako narzędzie egzekucji prawa przez organy ochrony danych. Powiadomienie tego typu organu o naruszeniu bezpieczeństwa może doprowadzić do wszczęcia dochodzenia w sprawie działalności administratora danych.

77. Szczegółowe zasady dotyczące naruszania bezpieczeństwa zawarte w poprawionej dyrektywie o prywatności i łączności elektronicznej zostały szeroko omówione podczas parlamentarnego etapu tworzenia ram prawnych poprzedzających przyjęcie dyrektywy. W ramach debaty uwzględniono opinię grupy roboczej art. 29 i EIOD, a także poglądy zainteresowanych stron. Wprowadzone zasady stanowią odzwierciedlenie poglądów rozmaitych interesariuszy. Stanowią one próbę zrównoważenia interesów – kryteria skutkujące obowiązkiem zawiadamiania są w zasadzie wystarczające do ochrony osób fizycznych, lecz nie nakładają zbyt kłopotliwych ani nieprzydatnych wymogów.

6.4. *Wzmocnienie zgody*

78. W art. 7 dyrektywy o ochronie danych wymieniono 6 podstaw prawnych przetwarzania danych osobowych. Jedną z nich jest zgoda danej osoby. Administrator danych może przetwarzać dane osobowe w zakresie, w jakim osoba fizyczna wyraziła świadomą zgodę na gromadzenie i dalsze przetwarzanie jej danych.

79. W praktyce użytkownicy mają często ograniczoną kontrolę nad swoimi danymi, zwłaszcza w środowiskach technologicznych. Czasami wykorzystywana jest metoda zgody dorozumianej, czyli domniemanej. Może być ona domniemana na podstawie działań danej osoby (np. działań polegających na korzystaniu ze strony internetowej, co uznawane jest za wyrażenie zgody na zapisywanie danych użytkownika dla celów marketingowych).

([38]) Zob. Komunikat, s. 6.

Zgodę można wywnioskować również z milczenia lub zaniechania (brak odznaczenia zaznaczonego pola uznaje się za wyrażenie zgody).

80. Zgodnie z dyrektywą zgoda jest ważna, jeżeli jest konkretna, świadoma i dobrowolna. Musi być to świadome wskazanie przez osobę, której dane dotyczą na to, że wyraża przyzwolenie na przetwarzanie odnoszących się do niej danych osobowych. Sposób wyrażenia zgody musi być jednoznaczny.

81. Zgoda domniemana na postawie działania, a zwłaszcza zgoda poprzez milczenie lub brak działania nie stanowi jednoznacznej zgody. Nie zawsze jednak jasne jest, co stanowi prawdziwą, jednoznaczną zgodę. Niektórzy administratorzy danych wykorzystują tę niejasność stosując metody nieodpowiednie do otrzymania prawdziwej, jednoznacznej zgody.

82. W świetle powyższego EIOD popiera zdanie Komisji, co do potrzeby lepszego objaśnienia granic zgody i zagwarantowania, że jako zgoda traktowana jest jedynie zgoda interpretowana w sposób solidny. W tym kontekście EIOD sugeruje co następuje ([39]):

— należy rozważyć rozszerzenie katalogu sytuacji, w których wymagana jest wyraźna zgoda, a który obecnie ogranicza się do danych wrażliwych,

— należy wprowadzić dodatkowe zasady wyrażania zgody w środowisku on-line,

— należy przyjąć dodatkowe zasady wyrażania zgody na przetwarzanie danych dla celów drugorzędnych (tj. gdy przetwarzanie jest procesem drugorzędnym w stosunku do procesu głównego lub nie jest procesem oczywistym),

— w ramach dodatkowego narzędzia prawnego, które może zostać przyjęte przez Komisję na mocy art. 290 TFUE, należy określić rodzaj wymaganej zgody, na przykład szczebel zgody na przetwarzanie danych z chipów RFID na produktach konsumpcyjnych lub na inne konkretne techniki.

6.5. *Przenoszalność danych i prawo do bycia zapomnianym*

83. Przenoszalność danych i prawo do bycia zapomnianym to dwa związane ze sobą pojęcia zawarte w komunikacie celem wzmocnienia praw osób, których dane dotyczą. Są one uzupełnieniem wobec zasad wspomnianych już w dyrektywie. Gwarantują prawo osoby, której dane dotyczą, do odmowy dalszego przetwarzania jej danych osobowych, a także obowiązek usunięcia informacji niepotrzebnych już z punktu widzenia przetwarzania spoczywający na administratorze danych.

84. Te dwa nowe pojęcia tworzą wartość dodaną głównie w kontekście społeczeństwa informacyjnego, gdzie coraz więcej danych gromadzonych jest automatycznie i przechowywanych przez nieograniczony czas. Praktyka pokazuje, że nawet, jeśli dane udostępniła sama osoba, której one dotyczą, stopień skutecznej kontroli nad nimi jest bardzo ograniczony. Jest to zwłaszcza prawdziwe w obliczu gigantycznej pamięci, jaką stał się obecnie internet. Poza tym z ekonomicznego punktu widzenia dla administratora danych bardziej kosztowne jest usuwanie danych niż ich przechowywanie. Korzystanie z praw jednostki sprzeciwia się więc naturalnej tendencji ekonomicznej.

85. Zarówno przenoszalność danych jak i prawo do bycia zapomnianym mogłyby wpłynąć na zmianę równowagi na korzyść osób, których dane dotyczą. Celem przenoszalności danych byłoby osiągnięcie większej kontroli podmiotu danych nad dotyczącymi go informacjami, natomiast prawo do bycia zapomnianym gwarantowałoby, że informacje automatycznie znikałyby po upływie pewnego czasu jeżeli osoba, której dane dotyczą, nie podjęłaby działania lub nie była świadoma faktu, że dane są przechowywane.

86. Przenoszalność danych rozumiana jest jako zdolność użytkowników do zmiany preferencji co do przetwarzania ich danych, zwłaszcza w związku z usługami w zakresie nowych technologii. Coraz częściej ma to zastosowanie do usług, które wiążą się z przechowywaniem informacji, także danych osobowych, takich jak telefonia komórkowa, usługi przechowywania zdjęć, e-maili czy innych informacji, często z wykorzystaniem usług przetwarzania w chmurze.

87. Osoby fizyczne muszą mieć możliwość łatwej i swobodnej zmiany dostawcy i przeniesienia danych osobowych do innego usługodawcy. EIOD stoi na stanowisku, że istniejące prawa zawarte w dyrektywie 95/46/WE Można by wzmocnić poprzez dodanie zapisu oprawie do przenoszalności, zwłaszcza w kontekście usług na rzecz społeczeństwa informacyjnego, aby pomóc zagwarantować, że usługodawcy i inni administratorzy zapewnią im dostęp do danych osobowych, a jednocześnie zagwarantują, że wcześniejsi dostawcy lub inni administratorzy usuną te dane, nawet jeśli pragnęliby je zatrzymać dla własnych, uzasadnionych celów.

88. Nowo skodyfikowane „prawo do bycia zapomnianym" zagwarantowałoby usuwanie danych osobowych lub zakaz ich wykorzystywania bez potrzeby działania ze strony danej osoby, lecz pod warunkiem, że dane przechowywane były przez pewien określony czas. Innymi słowy, dane otrzymałyby coś na podobieństwo daty przydatności. Zasada ta została już ugruntowana w ramach orzecznictwa sądów krajowych i jest stosowana

([39]) Grupa robocza art. 29 pracuje obecnie nad opinią dotyczącą „zgody". Opracowanie jej może skutkować powstaniem dodatkowych sugestii.

w niektórych sektorach, na przykład w aktach policyjnych, rejestrach przestępców czy dokumentacji dotyczącej postępowań dyscyplinarnych – w niektórych prawodawstwach krajowych informacje o osobach fizycznych są automatycznie usuwane lub zaprzestaje się korzystania z nich i udostępniania ich, zwłaszcza po upływie określonego czasu, bez potrzeby wcześniejszej analizy każdego z przypadków.

89. W tym sensie nowe „prawo do bycia zapomnianym" powinno wiązać się z przenoszalnością danych. Wytworzona przez nie wartość dodana polegałaby na tym, że osoba, której dane dotyczą, nie musiałaby dokładać starań ani naciskać, aby jej dane zostały usunięte, gdyż proces ten odbywałby się w sposób obiektywny i zautomatyzowany. Administrator danych byłby uprawniony do zachowania danych jedynie w szczególnych okolicznościach, gdy stwierdzono by specjalną potrzebę dłuższego ich przechowywania. „Prawo do bycia zapomnianym" przeniosłoby ciężar dowodu z osoby, której dane dotyczą, na administratora danych i stworzyłoby dla przetwarzania danych osobowych otoczenie „uwzględniania ochrony prywatności w fazie projektowania".

90. EIOD uważa, iż prawo do bycia zapomnianym mogłoby okazać się szczególnie przydatne w ramach usług na rzecz społeczeństwa informacyjnego. Obowiązek usunięcia lub nieudostępniania informacji po upływie pewnego określonego czasu ma sens zwłaszcza w mediach czy internecie, a najbardziej w kontekście portali społecznościowych. Byłby on również przydatny w przypadku sprzętowych terminali danych – dane zapisane na urządzeniach lub komputerach przenośnych byłyby automatycznie usuwane lub blokowane po upływie określonego czasu, gdy nie znajdowałyby się już w posiadaniu danej osoby. W tym sensie prawo do bycia zapominanym przekłada się na obowiązek „uwzględniania ochrony prywatności w fazie projektowania".

91. Podsumowując EIOD uważa, że zarówno przenoszalność danych jak i prawo do bycia zapomnianym to przydatne pojęcia. Warto byłoby włączyć je do wspomnianego narzędzia prawnego, lecz ograniczając jedynie do środowiska elektronicznego.

6.6. *Przetwarzanie danych osobowych dzieci*

92. Dyrektywa 95/46/WE nie zawiera zapisów odnoszących się bezpośrednio do przetwarzania danych osobowych dzieci. Nie uznaje ona potrzeby szczególnej ochrony dzieci w specyficznych okolicznościach z uwagi na ich bezbronność, tworzy również pewną niejasność prawną, zwłaszcza w następujących kwestiach:

— gromadzenie danych osobowych dzieci i sposób, w jaki należy je o tym fakcie informować,

— sposób uzyskiwania zgody dzieci. Jako że nie istnieją konkretne zasady uzyskiwania zgody dzieci ani nie ustalono wieku, poniżej którego jest się dzieckiem, kwestie te reguluje prawo krajowe, które jest różne w poszczególnych państwach członkowskich ([40]),

— tryb i warunki, na których dzieci lub ich przedstawiciele prawni mogliby korzystać z praw zawartych w dyrektywie.

93. EIOD uważa, że szczególny interes dzieci byłby lepiej chroniony, gdyby nowe narzędzie prawne zawierało dodatkowe zapisy dotyczące konkretnie zbierania i dalszego przetwarzania danych dzieci. Gwarantowałyby one pewność prawa w tej konkretnej dziedzinie i działałyby na korzyść administratorów danych, którzy są obecnie związani rozmaitymi wymogami prawnymi.

94. EIOD sugeruje włączenie do wspomnianego narzędzia prawnego następujących zapisów:

— wymóg dostosowania informacji do poziomu zrozumienia dzieci, aby umożliwić im zrozumienie faktu gromadzenia ich danych osobowych,

— inne wymogi co do informacji dostosowane do poziomu dzieci dotyczące sposobu w jaki należy dostarczać informacje oraz być może również ich treści,

— szczególny zapis chroniący dzieci przed reklamą behawioralną,

— zasada celowości powinna zostać wzmocniona w zakresie danych dzieci,

— niektórych kategorii danych nie powinno się zbierać od dzieci,

— ograniczenie wiekowe – poniżej pewnego wieku informacje od dzieci można zbierać jedynie za wyraźną zgodą rodziców, którą można zweryfikować,

— jeżeli potrzebna jest zgoda rodziców, należałoby ustanowić zasady weryfikacji wieku dziecka – innymi słowy sprawdzania, czy dziecko jest małoletnie i czy

([40]) Zgoda jest zazwyczaj powiązana z wiekiem, w jakim dzieci mogą nawiązywać stosunki umowne. Jest to wiek, gdy dzieci osiągają pewien poziom dojrzałości. Na przykład w Hiszpanii prawo wymaga uzyskania zgody rodziców na gromadzenie danych dzieci, które są młodsze niż 14 lat. Dzieci starsze są w stanie same wyrazić zgodę. W Wielkiej Brytanii ustawa o ochronie danych nie precyzuje konkretnego wieku ani progu, jednak brytyjski urząd ds. ochrony danych stoi na stanowisku, iż zgodę wyrażać mogą dzieci powyżej 12. roku życia. Natomiast dzieci poniżej 12. roku życia nie mogą wyrażać zgody i aby otrzymać ich dane osobowe, należy najpierw uzyskać zgodę rodzica lub opiekuna.

rodzice udzielili zgody. jest to obszar, w którym Unia mogłaby czerpać inspirację z innych krajów, np. ze Stanów Zjednoczonych ([41]).

6.7. *Mechanizmy przyznawania odszkodowań zbiorowych*

95. Wzmocnienie merytoryczne praw jednostki byłoby bezzasadne wskutek braku skutecznych mechanizmów proceduralnych służących ich egzekwowaniu. W tym kontekście EIOD zaleca wprowadzenie mechanizmów przyznawania odszkodowań zbiorowych za naruszenie zasad ochrony prywatności do prawodawstwa UE. Mechanizmy przyznawania odszkodowań zbiorowych, dzięki którym grupy obywateli mogą wspólnie ubiegać się o odszkodowanie w ramach jednego postępowania, mogą stanowić potężne narzędzie ułatwiające egzekwowanie zasad ochrony danych ([42]). Innowację tę popierają także organy ochrony danych w ramach dokumentu grupy roboczej „Przyszłość prywatności".

96. W przypadkach mniejszej wagi mało prawdopodobne jest, aby ofiary naruszenia zasad ochrony danych składały indywidualne pozwy przeciwko administratorom danych z uwagi na koszty, opóźnienia, niepewność wyniku, ryzyko i obciążenie, na jakie byłyby narażone. Trudności te można przezwyciężyć lub znacząco zmniejszyć dzięki wprowadzeniu systemu odszkodowań zbiorowych, który umożliwia ofiarom naruszenia zasad łączenie indywidualnych roszczeń w ramach jednego powództwa. EIOD poparłby również wprowadzenie możliwości wszczynania postępowań odszkodowawczych w imieniu ofiar naruszenia zasad ochrony danych przez kompetentne podmioty, takie jak stowarzyszenia konsumentów czy organy publiczne. Postępowania te prowadzone byłyby bez uszczerbku dla prawa osoby, której dane dotyczą, do wszczęcia postępowania indywidualnego.

97. Powództwa zbiorowe są istotne nie tylko z punktu widzenia zagwarantowania pełnej rekompensaty lub innych działań naprawczych, odgrywają także pośrednio funkcję odstraszającą. Ryzyko wypłacenia wysokiego odszkodowania zbiorowego w ramach tego typu powództwa stanowią doskonała zachętę dla administratorów danych, by zapewniać zgodność w sposób skuteczny. W tym względzie egzekwowanie prawa przez osoby prywatne za pośrednictwem mechanizmów przyznawania odszkodowań zbiorowych stanowiłoby znakomite uzupełnienie egzekwowania prawa przez organy publiczne.

98. W komunikacie nie ma jednak o tej kwestii mowy. EIOD zdaje sobie sprawę, że na szczeblu europejskim toczy się obecnie debata nad wprowadzeniem możliwości przyznawania konsumentom odszkodowań zbiorowych. Jest on również świadom ryzyka ekscesów, jakie mogą mieć miejsce wskutek wprowadzenia tych mechanizmów, co pokazuje doświadczenie innych systemów prawnych. Czynniki te nie stanowią jednak, w jego odczuciu, argumentów wystarczających by odrzucić czy odłożyć w czasie wprowadzenie ich do prawodawstwa w zakresie ochrony danych, a to ze względu na korzyści, jakie mogą potencjalnie przynieść ([43]).

7. **Wzmocnienie roli organizacji/administratorów**

7.1. *Uwagi ogólne*

99. EIOD stoi na stanowisku, że oprócz wzmacniania praw jednostki, nowoczesne narzędzie prawne ochrony danych musi zawierać także niezbędne narzędzie służące zwiększeniu odpowiedzialności administratorów danych. Ramy muszą zawierać zwłaszcza bodźce dla administratorów danych z sektora prywatnego i publicznego, aby aktywnie włączali środki ochrony danych do procesów biznesowych. Narzędzia te byłyby przydatne przede wszystkim dlatego, że – jak już wcześniej wspomniałem – postęp technologiczny skutkuje znacznym wzrostem skali gromadzenia, wykorzystywania i przekazywania danych osobowych, co wzmaga ryzyko w zakresie prywatności i ochrony danych osobowych osób fizycznych, które należy skutecznie kompensować. Po drugie, w obecnych ramach brakuje – za wyjątkiem kilku dobrze zdefiniowanych przepisów (patrz poniżej) – tego typu narzędzi, w związku z czym administratorzy danych mogą prezentować *reaktywne* podejście do ochrony danych i prywatności i podejmować działania dopiero wtedy, gdy zaistnieje konkretny problem. Podejście to znajduje odzwierciedlenie w statystykach, które wskazują na powtarzające się problemy związane z niskiej jakości praktykami w zakresie zgodności i utratą danych.

100. Według EIOD istniejące ramy nie wystarczą, aby skutecznie chronić dane osobowe w obecnych i przyszłych warunkach. Im wyższe ryzyko tym większa potrzeba wdrożenia konkretnych działań celem ochrony informacji na szczeblu praktycznym i zapewnienia skutecznej ochrony. Dopóki nie wprowadzi się w życie aktywnych środków, dopóty zdarzać się będą błędy, niefortunne wypadki i zaniedbania narażające na szwank prywatność osób fizycznych w coraz bardziej zdigitalizowanym świecie. Aby to osiągnąć, EIOD proponuje następujące działania:

7.2. *Wzmocnienie rozliczalności administratorów danych*

101. EIOD zaleca dodanie do narzędzia prawnego nowego zapisu wymagającego, aby administratorzy danych wdrożyli odpowiednie, skuteczne środki służące wprowadzeniu w życie zasad i obowiązków wynikających z narzędzia i mogli ten fakt na życzenie wykazać.

([41]) W Stanach Zjednoczonych COPPA wymaga, aby operatorzy komercyjnych stron internetowych i serwisów skierowanych do dzieci poniżej 13 roku życia uzyskiwali zgodę rodziców na zbieranie ich danych osobowych, a operatorzy stron komercyjnych skierowanych do ogółu społeczeństwa muszą posiadać wiedzę, iż konkretni użytkownicy to dzieci.

([42]) Zob. też: Opinia EIOD z dnia 25 lipca 2007 r. w sprawie komunikatu Komisji dla Parlamentu Europejskiego i Rady w sprawie kontynuacji programu prac na rzecz skuteczniejszego wdrażania dyrektywy o ochronie danych, (Dz.U. C 255 z 27.10.2007, s. 10).

([43]) Niektóre przepisy krajowe ustanawiają już podobne mechanizmy.

102. Tego typu zapis nie jest nowością. Art. 6 ust. 2 dyrektywy 95/46/WE odnosi się do zasad związanych z jakością danych mówiąc, że „n a administratorze danych spoczywa obowiązek zapewnienia przestrzegania przepisów ust. 1". Art. 17 ust. 1 wymaga, aby administrator danych wprowadził odpowiednie środki techniczne i organizacyjne. Zakres tych zapisów jest jednak ograniczony. Dodanie ogólnego zapisu dotyczącego rozliczalności stanowiłoby dla administratorów bodziec, aby wprowadzić aktywne środki celem uzyskania zgodności ze wszystkimi elementami prawa ochrony danych.

103. Zapis dotyczący rozliczalności skutkowałby tym, że administratorzy danych mieliby obowiązek wprowadzenia wewnętrznych mechanizmów i systemów kontroli, które gwarantowałyby zgodność z zasadami i obowiązkami, które nakładają ramy. Wymagałoby to na przykład objęcie kierownictwa najwyższego szczebla polityką ochrony danych, stworzenia procedur mapowania celem zagwarantowania odpowiedniej identyfikacji wszystkich operacji przetwarzania danych, ustanowienia wiążącej polityki ochrony danych, która powinna być nieustannie rewidowana i uaktualniana, by objąć nowe operacje przetwarzania danych, zgodnie z zasadami dotyczącymi jakości danych, zawiadamiania, bezpieczeństwa, dostępu itp. Administratorzy danych musieliby gromadzić dokumentację poświadczającą zgodność, która udostępniana byłaby na wniosek odpowiednich organów. Wykazywanie zgodności wobec opinii publicznej powinno w niektórych przypadkach być również obowiązkowe. Można by to osiągnąć na przykład poprzez ustanowienie obowiązku kontrolerów danych, by włączali kwestię ochrony danych do publikowanych raportów rocznych, gdy są one wymagane na mocy innych przepisów.

104. Rodzaje wdrożonych środków wewnętrznych i zewnętrznych muszą być oczywiście odpowiednie i zależeć od sytuacji faktycznej, jak i od okoliczności danego przypadku. To znaczna różnica czy administrator danych przetwarza kilkaset wpisów klientów, na które składa się tylko ich imię, nazwisko i adres, czy też dane milionów pacjentów wraz z historią choroby. To samo odnosi się do sposobów oceny skuteczności wprowadzonych środków. Istnieje potrzeba skalowalności.

105. Ogólne kompleksowe narzędzie prawne ochrony danych nie powinno ustanawiać szczególnych wymogów rozliczalności, jedynie jej najważniejsze elementy. W komunikacie przewidziano pewne elementy mające na celu wzmocnienie odpowiedzialności administratorów danych, które przyjmuje się z zadowoleniem. EIOD w pełni popiera zwłaszcza wprowadzenie obowiązku zatrudniania inspektorów ochrony danych i przeprowadzania ocen wpływu na prywatność po przekroczeniu pewnej wartości progowej.

106. EIOD zaleca ponadto delegowanie uprawnień na rzecz Komisji w myśl art. 290 TFUE, aby uzupełnić podstawowe wymogi niezbędne do osiągnięcia zgodności ze standardem rozliczalności. Korzystanie z tych uprawnień wpłynęłoby na wzrost pewności prawnej administratorów danych i harmonizację zgodności w całej UE. W procesie tworzenia konkretnych instrumentów należy skonsultować się z grupą roboczą art. 29 oraz z EIOD.

107. Konkretne środki związane z rozliczalnością, które mają być wdrażane przez administratorów danych, mogą zostać również narzucone przez organy ochrony danych w kontekście ich uprawnień związanych z egzekucją. W tym celu organy ochrony danych powinny zostać wyposażone w nowe uprawnienia umożliwiające im wyznaczanie działań naprawczych lub nakładanie sankcji. Mogłoby to być na przykład tworzenie wewnętrznych programów zgodności celem wdrożenia idei „uwzględniania ochrony prywatności w fazie projektowania" w ramach konkretnych produktów i usług itp. Działania naprawcze powinny być nakazywane jedynie wówczas, gdy byłyby odpowiednie, proporcjonalne i skuteczne z punktu widzenia zagwarantowania zgodności ze stosownymi i dającymi się wyegzekwować normami prawnymi.

7.3. *„Uwzględnianie ochrony prywatności w fazie projektowania"*

108. „Uwzględnianie ochrony prywatności w fazie projektowania" odnosi się do integracji ochrony danych i prywatności od samego początku istnienia nowych produktów, usług i procedur, które wiążą się z przetwarzaniem danych osobowych. Według EIOD „uwzględnianie ochrony prywatności w fazie projektowania" stanowi część składową rozliczalności. Administratorzy danych musieliby również udowodnić, że wcielili w życie „uwzględnianie ochrony prywatności w fazie projektowania" tam, gdzie to konieczne. Niedawno podczas 32. międzynarodowej konferencji rzeczników ochrony danych i prywatności przyjęto rezolucję, w której uznaje się „uwzględnianie ochrony prywatności w fazie projektowania" za główny składnik podstawowej ochrony prywatności ([44]).

109. Dyrektywa 95/46/WE zawiera zapisy zachęcające do „uwzględniania ochrony prywatności w fazie projektowania" ([45]), lecz nie ustanawia takiego obowiązku. EIOD jest zadowolony z poparcia, jakie zostało w ramach komunikatu udzielone idei „uwzględniania ochrony prywatności w fazie projektowania", które stanowi narzędzie gwarantujące zgodność z zasadami ochrony danych.

([44]) Rezolucja w sprawie uwzględniania ochrony prywatności w fazie projektowania, przyjęta podczas 32. międzynarodowej konferencji rzeczników ochrony danych i prywatności, Jerozolima 27–29 października 2010 r.

([45]) Dyrektywa zawiera przepisy, które pośrednio, w różnych sytuacjach, mogą wymagać wprowadzenia zasady „uwzględniania ochrony prywatności w fazie projektowania". Zwłaszcza art. 17 wymaga od administratorów danych wprowadzenia odpowiednich środków technicznych i organizacyjnych w celu zapobiegania nielegalnemu przetwarzaniu danych. Dyrektywa o prywatności i łączności elektronicznej jest bardziej jednoznaczna. Jej art. 14 ust. 3 stanowi, że „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".

Sugeruje on dodanie wiążącego zapisu ustanawiającego obowiązek „uwzględniania ochrony prywatności w fazie projektowania", który mógłby wzbogacić brzmienie motywu 46 dyrektywy 95/46/WE. Zapis ten jednoznacznie nakładałby na administratorów danych obowiązek przyjęcia odpowiednich rozwiązań technicznych i organizacyjnych, zarówno przy projektowaniu systemu przetwarzania danych, jak i podczas samego ich przetwarzania, zwłaszcza w celu zagwarantowania ochrony i niedopuszczenia do niedozwolonego przetwarzania danych ([46]).

110. Na mocy tak skonstruowanego zapisu administratorzy danych mieliby m.in. obowiązek zagwarantować, że systemy przetwarzania danych zostały zaprojektowane tak, by przetwarzać jak najmniej danych osobowych, włączać prywatność do ustawień standardowych – na przykład w serwisach społecznościowych z zasady ukrywać profile użytkowników, oraz stosować narzędzia umożliwiające użytkownikom lepszą ochronę ich danych (np. kontrola dostępu, kodowanie).

111. Zalety wyraźniejszego odniesienia do „uwzględniania ochrony prywatności w fazie projektowania" można streścić w następujący sposób:

— podkreśliłoby to znaczenie tej zasady *per se* jako narzędzia służącego zagwarantowaniu, że procesy, produkty i usługi będą projektowane od początku z myślą o ochronie prywatności,

— ograniczyłoby to nadużycia w zakresie prywatności, gdyż ograniczyłoby niepotrzebne gromadzenie danych i umożliwiło osobom fizycznym dokonywanie realnych wyborów dotyczących ich danych osobowych,

— pomogłoby to unikać sytuacji, gdy trzeba doraźnie rozwiązywać problemy, które są trudne lub niemożliwe do rozwiązania,

— ułatwiłoby to skuteczne stosowanie i egzekwowanie tej zasady przez organy ochrony danych.

112. Skumulowany rezultat wprowadzenia wspomnianego obowiązku wpłynąłby na zwiększenie zapotrzebowana na produkty i usługi uwzględniające ochronę prywatności w fazie projektowania, co przełożyłoby się na większą liczbę bodźców dla przemysłu by zapotrzebowanie to zaspokoić. Należy ponadto rozważyć nałożenie odrębnego obowiązku na projektantów i wytwórców nowych produktów i usług, który miałby wpływ na ochronę danych i prywatność. EIOD sugeruje dodanie odrębnego obowiązku, który pomógłby administratorom danych osiągnąć zgodność z ich obowiązkami.

113. Kodyfikacja „uwzględniania ochrony prywatności w fazie projektowania" mogłaby zostać uzupełniona dzięki zapisowi ustanawiającemu ogólne wymogi tej koncepcji mające zastosowanie do wszystkich sektorów, produktów i usług, jak na przykład zagwarantowanie sposobów wzmocnienia pozycji użytkownika, które zostałyby wprowadzone zgodnie z tą zasadą.

114. EIOD zaleca ponadto delegowanie uprawnień na rzecz Komisji w myśl art. 290 TFUE, aby odpowiednio uzupełnić podstawowe wymogi „uwzględniania ochrony prywatności w fazie projektowania" dla wybranych produktów i usług. Korzystanie z tych uprawnień wpłynęłoby na wzrost pewności prawnej administratorów danych i harmonizację zgodności w całej UE. W procesie tworzenia konkretnych instrumentów należy skonsultować się z grupą roboczą art. 29 oraz z EIOD (patrz również punkt 106 dotyczący rozliczalności).

115. Organy ochrony danych powinny zostać wyposażone w uprawnienia umożliwiające im wyznaczanie działań naprawczych lub nakładanie sankcji na tych samych restrykcyjnych warunkach, które omówione zostały w punkcie 107, gdyby administratorzy danych w oczywisty sposób nie dopełnili podjęcia konkretnych kroków tam, gdzie jest to wymagane.

7.4. *Usługi certyfikacji*

116. W komunikacie uznaje się potrzebę zbadania możliwości stworzenia unijnych systemów certyfikacji dla produktów i usług odpowiadających wymogom ochrony prywatności. EIOD w pełni ten pomysł popiera i sugeruje dodanie zapisu gwarantującego ich utworzenie i potencjalne wdrożenie w całej UE, który mógłby zostać rozwinięty na późniejszym etapie w ramach przepisów dodatkowych. Zapis ten powinien dopełniać postanowienia dotyczące rozliczalności i „uwzględniania ochrony prywatności w fazie projektowania".

117. Dobrowolne systemy certyfikacji umożliwiałyby weryfikację faktu, czy administrator danych ustanowił środki uzyskania zgodności z narzędziem prawnym. Ponadto administratorzy danych – a także produkty i usługi – korzystające z oznaczeń kontrolnych zdobędą najprawdopodobniej przewagę nad konkurentami. Tego typu systemy przydatne byłyby również organom ochrony danych, gdyż ułatwiałyby im nadzór i egzekucję.

8. **Globalizacja i właściwe prawo**

8.1. *Wyraźna potrzeba bardziej spójnej ochrony*

118. Jak wspomniano w rozdziale 2, ilość danych osobowych przekazywanych poza granice Unii rośnie w postępie geometrycznym wskutek rozwoju nowych technologii, rosnącej roli przedsiębiorstw międzynarodowych oraz rosnącego wpływu rządów na przetwarzanie i współdzielenie danych osobowych na międzynarodową skalę. Jest to jedna z głównych przesłanek uzasadniających rewizję obecnie obowiązujących ram prawnych. W związku z tym EIOD prosi o ambicję i skuteczność właśnie w tym obszarze, gdyż istnieje wyraźna potrzeba bardziej spójnej ochrony, gdy dane przetwarzane są poza granicami Unii.

([46]) W obecnych ramach motyw 46 zachęca administratorów danych, aby wdrażali tego typu środki, lecz motywy nie mają mocy wiążącej.

8.2. *Inwestowanie w zasady międzynarodowe*

119. Według EIOD istnieje zapotrzebowanie na więcej inwestycji w tworzenie zasad międzynarodowych. Wyższy stopień harmonizacji w zakresie poziomu ochrony danych osobowych na całym świecie znacząco wpłynąłby na wyjaśnienie treści zasad, których należy przestrzegać, oraz warunków przekazywania danych. Globalne zasady powinny godzić wymóg wysokiego standardu ochrony danych – wraz z kluczowymi elementami ochrony danych w UE – z regionalną specyfiką.

120. EIOD popiera ambitne prace prowadzone dotychczas w ramach międzynarodowej konferencji rzeczników ochrony danych mające na celu stworzenie i popularyzację tzw. „standardów madryckich" celem zintegrowania ich w jeden wiążący instrument i być może zainicjowania międzyrządowej konferencji ([47]). Wzywa on Komisję do podjęcia niezbędnych inicjatyw mających na celu uproszczenie realizacji tego celu.

121. W opinii EIOD ważne jest również, by zapewnić spójność pomiędzy inicjatywą na rzecz międzynarodowych standardów, obecnym przeglądem unijnych ram ochrony danych i innymi zmianami, takimi jak na przykład bieżąca rewizja wytycznych OECD w sprawie ochrony prywatności i konwencji nr 108 Rady Europy, którą mogą również podpisywać państwa trzecie (patrz również punkt 17). EIOD uważa, że Komisja ma tu do odegrania specjalną rolę, gdyż musi określić sposób promowania spójności w negocjacjach z OECD i Radą Europy.

8.3. *Jaśniejsze określenie kryteriów właściwego prawa*

122. Ponieważ nie da się łatwo osiągnąć pełnej spójności, pewien poziom różnic pomiędzy prawem w ramach Unii i *a fortiori* poza jej granicami pozostanie, przynajmniej w najbliższej przyszłości. EIOD uważa, że nowe narzędzie prawne będzie musiało jaśniej określać kryteria ustalania prawa właściwego i gwarantować usprawnione mechanizmy przepływu danych, a także rozliczalność osób zaangażowanych w przepływy.

123. Narzędzie prawne powinno w pierwszym rzędzie gwarantować, że przepisy UE mają zastosowanie, gdy dane osobowe przetwarzane są poza granicami Unii, lecz istnieje uzasadniona potrzeba ich stosowania. Potrzebę tę ilustruje na przykład usługa przetwarzania w chmurze świadczona przez podmioty spoza Europy, lecz skierowana do mieszkańców Unii. W środowisku, gdzie dane nie są fizycznie gromadzone i przetwarzane w określonym miejscu, a usługodawcy i użytkownicy zlokalizowani w różnych krajach ingerują w dane, trudno jest określić kto ponosi odpowiedzialność za zgodność z zasadami ochrony danych. Wytyczne dotyczące sposobu interpretacji i stosowania postanowień dyrektywy 95/46/WE w tego typu przypadkach istnieją, wydają je zwłaszcza organy ochrony danych, lecz same wytyczne nie wystarczą, aby zagwarantować pewność prawa w nowym otoczeniu.

124. Potrzebę większej precyzji ram prawnych i uproszczenia kryteriów ustalania właściwego prawa na terytorium UE podkreśla w najnowszej opinii grupa robocza art. 29 ([48]).

125. Według EIOD lepszym pomysłem byłoby ustanowienie narzędzia prawnego w ramach rozporządzenia, dzięki któremu takie same zasady obowiązywałyby we wszystkich państwach członkowskich. Dzięki rozporządzeniu potrzeba ustalania prawa właściwego traci na znaczeniu, dlatego też m.in. EIOD opowiada się za przyjęciem tego rodzaju aktu prawnego. Niestety rozporządzenie pozostawia państwom członkowskim pewne pole manewru. Jeżeli w ramach nowego narzędzia stworzone zostanie znaczne pole manewru, EIOD popierał będzie sugestię grupy roboczej, aby przejść od dystrybutywnego stosowania rozbieżnych przepisów krajowych do scentralizowanego stosowania jednego prawodawstwa we wszystkich państwach członkowskich, gdzie administrator danych prowadzi placówki. Apeluje on również o szerszą współpracę i koordynację pomiędzy organami ochrony danych w przypadku spraw i skarg transgranicznych (patrz rozdział 10).

8.4. *Usprawnianie mechanizmów przepływu danych*

126. Potrzeba spójności i punktów odniesienia na wysokim szczeblu musi zostać uwzględniona nie tylko celem stworzenia globalnych zasad ochrony danych, lecz również zabezpieczenia międzynarodowego przekazywania danych. EIOD w pełni popiera cel Komisji, jakim jest usprawnienie obecnie stosowanych procedur międzynarodowego przekazywania danych i zagwarantowanie jednolitego i spójnego podejścia do krajów trzecich i organizacji międzynarodowych.

127. Mechanizm przepływu danych obejmuje zarówno przekazywanie danych z sektora prywatnego, zwłaszcza na mocy zapisów umownych lub Wiążących Reguł Korporacyjnych (BCR), jak i przepływ pomiędzy władzami publicznymi. Wiążące Reguły Korporacyjne są jednym z elementów, który wymaga bardziej spójnego i usprawnionego podejścia. EIOD zaleca jasne sprecyzowanie warunków dla Wiążących Reguł Korporacyjnych w ramach nowego narzędzia prawnego, aby ([49]):

— wyraźnie wskazać, że Wiążące Reguły Korporacyjne są narzędziem oferującym adekwatne zabezpieczenia,

— ustanowić kluczowe elementy/warunki przyjęcia Wiążących Reguł Korporacyjnych,

([47]) Jak sugeruje rezolucja w sprawie standardów międzynarodowych przyjęta podczas 32. międzynarodowej konferencji rzeczników ochrony danych i prywatności, Jerozolima 27–29 października 2010 r.

([48]) Opinia grupy roboczej art. 29 nr 8/2010 o prawie właściwym, dokument WP 179.

([49]) Więcej informacji o przepływie międzynarodowym znaleźć można w rozdziale 8 wspomnianej opinii.

— stworzyć procedury współpracy na rzecz przyjęcia Wiążących Reguł Korporacyjnych, wraz z kryteriami wyboru głównego organu nadzorczego (punktu kompleksowej kontroli).

9. **Obszar policji i wymiaru sprawiedliwości**

9.1. *Ogólne narzędzie*

128. Komisja wielokrotnie podkreślała znaczenie wzmocnienia ochrony danych w kontekście egzekwowania prawa i zapobiegania przestępczości w sytuacji znacznej intensyfikacji wymiany i wykorzystywania danych osobowych. Również zatwierdzony przez Radę Europejską program sztokholmski odnosi się do silnego systemu ochrony danych jako podstawowego warunku europejskiej strategii zarządzania informacjami ([50]).

129. Przegląd ogólnych ram ochrony danych stanowi idealną okazję do poczynienia postępów w tej dziedzinie, zwłaszcza że w komunikacie słusznie opisuje decyzję ramową 2008/977 jako nieadekwatną ([51]).

130. W punkcie 3.2.5 niniejszej opinii EIOD zawarł argumenty przemawiające za włączeniem obszaru policji i współpracy sądowej do ogólnego narzędzia. Włączenie policji i wymiaru sprawiedliwości niesie ze sobą wiele dodatkowych korzyści. Oznacza to, że zasady nie będą stosowały się wyłącznie do transgranicznej wymiany danych ([52]), lecz także do przetwarzania krajowego. Adekwatna ochrona w zakresie wymiany danych z krajami trzecimi będzie skuteczniej zagwarantowana, także w ramach umów międzynarodowych. Organy ochrony danych będą dysponowały ponadto tymi samymi szerokimi i zharmonizowanymi uprawieniami w stosunku do policji i wymiaru sprawiedliwości, jakie mają wobec innych administratorów danych. Obecnie obowiązujące brzmienie art. 13, na mocy którego państwa członkowskie mogą wprowadzać przepisy szczególne ograniczające obowiązki i prawa wynikające z ogólnego narzędzia z uwagi na szczególny interes publiczny, będą musiały być stosowane w sposób tak samo restrykcyjny jak w innych obszarach. Szczególne zabezpieczenia ujęte w ogólnym narzędziu w tym obszarze będą zwłaszcza musiały być przestrzegane także w prawodawstwie krajowym przyjętym w obszarze policji i współpracy sądowej.

9.2. *Dodatkowe szczególne zasady dotyczące policji i wymiaru sprawiedliwości*

131. Włączenie dodatkowych zasad nie wyklucza jednak wprowadzania specjalnych zasad i derogacji, które w odpowiedni sposób uwzględniałyby specyficzny charakter tego sektora zgodnie z deklaracją nr 21 dołączoną do traktatu lizbońskiego. Przewidziane mogą być ograniczenia co do korzystania z prawa do ochrony danych, lecz muszą one być niezbędne, proporcjonalne i w żadnym wypadku nie wpływać na fundamentalne elementy tego prawa. Należy w tym kontekście podkreślić, że dyrektywa 95/46WE, także jej art. 13, obecnie stosuje się do egzekucji prawa w rozmaitych obszarach (np. podatki, cło, zapobieganie oszustwom), które nie odbiegają od wielu czynności z obszaru policji i wymiaru sprawiedliwości.

132. Należy ponadto ustanowić szczególne zabezpieczenia, aby zrekompensować osobom, których dane dotyczą, bardziej wnikliwe przetwarzanie danych zapewniając im dodatkową ochronę.

133. W świetle powyższego EIOD uważa, że nowe ramy powinny, zgodnie z konwencją nr 108 i rekomendacją R (87) 15, obejmować co najmniej następujące elementy:

— należy wyodrębnić różne kategorie danych odpowiednio do ich stopnia poprawności i wiarygodności z uwzględnieniem zasady, że dane oparte na faktach należy odróżnić od danych opartych na opiniach i osobistych ocenach,

— należy wprowadzić rozróżnienie między różnymi kategoriami osób, których dane dotyczą (przestępcy, podejrzani, pokrzywdzeni, świadkowie itd.) i zbiorami danych (tymczasowe, stałe i zbiory wywiadu). Należy ustanowić specjalne warunki i gwarancje dotyczące przetwarzania danych odnoszących się do osób spoza kręgu podejrzanych,

— mechanizmy gwarantowania okresowej weryfikacji i sprostowania, aby stać na straży jakości przetwarzanych danych,

— szczególne przepisy lub zabezpieczenia mogą zostać stworzone w związku z coraz istotniejszą kwestią przetwarzania danych biometrycznych i genetycznych w dziedzinie egzekucji prawa. Ich wykorzystywanie powinno ograniczać się do przypadków, gdy nie istnieją mniej inwazyjne środki gwarantujące ten sam efekt ([53]),

— warunki przekazywania danych osobowych niewłaściwym organom i partnerom prywatnym oraz dostępu i dalszego wykorzystywania danych osobowych gromadzonych przez partnerów prywatnych przez organy wymiaru sprawiedliwości.

([50]) Zob. opinia Europejskiego Inspektora Ochrony Danych z dnia 30 września 2010 r. w sprawie Komunikatu Komisji do Parlamentu Europejskiego i Rady – „Przegląd zarządzania informacjami w przestrzeni wolności, bezpieczeństwa i sprawiedliwości", punkty 9–19.

([51]) Zob. punkt 3.2.5 powyżej.

([52]) Zakres decyzji ramowej 2008/977 jest obecnie ograniczony.

([53]) Zob. dokument grupy roboczej dotyczący „Przyszłości prywatności", punkt 112.

9.3. *Sektorowe systemy ochrony danych*

134. Jak mówi komunikat „decyzja ramowa nie zastępuje różnych sektorowych aktów legislacyjnych dotyczących współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych przyjętych na szczeblu UE, w szczególności tych, które regulują funkcjonowanie Europolu, Eurojustu, systemu informacyjnego Schengen (SIS) oraz systemu informacji celnej (CIS), i które przewidują szczególne systemy ochrony danych, lub które zazwyczaj odsyłają do instrumentów ochrony danych Rady Europy".

135. W opinii EIOD nowe ramy prawne powinny być – w miarę możliwości – jasne, proste i spójne. Gdy istnieje duża liczba różnych systemów mających zastosowanie np. do Europolu, Eurojustu, SIS i Prüm, zachowanie zgodności z zasadami jest nadal lub nawet staje się bardziej skomplikowane. Jest to jeden z powodów, dla których EIOD preferuje kompleksowe narzędzie prawne dla wszystkich sektorów.

136. EIOD rozumie jednak, że ujednolicenie zasad obowiązujących różne systemy wymagałoby znacznych nakładów pracy, którą trzeba wykonywać precyzyjnie. Uważa on, że stopniowe podejście, o którym mowa w komunikacie, jest zasadne, o ile zaangażowanie w zagwarantowanie wysokiego stopnia ochrony danych w sposób spójny i skuteczny pozostaje celem jasno określonym i widocznym. Precyzyjniej rzecz ujmując:

— na pierwszym etapie ogólne narzędzie prawne ochrony danych powinno znaleźć zastosowanie do wszystkich przypadków przetwarzania danych w obszarze policji i współpracy sądowej, biorąc pod uwagę korekty na rzecz policji i wymiaru sprawiedliwości (w myśl punktu 9.2),

— na drugim etapie sektorowe systemy ochrony danych należałoby ujednolicić z ogólnym narzędziem. Komisja powinna wziąć na siebie przyjęcie propozycji dla drugiego etapu w krótkim i precyzyjnie zdefiniowanym horyzoncie czasowym.

10. **Organy ochrony danych i współpraca między nimi**

10.1. *Wzmocnienie roli organów ochrony danych*

137. EIOD w pełni popiera cel Komisji, jakim jest rozwiązanie problemu statusu organów ochrony danych, a konkretniej poprawa ich niezależności, zasobów i uprawnień w zakresie egzekucji prawa.

138. EIOD kładzie również nacisk na potrzebę jaśniejszego określenia kluczowej kwestii niezależności organów ochrony danych w ramach nowego narzędzia prawnego. Europejski Trybunał Sprawiedliwości wydał niedawno decyzję w sprawie C-518/07 ([54]), w której podkreśla, że niezależność oznacza brak wpływów zewnętrznych. Organ ochrony danych nie może prosić nikogo o wskazówki ani ich przyjmować. EIOD zaleca jednoznaczną kodyfikację elementów dotyczących niezależności w ramach prawa.

139. Aby odpowiednio realizować zadania, organy ochrony danych muszą dysponować odpowiednimi zasobami ludzkimi i finansowymi. EIOD sugeruje włączenie tego wymogu do przepisów prawa ([55]). Pragnie również podkreślić potrzebę zagwarantowania, że organy mają w pełni zharmonizowane uprawnienia śledcze, a także że nakładają w wystarczającym stopniu odstraszające i naprawcze środki i sankcje. Pomogłoby to zwiększyć pewność prawa ze strony osób, których dane dotyczą, i administratorów danych.

140. Zwiększenie niezależności, zasobów i uprawnień organów ochrony danych powinno iść w parze z lepszą współpracą na szczeblu wielostronnym, zwłaszcza w obliczu rosnącej liczby problemów związanych z przetwarzaniem danych na skalę europejską. Najważniejszą strukturą dla celów współpracy byłaby oczywiście grupa robocza art. 29.

10.2. *Wzmocnienie roli grupy roboczej*

141. Historia pokazuje, że funkcjonowanie grupy podlegało ewolucji od momentu jej założenia w 1997 r. Uzyskała ona większą niezależność i w praktyce może nie stanowić już zwykłej grupy roboczej doradzającej Komisji. EIOD sugeruje więc wprowadzenie dalszych ulepszeń w zakresie funkcjonowania grupy roboczej, jej infrastruktury i niezależności.

142. EIOD uważa, że siła grupy jest nierozerwalnie związana z niezależnością i uprawnieniami jej członków. Autonomia grupy roboczej powinna zostać zagwarantowana w nowych ramach prawnych zgodnie z kryteriami stworzonymi dla celów osiągnięcia pełnej niezależności organów ochrony danych przez Europejski Trybunał Sprawiedliwości w sprawie C-518/07. EIOD uważa, że grupie roboczej należy zapewnić wystarczające zasoby i budżet, a także wzmocniony sekretariat, aby mogła pracować sprawniej.

143. Co się tyczy sekretariatu grupy, EIOD docenia fakt, że jest on zintegrowany z Wydziałem Ochrony Danych Dyrekcji Generalnej ds. Sprawiedliwości, dzięki czemu grupa robocza posiada efektywne, elastyczne kontakty i otrzymuje aktualne informacje o postępach w dziedzinie ochrony danych. Z drugiej jednak strony EIOD ma wątpliwości co do faktu, że Komisja (a raczej wydział) jest jednocześnie członkiem, sekretariatem i adresatem opinii grupy. Uzasadniałoby to większą niezależność sekretariatu. EIOD zachęca Komisję, aby oceniła – po konsultacjach z zainteresowanymi stronami – jak można by najlepiej zagwarantować jego niezawisłość.

([54]) Sprawa C-518/07, *Komisja przeciwko Republice Federalnej Niemiec*, nieopublikowana w Zb. Orz.

([55]) Zob. na przykład art. 43 ust. 2 rozporządzenia (WE) nr 45/2001, który ustanawia tego typu wymogi dla EIOD.

144. Wzmocnienie uprawnień organów ochrony danych wymaga również większych uprawnień grupy roboczej, która dysponowałaby strukturą obejmującą lepsze zasady i zabezpieczenia, a także większą przejrzystość. Aspekty te zostaną rozwinięte dla potrzeb roli grupy roboczej związanej z doradztwem oraz egzekucją prawa.

10.3. *Rola grupy roboczej związana z doradztwem*

145. Stanowiska grupy roboczej muszą być skutecznie wdrażane w zakresie jej roli związanej z doradzaniem Komisji, zwłaszcza w związku z interpretowaniem i stosowaniem zasad zawartych w dyrektywie i innych narzędziach ochrony danych – innymi słowy po to, by zagwarantować autorytatywny charakter jej stanowisk. Należy prowadzić dalsze dyskusje pomiędzy organami ochrony danych, aby określić sposób, w jaki można by ująć tę kwestię w ramach narzędzia prawnego.

146. EIOD zaleca rozwiązania, które uczyniłyby opinie grupy roboczej bardziej autorytatywnymi bez potrzeby znacznej zmiany sposobu jej funkcjonowania. EIOD sugeruje włączenie obowiązku organów ochrony danych i Komisji, aby w jak największym stopniu uwzględniać opinie i wspólne stanowiska przyjęte przez grupę roboczą, w oparciu o model stosowany wobec stanowisk Organu Europejskich Regulatorów Łączności Elektronicznej (BEREC) ([56]). Nowe narzędzie prawne powinno ponadto wyznaczać grupie roboczej jednoznaczne zadanie, jakim jest przyjmowanie „zaleceń interpretacyjnych". Dzięki alternatywnym rozwiązaniom stanowiska grupy roboczej odgrywałyby większą rolę, również w sądach.

10.4. *Skoordynowane egzekwowanie prawa przez grupę roboczą*

147. W obecnych ramach egzekwowanie przepisów dotyczących ochrony danych w państwach członkowskich leży w gestii 27 organów ochrony danych, których działania nie są skoordynowane w zakresie prowadzenia poszczególnych spraw. Co się tyczy spraw, których zasięg obejmuje więcej niż jedno państwo członkowskie lub których wymiar jest ogólnoświatowy, wpływa to na zwiększenie kosztów przedsiębiorstw, które muszą tę samą czynność uzgadniać z wieloma różnymi organami, oraz na zwiększenie ryzyka niespójnego stosowania zasad ochrony danych: w wyjątkowych sytuacjach ta sama czynność związana z przetwarzaniem danych może być uznana przez jeden organ ochrony danych za legalną, a przez inny zabroniona.

148. Pewne sprawy mają wymiar strategiczny, którym należy zajmować się w sposób scentralizowany. Działalność grupy roboczej art. 29 ułatwia koordynację i egzekwowanie prawa przez różne organy ochrony danych ([57]) w ważnych sprawach związanych z ochroną danych mających implikacje międzynarodowe. Tak stało się w przypadku portali społecznościowych i wyszukiwarek ([58]), a także skoordynowanych inspekcji przeprowadzonych w różnych państwach członkowskich w zakresie telekomunikacji i ubezpieczeń zdrowotnych.

149. Istnieją jednakże ograniczenia działalności związanej z egzekwowaniem prawa, którą grupa robocza może prowadzić w obecnych ramach. Grupa może przyjmować wspólne stanowiska, lecz nie istnieje żadne narzędzie służące zagwarantowaniu, że zostaną one skutecznie wcielone w życie.

150. EIOD sugeruje włączenie do narzędzia prawnego dodatkowych zapisów wspierających skoordynowaną egzekucję prawa, zwłaszcza:

— obowiązku organów ochrony danych i Komisji, aby w jak największym stopniu uwzględniać opinie i wspólne stanowiska przyjęte przez grupę roboczą art. 29 ([59]),

— obowiązku organów ochrony danych, aby rzetelnie współpracowały ze sobą nawzajem, z Komisją i grupą roboczą art. 29 ([60]). Aby praktycznie zilustrować rzetelną współpracę, należałoby stworzyć procedurę w ramach której organy ochrony danych informowałyby Komisję lub grupę roboczą o krajowych działaniach związanych z egzekucją z elementem transgranicznym, analogiczną do procedury stosowanej w obecnych ramach w związku z krajowymi decyzjami krajowymi,

— precyzyjnego określenia zasad głosowania, aby poprawić zaangażowanie organów ochrony danych we wdrażanie decyzji grupy roboczej. Można by określić, że grupa robocza podejmuje decyzje na podstawie konsensusu, a jeśli nie można go osiągnąć, podejmuje decyzje o działaniach związanych z egzekucją jedynie kwalifikowaną większością głosów. Ponadto można by zawrzeć w motywie zapis, że organy ochrony danych,

([56]) Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1211/2009 z dnia 25 listopada 2009 r. ustanawiające Organ Europejskich Regulatorów Łączności Elektronicznej (BEREC) oraz Urząd, (Dz.U. L 337 z 18.12.2009, s. 1).

([57]) Oprócz grupy roboczej art. 29, Europejska Konferencja Komisarzy ds. Ochrony Danych stworzyła około 10 lat temu także stałe warsztaty, których zadaniem jest rozpatrywanie w skoordynowany sposób transgranicznych skarg. Choć warsztaty niezaprzeczalnie tworzą wartość dodaną w zakresie wymiany pomiędzy personelem organów ochrony danych i stanowią rzetelną sieć punktów kontaktowych, nie stanowią jednak mechanizmu koordynacji podejmowania decyzji.

([58]) Zob. pisma grupy roboczej art. 29 z dnia 12 maja 2010 r. i z dnia 26 maja 2010 r. opublikowane na stronie internetowej grupy: (http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010-others_en.htm).

([59]) Jak wspomniano powyżej, podobny obowiązek wynika z rozporządzenia (WE) nr 1211/2009, które definiuje rolę Organu Europejskich Regulatorów Łączności Elektronicznej (BEREC).

([60]) Zob. art. 3 rozporządzenia (WE) nr 1211/2009, cytowany powyżej.

które głosują za danym dokumentem, mają obowiązek lub zobowiązanie polityczne, aby wdrożyć go na szczeblu krajowym.

151. EIOD wniósłby sprzeciw wobec wprowadzenia ostrzejszych środków, takich jak na przykład nadanie mocy wiążącej stanowiskom grupy roboczej art. 29. Zachwiałoby to niezależnym statusem poszczególnych organów ochrony danych, który muszą gwarantować państwa członkowskie w ramach prawodawstwa krajowego. Gdyby decyzje grupy roboczej miały bezpośredni wpływ na osoby trzecie, na przykład administratorów danych, należałoby stworzyć nowe procedury obejmujące takie zabezpieczenia jak przejrzystość i odszkodowania, łącznie z apelacją do Europejskiego Trybunału Sprawiedliwości.

10.5. *Współpraca pomiędzy EIOD a grupą roboczą*

152. Sposób współpracy pomiędzy EIOD a grupą roboczą również mógłby ulec dostrojeniu. EIOD jest członkiem grupy roboczej. W ramach jej prac wnosi on swój wkład w jej stanowiska dotyczące głównych strategicznych zmian w UE, zapewniając jednocześnie spójność z własnymi stanowiskami. EIOD pragnie podkreślić, że liczba kwestii związanych z prywatnością stale rośnie, zarówno w sektorze prywatnym jak i publicznym. Mogą one mieć implikacje na szczeblu krajowym w wielu państwach członkowskich, dlatego też grupa robocza ma w tym kontekście do odegrania szczególną rolę.

153. EIOD ma również zadanie uzupełniające powyższe, mianowicie doradzanie w kwestii zmian w kontekście UE, które powinien nadal realizować. Jako organ europejski sprawuje on rolę doradczą wobec instytucji UE w taki sam sposób, w jaki krajowe organy ochrony danych doradzają rządom swoich państw.

154. EIOD i grupa robocza prowadzą działalność z innej, lecz uzupełniającej się perspektywy. Z tych przyczyn istnieje potrzeba zachowania i być może również poprawy koordynacji pomiędzy grupą roboczą a EIOD, aby zagwarantować współpracę w zakresie głównych kwestii związanych z ochroną danych, na przykład poprzez regularną koordynację programów działań ([61]), oraz poprzez zagwarantowanie przejrzystości w sprawach o zasięgu krajowym lub specyficznie unijnym.

155. Dyrektywa w obecnie obowiązującym brzmieniu nie wspomina o koordynacji, ponieważ instytucja EIOD nie istniała jeszcze w momencie jej przyjęcia. Po 6 latach ich istnienia fakt, że EIOD i grupa robocza uzupełniają się, jest wyraźnie widoczny i mógłby zostać formalnie uznany. EIOD pragnie przypomnieć, że w myśl rozporządzenia (WE) nr 45/2001 ma on obowiązek współpracować z krajowymi organami ochrony danych, a także uczestniczyć w pracach grupy roboczej. EIOD zaleca, aby współpraca została wyraźnie ujęta w ramach nowego narzędzia prawnego, a także – gdy jest to konieczne – jej struktura, na przykład poprzez ustanowienie procedury współpracy.

10.6. *Współpraca pomiędzy EIOD a organami ochrony danych w zakresie nadzoru nad systemami UE*

156. Rozważania te odnoszą się również do obszarów, gdzie nadzór musi być koordynowany pomiędzy szczeblem europejskim a krajowym, tak jak w przypadku organów unijnych, które przetwarzają znaczną ilość danych dostarczanych przez władze krajowe, lub też wielkoskalowych systemów informatycznych obejmujących składowe europejskie i krajowe.

157. Istniejący system obejmujący niektóre organy UE i wielkoskalowe systemy informatyczne (np. Europol, Eurojust i system informacyjny Schengen (SIS) pierwszej generacji mają wspólne organy nadzorcze, w których skład wchodzą przedstawiciele krajowych organów ochrony danych) jest pozostałością współpracy międzyrządowej w okresie przed przyjęciem traktatu lizbońskiego, w związku z czym nie uwzględnia struktury instytucjonalnej UE, której integralną część stanowią obecnie Europol i Eurojust, a która obejmuje teraz również „dorobek Schengen" ([62]).

158. W komunikacie zapowiedziano, że Komisja rozpocznie w 2011 r. proces konsultacji z zainteresowanymi stronami dotyczących rewizji trzech systemów nadzoru. EIOD wzywa Komisję, aby jak najszybciej (w krótkim, dokładnie określonym czasie, patrz wyżej) przyjęła stanowisko w trwającej obecnie debacie na temat nadzoru. W dyskusji tej EIOD przyjmie następujący punkt widzenia:

159. Jako punkt wyjścia należy zagwarantować, że wszystkie organy nadzorcze spełniają niezbędne kryteria niezależności, zasobów i uprawnień w zakresie egzekwowania prawa. Ponadto zagwarantować należy uwzględnienie perspektyw i kompetencji istniejących na szczeblu unijnym. Oznacza to, że współpraca powinna odbywać się nie tylko pomiędzy władzami krajowymi, lecz również z europejskim organem ochrony danych (czyli obecnie z EIOD). EIOD uważa postępowanie według modelu, który spełniałby te wymogi, za konieczne ([63]).

160. W ostatnich latach powstał model „skoordynowanego nadzoru". Funkcjonuje on obecnie w ramach Eurodac i niektórych części Systemu Informacji Celnej, lecz niedługo obejmie również wizowy system informacyjny (VIS) i system informacyjny Schengen drugiej generacji (SIS II). Na model ten składają się trzy warstwy: 1) nadzór na szczeblu krajowym zapewniają organy ochrony danych; 2) nadzór na szczeblu unijnym zapewnia EIOD; 3) koordynacja gwarantowana jest w drodze regularnych

([61]) Np. na podstawie corocznie publikowanego i regularnie uaktualnianego wykazu działań legislacyjnych, który znaleźć można na stronie internetowej EIOD.

([62]) W myśl rozporządzenia (WE) nr 45/2001 EIOD ma obowiązek współpracować z tymi organami.

([63]) W przypadku Eurojust model ten powinien również uwzględniać fakt, iż nadzór nad ochroną danych obejmuje poszanowanie dla niezależności władzy sądowniczej, gdy Eurojust przetwarza dane w kontekście postępowań karnych.

spotkań zwoływanych przez EIOD działający w charakterze sekretariatu tego mechanizmu koordynacji. Model ten okazał się skuteczny i efektywny, w związku z czym powinien być w przyszłości uwzględniany w ramach innych systemów informacyjnych.

C. **JAK POPRAWIĆ STOSOWANIE DOTYCHCZASOWYCH RAM?**

11. **W krótkim horyzoncie czasowym**

161. Choć proces przeglądu trwa, należy niemniej dołożyć starań, by zagwarantować pełne i skuteczne wdrożenie dotychczasowych zasad, gdyż będą one miały zastosowanie do momentu przyjęcia przyszłych ram i ich implementacji do prawodawstwa państw członkowskich. Idąc tym tropem można określić kilka kierunków działań.

162. Po pierwsze Komisja powinna nadal monitorować przestrzeganie przez państwa członkowskie dyrektywy 95/46/WE i odpowiednio korzystać z uprawnień nadanych jej na mocy art. 258 TFUE. Niedawno rozpoczęło się postępowanie w sprawie uchybienia zobowiązaniom państwa członkowskiego w związku z niepoprawną implementacją art. 28 dyrektywy w zakresie wymaganej niezależności organów ochrony danych ([64]). Zgodność należy monitorować i egzekwować również w innych obszarach ([65]). EIOD z zadowoleniem przyjmuje więc i w pełni popiera zobowiązanie, jakie podjęła Komisja w ramach komunikatu, aby prowadzić aktywną politykę ścigania naruszeń. Komisja powinna także kontynuować zorganizowany dialog dotyczący implementacji z państwami członkowskimi ([66]).

163. Po drugie, należy zachęcać do egzekwowania prawa na szczeblu krajowym, aby zagwarantować stosowanie zasad ochrony danych w praktyce, również wobec nowych zjawisk technologicznych i podmiotów działających globalnie. Organy ochrony danych muszą w pełni korzystać z przysługujących im uprawnień śledczych i karnych. Ważne jest, aby dotychczasowe prawa osób, których dane dotyczą, zwłaszcza prawa dostępu do danych, były w pełni realizowane w praktyce.

164. Po trzecie, w krótkim horyzoncie czasowym niezbędna wydaje się lepsza koordynacja w zakresie egzekwowania prawa. Rola, jaką pełni w tym względzie grupa robocza art. 29 i jej dokumenty interpretacyjne, jest kluczowa, lecz organy ochrony danych powinny dołożyć wszelkich starań, by wcielić je w życie. Należy unikać rozbieżnych wyników w przypadkach o zasięgu ogólnounijnym lub globalnym, a w ramach grupy roboczej można i trzeba tworzyć wspólne podejścia. Znaczną wartość dodaną mogą również wytworzyć skoordynowane ogólnounijne śledztwa prowadzone pod auspicjami grupy roboczej.

165. Po czwarte, zasady ochrony danych powinny być aktywnie włączane do nowych przepisów, które mogą mieć bezpośredni lub pośredni wpływ na ochronę danych. Na szczeblu Unii EIOD dokłada starań, aby przyczynić się do powstawania lepszych przepisów europejskich. Tego typu starania należy podejmować także na szczeblu krajowym. Organy ochrony danych powinny więc w pełni korzystać z uprawnień doradczych, aby zagwarantowane zostało aktywne podejście do tych kwestii. Organy ochrony danych, w tym również EIOD, mogą odegrać aktywną rolę w zakresie monitorowania zmian technologicznych. Monitorowanie jest ważne z punktu widzenia wczesnej identyfikacji pojawiających się trendów, podkreślania ich potencjalnych implikacji względem ochrony danych, wspierania rozwiązań sprzyjających ochronie danych i podnoszenia wiedzy zainteresowanych stron.

166. Po piąte, należy realizować aktywną współpracę pomiędzy rozmaitymi podmiotami na szczeblu międzynarodowym, w związku z czym, ważne jest, aby wzmacniać międzynarodowe instrumenty współpracy. Na pełne poparcie zasługują inicjatywy takie jak standardy madryckie czy nieprzerwane prace Rady Europy i OECD. W tym kontekście cieszy, że również Federalna Komisja Handlu współpracuje z komisarzami prywatności i danych osobowych w ramach Międzynarodowej Konferencji.

D. **WNIOSKI**

UWAGI OGÓLNE

167. Generalnie EIOD z zadowoleniem przyjmuje komunikat Komisji, gdyż stoi na stanowisku, iż przegląd obecnie obowiązujących ram prawnych ochrony danych jest niezbędny, aby zagwarantować skuteczną ochronę w ciągle rozwijającym się i zglobalizowanym społeczeństwie informacyjnym.

168. W komunikacie określono najważniejsze problemy i wyzwania. EIOD podziela pogląd Komisji, że silny system ochrony danych potrzebny będzie nadal w przyszłości w oparciu o założenie, że istniejące ogólne zasady ochrony danych są nadal aktualne w społeczeństwie, które podlega fundamentalnym zmianom. EIOD w pełni podziela wyrażoną w komunikacie opinię, że wyzwania są ogromne i podkreśla, że proponowane rozwiązania powinny być w związku z tym odpowiednio ambitne i wpływać na wzmocnienie skuteczności ochrony. EIOD prosi więc o bardziej ambitne podejście do wielu z powyższych kwestii.

169. EIOD w pełni popiera kompleksowe podejście do kwestii ochrony danych. Pragnie z przykrością zauważyć, że Komisja wyłączyła pewne obszary, takie jak przetwarzanie danych przez instytucje i organy UE, z zakresu ogólnego instrumentu prawnego. Gdyby Komisja zdecydowała się te

([64]) Zob. sprawa C-518/07 cytowaną powyżej oraz komunikat prasowy Komisji z dnia 28 października 2010 r. (IP/10/1430).

([65]) Komisja wszczęła postępowanie w sprawie uchybienia zobowiązaniom państwa członkowskiego przeciwko Wielkiej Brytanii w związku z rzekomym naruszeniem rozmaitych przepisów dotyczących ochrony danych, łącznie z wymogiem dotyczącym poufności komunikacji elektronicznej w związku z reklamą behawioralną. Zob. komunikat prasowy Komisji z dnia 9 kwietnia 2009 r. (IP/09/570).

([66]) Zob. pierwsze sprawozdanie Komisji z implementacji dyrektywy o ochronie danych, op. cit., s. 22 i nast.

obszary pominąć, EIOD wzywa ją do przyjęcia propozycji na szczeblu UE w jak najkrótszym czasie, najlepiej do końca 2011 r.

NAJWAŻNIEJSZE ZAGADNIENIA

170. Punkty wyjścia procesu przeglądu dla EIOD są następujące:

— ustalenia co do ochrony danych muszą w jak największym stopniu aktywnie wspierać, a nie utrudniać, realizację innych uzasadnionych interesów (takich jak gospodarka europejska, bezpieczeństwo obywateli i rozliczalność rządów),

— ogólne zasady ochrony danych powinny, lecz nie mogą zostać zmienione,

— dalsza harmonizacja powinna stanowić jeden z głównych celów tego przeglądu,

— środkiem ciężkości procesu przeglądu powinna stać się perspektywa praw podstawowych. Celem praw podstawowych jest ochrona obywateli w każdych okolicznościach,

— nowe narzędzie prawne musi obejmować policję i wymiar sprawiedliwości,

— nowe narzędzie prawne należy sformułować w sposób jak najbardziej neutralny z technologicznego punktu widzenia, musi ono też gwarantować pewność prawa w długim horyzoncie czasowym.

ELEMENTY NOWYCH RAM

Harmonizacja i uproszczenie

171. EIOD z zadowoleniem przyjmuje zobowiązanie Komisji do przeanalizowania środków do osiągnięcia dalszej harmonizacji ochrony danych na szczeblu UE. EIOD określa obszary, w których należy pilnie przeprowadzić dalszą, lepszą harmonizację: są to definicje, podstawy przetwarzania danych, prawa osób, których dane dotyczą, przekazywanie międzynarodowe i organy ochrony danych.

172. EIOD sugeruje rozważenie następujących alternatyw uproszczenia lub ograniczenia zakresu wymogów co do zawiadamiania:

— ograniczenia obowiązku zawiadamiania o szczególnych rodzajach operacji przetwarzania wiążących się z określonym ryzykiem,

— prosty obowiązek rejestracji dotyczący administratorów danych (w przeciwieństwie do szerokiego zakresu rejestracji wszystkich operacji przetwarzania danych),

— wprowadzenia standardowego europejskiego formularza zawiadomienia.

173. Według EIOD rozporządzenie, jednolite narzędzie mające bezpośrednie zastosowanie w państwach członkowskich, stanowi najskuteczniejszy środek ochrony prawa podstawowego do ochrony danych, a także osiągnięcia dalszej konwergencji na rynku wewnętrznym.

Wzmocnienie praw osób fizycznych

174. EIOD w pełni popiera zapisy komunikatu, które proponują wzmocnienie praw osób fizycznych. Sugeruje następujące posunięcia:

— w prawie należy zapisać zasadę przejrzystości. Jednak jeszcze ważniejsze jest, by wzmacniać istniejące przepisy dotyczące przejrzystości (takie jak obowiązujący art. 10 i 11 dyrektywy 95/46/WE),

— do ogólnego narzędzia prawnego należy wprowadzić zapis o zawiadamianiu o naruszeniu przepisów dotyczących danych osobowych, który rozszerzałby obowiązek niektórych usługodawców, o którym mowa w zrewidowanej dyrektywie o prywatności i łączności elektronicznej, o wszystkich administratorów danych,

— należy jasno sprecyzować granice zgody. Należy rozważyć rozszerzenie katalogu przypadków, gdy wymagana jest jednoznaczna zgoda, a także wprowadzenie dodatkowych zasad dla otoczenia internetowego,

— należy wprowadzić dodatkowe prawa, takie jak przenoszalność danych i prawo do bycia zapomnianym, zwłaszcza w zakresie internetowych usług społeczeństwa informacyjnego,

— interes dzieci byłby lepiej chroniony dzięki dodatkowym zapisom dotyczącym konkretnie zbierania i dalszego przetwarzania danych dzieci,

— zaleca się wprowadzenie mechanizmów przyznawania odszkodowań zbiorowych za naruszenie zasad ochrony prywatności do prawodawstwa UE celem umożliwienia wszczynania postępowań odszkodowawczych w imieniu grup ofiar przez kompetentne podmioty.

Wzmocnienie obowiązków organizacji/ administratorów

175. Nowe ramy muszą zawierać bodźce dla administratorów danych, aby aktywnie włączali środki ochrony danych do procesów biznesowych. EIOD proponuje wprowadzenie ogólnych zapisów dotyczących rozliczalności i „uwzględniania ochrony prywatności w fazie projektowania". Należy także stworzyć zapis dotyczący systemów certyfikacji w zakresie prywatności.

Globalizacja i prawo właściwe

176. EIOD popiera ambitne prace prowadzone w ramach międzynarodowej konferencji rzeczników ochrony danych mające na celu rozwinięcie tzw. „standardów madryckich" celem zintegrowania ich w jeden wiążący instrument i być może zainicjowania międzyrządowej konferencji. EIOD wzywa Komisję, aby podjęła w tym celu konkretne działania w ścisłej współpracy z OECD i Radą Europy.

177. Nowe narzędzie prawne musi jasno precyzować kryteria ustalania właściwego prawa. Powinno w pierwszym rzędzie gwarantować, że przepisy UE mają zastosowanie, gdy dane osobowe przetwarzane są poza granicami Unii, lecz istnieje uzasadniona potrzeba stosowania tychże przepisów. Jeżeli ramy prawne przyjęłyby formę rozporządzenia, we wszystkich państwach członkowskich obowiązywałyby identyczne reguły i ustalenie właściwego prawa (w ramach UE) stałoby się kwestią drugorzędną.

178. EIOD w pełni popiera cel, jakim jest zagwarantowanie jednolitego i spójnego podejścia do krajów trzecich i organizacji międzynarodowych. Wiążące Reguły Korporacyjne (BCR) powinny zostać włączone do wspomnianego narzędzia prawnego.

Obszar policji i wymiaru sprawiedliwości

179. Kompleksowy instrument obejmujący policję i wymiar sprawiedliwości nie wyklucza jednak wprowadzania specjalnych zasad, które w odpowiedni sposób uwzględniałyby specyficzny charakter tego sektora zgodnie z deklaracją nr 21 dołączoną do traktatu lizbońskiego. Należy ustanowić szczególne zabezpieczenia, aby zrekompensować osobom, których dane dotyczą, bardziej wnikliwe przetwarzanie danych zapewniając im dodatkową ochronę.

180. Nowe ramy prawne powinny być – w miarę możliwości – jasne, proste i spójne. Należy unikać dużej liczby różnych systemów mających zastosowanie np. do Europolu, Eurojustu, SIS czy Prüm. EIOD rozumie, że ujednolicenie zasad obowiązujących różne systemy wymagałoby pracy, którą trzeba wykonywać precyzyjnie i stopniowo.

Organy ochrony danych i ich współpraca

181. EIOD w pełni popiera cel Komisji, jakim jest rozwiązanie problemu statusu organów ochrony danych, poprawa ich niezależności, zasobów i uprawnień w zakresie egzekucji prawa. Zaleca on:

— jaśniejsze określenie kluczowej kwestii niezależności organów ochrony danych w ramach nowego narzędzia prawnego, zgodnie z zaleceniami ETS,

— uwzględnienie w zapisach, że organy ochrony danych muszą dysponować wystarczającymi zasobami,

— udzielenie władzom zharmonizowanych uprawnień śledczych i karnych.

182. EIOD sugeruje wprowadzenie dalszych ulepszeń w zakresie funkcjonowania grupy roboczej art. 29, jej infrastruktury i niezależności. Grupie roboczej należy zapewnić wystarczające zasoby, a także wzmocniony sekretariat.

183. EIOD sugeruje wzmocnienie roli grupy roboczej związanej z doradztwem poprzez wprowadzenie obowiązku organów ochrony danych i Komisji, *aby w jak największym stopniu uwzględniać opinie i wspólne stanowiska* przyjęte przez grupę roboczą. EIOD nie popiera nadania mocy wiążącej stanowiskom grupy roboczej, zwłaszcza z uwagi na niezależność poszczególnych organów ochrony danych. EIOD zaleca Komisji wprowadzenie przepisów szczególnych mających na celu wzmocnienie jej współpracy z EIOD w ramach nowego narzędzia prawnego.

184. EIOD wzywa Komisję, aby jak najszybciej zajęła stanowisko w sprawie nadzoru nad organami UE i wielkoskalowymi systemami informatycznymi, uwzględniając fakt, że wszystkie organy nadzoru powinny spełniać niezbędne kryteria niezależności, wystarczających zasobów i uprawnień w zakresie egzekwowania prawa. Należy także zagwarantować właściwą reprezentację perspektywy UE. EIOD popiera model skoordynowanego nadzoru.

Ulepszenia dotychczasowego systemu:

185. EIOD zachęca Komisję do:

— dalszego monitorowania przestrzegania przez państwa członkowskie dyrektywy 95/46/WE i odpowiedniego korzystania z uprawnień nadanych jej na mocy art. 258 TFUE,

— wspierania egzekucji prawa na szczeblu krajowym i jej koordynacji,

— aktywnego włączania zasad ochrony danych do nowych przepisów, które mogą mieć bezpośredni lub pośredni wpływ na ochronę danych,

— realizacji dalszej aktywnej współpracy pomiędzy rozmaitymi podmiotami na szczeblu międzynarodowym.

Sporządzono w Brukseli dnia 14 stycznia 2011 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych