Streszczenie opinii Europejskiego Inspektora Ochrony Danych w sprawie wspólnego komunikatu Komisji oraz Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń" oraz wniosku Komisji dotyczącego dyrektywy w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii

(Niniejsza opinia jest dostępna w pełnym brzmieniu w języku angielskim, francuskim i niemieckim na stronie internetowej EIOD: http://www.edps.europa.eu)

(2014/C 32/10)

1. **Wprowadzenie**

1.1. *Konsultacje z EIOD*

1. W dniu 7 lutego 2013 r. Komisja oraz Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa przyjęli wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów zatytułowany „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń" ([1]) (zwany dalej „wspólnym komunikatem", „strategią bezpieczeństwa cybernetycznego" lub „strategią").

2. W tym samym dniu Komisja przyjęła wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii ([2]) (zwany dalej „proponowaną dyrektywą" lub „wnioskiem"). Wniosek przesłano EIOD do konsultacji w dniu 7 lutego 2013 r.

3. Przed przyjęciem wspólnego komunikatu i wniosku EIOD miał możliwość przedstawienia Komisji nieformalnych uwag. EIOD z zadowoleniem przyjmuje fakt uwzględnienia części jego uwag we wspólnym komunikacie i wniosku.

4. **Wnioski**

74. EIOD z zadowoleniem przyjmuje fakt, że Komisja oraz Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa przedstawili kompleksową strategię bezpieczeństwa cybernetycznego wraz z wnioskiem dotyczącym dyrektywy w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii. Strategia ta uzupełnia wcześniejsze działania polityczne UE w dziedzinie bezpieczeństwa sieci i informacji.

75. EIOD z zadowoleniem przyjmuje fakt, że strategia wychodzi poza tradycyjne przeciwstawienie bezpieczeństwa prywatności dzięki temu, iż wyraźnie uznaje się w niej prywatność i ochronę danych za podstawowe wartości, które powinny wyznaczać kierunek polityki bezpieczeństwa cybernetycznego w obrębie UE oraz poza jej granicami. EIOD zauważa, że strategia bezpieczeństwa cybernetycznego oraz proponowana dyrektywa w sprawie bezpieczeństwa sieci i informacji mogą w zasadniczy sposób przyczynić się do zapewnienia poszanowania praw osób fizycznych do prywatności i ochrony danych w środowisku internetowym. Jednocześnie należy dopilnować, aby nie prowadziły one do stosowania środków stanowiących bezprawną ingerencję w prawa osób fizycznych do prywatności i ochrony danych.

76. EIOD z zadowoleniem przyjmuje również fakt, że w strategii kilkakrotnie wspomina się o ochronie danych, którą uwzględniono też w proponowanej dyrektywie w sprawie bezpieczeństwa sieci i informacji. Z ubolewaniem stwierdza jednak, iż w strategii i w proponowanej dyrektywie nie podkreślono w wyraźniejszy sposób wkładu istniejącego oraz przyszłego prawa o ochronie danych w bezpieczeństwo, nie dopilnowano też w pełni, aby wszelkie obowiązki wynikające z proponowanej dyrektywy lub z innych elementów strategii uzupełniały obowiązki w zakresie ochrony danych oraz nie pokrywały się ze sobą ani też nie były wzajemnie sprzeczne.

77. Ponadto EIOD zauważa, że wskutek nieuwzględnienia i niewzięcia w pełni pod uwagę innych równoległych inicjatyw Komisji oraz trwających procedur ustawodawczych dotyczących np. reform w zakresie ochrony danych oraz proponowanego rozporządzenia w sprawie elektronicznej identyfikacji i usług zaufania strategia bezpieczeństwa cybernetycznego nie prezentuje w istocie kompleksowego i całościowego spojrzenia na bezpieczeństwo cybernetyczne w UE, co grozi utrwaleniem fragmentarycznego oraz

([1]) JOIN(2013) 1 final.
([2]) COM(2013) 48 final.

niespójnego podejścia. EIOD zwraca też uwagę, że proponowana dyrektywa w sprawie bezpieczeństwa sieci i informacji nadal nie umożliwia kompleksowego podejścia do bezpieczeństwa w UE, a obowiązek określony w prawie o ochronie danych jest prawdopodobnie najszerzej zakrojonym obowiązkiem w zakresie bezpieczeństwa sieci i informacji na mocy prawa UE.

78. EIOD ubolewa także, iż nie uwzględniono w należyty sposób ważnej roli organów ochrony danych w ustanawianiu i egzekwowaniu obowiązków w zakresie bezpieczeństwa oraz w poprawie bezpieczeństwa cybernetycznego.

79. Jeżeli chodzi o strategię bezpieczeństwa cybernetycznego, EIOD podkreśla, że:

— szczególnie ważne jest jasne zdefiniowanie pojęć „odporności na zagrożenia cybernetyczne", „cyberprzestępczości" i „obrony cybernetycznej", gdyż terminy te są używane jako uzasadnienie dla pewnych środków specjalnych, które mogłyby skutkować ingerencją w prawa podstawowe, w tym w prawo do prywatności i ochrony danych. Definicje „cyberprzestępczości" przedstawione w strategii oraz w Konwencji o cyberprzestępczości pozostają wszakże bardzo szerokie. Wskazane byłoby opracowanie jasnej i *wąskiej* definicji „cyberprzestępczości" w miejsce definicji nadmiernie szerokiej,

— prawo o ochronie danych powinno mieć zastosowanie do wszystkich działań w ramach strategii, gdy tylko dotyczą one środków związanych z przetwarzaniem danych osobowych. Chociaż w sekcjach dotyczących cyberprzestępczości i obrony cybernetycznej nie wspomina się wyraźnie o prawie o ochronie danych, EIOD podkreśla, że wiele spośród planowanych działań w tych obszarach będzie się wiązać z przetwarzaniem danych osobowych, a zatem będzie podlegać obowiązującemu prawu o ochronie danych. Zauważa również, iż wiele działań polega na ustanowieniu mechanizmów koordynacji, które będą wymagać wdrożenia odpowiednich zabezpieczeń służących ochronie danych w związku ze sposobami wymiany danych osobowych,

— w kontekście bezpieczeństwa cybernetycznego ważną rolę odgrywają organy ochrony danych. Jako strażnicy praw osób fizycznych do prywatności i ochrony danych organy ochrony danych są aktywnie zaangażowane w ochronę ich danych osobowych zarówno w środowisku internetowym, jak i poza nim. W związku z tym powinny one zostać należycie włączone w nadzór nad środkami wykonawczymi, które wiążą się z przetwarzaniem danych osobowych (takimi jak uruchomienie unijnego projektu pilotażowego dotyczącego zwalczania botnetów i złośliwego oprogramowania). Inne podmioty aktywne w dziedzinie bezpieczeństwa cybernetycznego powinny również współpracować z nimi podczas wykonywania swoich zadań, na przykład w zakresie wymiany najlepszych praktyk i działań podnoszących świadomość. EIOD i krajowe organy ochrony danych powinni także zostać należycie włączeni w organizację konferencji wysokiego szczebla, która zostanie zwołana w 2014 r. w celu oceny postępów w realizacji strategii.

80. W odniesieniu do proponowanej dyrektywy w sprawie bezpieczeństwa sieci i informacji EIOD zaleca, aby prawodawca:

— zapewnił większą jasność i pewność dotyczącą zawartej w art. 3 pkt 8 definicji podmiotów gospodarczych, które wchodzą w zakres wniosku, oraz stworzył wyczerpujący wykaz obejmujący wszystkie stosowne zainteresowane strony w celu zapewnienia w pełni zharmonizowanego i zintegrowanego podejścia do bezpieczeństwa w obrębie UE,

— wyjaśnił w art. 1 ust. 2 lit. c), że proponowana dyrektywa ma zastosowanie do instytucji i organów UE, oraz zawarł w art. 1 ust. 5 wniosku odniesienie do rozporządzenia (WE) nr 45/2001,

— uznał bardziej horyzontalną rolę przedmiotowego wniosku w zakresie bezpieczeństwa poprzez wyraźne wskazanie w art. 1, że powinien on mieć zastosowanie bez uszczerbku dla istniejących lub przyszłych bardziej szczegółowych przepisów w poszczególnych obszarach (takich jak te, które mają obowiązywać dostawców usług zaufania w proponowanym rozporządzeniu w sprawie identyfikacji elektronicznej),

— dodał motyw wyjaśniający potrzebę uwzględnienia ochrony danych w sposób domyślny już we wczesnej fazie projektowania mechanizmów ustanawianych we wniosku oraz przez cały okres funkcjonowania stosownych procesów, procedur, organizacji, technik i infrastruktury, przy uwzględnieniu proponowanego rozporządzenia o ochronie danych,

— wyjaśnił definicje „sieci i systemów informatycznych" w art. 3 pkt 1 oraz „incydentu" w art. 3 pkt 4 i zastąpił w art. 5 ust. 2 zobowiązanie do „opracowania planu oceny zagrożeń" zobowiązaniem do „opracowania i utrzymania ram zarządzania ryzykiem",

— wskazał w art. 1 ust. 6, że przetwarzanie danych osobowych jest uzasadnione na podstawie art. 7 lit. e) dyrektywy 95/46/WE w zakresie, w jakim jest to konieczne do osiągnięcia celów interesu publicznego realizowanych przez proponowaną dyrektywę. Trzeba wszakże zapewnić należyte poszanowanie zasad konieczności i proporcjonalności, aby przetwarzane były tylko dane ściśle niezbędne do celów, które mają zostać osiągnięte,

— określił w art. 14 okoliczności, w których wymagane jest zgłoszenie, jak również treść i formę zgłoszenia, w tym rodzaje danych osobowych, które powinny podlegać zgłoszeniu, oraz to, czy i w jakim stopniu zgłoszenie oraz towarzyszące mu dokumenty będą zawierać szczegóły dotyczące danych osobowych, których dotyczy konkretny incydent zagrażający ich bezpieczeństwu (np. adresów IP). Należy wziąć pod uwagę fakt, że właściwe organy ds. bezpieczeństwa sieci i informacji powinny mieć prawo do gromadzenia oraz przetwarzania danych osobowych w związku z incydentami zagrażającymi ich bezpieczeństwu wyłącznie, gdy jest to bezwzględnie konieczne. We wniosku należy też określić odpowiednie zabezpieczenia, aby zapewnić adekwatną ochronę danych przetwarzanych przez właściwe organy ds. bezpieczeństwa sieci i informacji,

— wyjaśnił w art. 14, że zgłoszenia incydentów na mocy art. 14 ust. 2 powinny mieć zastosowanie bez uszczerbku dla obowiązków w zakresie zgłaszania naruszeń dotyczących danych osobowych na mocy obowiązującego prawa o ochronie danych. We wniosku należy określić najważniejsze aspekty procedury współpracy właściwych organów ds. bezpieczeństwa sieci i informacji z organami ochrony danych w przypadkach, gdy incydent w zakresie bezpieczeństwa wiąże się z naruszeniem dotyczącym danych osobowych,

— zmienił art. 14 ust. 8 tak, aby wyłączenie mikroprzedsiębiorstw z obowiązku zgłoszeń nie miało zastosowania do tych podmiotów, które odgrywają zasadniczą rolę w świadczeniu usług społeczeństwa informacyjnego, na przykład ze względu na charakter przetwarzanych informacji (np. danych biometrycznych lub danych szczególnie chronionych),

— uzupełnił wniosek o przepisy dotyczące dalszej wymiany danych osobowych przez właściwe organy ds. bezpieczeństwa sieci i informacji z innymi odbiorcami w celu dopilnowania, aby: (i) dane osobowe były ujawniane jedynie tym odbiorcom, którzy muszą je przetwarzać w celu wykonywania swoich zadań zgodnie z właściwą podstawą prawną; oraz (ii) informacje te były ograniczone do zakresu niezbędnego do wykonywania zadań. Należy również zwrócić uwagę na to, w jaki sposób podmioty dostarczające dane do sieci służącej ich wymianie zapewniają zgodność z zasadą celowości,

— określił maksymalny okres zatrzymywania danych osobowych do celów określonych w proponowanej dyrektywie, w szczególności w kontekście ich zatrzymywania przez właściwe organy ds. bezpieczeństwa sieci i informacji oraz w obrębie bezpiecznej infrastruktury sieci współpracy,

— przypomniał właściwym organom ds. bezpieczeństwa sieci i informacji o obowiązku dostarczenia odpowiednich informacji o przetwarzaniu danych osobowych osobom, których dane dotyczą, na przykład poprzez zamieszczenie polityki prywatności na stronie internetowej,

— dodał przepis dotyczący poziomu bezpieczeństwa, który mają zapewnić właściwe organy ds. bezpieczeństwa sieci i informacji w odniesieniu do gromadzonych, przetwarzanych oraz wymienianych informacji. W kontekście ochrony danych osobowych przez właściwe organy ds. bezpieczeństwa sieci i informacji należy zamieścić odniesienie do wymogów bezpieczeństwa określonych w art. 17 dyrektywy 95/46/WE,

— wyjaśnił w art. 9 ust. 2, że kryteria udziału państw członkowskich w bezpiecznym systemie wymiany informacji powinny zapewniać zagwarantowanie wysokiego poziomu bezpieczeństwa i odporności przez wszystkich uczestników systemów wymiany informacji na wszystkich etapach ich przetwarzania. Kryteria te powinny obejmować odpowiednie środki służące zapewnieniu poufności i bezpieczeństwa zgodnie z art. 16 i 17 dyrektywy 95/46/WE oraz art. 21 i 22 rozporządzenia (WE) nr 45/2001. Komisja powinna zostać w wyraźny sposób związana tymi kryteriami w związku ze swoim udziałem jako administratora w bezpiecznym systemie wymiany informacji,

— dodał w art. 9 opis ról i obowiązków Komisji oraz państw członkowskich związanych z ustanowieniem, eksploatacją i utrzymaniem bezpiecznego systemu wymiany informacji, jak też wskazał, że system ten należy zaprojektować zgodnie z zasadami uwzględnienia ochrony danych już w fazie projektowania i w sposób domyślny oraz uwzględnienia bezpieczeństwa już w fazie projektowania, oraz

— dodał w art. 13, że dane osobowe powinny w każdym przypadku być przekazywane odbiorcom znajdującym się w krajach poza UE zgodnie z art. 25 i 26 dyrektywy 95/46/WE oraz art. 9 rozporządzenia (WE) nr 45/2001.

Sporządzono w Brukseli dnia 14 czerwca 2013 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych