EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Streszczenie opinii Europejskiego Inspektora Ochrony Danych w sprawie strategii w zakresie cyberbezpieczeństwa oraz dyrektywy w sprawie bezpieczeństwa sieci i informacji (NIS 2.0)

(Pełny tekst niniejszej opinii jest dostępny w wersji angielskiej, francuskiej i niemieckiej na stronie internetowej EIOD: www.edps.europa.eu)

(2021/C 183/03)

W dniu 16 grudnia 2020 r. Komisja Europejska przyjęła wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, uchylającej dyrektywę (UE) 2016/1148 („wniosek"). Jednocześnie Komisja Europejska i Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa wydali wspólny komunikat do Parlamentu Europejskiego i Rady zatytułowany „Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę" („strategia").

EIOD w pełni popiera ogólny cel strategii, jakim jest zapewnienie globalnego i otwartego internetu z silnymi zabezpieczeniami przed zagrożeniami dla bezpieczeństwa i praw podstawowych, uznanie strategicznej wartości internetu i zarządzania nim oraz wzmocnienie działań Unii w tym obszarze, w modelu obejmującym wiele zainteresowanych stron.

W związku z tym EIOD z zadowoleniem przyjmuje cel wniosku, jakim jest wprowadzenie zmian systemowych i strukturalnych do obecnej dyrektywy w sprawie bezpieczeństwa sieci i informacji w celu objęcia nią szerszego zestawu podmiotów w całej Unii, z silniejszymi środkami bezpieczeństwa, w tym obowiązkowym zarządzaniem ryzykiem, minimalnymi standardami oraz odpowiednimi przepisami dotyczącymi nadzoru i egzekwowania. W związku z tym EIOD uważa, że konieczne jest pełne włączenie instytucji, urzędów, organów i agencji Unii do ogólnounijnych ogólnych ram cyberbezpieczeństwa w celu osiągnięcia jednolitego poziomu ochrony poprzez wyraźne włączenie instytucji, urzędów, organów i agencji Unii do zakresu wniosku.

EIOD podkreśla ponadto znaczenie włączenia perspektywy prywatności i ochrony danych do środków z zakresu cyberbezpieczeństwa wynikających z wniosku lub z innych inicjatyw w zakresie cyberbezpieczeństwa zawartych w strategii, aby zapewnić całościowe podejście i umożliwić synergię podczas zarządzania cyberbezpieczeństwem i ochrony przetwarzanych przez nie danych osobowych. Równie ważne jest, aby wszelkie potencjalne ograniczenia prawa do ochrony danych osobowych i prywatności wynikające z takich środków spełniały kryteria określone w art. 52 Karty praw podstawowych Unii Europejskiej, a w szczególności by zostały osiągnięte za pomocą środka ustawodawczego i były zarówno konieczne, jak i proporcjonalne.

EIOD oczekuje, że wniosek nie będzie miał wpływu na stosowanie obowiązujących przepisów UE regulujących przetwarzanie danych osobowych, w tym na zadania i uprawnienia niezależnych organów nadzorczych właściwych do monitorowania zgodności z tymi aktami. Oznacza to, że wszystkie systemy i usługi cyberbezpieczeństwa związane z zapobieganiem zagrożeniom cybernetycznym, ich wykrywaniem i reagowaniem na nie powinny być zgodne z obowiązującymi ramami ochrony prywatności i ochrony danych. W związku z tym EIOD uważa, że na potrzeby wniosku istotne i konieczne jest ustanowienie jasnej i jednoznacznej definicji terminu „cyberbezpieczeństwo".

EIOD wydaje szczegółowe zalecenia w celu zapewnienia, by wniosek prawidłowo i skutecznie uzupełniał obowiązujące prawodawstwo Unii w zakresie ochrony danych osobowych, w szczególności ogólne rozporządzenie o ochronie danych i dyrektywę o prywatności i łączności elektronicznej, w razie potrzeby również poprzez zaangażowanie EIOD i Europejskiej Rady Ochrony Danych oraz ustanowienie jasnych mechanizmów współpracy między właściwymi organami z różnych obszarów regulacyjnych.

Ponadto przepisy dotyczące zarządzania internetowymi rejestrami domen najwyższego poziomu (TLD) powinny jasno określać odpowiedni zakres i warunki prawne. Koncepcja proaktywnego skanowania sieci i systemów informatycznych przez CSIRT wymaga również dalszych wyjaśnień co do zakresu i rodzajów przetwarzanych danych osobowych. Zwraca się uwagę na ryzyko związane z ewentualnym niezgodnym z przepisami przekazywaniem danych w związku z outsourcingiem usług w zakresie cyberbezpieczeństwa lub nabywaniem produktów z zakresu cyberbezpieczeństwa i ich łańcucha dostaw.

EIOD z zadowoleniem przyjmuje apel o propagowanie stosowania szyfrowania, a w szczególności szyfrowania typu „end-to-end", i ponownie podkreśla swoje stanowisko w sprawie szyfrowania jako krytycznej i niezastąpionej technologii skutecznej ochrony danych i prywatności, której obejście pozbawiłoby mechanizm wszelkiej zdolności ochrony ze względu na ich ewentualne bezprawne wykorzystanie i utratę zaufania do kontroli bezpieczeństwa. W tym celu należy wyjaśnić, że żaden z elementów wniosku nie powinien być rozumiany jako poparcie dla osłabienia szyfrowania typu „end-to-end" za pomocą „backdoor" lub podobnych rozwiązań.

1. **WPROWADZENIE I KONTEKST**

1. W dniu 16 grudnia 2020 r. Komisja Europejska przyjęła wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, uchylającej dyrektywę (UE) 2016/1148 ([1]) („wniosek").

2. W tym samym dniu Komisja Europejska i Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa wydali wspólny komunikat do Parlamentu Europejskiego i Rady zatytułowany „Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę" („strategia"). ([2])

3. Strategia ma na celu wzmocnienie strategicznej autonomii Unii w dziedzinie cyberbezpieczeństwa oraz poprawę jej odporności i zbiorowej reakcji, a także stworzenie globalnego i otwartego internetu z silną ochroną w celu przeciwdziałania zagrożeniom dla bezpieczeństwa oraz dla podstawowych praw i wolności obywateli w Europie ([3]).

4. Strategia zawiera propozycje inicjatyw regulacyjnych, inwestycyjnych i politycznych w trzech obszarach działań UE: (1) odporność, suwerenność technologiczna i przywództwo, (2) budowanie zdolności operacyjnej do zapobiegania, powstrzymywania i reagowania oraz (3) rozwijanie globalnej i otwartej cyberprzestrzeni.

5. Wniosek stanowi jedną z inicjatyw regulacyjnych strategii, w szczególności w dziedzinie odporności, suwerenności technologicznej i przywództwa.

6. Zgodnie z uzasadnieniem celem wniosku jest modernizacja istniejących ram prawnych, tj. dyrektywy (UE) 2016/1148 Parlamentu Europejskiego i Rady („dyrektywa w sprawie bezpieczeństwa sieci i informacji") ([4]). Wniosek ma na celu wykorzystanie i uchylenie obecnej dyrektywy w sprawie bezpieczeństwa sieci i informacji, która była pierwszym ogólnounijnym prawodawstwem dotyczącym cyberbezpieczeństwa i przewiduje środki prawne mające na celu zwiększenie ogólnego poziomu cyberbezpieczeństwa w Unii. We wniosku uwzględniono coraz większą cyfryzację rynku wewnętrznego w ostatnich latach oraz zmieniający się krajobraz zagrożeń dla cyberbezpieczeństwa, które nasiliły od początku kryzysu związanego z COVID-19. Wniosek ma na celu wyeliminowanie kilku zidentyfikowanych niedociągnięć dyrektywy w sprawie bezpieczeństwa sieci i informacji i zwiększenie poziomu cyberodporności wszystkich sektorów, publicznych i prywatnych, które pełnią ważną funkcję dla gospodarki i społeczeństwa.

7. Główne elementy wniosku są następujące:

   (i) rozszerzenie zakresu obowiązującej dyrektywy w sprawie bezpieczeństwa sieci i informacji poprzez dodanie nowych sektorów na podstawie ich krytyczności dla gospodarki i społeczeństwa;

   (ii) zaostrzone wymogi w zakresie bezpieczeństwa dla objętych dyrektywą przedsiębiorstw i podmiotów poprzez wprowadzenie podejścia do zarządzania ryzykiem przewidującego minimalny wykaz podstawowych elementów bezpieczeństwa, które należy stosować;

   (iii) rozwiązanie kwestii bezpieczeństwa łańcuchów dostaw i relacji z dostawcami poprzez zobowiązanie poszczególnych przedsiębiorstw uwzględnienia zagrożeń dla cyberbezpieczeństwa w łańcuchach dostaw i relacjach z dostawcami;

   (iv) zacieśnienie współpracy między organami państw członkowskich oraz współpracy z instytucjami, urzędami, organami i agencjami Unii w zakresie działań związanych z cyberbezpieczeństwem, w tym zarządzania kryzysowego w cyberprzestrzeni.

8. W dniu 14 stycznia 2021 r. EIOD otrzymał od Komisji Europejskiej wniosek o formalne konsultacje w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, uchylającej dyrektywę (UE) 2016/1148.

3. **WNIOSKI**

77. W świetle powyższego EIOD wydaje następujące zalecenia:

W odniesieniu do strategii cyberbezpieczeństwa

— uwzględnienie faktu, że pierwszym krokiem w kierunku ograniczenia zagrożeń dla ochrony danych i prywatności, które są związane z nowymi technologiami służącymi poprawie cyberbezpieczeństwa, takimi jak sztuczna inteligencja, jest stosowanie wymogów ochrony danych już w fazie projektowania oraz wymogów domyślnych określonych w art. 25 RODO, co pomoże w integracji odpowiednich zabezpieczeń, takich jak pseudonimizacja, szyfrowanie, dokładność danych, minimalizacja danych, przy projektowaniu i wykorzystywaniu tych technologii i systemów;

— uwzględnienie znaczenia, jakie ma włączenie perspektywy prywatności i ochrony danych do polityk i norm związanych z cyberbezpieczeństwem, a także do tradycyjnego zarządzania cyberbezpieczeństwem w celu zapewnienia całościowego podejścia i umożliwienia synergii między organizacjami publicznymi i prywatnymi podczas zarządzania cyberbezpieczeństwem i ochrony przetwarzanych przez nie informacji bez niepotrzebnego powielania wysiłków;

— rozważenie i zaplanowanie wykorzystania zasobów przez EUI w celu wzmocnienia ich zdolności w zakresie cyberbezpieczeństwa, w tym w sposób w pełni zgodny z wartościami UE;

— uwzględnienie aspektów cyberbezpieczeństwa związanych z prywatnością i ochroną danych poprzez inwestowanie w strategie polityczne, praktyki i narzędzia, w przypadku których perspektywa prywatności i ochrony danych jest zintegrowana z tradycyjnym zarządzaniem cyberbezpieczeństwem, a skuteczne gwarancje ochrony danych są włączane do działań związanych z cyberbezpieczeństwem podczas przetwarzania danych osobowych.

W odniesieniu do zakresu strategii i wniosku – dla instytucji, urzędów, organów i agencji Unii

— uwzględnienie potrzeb i roli instytucji UE, tak aby zostały włączone do ogólnounijnych ogólnych ram cyberbezpieczeństwa jako podmioty korzystające z takiego samego wysokiego poziomu ochrony jak podmioty w państwach członkowskich;

— wyraźne włączenie instytucji, urzędów, organów i agencji Unii do zakresu wniosku.

W odniesieniu do związku z obowiązującym prawodawstwem Unii dotyczącym ochrony danych osobowych

— wyjaśnienie w art. 2 wniosku, że unijne przepisy dotyczące ochrony danych osobowych, w szczególności RODO i dyrektywa o prywatności i łączności elektronicznej, mają zastosowanie do wszelkich operacji przetwarzania danych osobowych objętych zakresem wniosku (zamiast tylko w określonych kontekstach); oraz

— wyjaśnienie w odpowiednim motywie, że wniosek nie ma wpływu na stosowanie obowiązujących przepisów UE regulujących przetwarzanie danych osobowych, w tym na zadania i uprawnienia niezależnych organów nadzorczych właściwych do monitorowania zgodności z tymi instrumentami.

W odniesieniu do definicji cyberbezpieczeństwa

— wyjaśnienie poszczególnych znaczeń terminów „cyberbezpieczeństwo" i „bezpieczeństwo sieci i systemów informatycznych" oraz stosowanie terminu „cyberbezpieczeństwo" w ogóle oraz terminu „bezpieczeństwo sieci i systemów informatycznych" tylko wtedy, gdy pozwala na to kontekst (np. czysto techniczny, bez uwzględnienia wpływu na użytkowników systemów i inne osoby).

W odniesieniu do nazw domen i danych rejestracyjnych („dane WHOIS")

— jasne określenie, co stanowi „istotne informacje" do celów identyfikacji i skontaktowania się z posiadaczami nazw domen i punktami kontaktowymi zarządzającymi nazwami domen w przypadku TLD;

— bardziej szczegółowe wyjaśnienie, które kategorie danych rejestracyjnych domeny (niestanowiące danych osobowych) powinny być przedmiotem publikacji;

— doprecyzowanie, które podmioty (publiczne lub prywatne) mogą być *„ubiegającymi się o prawnie uzasadniony dostęp"*;

— wyjaśnienie, czy dane osobowe przechowywane przez rejestry TLD i podmioty świadczące usługi rejestracji nazw domen na potrzeby TLD powinny być również dostępne dla podmiotów spoza EOG, a jeżeli tak, należałoby jasno określić warunki, ograniczenia i procedury takiego dostępu, uwzględniając również, w stosownych przypadkach, wymogi art. 49 ust. 2 RODO; oraz

— udzielenie dalszych wyjaśnień co do tego, co stanowi *„zgodny z prawem i należycie uzasadniony"* wniosek, na podstawie którego udzielany jest dostęp oraz na jakich warunkach.

W odniesieniu do „proaktywnego skanowania sieci i systemów informatycznych" przez CSIRT

— wyraźne określenie rodzajów proaktywnego skanowania, o którego przeprowadzenie CSIRT może zostać poproszony, oraz określenie głównych kategorii danych osobowych, których dotyczy wniosek.

W odniesieniu do outsourcingu i łańcucha dostaw

— przy ocenie łańcuchów dostaw technologii i systemów przetwarzających dane osobowe – uwzględnienie cech umożliwiających skuteczne wdrożenie zasady ochrony danych już na etapie projektowania i domyślnej ochrony danych;

— uwzględnianie szczególnych wymogów w kraju pochodzenia, które mogą stanowić przeszkodę w przestrzeganiu unijnych przepisów dotyczących prywatności i ochrony danych, przy ocenie ryzyka związanego z łańcuchem dostaw usług, systemów lub produktów ICT; oraz

— włączenie do tekstu prawnego obowiązkowej konsultacji z EROD przy określaniu wyżej wymienionych cech oraz, w razie konieczności, do skoordynowanej oceny ryzyka sektorowego, o której mowa w motywie 46.

— zalecenie umieszczenia w motywie wzmianki, że produkty typu open source (oprogramowanie i sprzęt) z zakresu cyberbezpieczeństwa, w tym szyfrowanie typu open source, mogą zapewnić niezbędną przejrzystość umożliwiającą ograniczenie ryzyka właściwego łańcuchowi dostaw.

W odniesieniu do szyfrowania

— wyjaśnienie w motywie 54, że żaden z elementów wniosku nie powinien być rozumiany jako poparcie dla osłabienia szyfrowania typu „end-to-end" za pomocą „backdoor" lub podobnych rozwiązań.

W odniesieniu do środków zarządzania ryzykiem w cyberbezpieczeństwie

— należy uwzględnić zarówno w motywach, jak i w zasadniczej części wniosku koncepcję, zgodnie z którą włączenie perspektywy prywatności i ochrony danych do tradycyjnego zarządzania ryzykiem w zakresie cyberbezpieczeństwa zapewni całościowe podejście i umożliwi synergię z organizacjami publicznymi i prywatnymi przy zarządzaniu cyberbezpieczeństwem i ochronie przetwarzanych przez nie informacji bez niepotrzebnego powielania wysiłków;

— dodanie do tekstu prawnego obowiązku konsultowania się przez ENISA z EROD przy sporządzaniu odpowiednich porad.

W odniesieniu do naruszeń ochrony danych osobowych

— zmiana sformułowania „w rozsądnym terminie" w art. 32 ust. 1 na „bez zbędnej zwłoki".

W odniesieniu do grupy współpracy

— włączenie do tekstu prawnego uczestnictwa EROD w grupie współpracy, z uwzględnieniem związku między zadaniem tej grupy a ramami ochrony danych.

W odniesieniu do właściwości i terytorialności

— wyjaśnienie w tekście prawnym, że wniosek nie ma wpływu na kompetencje organów nadzorczych ds. ochrony danych na mocy RODO;

— zapewnienie kompleksowej podstawy prawnej dla współpracy i wymiany informacji między właściwymi organami i organami nadzorczymi, z których każdy działa w ramach odpowiednich własnych zakresów kompetencji;

— wyjaśnienie, że właściwe organy przewidziane we wniosku powinny mieć możliwość przekazywania właściwym organom nadzorczym na mocy rozporządzenia (UE) 2016/679, na wniosek lub z własnej inicjatywy, wszelkich informacji uzyskanych w kontekście wszelkich audytów i dochodzeń związanych z przetwarzaniem danych osobowych, oraz powinny zawierać w tym celu wyraźną podstawę prawną.

Bruksela, dnia 11 marca 2021 r.

Wojciech Rafał WIEWIÓROWSKI

(1) Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, uchylającej dyrektywę (UE) 2016/1148, COM(2020) 823 final.
(2) Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę, JOIN (2020) 18 final.
(3) Zob. rozdział I. WPROWADZENIE, s. 4 strategii.
(4) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194 z 19.7.2016, s. 1).