Streszczenie opinii Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego rozporządzenia ustanawiającego środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach Unii

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

(2022/C 258/07)

W dniu 22 marca 2022 r. Komisja Europejska przyjęła wniosek dotyczący rozporządzenia ustanawiającego środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach Unii („wniosek").

EIOD z zadowoleniem przyjmuje cel wniosku, jakim jest poprawa stanu cyberbezpieczeństwa w unijnych instytucjach, organach, urzędach i agencjach, a także nową rolę dawnego „zespołu reagowania na incydenty komputerowe", obecnie zwanego Centrum ds. Cyberbezpieczeństwa (CERT-UE), biorąc pod uwagę wzmożoną transformację cyfrową, szybko zmieniający się krajobraz zagrożeń cyberbezpieczeństwa oraz niedawną transformację cyfrową spowodowaną także pandemią COVID-19.

EIOD wyraża ubolewanie, że wniosek nie jest zgodny z dyrektywą w sprawie bezpieczeństwa sieci i informacji (NIS) i wnioskiem dotyczącym zmienionej dyrektywy w sprawie bezpieczeństwa sieci i systemów informatycznych (NIS 2), dzięki czemu osiągnięto by spójne i jednolite zasady dla państw członkowskich i unijnych instytucji, organów, urzędów i agencji, co przyczyniłoby się do ogólnego poziomu cyberbezpieczeństwa w Unii. EIOD zaleca, aby uzupełnić wniosek o zapis o minimalnych wymogach bezpieczeństwa mających być co najmniej takimi samymi lub wyższymi niż minimalne wymogi bezpieczeństwa podmiotów objętych dyrektywą NIS i wnioskiem NIS 2.

Aby spełnić wymogi wniosku, unijne instytucje, organy, urzędy i agencje oraz CERT-UE będą musiały wprowadzić pewne procesy i środki cyberbezpieczeństwa, co będzie wiązać się z dodatkowym przetwarzaniem danych osobowych. Aby osiągnąć pewność prawa i przewidywalność oraz zapewnić zgodność z EUDPR, EIOD zdecydowanie zaleca, aby we wniosku lub przynajmniej w akcie delegowanym, który będzie przyjęty przez Komisję w późniejszym terminie, wyraźnie określono podstawę prawną przetwarzania danych osobowych przez CERT-UE i unijne instytucje, organy, urzędy i agencje i uwzględniono w szczególności cele przetwarzania i kategorie danych osobowych.

EIOD podkreśla znaczenie uwzględnienia perspektywy prywatności i ochrony danych w zarządzaniu cyberbezpieczeństwem, aby osiągnąć pozytywną synergię między wnioskiem a przepisami dotyczącymi prywatności i ochrony danych. Przedstawia także szczegółowe zalecenia dotyczące sposobu osiągnięcia takiej synergii, w tym szczegółowe zobowiązanie urzędników UE odpowiedzialnych za cyberbezpieczeństwo do ścisłej współpracy z inspektorem ochrony danych wyznaczonym zgodnie z EUDPR.

EIOD zdecydowanie zaleca, aby wniosek przewidywał ścisłą współpracę między CERT-UE a EIOD w takich działaniach, jak reagowanie na incydenty skutkujące naruszeniem danych osobowych, reagowanie na istotne podatności na zagrożenia, istotne incydenty lub poważne ataki, które mogą potencjalnie skutkować naruszeniem danych osobowych, a także gdy CERT-UE otrzymuje sygnały, że naruszenie przepisów wniosku wiąże się z naruszeniem danych osobowych.

EIOD zdecydowanie zachęca również do tego, aby we wniosku uwzględnić udział EIOD w Międzyinstytucjonalnej Radzie ds. Cyberbezpieczeństwa (IICB).

1. WPROWADZENIE I KONTEKST

1. W dniu 22 marca 2022 r. Komisja Europejska przyjęła wniosek dotyczący rozporządzenia ustanawiającego środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach Unii ([1]) („wniosek").

2. Tego samego dnia Komisja Europejska przyjęła wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie bezpieczeństwa informacji w instytucjach, organach, urzędach i agencjach Unii ([2]) („wniosek w sprawie INFOSEC").

([1]) COM(2022) 122 final.
([2]) COM(2022) 119 final.

3. Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę przedstawiona w dniu 16 grudnia 2020 r. ([3]) („strategia") przewiduje oba wnioski. Głównym celem strategii jest wzmocnienie strategicznej autonomii Unii w dziedzinie cyberbezpieczeństwa oraz poprawa 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 ([4]).

4. Wniosek stanowi jedną z inicjatyw regulacyjnych strategii, w szczególności w dziedzinie cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach UE. Zgodnie z uzasadnieniem cel wniosku jest dwutorowy. Uwzględnia:

   — zaradzenie coraz bardziej nieprzyjaznemu krajobrazowi zagrożeń cyberbezpieczeństwa oraz nasileniu zaawansowanych cyberataków, których ofiarami są unijne instytucje, organy i agencje, co wymaga dodatkowych inwestycji na rzecz osiągnięcia wysokiego poziomu dojrzałości cybernetycznej oraz

   — wsparcie unijnego zespołu reagowania na incydenty komputerowe (CERT-UE) za pomocą ulepszonego mechanizmu finansowania, który jest niezbędny do zwiększenia jego zdolności do pomocy instytucjom, organom i agencjom UE w stosowaniu nowych przepisów dotyczących cyberbezpieczeństwa oraz do poprawy ich cyberodporności.

5. EIOD zauważa, że przedmiot omawianego wniosku wiąże się z wnioskiem dotyczącym dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylającej dyrektywę (UE) 2016/1148 („wniosek NIS 2"). EIOD nadmienia, że wydał opinię 5/2021 w sprawie strategii cyberbezpieczeństwa ([5]) i dyrektywy NIS 2 („opinia NIS 2") ([6]). Z tego powodu przedmiotowa opinia będzie odnosić się do opinii NIS 2.

6. Zgodnie ze strategią wniosek ma na celu dalszą poprawę odporności wszystkich unijnych instytucji, organów i agencji oraz ich zdolności reagowania na incydenty. Jest on również zgodny z priorytetami Komisji dotyczącymi rozwinięcia Europy na miarę ery cyfrowej i zbudowania gospodarki gotowej na przyszłość, która to gospodarka będzie przynosić korzyści obywatelom. Ponadto podkreśla się w nim, że bezpieczeństwo i odporność administracji publicznej jest podstawą cyfrowej transformacji całego społeczeństwa.

7. Zgodnie z uzasadnieniem we wniosku:

   — przedstawia się środki mające na celu zapewnienie wysokiego wspólnego poziomu cyberbezpieczeństwa dla instytucji, organów i agencji Unii Europejskiej;

   — ustanawia się Międzyinstytucjonalną Radę ds. Cyberbezpieczeństwa, która będzie odpowiedzialna za monitorowanie wdrażania proponowanego rozporządzenia;

   — ustanawia się nową rolę zespołu reagowania na incydenty komputerowe w instytucjach, agencjach i organach UE („CERT-UE") ([7]) jako Centrum ds. Cyberbezpieczeństwa dla unijnych instytucji, organów i agencji, uwzględniając rozwój sytuacji w państwach członkowskich i na świecie.

8. W dniu 22 marca 2022 r. Komisja Europejska zwróciła się do EIOD o wydanie opinii w sprawie wniosku zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 („EUDPR") ([8]). Uwagi i zalecenia zawarte w przedmiotowej opinii ograniczają się do tych przepisów wniosku, które są najistotniejsze z punktu widzenia ochrony danych i prywatności.

([3]) Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę | Kształtowanie cyfrowej przyszłości Europy (europa.eu), w tym wspólny komunikat Komisji Europejskiej i Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa (JOIN (2020)18).

([4]) Zob. rozdział I. WPROWADZENIE Strategii, str. 4

([5]) Wspólny komunikat Komisji Europejskiej i Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa do Parlamentu Europejskiego i Rady pt. „Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę".

([6]) Opinia EIOD 5/2021 w sprawie strategii cyberbezpieczeństwa i dyrektywy NIS 2.

([7]) Obecną rolę CERT-UE określa porozumienie międzyinstytucjonalne 2018/C 12/01.

([8]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295, z 21.11.2018, s. 39).

4. **WNIOSKI**

48. W świetle powyższego EIOD wydaje następujące główne zalecenia:

— EIOD zaleca, aby w motywie dodać, że wniosek opiera się na wniosku NIS 2, oraz aby w motywach 4 i 5 dokładniej wyjaśnić związek między wnioskiem a dyrektywą NIS oraz wnioskiem NIS 2. Ponadto EIOD sugeruje, aby do tekstu głównego dodać następujące sformułowanie: „Minimalne wymogi bezpieczeństwa powinny być co najmniej takie same lub wyższe niż minimalne wymogi bezpieczeństwa podmiotów objętych dyrektywą NIS i wnioskiem NIS 2";

— EIOD zdecydowanie zaleca, aby we wniosku wyraźnie określić podstawę prawną przetwarzania danych osobowych przez CERT-UE i unijne instytucje, organy, urzędy i agencje, w tym w szczególności cele przetwarzania i kategorie danych osobowych. Ponadto należy wyraźnie określić następujące elementy: a) identyfikator administratora lub administratorów, podmiotów przetwarzających lub współadministratorów, stosownie do przypadku; b) kategorie osób, których dane dotyczą; c) okresy przechowywania danych lub przynajmniej kryteria ustalania takich okresów. EIOD uważa, że powyższe elementy należy wyraźnie opisać we wniosku lub przynajmniej w akcie delegowanym, który zostanie przyjęty przez Komisję w późniejszym terminie. Wniosek powinien przewidywać taką delegację;

— EIOD zdecydowanie zaleca, aby do wykazu podstawowych środków cyberbezpieczeństwa zawartego w załączniku II do wniosku włączyć „szyfrowanie w spoczynku", „szyfrowanie w tranzycie" oraz „szyfrowanie *end-to-end*";

— EIOD zdecydowanie zaleca, aby we wniosku przewidzieć szczególny obowiązek współpracy lokalnego urzędnika ds. cyberbezpieczeństwa, o którym mowa w art. 4 ust. 5, z inspektorem ochrony danych wyznaczonym zgodnie z art. 43 EUDPR w zakresie pokrywających się działań, takich jak uwzględnienie ochrony danych już w fazie projektowania i domyślnej ochrony w środkach cyberbezpieczeństwa, wybór środków cyberbezpieczeństwa, które obejmują dane osobowe, zintegrowane zarządzanie ryzykiem oraz zintegrowane postępowanie w przypadku incydentów bezpieczeństwa;

— EIOD zdecydowanie zaleca, aby w art. 12 „Misja i zadania CERT-UE" wniosku dodać zapis: „Przy zajmowaniu się incydentami skutkującymi naruszeniem danych osobowych lub poufności łączności elektronicznej CERT-UE ściśle współpracuje z EIOD";

— EIOD zaleca, aby dodać obowiązek informowania EIOD przez CERT-UE o zajmowaniu się istotnymi podatnościami na zagrożenia, istotnymi incydentami lub poważnymi atakami, które mogą potencjalnie prowadzić do naruszenia danych osobowych lub poufności komunikacji elektronicznej;

— EIOD zaleca, aby w art.12 zapisać, że EIOD będzie uczestniczyć w działaniach CERT-UE podnoszących świadomość w zakresie cyberbezpieczeństwa w unijnych instytucjach, organach, urzędach i agencjach, aby poruszyć kwestię wzajemnych zależności między naruszeniem danych osobowych a cyberincydentami;

— EIOD zaleca, aby do art. 12 wniosku „Misja i zadania CERT-UE" dodać przepis, który określałby, że gdy do CERT-UE docierają sygnały, że naruszenie przez unijne instytucje, organy, urzędy i agencje obowiązków określonych we wniosku pociąga za sobą naruszenie danych osobowych, bez zbędnej zwłoki zawiadamia EIOD;

— EIOD zdecydowanie zaleca, aby w art. 9 ust. 3 dodać Europejskiego Inspektora Ochrony Danych jako stałego uczestnika IICB z jednym przedstawicielem.

Bruksela, 17 maja 2022 r.

Wojciech Rafał WIEWIÓROWSKI