Opinia Europejskiego Inspektora Ochrony Danych dotycząca komunikatu Komisji do Parlamentu Europejskiego i Rady – „Strategia bezpieczeństwa wewnętrznego UE w działaniu: pięć kroków w kierunku bezpieczniejszej Europy"

(2011/C 101/02)

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 wniosek o wydanie opinii zgodnie z rozporządzeniem (WE) nr 45/2001 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. Dnia 22 listopada 2010 r. Komisja przyjęła komunikat zatytułowany „Strategia bezpieczeństwa wewnętrznego UE w działaniu: pięć kroków w kierunku bezpieczniejszej Europy" (zwany dalej „Komunikatem") ([3]). Został on przekazany do EIOD do konsultacji.

2. EIOD z zadowoleniem przyjmuje fakt, że Komisja się z nim skonsultowała. Jeszcze przed przyjęciem komunikatu EIOD przedstawił nieformalne uwagi do jego projektu. Niektóre z nich uwzględniono w wersji ostatecznej komunikatu.

Kontekst komunikatu

3. Strategia bezpieczeństwa wewnętrznego UE (zwana dalej „strategią ISS" – ang. *Internal Security Strategy*), której dotyczy komunikat, przyjęta została dnia 23 lutego 2010 r. w czasie hiszpańskiej prezydencji ([4]). Opisuje ona europejski model bezpieczeństwa, który łączy w sobie m.in. działania w zakresie współpracy policyjnej i sądowej, zarządzanie granicami i ochronę ludności oraz poszanowanie wspólnych wartości europejskich, takich jak prawa podstawowe. Jej głównymi celami są:

   — przedstawienie społeczeństwu istniejących unijnych narzędzi, które pomagają zagwarantować bezpieczeństwo i wolność obywateli UE, oraz wartość dodaną, jaką generuje działanie UE w tej dziedzinie;

   — dalszy rozwój wspólnych narzędzi i kierunków polityki w ramach bardziej zintegrowanego podejścia, które obejmuje nie tylko skutki braku bezpieczeństwa, lecz także jego przyczyny;

   — wzmocnienie współpracy policyjnej i sądowej, zarządzania granicami, ochrony ludności oraz zarządzania katastrofami.

4. Celem strategii ISS jest zwalczanie najbardziej naglących zagrożeń i wyzwań dla bezpieczeństwa UE, takich jak poważna i zorganizowana przestępczość, terroryzm i cyberprzestępczość, zarządzanie zewnętrznymi granicami UE oraz budowanie odporności na klęski żywiołowe i katastrofy wywołane przez działalność człowieka. Strategia zapewnia ogólne wytyczne, zasady i kierunki dotyczące tego, jak Unia powinna reagować na wspomniane kwestie i wzywa Komisję do zaproponowania określonych czasowo działań mających na celu jej wdrożenie.

5. Ponadto ważne jest, aby w tym kontekście odnieść się do najnowszych konkluzji Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych w sprawie opracowania i realizacji cyklu polityki unijnej dotyczącej poważnej i zorganizowanej przestępczości międzynarodowej przyjętych w dniach 8-9 listopada 2010 r. ([5]) (zwanych dalej „konkluzjami z listopada 2010 r."). Dokument ten następuje po konkluzjach Rady w sprawie architektury bezpieczeństwa wewnętrznego z 2006 r. ([6]). Wzywa on Radę i Komisję do zdefiniowania kompleksowej strategii ISS opartej na wspólnych wartościach i zasadach UE potwierdzonych przez Kartę praw podstawowych Unii Europejskiej ([7]).

([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) 673 wersja ostateczna.
([4]) Dokument 5842/2/10.
([5]) 3043. posiedzenie Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych, 8-10 listopada 2010 r., Bruksela.
([6]) Dokument 7039/2/06 JAI 86 CATS 34.
([7]) Cykl polityki unijnej dotyczącej poważnej i zorganizowanej przestępczości międzynarodowej, o którym mowa w konkluzjach z listopada 2010 r., składa się z 4 etapów: 1) opracowanie polityki na podstawie oceny zagrożenia poważną i zorganizowaną przestępczością w Unii Europejskiej (EU SOCTA – European Union Serious and Organised Crime Threat Assessment), 2) realizacja polityki i podejmowanie decyzji na podstawie ograniczonej liczby priorytetów, które zostaną określone przez Radę, 3) wdrażanie i monitorowanie rocznych planów działań operacyjnych (OAP), oraz 4) pod koniec danego cyklu polityki przeprowadzona zostanie szczegółowa ocena, która posłuży jako wkład w kolejny cykl.

6. Spośród kierunków i celów, które powinny być motorami wdrażania strategii ISS, konkluzje z listopada 2010 r. odnoszą się do refleksji nad podejściem proaktywnym i opartym na informacjach, ścisłej współpracy pomiędzy unijnymi agencjami, łącznie z dalszą poprawą jakości wymiany informacji, oraz do celu, jakim jest uświadamianie obywatelom istotności pracy wykonywanej przez Unię celem zapewnienia im ochrony. Konkluzje wzywają także Komisję do utworzenia Wieloletniego Planu Strategicznego (dalej: WPS) dla każdego z priorytetów, definiującego najbardziej odpowiednią strategię podejścia do problemu, we współpracy z ekspertami z odpowiednich agencji i państw członkowskich. Wzywają one także Komisję do stworzenia niezależnego mechanizmu oceny wdrażania WPS w drodze konsultacji z państwami członkowskimi i ekspertami z agencji unijnych. EIOD porusza te kwestie w dalszej części niniejszej opinii, gdyż są one ściśle powiązane z ochroną danych osobowych, prywatnością i innymi związanymi z nimi prawami i wolnościami podstawowymi lub też mają na nie znaczący wpływ.

Treść i cel komunikatu

7. W komunikacie zawarto 5 celów strategicznych, które związane są z prywatnością i ochroną danych:

   — rozbijanie międzynarodowych siatek przestępczych,

   — zwalczanie terroryzmu i walka z radykalizacją postaw i werbowaniem terrorystów,

   — podniesienie poziomu ochrony obywateli i przedsiębiorstw w cyberprzestrzeni,

   — poprawa bezpieczeństwa poprzez zarządzanie granicami, oraz

   — zwiększenie odporności Europy na kryzysy i katastrofy.

8. Proponowana w ramach komunikatu realizacja strategii bezpieczeństwa wewnętrznego UE w działaniu obejmuje wspólny program dla państw członkowskich, Parlamentu Europejskiego, Komisji, Rady, agencji i innych organów, łącznie z organizacjami społeczeństwa obywatelskiego i władzami lokalnymi; sugeruje również, iż wszystkie te organy powinny w najbliższych 4 latach współpracować, by osiągnąć cele strategii ISS.

9. Komunikat bazuje na traktacie lizbońskim i uznaje wytyczne zawarte w programie sztokholmskim (oraz planie działań), które w rozdziale 4.1 podkreślają potrzebę kompleksowej strategii ISS opartej na poszanowaniu praw podstawowych, ochronie międzynarodowej i praworządności. Ponadto zgodnie z programem sztokholmskim tworzenie, monitorowanie i wdrażanie strategii bezpieczeństwa wewnętrznego powinno stać się jednym z priorytetowych zadań Stałego Komitetu Współpracy Operacyjnej w zakresie Bezpieczeństwa Wewnętrznego (COSI) utworzonego na mocy art. 71 TFUE. Aby zagwarantować skuteczne egzekwowanie strategii ISS, powinna ona obejmować również zagadnienia związane z bezpieczeństwem zintegrowanego zarządzania granicami, a także (w odpowiednich przypadkach) ze współpracą w sprawach kryminalnych podlegających współpracy operacyjnej w dziedzinie bezpieczeństwa wewnętrznego. Należy w tym kontekście wspomnieć również, że program sztokholmski wzywa do zastosowania zintegrowanego podejścia do strategii ISS, które powinno również uwzględniać strategię bezpieczeństwa zewnętrznego stworzoną przez UE, a także inne kierunki polityki unijnej, zwłaszcza dotyczące rynku wewnętrznego.

Cel opinii

10. Komunikat odnosi się do rozmaitych obszarów polityki, które składają sie na „bezpieczeństwo wewnętrzne" Unii Europejskiej w szerokim ujęciu lub też mają na nie wpływ.

11. Celem niniejszej opinii nie jest analiza wszystkich obszarów polityki wraz z poszczególnymi tematami ujętymi w komunikacie, lecz:

   — spojrzenie na cele strategii ISS proponowane w komunikacie z perspektywy prywatności i ochrony danych oraz – z tego punktu widzenia – podkreślenie niezbędnych powiązań z innymi strategiami dyskutowanymi i przyjmowanymi obecnie na poziomie UE;

   — zdefiniowanie pewnej liczby pojęć dotyczących ochrony danych, które należałoby uwzględnić podczas projektowania, tworzenia i wdrażania strategii ISS na poziomie UE;

   — przedstawienie – gdy jest to przydatne i odpowiednie – propozycji jak najlepszego uwzględnienia problemów związanych z ochroną danych przy wdrażaniu działań proponowanych w ramach komunikatu.

12. EIOD pragnie osiągnąć wspomniane cele zwłaszcza poprzez podkreślanie powiązań pomiędzy strategią ISS a strategią w zakresie zarządzania informacjami i pracę nad pełnymi ramami ochrony danych. Ponadto EIOD odnosił się będzie do takich pojęć jak najlepsze dostępne techniki, „uwzględniania ochrony prywatności w fazie projektowania", prywatność i ocena wpływu ochrony danych, a także prawa osoby, której dotyczą dane, które mają bezpośredni wpływ na projektowanie i wdrażanie strategii ISS. W niniejszej opinii zawarto również komentarze dotyczące niektórych wybranych obszarów polityki, takich jak zintegrowane zarządzanie granicami, łącznie z EUROSUR i przetwarzaniem danych osobowych przez FRONTEX, jak również innych dziedzin, takich jak cyberprzestrzeń czy Program śledzenia środków finansowych należących do terrorystów.

II. UWAGI NATURY OGÓLNEJ

Potrzeba bardziej kompleksowego, sprzyjającego włączeniu społecznemu i „strategicznego" podejścia do strategii UE związanych ze strategią ISS

13. Rozmaite strategie unijne opierające się na traktacie lizbońskim i programie sztokholmskim, mające bezpośredni lub pośredni wpływ na ochronę danych, są obecnie omawiane i proponowane na poziomie UE. Strategia ISS jest jedną z nich. Jest ona bezpośrednio powiązana z innymi strategiami (tymi, o których mowa w najnowszych komunikatach Komisji, lub przewidywanymi na najbliższą przyszłość), takimi jak strategia UE w zakresie zarządzania informacjami, europejski model wymiany informacji, strategia wdrażania Karty praw podstawowych Unii Europejskiej, kompleksowa strategia ochrony danych czy unijna polityka przeciwdziałania terroryzmowi. W niniejszej opinii EIOD zwraca szczególną uwagę na powiązania ze strategią w zakresie zarządzania informacjami i kompleksowymi ramami ochrony danych opartymi na art. 16 TFUE, które mają najbardziej oczywiste powiązania ze strategią ISS z punktu widzenia ochrony danych.

14. Wszystkie te strategie tworzą skomplikowaną „mozaikę" powiązanych ze sobą wytycznych dotyczących polityki, programów i planów działań wzywających do stworzenia kompleksowego i zintegrowanego podejścia na poziomie UE.

15. Bardziej ogólnie można stwierdzić, że jeżeli podejście zakładające „łączenie strategii" zostanie włączone do przyszłych działań, to okaże się, że istnieje na poziomie UE wizja *strategii UE*, oraz że strategie te, a także niedawno przyjęte komunikaty je rozszerzające, są ze sobą ściśle powiązane, co jest prawdą, ponieważ program sztokholmski stanowi dla nich wszystkich punkt odniesienia. Skutkowałoby to również pozytywną synergią pomiędzy różnymi kierunkami polityki dotyczącymi obszaru wolności, bezpieczeństwa i sprawiedliwości, pozwoliłoby także uniknąć potencjalnego dublowania prac i wysiłków w tej dziedzinie. Co równie ważne, podejście to prowadziłoby także do bardziej skutecznego i spójnego stosowania zasad ochrony danych w kontekście wszystkich powiązanych ze sobą strategii.

16. EIOD pragnie podkreślić, że jednym z filarów strategii ISS jest skuteczne zarządzanie informacją w Unii Europejskiej, które powinno opierać się na gruncie zasad konieczności i proporcjonalności, aby uzasadnić potrzebę wymiany informacji.

17. Ponadto, jak wspomniano w opinii EIOD dotyczącej komunikatu w sprawie zarządzania informacją ([8]), EIOD podkreśla, że każdy nowy środek ustawodawczy ułatwiający przechowywanie i wymianę danych osobowych powinien być proponowany wyłącznie w oparciu o konkretne dowody potwierdzające jego niezbędność ([9]). Wymóg natury prawnej powinien zostać przy wdrażaniu strategii ISS przekształcony w proaktywne podejście dotyczące polityki. Potrzeba kompleksowego podejścia do strategii ISS wiąże się również w sposób nieunikniony z koniecznością dokonania oceny wszystkich istniejących instrumentów i narzędzi z dziedziny bezpieczeństwa wewnętrznego zanim zaproponowane zostaną nowe.

18. W tym kontekście EIOD pragnąłby zasugerować częstsze stosowanie klauzul gwarantujących okresową ocenę istniejących instrumentów, takich jak te zastosowane w dyrektywie w sprawie zatrzymywania danych, która obecnie podlega ocenie ([10]).

Ochrona danych jako cel strategii ISS

19. Komunikat odwołuje się do ochrony danych osobowych w ustępie „Polityka bezpieczeństwa oparta na wspólnych wartościach", który mówi, że instrumenty i działania na rzecz realizacji strategii ISS muszą opierać się na wspólnych wartościach, do których należą praworządność i poszanowanie praw podstawowych, jak to zostało określone w Karcie praw podstawowych Unii Europejskiej. W tym kontekście stanowi on, że „[w] przypadkach, gdy ma miejsce wymiana informacji służąca egzekwowaniu prawa w UE, musimy zadbać także o ochronę sfery prywatnej osób i ich podstawowego prawa do ochrony danych osobowych".

20. Inspektor przyjmuje tę deklarację z zadowoleniem, lecz w obecnej formie nie może być ona postrzegana jako wystarczająca z punktu widzenia kwestii ochrony danych w ramach strategii ISS. Komunikat nie omawia kwestii ochrony danych w sposób bardziej szczegółowy ([11]), nie objaśnia też w jaki sposób poszanowanie prywatności i ochrona danych osobowych zagwarantowane zostaną w praktyce w ramach działań wdrażających strategię ISS.

([8]) Opinia EIOD z dnia 30 września 2010 r. w sprawie Komunikatu Komisji do Parlamentu Europejskiego i Rady – „Przegląd zarządzania informacjami w przestrzeni wolności, bezpieczeństwa i sprawiedliwości".

([9]) Jest to wymóg prawny; zob. zwłaszcza wyrok Trybunału Sprawiedliwości w sprawach połączonych C-92/09 i C-93/09 z dnia 2 listopada 2010 r. EIOD opowiadał się bardziej konkretnie za tym podejściem w ramach innych opinii dotyczących projektów aktów ustawodawczych powiązanych z przestrzenią swobody, bezpieczeństwa i sprawiedliwości, takich jak np. opinia z dnia 19 października 2005 r. w sprawie trzech wniosków dotyczących systemu informacyjnego Schengen drugiej generacji (SIS II); opinia z dnia 20 grudnia 2007 r. dotycząca projektu wniosku w sprawie ramowej decyzji Rady w sprawie wykorzystania danych dotyczących przelotu pasażera (danych PNR) przez wymiar sprawiedliwości; opinia z dnia 18 lutego 2009 r. dotycząca wniosku w sprawie rozporządzenia dotyczącego ustanowienia systemu „Eurodac" do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (WE) nr […/…] [ustanawiającego kryteria i mechanizmy ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela kraju trzeciego lub bezpaństwowca]; opinia z dnia 18 lutego 2009 r. dotycząca wniosku w sprawie rozporządzenia ustanawiającego kryteria i mechanizmy ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela kraju trzeciego lub bezpaństwowca; oraz opinia z dnia 7 października 2009 w sprawie wniosku dotyczącego dostępu wymiaru sprawiedliwości do EURODAC.

([10]) 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.

([11]) O ochronie danych mowa jest w sposób bardziej szczegółowy w kontekście kwestii przetwarzania danych osobowych przez FRONTEX.

21. W opinii EIOD realizacja strategii bezpieczeństwa wewnętrznego UE w działaniu powinna jako jeden z celów obrać sobie *ochronę* w szerokim znaczeniu tego słowa, aby zagwarantować *odpowiednią* równowagę pomiędzy – z jednej strony – ochroną obywateli przed istniejącymi zagrożeniami, a – z drugiej strony – ochroną ich prywatności i prawa do ochrony danych osobowych. Innymi słowy kwestie bezpieczeństwa i prywatności muszą być traktowane z taką samą powagą w ramach tworzenia strategii ISS, co pozostawałoby w zgodzie z programem sztokholmskim i konkluzjami Rady.

22. Krótko mówiąc, zapewnianie bezpieczeństwa przy pełnym poszanowaniu prywatności i ochrony danych powinno samo w sobie stanowić cel strategii bezpieczeństwa wewnętrznego UE. Powinno to zostać odzwierciedlone w ramach wszystkich działań podejmowanych przez państwa członkowskie i instytucje unijne celem realizacji tej strategii.

23. W tym kontekście EIOD pragnie odnieść się do komunikatu (2010) 609 dotyczącego całościowego podejścia do kwestii ochrony danych osobowych w Unii Europejskiej ([12]). EIOD wyda wkrótce opinię dotyczącą tego komunikatu, lecz pragnie w tym miejscu podkreślić, że skuteczna strategia ISS nie może zostać ustanowiona bez wsparcia, jakim byłby uzupełniający ją solidny system ochrony danych, który gwarantowałby wzajemne zaufanie i wyższą skuteczność.

III. POJĘCIA MAJĄCE ZASTOSOWANIE DO PROJEKTOWANIA I WDRAŻANIA STRATEGII ISS

24. Oczywistym jest, że niektóre działania wynikające z celów strategii ISS mogą wpłynąć na zwiększenie ryzyka z punktu widzenia prywatności i ochrony danych osób fizycznych. Aby ryzyko to zrównoważyć, EIOD pragnie zwłaszcza zwrócić uwagę na pojęcia takie jak „uwzględnianie ochrony prywatności w fazie projektowania", prywatność i ocena wpływu ochrony danych, prawa osoby, której dotyczą dane, oraz najlepsze dostępne techniki. Wszystkie z nich należy wziąć pod uwagę w procesie wdrażania strategii ISS, gdyż mogą one wnieść użyteczny wkład w tworzenie kierunków polityki w tej dziedzinie, które bardziej sprzyjałyby prywatności i ochronie danych.

„Uwzględnianie ochrony prywatności w fazie projektowania"

25. EIOD przy różnych okazjach i w ramach rozmaitych opinii wyrażał swoje poparcie dla koncepcji „uwzględniania ochrony prywatności w fazie projektowania" (ang. *privacy by design* lub *privacy by default*). Jest ona obecnie rozwijana zarówno dla sektora prywatnego jak i publicznego, tym samym musi odgrywać istotną rolę w kontekście bezpieczeństwa wewnętrznego UE obszarze policji i wymiaru sprawiedliwości ([13]).

26. W komunikacie nie ma jednak o niej mowy. EIOD sugeruje więc, aby koncepcja ta została włączona do działań, które będą proponowane i podejmowane celem wdrożenia strategii ISS, zwłaszcza w kontekście celu 4 „Poprawa bezpieczeństwa poprzez zarządzanie granicami", który mówi wprost o szerszym zastosowaniu nowych technologii do celów kontroli granicznych i ochrony granic.

Ocena skutków dla prywatności i ochrony danych

27. W ramach przyszłych prac nad projektem i wdrażaniem strategii ISS na bazie komunikatu, EIOD zachęca Komisję do głębszej refleksji nad tym, co oznacza rzeczywista „ocena skutków dla prywatności i ochrony danych" (PIA) w obszarze wolności, bezpieczeństwa i wymiaru sprawiedliwości, zwłaszcza dla strategii ISS.

28. Komunikat mówi o zagrożeniach o ocenie ryzyka, co Inspektor przyjmuje z zadowoleniem, nie wspomina się jednak w ogóle o ocenach skutków dla prywatności i ochrony danych. EIOD jest przekonany, że prace nad implementacją komunikatu dotyczącego strategii ISS stanowią możliwość szczegółowego omówienia ocen skutków dla prywatności i ochrony danych w kontekście bezpieczeństwa wewnętrznego. EIOD zauważa, że ani komunikat ani wytyczne Komisji dotyczące oceny skutków ([14]) nie omawiają tego aspektu, ani nie czynią z niego wymogu dotyczącego polityki.

29. W związku z tym EIOD zaleca, by w ramach wdrażania przyszłych instrumentów przeprowadzano bardziej szczegółową i dokładną ocenę skutków dla prywatności i ochrony danych, albo w postaci odrębnej oceny, albo w ramach ogólnej oceny skutków dla praw podstawowych przeprowadzanej przez Komisję. Ocena skutków powinna zawierać nie tylko ogólne zasady czy analizować opcje dotyczące polityki, jak to ma miejsce obecnie, lecz także zalecać określone i konkretne zabezpieczenia.

30. Należy zatem opracować szczegółowe wskaźniki i charakterystyki w celu zapewnienia gruntownej refleksji nad każdym wnioskiem, który ma wpływ na ochronę prywatności i danych w obszarze bezpieczeństwa wewnętrznego UE, wraz z takimi aspektami jak zasada proporcjonalności, konieczności czy celowości.

31. Ponadto przydatne mogłoby się tu okazać odniesienie do art. 4 zalecenia RFID ([15]), w którym Komisja wezwała państwa członkowskie do zapewnienia przez sektor, we współpracy z odpowiednimi zainteresowanymi stronami społeczeństwa obywatelskiego ram do ocen skutków w zakresie ochrony danych i prywatności. Również przyjęta w listopadzie 2009 r. w Madrycie rezolucja Międzynarodowej Konferencji Komisarzy ds. Ochrony Danych

([12]) Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej", COM(2010) 609.

([13]) W opinii EIOD dotyczącej komunikatu Komisji w sprawie programu sztokholmskiego zalecano wprowadzenie obowiązku prawnego dla budujących i korzystających z systemów informacyjnych polegającego na opracowywaniu i korzystaniu z nich zgodnie z zasadą „uwzględniania ochrony prywatności w fazie projektowania".

([14]) SEC(2009) 92 z 15.1.2009 r.

([15]) C(2009) 3200 wersja ostateczna z 12.5.2009 r.

i Prywatności zachęcała do wdrożenia PIA przed wdrożeniem nowych systemów i technologii informatycznych do przetwarzania danych osobowych lub istotnych zmian w obecnym przetwarzaniu.

Prawa osób, których dotyczą dane

32. EIOD zauważa, że komunikat nie odnosi się konkretnie do istotnej kwestii praw podmiotów danych, które stanowią znaczący element ochrony danych i powinny mieć wpływ na projekt strategii ISS. Kluczowe jest zapewnienie, by w różnych systemach i instrumentach, które wiążą się z bezpieczeństwem wewnętrznym UE, osoby im podlegające miały podobne prawa w zakresie przetwarzania ich danych osobowych.

33. Wiele systemów, o których mowa w komunikacie, ustanawia szczególne zasady dotyczące praw podmiotów danych (dla takich kategorii osób jak poszkodowani, podejrzani czy migranci), jednak istnieje wiele nieuzasadnionych różnic pomiędzy systemami i instrumentami.

34. Dlatego też EIOD zachęca Komisję do bliższego przyjrzenia się kwestii dostosowania praw podmiotów danych w UE w niedalekiej przyszłości w kontekście strategii ISS i strategii w zakresie zarządzania informacjami.

35. Szczególny nacisk należy położyć na mechanizmy dochodzenia zadośćuczynienia. Strategia ISS powinna gwarantować, że w przypadku, gdy prawa danej osoby nie są w pełni przestrzegane, administratorzy danych zapewnią łatwo dostępne, skuteczne i przystępne procedury wnoszenia skarg.

Najlepsze dostępne techniki

36. Wdrożenie strategii ISS będzie w sposób nieunikniony związane z wykorzystanie infrastruktury informatycznej wspierającej działania przewidziane w komunikacie. Najlepsze dostępne techniki należy rozumieć jako mechanizmy służące osiągnięciu odpowiedniej równowagi pomiędzy celami strategii ISS a poszanowaniem praw jednostki. W tym kontekście EIOD pragnąłby powtórzyć zalecenie zawarte we wcześniejszych opiniach ([16]) dotyczące konieczności, aby Komisja zdefiniowała i promowała wraz z zainteresowanymi przedstawicielami przemysłu konkretne działania mające na celu stosowanie najlepszych dostępnych technik. Oznaczałyby to najskuteczniejszy i najbardziej zaawansowany etap tworzenia działań oraz metod ich stosowania, które wskazują praktyczną przydatność poszczególnych technik z punktu widzenia skutecznego osiągania planowanych wyników, zgodnie z unijnymi ramami ochrony prywatności i danych. Podejście to jest w pełni zgodne ze wspomnianą już koncepcją uwzględniania ochrony prywatności w fazie projektowania.

37. Gdy jest to przydatne i możliwe, dokumenty referencyjne dotyczące najlepszych dostępnych technik należy rozszerzyć celem zapewnienia wytycznych i większej pewności prawnej co do rzeczywistego wdrożenia działań w ramach strategii ISS. Wpłynęłoby to również na zwiększenie harmonizacji tego typu działań w poszczególnych państwach członkowskich. Zdefiniowanie najlepszych dostępnych technik sprzyjających prywatności i bezpieczeństwu ułatwiłoby także sprawowanie nadzoru organom ochrony danych, gdyż otrzymałyby one w ten sposób odniesienia techniczne zgodne z polityką prywatności i ochrony danych przyjęte przez administratorów danych.

38. EIOD pragnie również podkreślić znaczenie prawidłowego dostosowania strategii ISS do działań już podjętych w ramach siódmego programu ramowego w zakresie badań, rozwoju technologicznego i demonstracji i programu ramowego na rzecz bezpieczeństwa i ochrony swobód. Wspólna wizja drogi do stosowania najlepszych dostępnych technik umożliwi wprowadzenie innowacji w zakresie wiedzy i możliwości wymaganych, by chronić obywateli przy poszanowaniu praw podstawowych.

39. EIOD podkreśla wreszcie rolę, jaką odegrać mogłaby Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA) przy rozszerzaniu wytycznych i ocenie możliwości w zakresie bezpieczeństwa wymaganych, by zagwarantować integralność i dostępność systemów informatycznych, także w ramach promocji najlepszych dostępnych technik. W tym względzie EIOD z zadowoleniem przyjmuje włączenie Agencji jako kluczowego gracza w proces poprawy zdolności do reagowania na ataki cybernetyczne i zwalczania cyberprzestępczości ([17]).

Sprecyzowanie podmiotów i ich roli

40. W tym kontekście trzeba bardziej precyzyjnie określić podmioty, które tworzą architekturę strategii ISS lub biorą w niej udział. W komunikacie mowa jest o rozmaitych podmiotach i zainteresowanych stronach, takich jak obywatele, wymiar sprawiedliwości, agencje UE,

([16]) Opinia EIOD dotycząca inteligentnych systemów transportowych z lipca 2009 r. oraz opinia EIOD dotycząca komunikatu RFID z grudnia 2007 r.; zob. też Raport roczny EIOD z 2006 r., s. 48-49.

([17]) EIOD planuje wydanie opinii dotyczącej ram prawnych Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) jeszcze w grudniu 2010 r.

agencje krajowe, policja czy sektor biznesu. Ich konkretne role i kompetencje należałoby lepiej zdefiniować w odniesieniu do konkretnych działań proponowanych w ramach wdrażania strategii ISS.

IV. UWAGI DOTYCZĄCE OBSZARÓW POLITYKI ZWIĄZANYCH ZE STRATEGIĄ ISS

Zintegrowane zarządzanie granicami

41. W komunikacie mowa jest o tym, że po wejściu w życie traktatu lizbońskiego łatwiej jest Unii Europejskiej zadbać o synergię pomiędzy różnymi podejściami do zarządzania granicami w odniesieniu do przepływu osób i towarów. W dziedzinie przepływu osób mówi on, że „UE może traktować zarządzanie migracjami i walkę z przestępczością jako dwa bliźniacze cele zintegrowanej strategii zarządzania granicami". Dokument sugeruje, że zarządzanie granicami stanowi potencjalnie potężny oręż w walce z poważną i zorganizowaną przestępczością ([18]).

42. EIOD pragnie także zauważyć, że w komunikacie zidentyfikowano 3 strategiczne filary: 1) szersze zastosowanie nowych technologii do celów kontroli granicznych (SIS II, VIS, system wjazdu/wyjazdu i programu rejestrowania podróżnych); 2) szersze zastosowanie nowych technologii do ochrony granic (europejskiego systemu nadzoru granic, EUROSUR); oraz 3) usprawnienie koordynacji działań państw członkowskich poprzez Frontex.

43. EIOD pragnie przy okazji pisania niniejszej opinii przypomnieć prośby zawarte w wielu wcześniejszych opiniach – mianowicie by ustanowić na poziomie UE klarowną politykę dotyczącą zarządzania granicami, z pełnym poszanowaniem zasad ochrony danych. EIOD uważa, że bieżące prace nad strategią ISS i zarządzaniem informacjami stanowią znakomitą okazję, by podjąć bardziej konkretnie działania mające na celu stworzenie spójnego podejścia politycznego do tych obszarów.

44. EIOD pragnie zauważyć, że w komunikacie mowa jest nie tylko o istniejących systemach zakrojonych na dużą skalę oraz tych, które mogłyby zostać uruchomione w najbliższej przyszłości (takich jak SIS, SIS II czy VIS), lecz w tych samych wierszach mowa jest także o systemach, które mogą zostać zaproponowane przez Komisję w przyszłości, lecz co do których decyzji jeszcze nie podjęto (tj. o programie rejestrowania podróżnych (RTP) oraz systemie wjazdu/wyjazdu). Należy w tym kontekście przypomnieć, że cele i zasadność wprowadzenia tych systemów należy objaśnić i wykazać, również w świetle wyników konkretnych ocen wpływu przeprowadzonych przez Komisję. Jeżeli tak się nie stanie, komunikat odczytany zostanie jako zapowiedź procesu decyzyjnego bez wzmianki, że ostateczna decyzja o tym, czy w Unii Europejskiej należy stworzyć program rejestrowania podróżnych i system wjazdu/wyjazdu, nie została jeszcze podjęta.

45. EIOD proponuje więc, by w przyszłej pracy nad wdrożeniem strategii ISS unikać tego typu zapowiedzi. Jak już wcześniej wspomniano, podejmowanie jakichkolwiek decyzji dotyczących tworzenia nowych naruszających prywatność systemów zakrojonych na dużą skalę powinno mieć miejsce po dokonaniu adekwatnej oceny wszystkich istniejących systemów, z uwzględnieniem zasady konieczności i proporcjonalności.

EUROSUR

46. W komunikacie wspomniano, że Komisja przedstawi w 2011 r. wniosek ustawodawczy w sprawie ustanowienia EUROSUR jako wkładu w bezpieczeństwo wewnętrzne i zwalczanie przestępczości. Mowa jest również, że EUROSUR będzie korzystać z nowych technologii rozwijanych w ramach projektów badawczych finansowanych ze środków UE, takich jak obrazy satelitarne do wykrywania i śledzenia celów na granicach morskich, np. do śledzenia szybkich łodzi przewożących narkotyki do UE.

47. W tym kontekście EIOD pragnie zauważyć, że nie ma pewności, czy i w jakim zakresie wniosek ustawodawczy w sprawie EUROSUR, który ma zostać przedstawiony Komisji w 2011 r., będzie również obejmował kwestię przetwarzania danych osobowych w kontekście EUROSUR. Komisja nie przedstawia w komunikacie swojego stanowiska w tej sprawie. Kwestia ta jest jeszcze bardziej istotna, gdyż w komunikacie wyraźnie wspomina się o powiązaniach EUROSUR z agencją FRONTEX na płaszczyźnie taktycznej, operacyjnej i strategicznej (patrz uwaga na temat FRONTEX poniżej) i wnosi o ścisłą współpracę tych organów.

Przetwarzanie danych osobowych przez agencję FRONTEX

48. EIOD wydał w dniu 17 maja 2010 r. opinię dotyczącą przeglądu rozporządzenia w sprawie agencji FRONTEX ([19]). Wzywa w niej do prawdziwej debaty i głębokiej refleksji nad kwestią ochrony danych w kontekście wzmocnienia istniejących zadań agencji FRONTEX i wyznaczenia jej nowych obowiązków.

49. W komunikacie mowa jest o potrzebie zwiększenia wkładu agencji Frontex w zwalczanie przestępczości na granicach zewnętrznych w ramach celu 4 „Poprawa bezpieczeństwa poprzez zarządzanie granicami". W tym kontekście komunikat mówi, że w oparciu o dotychczasowe doświadczenia i w kontekście ogólnego podejścia UE do zarządzania informacjami Komisja jest zdania, że umożliwienie agencji

([18]) Nota nr 10/598 – Komunikat prasowy w sprawie komunikatu „Strategia bezpieczeństwa wewnętrznego UE w działaniu: pięć kroków w kierunku bezpieczniejszej Europy".

([19]) Opinia EIOD z dnia 17 maja 2010 r. dotycząca wniosku w sprawie rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie Rady (WE) nr 2007/2004 ustanawiające Europejską Agencję Zarządzania Współpracą Operacyjną na Zewnętrznych Granicach Państw Członkowskich Unii Europejskiej (FRONTEX).

FRONTEX przetwarzania i wykorzystywania tych informacji – w ograniczonym zakresie i zgodnie z jasno sprecyzowanymi przepisami w zakresie zarządzania danymi osobowymi – będzie stanowiło znaczący wkład w rozbijanie organizacji przestępczych. Jest to nowe podejście w porównaniu do propozycji Komisji dotyczącej przeglądu rozporządzenia w sprawie FRONTEX, które jest obecnie dyskutowane w Parlamencie Europejskim i Radzie i nie wspomina o przetwarzaniu danych osobowych.

50. W tym kontekście EIOD z zadowoleniem przyjmuje fakt, że w komunikacie zawarto pewne wskazówki co do okoliczności, gdy przetwarzanie danych może okazać się konieczne (np. analiza ryzyka, większa skuteczność wspólnych operacji lub wymiany informacji z Europolem). W komunikacie wyjaśniono, że informacji na temat członków grup przestępczych działających w siatkach przemytniczych, na które natrafia Frontex, nie można jednak obecnie wykorzystać do analizy ryzyka lub lepszego ukierunkowania przyszłych wspólnych operacji. Odpowiednie informacje na temat domniemanych przestępców nie docierają poza tym do właściwych organów krajowych ani do Europolu, gdzie mogłyby posłużyć do dalszych działań śledczych.

51. EIOD pragnie mimo to zauważyć, że w komunikacie nie ma mowy o trwającej obecnie dyskusji na temat przeglądu ram prawnych dotyczących agencji FRONTEX, która – jak już wspomniano – ma na celu stworzenie rozwiązań ustawodawczych. Brzmienie komunikatu podkreślające ponadto rolę agencji FRONTEX w kontekście celu, jakim jest rozbijanie organizacji przestępczych, może być odczytane jako rozszerzające mandat tej agencji. EIOD sugeruje, by wziąć tę kwestię pod uwagę zarówno w ramach przeglądu rozporządzenia w sprawie FRONTEX, jak w wdrożenia strategii ISS.

52. EIOD pragnie również podkreślić potrzebę zagwarantowania, że zadania Europolu i agencji FRONTEX nie będą się pokrywać. W tym kontekście EIOD z zadowoleniem przyjmuje wzmiankę Komisji, że powielanie się zadań wykonywanych przez FRONTEX i Europol nie powinno mieć miejsca. Jednak kwestia ta powinna zostać wyraźniej zaakcentowana w ramach rozporządzenia w sprawie agencji FRONTEX po przeglądzie, a także działań wdrażających strategię ISS, które zakładają ścisłą współpracę pomiędzy agencją FRONTEX a EUROPOLEM. Jest to szczególnie istotne z punktu widzenia zasady celowości i jakości danych. Uwaga ta odnosi się również do przyszłej współpracy z takimi agencjami jak Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA) czy Europejski Urząd Wsparcia w dziedzinie Azylu.

Stosowanie rozwiązań biometrycznych

53. Komunikat nie odnosi się konkretnie do obecnego zjawiska szerszego stosowania danych biometrycznych w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, w tym systemów informatycznych zakrojonych na dużą skalę i innych narzędzi zarządzania granicami.

54. EIOD pragnie więc skorzystać z tej okazji, by przypomnieć swoją propozycję ([20]), aby kwestia ta – niewątpliwie bardzo istotna z punktu widzenia ochrony danych – została wzięta poważnie pod uwagę przy wdrażaniu strategii ISS, zwłaszcza w kontekście zarządzania granicami.

55. EIOD zaleca również opracowanie jasnej i restrykcyjnej polityki w sprawie stosowania rozwiązań biometrycznych w obszarze wolności, bezpieczeństwa i sprawiedliwości, w oparciu o poważną ewaluację i ocenę jednostkową konieczności stosowania danych biometrycznych w kontekście strategii ISS, z pełnym poszanowaniem takich podstawowych zasad ochrony danych jak proporcjonalność, konieczność i celowość.

TFTP

56. W komunikacie ogłoszono, że Komisja opracuje w 2011 r. politykę UE w zakresie pozyskiwania i analizy danych z komunikatów finansowych zarejestrowanych na terenie UE. W tym kontekście EIOD pragnie przywołać swoją opinię z dnia 22 czerwca 2010 r. dotyczącą przetwarzania i przekazywania danych z komunikatów finansowych z Unii do Stanów Zjednoczonych do celów Programu śledzenia środków finansowych należących do terrorystów (TFTP II) ([21]). Wszystkie uwagi krytyczne wyrażone w ramach tej opinii są także zasadne i stosowne w kontekście planowanych prac nad unijnymi ramami dla danych z komunikatów finansowych, należy je więc uwzględnić w dyskusjach nad tą kwestią. Szczególną uwagę należy zwrócić na proporcjonalność pozyskiwania i przetwarzania dużej liczby danych dotyczących osób, które nie są podejrzanymi, a także na kwestię skutecznego nadzoru sprawowanego przez niezależne organy i wymiar sprawiedliwości.

Bezpieczeństwo obywateli i przedsiębiorstw w cyberprzestrzeni

57. EIOD z zadowoleniem przyjmuje wagę, jaką przykłada się w komunikacie do działań zapobiegawczych na poziomie UE. Inspektor stoi na stanowisku, że poprawa bezpieczeństwa sieci informatycznych jest jednym z zasadniczych warunków dobrze funkcjonującego społeczeństwa informacyjnego. EIOD popiera również konkretne działania mające na celu poprawę zdolności do reagowania na ataki cybernetyczne, budowę zdolności w zakresie egzekwowania prawa i sądownictwa oraz tworzenie partnerstw z przemysłem w celu wzmacniania pozycji obywateli i ich ochrony. Z zadowoleniem przyjmowana jest też rola, jaką odgrywa ENISA, jako katalizator wielu działań w ramach wspomnianego celu.

([20]) Zob. zwłaszcza opinię EIOD dotyczącą komunikatu – „Przegląd zarządzania informacjami w przestrzeni wolności, bezpieczeństwa i sprawiedliwości", o którym mowa w przypisie nr 8.

([21]) Opinia EIOD z dnia 22 czerwca 2010 r. dotycząca wniosku w sprawie projektu decyzji Rady w sprawie zawarcia Umowy pomiędzy Unią Europejską a Stanami Zjednoczonymi w sprawie przetwarzania i przekazywania danych z komunikatów finansowych przez Unię Europejską Stanom Zjednoczonym do celów Programu śledzenia środków finansowych należących do terrorystów (TFTP II).

58. Strategia bezpieczeństwa wewnętrznego UE w działaniu nie zawiera jednak rozwinięcia działań w cyberprzestrzeni, nie mówi w jaki sposób działania te zagrażają prawom jednostki ani jakie należałoby wprowadzić zabezpieczenia. EIOD sugeruje wdrożenie bardziej ambitnego podejścia do odpowiednich zabezpieczeń. Podejście to powinno mieć na celu ochronę podstawowych praw jednostki, łącznie z tymi, które mogą zostać naruszone przez działania mające przeciwdziałać potencjalnej działalności przestępczej w tym obszarze.

V. **WNIOSKI I ZALECENIA**

59. EIOD zwraca się o powiązanie rozmaitych strategii i komunikatów UE w procesie wdrażania strategii ISS. Podejście to powinno zostać powiązane z konkretnym planem działań wraz z rzeczywistą oceną potrzeb, której wynikiem powinna być pełna, zintegrowana i dobrze ustrukturyzowana polityka UE dotycząca strategii ISS.

60. Korzystając z okazji, EIOD pragnie podkreślić także znaczenie wymogu prawnego dotyczącego rzeczywistej oceny wszystkich istniejących instrumentów, z których będzie się korzystać w kontekście strategii ISS i wymiany informacji, przed zaproponowaniem nowych. W tym kontekście zaleca się dodanie zapisów dotyczących regularnej oceny skuteczności odpowiednich instrumentów.

61. EIOD sugeruje, aby w procesie tworzenia wieloletniego planu strategicznego, o który domagają się konkluzje Rady z listopada 2010 r., uwzględniono bieżące prace nad kompleksowymi ramami ochrony danych w oparciu o art. 16 TFUE, a zwłaszcza komunikat (2009) 609.

62. EIOD wysuwa pewna liczbę propozycji co do pojęć istotnych z punktu widzenia ochrony danych, które należałoby uwzględnić podczas realizacji strategii ISS, takich jak uwzględnianie ochrony prywatności w fazie projektowania, ocena skutków dla prywatności i ochrony danych czy najlepsze dostępne techniki.

63. EIOD zaleca, by w ramach wdrażania przyszłych instrumentów przeprowadzano ocenę skutków dla prywatności i ochrony danych, albo w postaci odrębnej oceny, albo w ramach ogólnej oceny skutków dla praw podstawowych przeprowadzanej przez Komisję.

64. Zachęca on również Komisję do opracowania bardziej spójnej i jednolitej polityki w odniesieniu do wymogów wstępnych dotyczących stosowania rozwiązań biometrycznych w dziedzinie strategii ISS i lepszego dostosowania na poziomie UE w kwestii praw osób, których dotyczą dane.

65. EIOD przedstawia wreszcie pewną liczbę uwag dotyczących przetwarzania danych osobowych w kontekście zarządzania granicami, zwłaszcza przez agencję FRONTEX, a także potencjalnie w kontekście EUROSUR.

Sporządzono w Brukseli dnia 17 grudnia 2010 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych