OPINIE

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych w sprawie komunikatu Komisji do Parlamentu Europejskiego i Rady – „Unijna polityka przeciwdziałania terroryzmowi: najważniejsze osiągnięcia i nadchodzące wyzwania"

(2011/C 56/02)

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:

I. WPROWADZENIE

1. W dniu 20 lipca 2010 r. Komisja przyjęła komunikat zatytułowany „Unijna polityka przeciwdziałania terroryzmowi: najważniejsze osiągnięcia i nadchodzące wyzwania" ([3]). Komunikat ma na celu zapewnienie „najważniejszych elementów politycznej oceny obecnej strategii UE w dziedzinie walki z terroryzmem", a także stanowi składnik strategii bezpieczeństwa wewnętrznego ([4]). Zawiera ocenę dotychczasowych osiągnięć oraz zarysowuje nadchodzące wyzwania i kierunki polityki UE w zakresie przeciwdziałania terroryzmowi.

2. Wiele spośród inicjatyw wspomnianych w komunikacie było już tematem odnośnych opinii lub uwag EIOD. Jednakże przedmiotowy komunikat prezentuje szeroką perspektywę polityczną i długoterminową orientację, co uzasadnia wydanie przez EIOD specjalnej opinii.

3. Niniejsza opinia ma zatem za zadanie wniesienie wkładu w bardziej fundamentalne wybory polityczne w dziedzinie, w której wykorzystanie danych osobowych jednocześnie ma zasadnicze znaczenie, odbywa się na wielką skalę i wiąże się ze szczególnymi zagrożeniami.

4. Opinia nie zawiera uwag dotyczących najnowszego komunikatu Komisji odnoszącego się do tej dziedziny, „Strategia bezpieczeństwa wewnętrznego UE w działaniu: pięć kroków w kierunku bezpieczniejszej Europy", przyjętego dnia 22 listopada 2010 r. ([5]) EIOD przeanalizuje wspomniany komunikat w osobnej opinii, w której również ponownie odniesie się do potrzeby wyraźnych powiązań między różnymi dokumentami.

5. W niniejszej opinii EIOD analizuje różne elementy komunikatu, jednocześnie przedstawiając porady i zalecenia mające na celu zagwarantowanie podstawowego prawa do ochrony danych osobowych w obszarze unijnej polityki przeciwdziałania terroryzmowi, zwłaszcza w związku z nadchodzącymi wyzwaniami i ustalaniem nowych kierunków polityki.

II. ANALIZA KOMUNIKATU I ODNOŚNE ZAGADNIENIA OCHRONY DANYCH

6. Opierając się na strukturze strategii UE w dziedzinie walki z terroryzmem z 2005 r., ([6]) w komunikacie w pierwszej kolejności omówiono cztery główne osie unijnej polityki przeciwdziałania terroryzmowi: zapobiegania, ochrony, ścigania i reagowania. Następnie w osobnym oddziale poruszono niektóre kwestie horyzontalne, a mianowicie poszanowania praw podstawowych, współpracy międzynarodowej i finansowania.

([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) 386 wersja ostateczna.
([4]) Zob. s. 2 komunikatu.
([5]) COM(2010) 673 wersja ostateczna.
([6]) Dok. 14469/4/05 z dnia 30 listopada 2005 r.

1. **Zapobieganie, ochrona, ściganie, reagowanie i potrzeba wdrożenia zasad ochrony danych**

7. „Zapobieganie" obejmuje szeroki wachlarz działań, od zapobiegania radykalizacji postaw i rekrutacji po kwestie wykorzystania Internetu do celów związanych z terroryzmem. W tym kontekście jako jedno z głównych osiągnięć prezentuje się w komunikacie decyzję ramową Rady w sprawie zwalczania terroryzmu, przyjętą w 2002 r. ([1]) i zmienioną w 2008 r. ([2]).

8. „Ochrona" ludności oraz infrastruktury to również bardzo szeroka dziedzina, obejmująca inicjatywy w zakresie bezpieczeństwa granic, bezpieczeństwa transportu, kontroli prekursorów materiałów wybuchowych, ochrony infrastruktury krytycznej i poprawy bezpieczeństwa łańcucha dostaw.

9. „Ściganie" obejmuje gromadzenie informacji, współpracę policyjną i sądową oraz zwalczanie działalności terrorystycznej i finansowania terroryzmu. Nadchodzące wyzwania w tym sektorze to ustanowienie ram unijnych w zakresie przetwarzania danych dotyczących przelotu pasażera ([3]), wykorzystanie art. 75 TFUE w celu opracowania ramowych zasad zamrażania funduszy i aktywów finansowych, a także wzajemne uznawanie pozyskanych dowodów w sprawach karnych.

10. „Reagowanie" odnosi się do zdolności do reagowania na skutki ataków terrorystycznych i obejmuje pomoc ofiarom terroryzmu.

11. Wszystkie te obszary wykazują ścisłe powiązania z inicjatywami, w odniesieniu do których EIOD zajął już stanowisko: z programem sztokholmskim, środkami ograniczającymi i zamrażaniem aktywów, zatrzymywaniem danych, skanerami ciała, prekursorami broni, danymi biometrycznymi, decyzją z Prüm, danymi dotyczącymi przelotu pasażera, umową w sprawie programu śledzenia środków finansowych należących do terrorystów, systemem informacyjnym Schengen, wizowym systemem informacyjnym, zintegrowanym zarządzaniem granicami, strategią UE w zakresie zarządzania informacjami oraz transgraniczną wymianą dowodów.

12. Z różnych względów z perspektywy ochrony danych największą wrażliwością cechują się obszary „zapobiegania" i „ochrony".

13. Po pierwsze, w tych obszarach z definicji konieczne jest zastosowanie analizy potencjalnego ryzyka, co w większości przypadków prowadzi do odbywającego się na dużą skalę „zapobiegawczego" przetwarzania dużych ilości danych osobowych dotyczących niepodejrzanych obywateli (np. kontrola Internetu, e-granice i skanery ciała).

14. Po drugie, komunikat przewiduje wzmocnienie partnerstw między organami ścigania a prywatnymi przedsiębiorstwami (takimi jak dostawcy usług internetowych, instytucje finansowe i spółki transportowe) w celu wymiany istotnych informacji i niekiedy „delegowania" do nich niektórych elementów zadań w zakresie ścigania. Pociąga to za sobą bardziej intensywne wykorzystanie przez władze publiczne, do celów ścigania, danych osobowych gromadzonych przez prywatne przedsiębiorstwa w celach handlowych.

15. Wiele z tych inicjatyw podjęto, często w szybkiej reakcji na akty terroru, bez dokładnego uwzględnienia możliwego powielania lub duplikowania już istniejących środków. W niektórych przypadkach nawet kilka lat po ich wejściu w życie nie ustalono, w jakim stopniu ingerencja w prywatność obywateli wynikająca z tych środków była naprawdę konieczna.

16. Ponadto istnieje większe prawdopodobieństwo, że „zapobiegawcze" wykorzystanie danych osobowych doprowadzi do dyskryminacji. Zapobiegawcza analiza informacji pociągałaby za sobą gromadzenie i przetwarzanie danych osobowych dotyczących szerokiej gamy kategorii osób fizycznych (np. wszystkich pasażerów, wszystkich użytkowników Internetu) bez względu na to, czy ciążą na nich jakieś konkretne podejrzenia. Analiza tych danych, zwłaszcza w połączeniu z technikami eksploracji danych, może poskutkować rzuceniem podejrzenia na niewinne osoby tylko dlatego, że ich profil (wiek, płeć, wyznanie itd.) lub wzorce zachowań (np. w zakresie podróży, korzystania z Internetu itd.) odpowiadają profilowi lub wzorcom zachowań osób mających związki z terroryzmem lub podejrzewanych o takie związki. Dlatego też, zwłaszcza w tym kontekście, niezgodne z prawem lub nieprawidłowe wykorzystanie (niekiedy szczególnie chronionych) danych osobowych w połączeniu z szerokimi uprawnieniami do stosowania środków przymusu, którymi dysponują organy ścigania, może prowadzić do dyskryminacji i piętnowania określonych osób lub grup osób.

17. Z tego punktu widzenia zapewnienie wysokiego poziomu ochrony danych stanowi również wkład w zwalczanie rasizmu, ksenofobii i dyskryminacji, a zatem, zgodnie z komunikatem, może również „przyczynić się (...) do zapobiegania radykalizacji postaw i rekrutacji terrorystów".

2. **Spójne podejście oparte na zasadzie konieczności**

18. Ważna uwaga ogólna dotyczy potrzeby zapewnienia spójności i wyraźnych powiązań między wszystkimi komunikatami i inicjatywami w dziedzinie spraw wewnętrznych, w szczególności w obszarze bezpieczeństwa wewnętrznego. Na przykład mimo że strategia UE w dziedzinie walki z terroryzmem jest ściśle powiązana ze strategią w zakresie zarządzania informacjami, strategią dotyczącą Karty praw podstawowych i europejskim modelem wymiany informacji, związki między wszystkimi odpowiednimi dokumentami nie są wyraźnie ani kompleksowo

([1]) 2002/475/WSiSW (Dz.U. L 164 z 22.6.2002, s. 3).
([2]) 2008/919/WSiSW (Dz.U. L 330 z 9.12.2008, s. 21).
([3]) Zapowiedzianych również w przedstawionym przez Komisję planie działań służących realizacji programu sztokholmskiego, COM(2010) 171 wersja ostateczna z dnia 20 kwietnia 2010 r.

przedstawione. Stało się to jeszcze bardziej oczywiste po przyjęciu w dniu 22 listopada 2010 r. komunikatu „Strategia bezpieczeństwa wewnętrznego UE w działaniu: pięć kroków w kierunku bezpieczniejszej Europy [1]".

19. EIOD zaleca zatem instytucjom UE, aby zapewniły przygotowanie i wprowadzenie w życie polityki oraz inicjatyw w dziedzinie spraw wewnętrznych w sposób gwarantujący spójne podejście i wyraźne powiązania między nimi, co umożliwi osiągnięcie odpowiednich i pozytywnych efektów synergicznych oraz zapobiegnie powielaniu pracy i wysiłków.

20. Ponadto EIOD zaleca, aby każda propozycja w tej dziedzinie w sposób wyraźny uwzględniała zasadę konieczności. W tym celu należy brać pod uwagę potencjalne przypadki powielania już istniejących instrumentów oraz ograniczyć gromadzenie i wymianę danych osobowych do zakresu naprawdę niezbędnego do realizowanych celów.

21. Na przykład w przypadku zawartej ze Stanami Zjednoczonymi umowy w sprawie programu śledzenia środków finansowych należących do terrorystów (TFTP II), EIOD zakwestionował jej rzeczywistą niezbędność dla osiągnięcia wyników, które można uzyskać, stosując instrumenty mniej naruszające prywatność, takie jak instrumenty określone już unijnymi i międzynarodowymi przepisami ramowymi [2]. W tej samej opinii EIOD zakwestionował konieczność masowego przesyłania danych osobowych zamiast przekazywania ich w bardziej ukierunkowany sposób.

22. W komunikacie jako jedno z wyzwań wymienia się „dopilnowanie, aby te instrumenty odpowiadały rzeczywistym potrzebom (w zakresie ścigania) przy jednoczesnym pełnym poszanowaniu prawa do prywatności i zasad ochrony danych". EIOD z zadowoleniem przyjmuje wyraźne uznanie tego wyzwania oraz wzywa instytucje UE do przeprowadzenia dokładnej oceny, w jakim stopniu instrumenty zarówno już wdrożone, jak i przewidywane, odpowiadają faktycznym potrzebom w zakresie ścigania, przy jednoczesnym unikaniu powielania środków bądź zbędnych ograniczeń życia prywatnego. W związku z tym istniejące instrumenty należy poddawać okresowym przeglądom w celu weryfikacji, czy stanowią one skuteczne sposoby zwalczania terroryzmu.

23. W licznych opiniach i uwagach EIOD podkreśla potrzebę dokonania oceny wszystkich istniejących instrumentów w zakresie wymiany informacji przed przedstawieniem propozycji dotyczących nowych instrumentów, a szczególny nacisk położył na to w niedawnej opinii dotyczącej komunikatu „Przegląd zarządzania informacjami w przestrzeni wolności, bezpieczeństwa i sprawiedliwości" [3]. Ocena skuteczności istniejących środków przy ustalaniu wpływu przewidywanych nowych środków na prywatność ma bowiem zasadnicze znaczenie, a istotną rolę powinno odgrywać pod tym względem działanie Unii Europejskiej, zgodnie z podejściem zaproponowanym w programie sztokholmskim.

24. Stwierdzenie powielania oraz braku skuteczności powinno skutkować korektami w wyborach politycznych lub nawet konsolidacją bądź odrzuceniem istniejących systemów gromadzenia i przetwarzania danych.

25. EIOD zaleca zwrócenie szczególnej uwagi na propozycje, które prowadziłyby do powszechnego gromadzenia danych osobowych wszystkich obywateli, a nie tylko podejrzanych. Szczególnie dokładne rozpatrzenie i uzasadnienie powinno być wymagane także w tych sytuacjach, w których przewiduje się przetwarzanie danych osobowych do celów innych niż cele, do których je początkowo zgromadzono, jak ma to np. miejsce w przypadku wykorzystania do celów ścigania danych przechowywanych w systemie Eurodac.

26. W komunikacie podkreślono również, że jednym z nadchodzących wyzwań będzie zapewnienie skuteczności polityki badań nad bezpieczeństwem, co pozwoliłoby na osiągnięcie wyższego poziomu bezpieczeństwa. EIOD popiera znajdujące się w komunikacie stwierdzenie, że skuteczne badania nad bezpieczeństwem powinny wzmacniać powiązania między różnymi podmiotami. W tym kontekście podstawowe znaczenie ma wykorzystanie specjalistycznej wiedzy w zakresie ochrony danych na bardzo wczesnym etapie badań nad bezpieczeństwem, co umożliwi ukierunkowanie wariantów strategicznych i zagwarantuje uwzględnienie prywatności w maksymalnym możliwym stopniu w nowych, zorientowanych na bezpieczeństwo technologiach, zgodnie z zasadą „poszanowania prywatności od samego początku".

3. **Zastosowanie środków ograniczających (zamrażanie aktywów)**

27. W odniesieniu do zastosowania środków ograniczających (zamrażanie aktywów) wobec niektórych krajów oraz osób podejrzanych o terroryzm, orzecznictwo Trybunału Sprawiedliwości wielokrotnie i konsekwentnie potwierdzało zasadnicze znaczenie poszanowania praw podstawowych w walce z terroryzmem, co wynika z potrzeby zapewnienia zarówno przestrzegania praw obywateli, jak i zgodności podejmowanych środków z prawem.

28. EIOD przedstawiał już opinie i uwagi dotyczące tej dziedziny [4], z jednej strony podkreślając usprawnienia w procedurach, ale z drugiej strony wzywając do dalszych udoskonaleń, zwłaszcza w odniesieniu do prawa do informacji oraz do dostępu do danych osobowych, jasnego

[1] Zob. ust. 4 niniejszej opinii.
[2] Opinia EIOD z dnia 22 czerwca 2010 r.
[3] Opinia EIOD z dnia 30 września 2010 r.

[4] Opinia z dnia 28 lipca 2009 r. w sprawie wniosku dotyczącego rozporządzenia Rady zmieniającego rozporządzenie Rady (WE) nr 881/2002 wprowadzające niektóre szczególne środki ograniczające skierowane przeciwko niektórym osobom i podmiotom związanym z Osamą bin Ladenem, siecią Al-Kaida i talibami, (Dz.U. C 276 z 17.11.2009, s. 1). Opinia z dnia 16 grudnia 2009 r. na temat różnych wniosków ustawodawczych nakładających określone środki ograniczające wobec Somalii, Zimbabwe, Korei Północnej oraz Gwinei, (Dz.U. C 73 z 23.3.2010, s. 1). Zob. także pismo EIOD z dnia 20 lipca 2010 r. w sprawie trzech wniosków ustawodawczych dotyczących niektórych środków ograniczających, mianowicie dotyczącego p. Milosevica i osób powiązanych z nim, wspierającego mandat Międzynarodowego Trybunału Karnego dla byłej Jugosławii oraz dotyczącego Erytrei. Wszystkie opinie i uwagi EIOD są dostępne na stronach internetowych EIOD, pod adresem http://www.edps.europa.eu

zdefiniowania ograniczeń dotyczących tych praw, a także dostępności skutecznych sądowych środków odwoławczych i niezależnego nadzoru.

29. Potrzebę dalszego udoskonalenia procedur i środków ochronnych dostępnych osobom umieszczonym na liście potwierdził niedawno Trybunał w tzw. sprawie „Kadi II" ([1]). W szczególności Trybunał podkreślił konieczność dokładnego informowania takich osób o powodach umieszczenia ich na liście. Jest to kwestia bardzo zbliżona do zagadnienia praw, wynikających z przepisów o ochronie danych, do dostępu do własnych danych osobowych i do ich poprawienia, zwłaszcza kiedy są nieprawidłowe lub nieaktualne. Te prawa, wyraźnie wymienione w art. 8 Karty praw podstawowych, stanowią zasadnicze elementy ochrony danych i mogą podlegać ograniczeniom jedynie w zakresie, w jakim takie ograniczenia są niezbędne, przewidywalne i określone prawnie.

30. W tym kontekście EIOD zgadza się z komunikatem, że jednym z nadchodzących wyzwań w dziedzinie polityki przeciwdziałania terroryzmowi będzie zastosowanie art. 75 TFUE. Ta nowa podstawa prawna, wprowadzona traktatem lizbońskim, w szczególności pozwala na stosowanie wobec osób fizycznych lub prawnych środków polegających na zamrożeniu aktywów. EIOD zaleca wykorzystanie tej podstawy prawnej także do ustanowienia zasad ramowych zamrażania aktywów w sposób zapewniający pełne poszanowanie praw podstawowych. EIOD może nadal wnosić wkład w rozwój odpowiednich instrumentów prawnych i procedur oraz ma nadzieję, że będzie należycie i terminowo konsultowany w związku z opracowaniem przez Komisję, zgodne z jej programem prac na 2011 r., specjalnych regulacji w tej dziedzinie ([2]).

31. W szerszej perspektywie potrzebne jest ustanowienie systemu ramowego ochrony danych mającego zastosowanie również do wspólnej polityki zagranicznej i bezpieczeństwa. Artykuł 16 TFUE zapewnia bowiem podstawę prawną dla określenia zasad ochrony danych także w tej dziedzinie. Odmienna podstawa prawna i procedura ustanowione w art. 39 TUE będą mieć zastosowanie tylko w przypadkach przetwarzania danych osobowych w tej dziedzinie przez państwa członkowskie. Jednak nawet jeśli traktat lizboński wzywa do wprowadzenia takich zasad ochrony danych i dostarcza narzędzia do ich ustanowienia, w niedawnym komunikacie „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej" ([3]) nie przewiduje się żadnej inicjatywy na chwilę obecną. W tym kontekście EIOD apeluje do Komisji o przedstawienie propozycji dotyczącej ram ochrony danych w dziedzinie wspólnej polityki zagranicznej i bezpieczeństwa.

([1]) Wyrok z dnia 30 września 2010 r. w sprawie T-85/09 *Kadi przeciwko Komisji*, patrz w szczególności ust. 157 i 177.

([2]) W programie prac Komisji na 2011 r. (COM(2010) 623 z 27.10.2010) wspomniano w załączniku II (Orientacyjna lista branych pod uwagę inicjatyw) „regulację ustanawiającą procedurę zamrażania funduszy osób podejrzewanych o działalność terrorystyczną w UE".

([3]) Komunikat Komisji (2010) 609 z dnia 4 listopada 2010 r.

4. **Poszanowanie praw podstawowych i współpraca międzynarodowa**

32. W rozdziale poświęconym poszanowaniu praw podstawowych podkreślono, że UE musi dawać przykład pod względem przestrzegania Karty praw podstawowych, która musi przyświecać wszystkim strategiom politycznym UE. EIOD przyjmuje to podejście z zadowoleniem.

33. Ponadto EIOD popiera stwierdzenie, że przestrzeganie praw podstawowych to nie tylko obowiązek wynikający z przepisów prawnych, ale również główny warunek promowania wzajemnego zaufania między organami krajowymi oraz zaufania społecznego.

34. W tym kontekście EIOD zaleca aktywne podejście i konkretne działania umożliwiające osiągnięcie tego celu, także jako środka skutecznego wprowadzenia w życie Karty praw podstawowych UE ([4]).

35. W przypadku wszystkich inicjatyw mających wpływ na ochronę danych osobowych, niezależnie od ich inicjatora i dziedziny, w której się je proponuje, należy zagwarantować dokonanie oceny wpływu na prywatność i przeprowadzenie na wczesnym etapie konsultacji z właściwymi organami ochrony danych.

36. W rozdziale komunikatu dotyczącym współpracy międzynarodowej podkreślono również potrzebę stworzenia „koniecznych warunków prawnych i politycznych dla zacieśnienia współpracy z partnerami zewnętrznymi UE w dziedzinie zwalczania terroryzmu".

37. W związku z tym EIOD przypomina o potrzebie zapewnienia stosowania odpowiednich środków ochronnych przy wymianie danych osobowych z państwami trzecimi i organizacjami międzynarodowymi, co ma zagwarantować należyte przestrzeganie praw obywateli w zakresie ochrony danych także w kontekście współpracy międzynarodowej.

38. Chodzi tu także o promowanie ochrony danych we współpracy z państwami trzecimi i organizacjami międzynarodowymi w celu zapewnienia zgodności z normami UE. Odpowiada to również zamiarowi Komisji dotyczącemu rozwoju wysokich standardów prawnych i technicznych ochrony danych w państwach trzecich i na poziomie międzynarodowym oraz usprawnienia współpracy z państwami trzecimi ([5]).

([4]) Zob. komunikat Komisji (2010) 573 z dnia 19 października 2010 r. w sprawie strategii skutecznego wprowadzania w życie Karty praw podstawowych przez Unię Europejską.

([5]) Zob. komunikat (2010) 609 „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej", s. 16–17.

39. Oczywistą możliwość podjęcia działań w tym zakresie zapewniają Unii Europejskiej środki ograniczające (zamrażanie aktywów), w przypadku których intensywność współpracy z państwami trzecimi i Organizacją Narodów Zjednoczonych nie powinna obniżać wysokiego poziomu ochrony praw podstawowych, jaki zapewnia system prawny UE.

III. **WNIOSKI**

40. EIOD z zadowoleniem przyjmuje uwagę, jaką w komunikacie poświęca się prawom podstawowym i ochronie danych oraz zaleca dalsze konkretne udoskonalenia w dziedzinie polityki przeciwdziałania terroryzmowi.

41. EIOD zaleca wspieranie konkretnymi inicjatywami poszanowania praw podstawowych w tej dziedzinie, a w szczególności prawa do ochrony danych osobowych, które jest niezbędne dla promowania pewności prawa, zaufania i współpracy w walce z terroryzmem, a także stanowi niezbędny warunek prawny dla rozwoju przewidywanych systemów.

42. EIOD popiera również podejście, zgodnie z którym w tej dziedzinie preferowany powinien być raczej systematyczny proces kształtowania polityki niż podejmowanie decyzji politycznych zależnie od poszczególnych zdarzeń, zwłaszcza kiedy w związku z takimi zdarzeniami nowe systemy przechowywania, gromadzenia i wymiany danych są tworzone bez odpowiedniej oceny dostępnych alternatyw.

43. W tym kontekście EIOD zaleca instytucjom UE przygotowywanie i wprowadzanie w życie polityki oraz inicjatyw w dziedzinie spraw wewnętrznych w sposób gwarantujący spójne podejście i wyraźne powiązania między nimi, co umożliwi osiągnięcie odpowiednich i pozytywnych efektów synergicznych oraz zapobiegnie powielaniu pracy i wysiłków.

44. W związku z tym EIOD zaleca prawodawcy UE położenie większego nacisku na ochronę danych poprzez zaangażowanie się w konkretne działania (z ustalonymi terminami), takie jak:

— ocena skuteczności już stosowanych środków, przy czym zasadnicze znaczenie ma uwzględnienie ich wpływu na prywatność, a istotną rolę powinno odgrywać pod tym względem działanie Unii Europejskiej,

— przy planowaniu nowych środków – uwzględnianie potencjalnych przypadków powielania już istniejących instrumentów, w tym ocena ich skuteczności, oraz ograniczenie gromadzenia i wymiany danych osobowych do zakresu naprawdę niezbędnego do realizowanych celów,

— przedstawienie projektu ustanowienia systemu ramowego ochrony danych mającego zastosowanie również do wspólnej polityki zagranicznej i bezpieczeństwa,

— zaproponowanie w dziedzinie środków ograniczających (zamrażanie aktywów) kompleksowego i globalnego podejścia gwarantującego zarówno skuteczność ścigania, jak i poszanowanie praw podstawowych, na podstawie art. 75 TFUE,

— przy przedstawianiu odnośnych wniosków dotyczących tej dziedziny – potraktowanie ochrony danych jako kluczowego zagadnienia w debacie dotyczącej podejmowanych środków, np. poprzez zagwarantowanie dokonania ocen wpływu na prywatność i ochronę danych oraz przeprowadzania w odpowiednim terminie konsultacji z właściwymi organami ochrony danych,

— zapewnienie wykorzystania specjalistycznej wiedzy w zakresie ochrony danych na bardzo wczesnym etapie badań nad bezpieczeństwem, co umożliwi ukierunkowanie wariantów strategicznych i zagwarantuje uwzględnienie prywatności w maksymalnym możliwym stopniu w nowych, zorientowanych na bezpieczeństwo technologiach,

— zapewnienie odpowiednich środków ochronnych przy przetwarzaniu danych osobowych w kontekście współpracy międzynarodowej, przy jednoczesnym promowaniu rozwoju i wprowadzaniu w życie zasad ochrony danych przez państwa trzecie i organizacje międzynarodowe.

Sporządzono w Brukseli dnia 24 listopada 2010 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych