Streszczenie opinii Europejskiego Inspektora Ochrony Danych na temat wniosku dotyczącego rozporządzenia w sprawie bezpieczeństwa informacji w instytucjach, organach i jednostkach organizacyjnych Unii

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

(2022/C 258/06)

22 marca 2022 r. Komisja Europejska przyjęła wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie bezpieczeństwa informacji w instytucjach, organach i jednostkach organizacyjnych Unii („wniosek").

EIOD z zadowoleniem przyjmuje cel wniosku, którym jest poprawa bezpieczeństwa informacji przetwarzanych przez instytucje, organy i jednostki organizacyjne Unii poprzez ustanowienie wspólnych zasad bezpieczeństwa informacji oraz promowanie spójnej kultury bezpieczeństwa informacji w ramach określonego instrumentu prawnego.

EIOD zauważa, że zakres bezpieczeństwa danych osobowych przewidziany w rozporządzeniu EUDPR tylko częściowo pokrywa się z zakresem bezpieczeństwa informacji przewidzianym we wniosku. W tym ostatnim skoncentrowano się na poufności informacji, podczas gdy w EUDPR zapewniono także integralność i dostępność. Ponadto przepisy EUDPR dotyczące bezpieczeństwa danych osobowych odnoszą się w szczególności do zagrożeń dla praw i wolności osób fizycznych.

Zgodnie z wnioskiem od instytucji, organów i jednostek organizacyjnych Unii wymaga się przyjęcia środków na rzecz bezpieczeństwa informacji, co nieuchronnie wiąże się z przetwarzaniem danych osobowych i danych z łączności elektronicznej, w tym danych o ruchu. Zdaniem EIOD należy wyraźnie zaznaczyć, że wszystkie środki na rzecz bezpieczeństwa informacji wiążące się z przetwarzaniem danych osobowych powinny być zgodne z obecnymi ramami prawnymi dotyczącymi ochrony danych i prywatności, a instytucje UE powinny podjąć odpowiednie zabezpieczenia techniczne i organizacyjne, aby zapewnić tę zgodność w sposób odpowiedzialny.

Aby osiągnąć pewność prawną i przewidywalność oraz zapewnić zgodność z EUDPR, EIOD zdecydowanie zaleca, aby we wniosku lub przynajmniej w akcie delegowanym, który ma zostać przyjęty przez Komisję w późniejszym terminie, jasno zdefiniować działania związane z przetwarzaniem danych osobowych, dozwolone dla celów tego rozporządzenia. EIOD zwraca również uwagę na konieczność zapewnienia zgodności z zasadami EUDPR dotyczącymi przekazywania danych osobowych do państw trzecich i organizacji międzynarodowych. Ponadto EIOD zaleca wyjaśnienie w motywie, że zastosowanie będą miały wszystkie przepisy EUDPR, w tym zasady transferów międzynarodowych.

EIOD podkreśla, jak ważne jest, aby uwzględnić perspektywy prywatności i ochrony danych w zarządzaniu bezpieczeństwem informacji w celu osiągnięcia pozytywnej synergii między wnioskiem a przepisami dotyczącymi prywatności i ochrony danych. Przedstawia również konkretne zalecenia dotyczące sposobu osiągnięcia takiej synergii, w tym: szczególne zobowiązanie urzędników UE odpowiedzialnych za bezpieczeństwo informacji do ścisłej współpracy z inspektorem ochrony danych wyznaczonym zgodnie z art. 43 EUDPR; włączenie pełnego szyfrowania transmisji do wykazu minimalnych środków bezpieczeństwa zawartego we wniosku, w stosownych przypadkach, a w szczególności przy wymianie szczególnie chronionych informacji jawnych; oraz promowanie zintegrowanego zarządzania ryzykiem w związku z bezpieczeństwem informacji i zintegrowanego procesu obsługi incydentów, które służą zarówno bezpieczeństwu informacji, jak i obowiązkom w zakresie ochrony danych dotyczącym powiadomień o naruszeniu danych.

1. WPROWADZENIE I INFORMACJE OGÓLNE

1. 22 marca 2022 r. Komisja Europejska przyjęła wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie bezpieczeństwa informacji w instytucjach, organach i jednostkach organizacyjnych Unii ([1]) („wniosek").

2. W tym samym dniu Komisja Europejska przyjęła kolejny wniosek dotyczący rozporządzenia ustanawiającego środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach i jednostkach organizacyjnych Unii ([2]) („Wniosek w sprawie cyberbezpieczeństwa").

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

3. Oba wnioski przewidziano w strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę przedstawionej 16 grudnia 2020 r. ([3]) („strategia"). Głównym założeniem strategii było 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 instytucji, organów i jednostek organizacyjnych Unii. Zgodnie ze strategią cel wniosku jest dwojaki:

— ułatwienie interoperacyjności systemów informacji niejawnych umożliwiającej bezproblemowy transfer informacji między różnymi podmiotami oraz

— umożliwienie przyjęcia międzyinstytucjonalnego podejścia do postępowania z informacjami niejawnymi UE oraz szczególnie chronionymi informacjami jawnymi, które mogłoby również służyć za wzór interoperacyjności między państwami członkowskimi; stwierdza się, że UE powinna również dalej rozwijać swoją zdolność do bezpiecznego komunikowania się z odpowiednimi partnerami, opierając się w miarę możliwości na istniejących ustaleniach i procedurach.

5. EIOD zauważa, że przedmiot omawianego wniosku jest również bezpośrednio związany z wnioskiem dotyczącym dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, uchylającej dyrektywę (UE) 2016/1148 („wniosek w sprawie NIS 2.0"). EIOD przypomina, że wydał opinię 5/2021 w sprawie strategii cyberbezpieczeństwa ([5]) oraz dyrektywy NIS 2.0 („opinia NIS 2.0") ([6]). Z tego powodu niniejsza opinia odnosi się do opinii NIS 2.0.

6. Zgodnie z uzasadnieniem wniosku ze względu na stale rosnącą liczbę szczególnie chronionych informacji jawnych oraz informacji niejawnych UE, którymi instytucje, organy i jednostki organizacyjne Unii muszą się wymieniać, a także biorąc pod uwagę gwałtowny rozwój zagrożeń, administracja europejska jest narażona na ataki we wszystkich obszarach swojej działalności. Informacje przetwarzane przez instytucje, organy i jednostki organizacyjne Unii są bardzo atrakcyjne dla agresorów i muszą być odpowiednio chronione.

7. Zgodnie z uzasadnieniem wniosek:

— ustanowiłby zharmonizowane i kompleksowe kategorie informacji, a także wspólne zasady postępowania dla wszystkich instytucji, organów i jednostek organizacyjnych Unii;

— utworzyłby uproszczony program współpracy w zakresie bezpieczeństwa informacji między instytucjami UE, który mógłby przyczynić się do stworzenia spójnej kultury bezpieczeństwa informacji w całej administracji europejskiej;

— zmodernizowałby politykę bezpieczeństwa informacji na wszystkich poziomach klasyfikacji lub kategorii dla wszystkich instytucji, organów i jednostek organizacyjnych Unii z uwzględnieniem transformacji cyfrowej i rozwoju telepracy jako praktyki strukturalnej.

8. 22 marca 2022 r. Komisja konsultowała się z Europejskim Inspektorem Ochrony Danych na podstawie art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 („EUDPR") ([7]). Uwagi i zalecenia zawarte w tej opinii ograniczają się do tych przepisów wniosku, które są najistotniejsze z punktu widzenia ochrony danych oraz prywatności.

([3]) Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę | Kształtowanie cyfrowej przyszłości Europy (europa.eu), w tym wspólny komunikat z Wysokim Przedstawicielem Unii ds. Zagranicznych i Polityki Bezpieczeństwa (JOIN(2020)18).

([4]) Zob. rozdział I. WPROWADZENIE, s. 4 strategii.

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

([6]) Opinia EIOD 5/2021 w sprawie strategii cyberbezpieczeństwa i dyrektywy NIS 2.0.

([7]) 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**

31. W świetle powyższego EIOD wydaje następujące główne zalecenia:

— EIOD zdecydowanie zaleca, aby we wniosku jasno zdefiniować działania związane z przetwarzaniem danych osobowych, dozwolone dla celów tego rozporządzenia, w tym: cel(e) przetwarzania; kategorie danych osobowych; kategorie osób, których dane dotyczą; określenie roli w stosownych przypadkach (administrator, podmiot przetwarzający, współadministratorzy), okresy zatrzymywania danych, odbiorcy w przypadku przekazywania danych podmiotom niepodlegającym EUDPR. EIOD uważa, że elementy te powinny zostać wyraźnie przewidziane we wniosku lub przynajmniej w akcie delegowanym, który zostanie przyjęty przez Komisję w późniejszym terminie. We wniosku powinno przewidzieć się takie przekazanie uprawnień.

— EIOD zaleca wyjaśnienie w motywie, że zastosowanie będą miały wszystkie przepisy EUDPR, w tym zasady transferów międzynarodowych. Motyw 6 można również wykorzystać do uwzględnienia wszelkich innych ogólnych zaleceń dotyczących ochrony danych zawartych w niniejszej opinii, które nie mają na celu zmiany przepisów materialnych.

— EIOD zdecydowanie zaleca włączenie pełnego szyfrowania transmisji do wykazu minimalnych środków bezpieczeństwa zawartego we wniosku, w stosownych przypadkach, a zwłaszcza w przypadku wymiany szczególnie chronionych informacji jawnych.

— EIOD zaleca dodanie w art. 5 ust. 3 zapisu, że wśród czynników branych pod uwagę w procesie zarządzania ryzykiem w zakresie bezpieczeństwa informacji należy również uwzględnić zagrożenia wynikające z dostępu na podstawie jurysdykcji państw trzecich (np. przez ich organy publiczne).

— EIOD zdecydowanie zaleca, aby w odpowiednim motywie wyjaśnić korzyści płynące z posiadania zintegrowanego zarządzania ryzykiem w związku z bezpieczeństwem informacji oraz zintegrowanego procesu obsługi incydentów, które służą zarówno bezpieczeństwu informacji, jak i obowiązkom w zakresie ochrony danych dotyczącym powiadomień o naruszeniu danych.

— EIOD zdecydowanie zaleca, aby we wniosku przewidziano nałożenie na urzędników UE odpowiedzialnych za bezpieczeństwo informacji szczególnego zobowiązania do ścisłej współpracy z inspektorem ochrony danych wyznaczonym zgodnie z art. 43 EUDPR. w takich działaniach jak: uwzględnianie ochrony danych już w fazie projektowania i domyślnej ochrony informacji w środkach bezpieczeństwa, wybór środków bezpieczeństwa, które obejmują dane osobowe, zintegrowane zarządzanie ryzykiem, zintegrowany proces obsługi cyberincydentów.

Bruksela, dnia 17 maja 2022 r.

Wojciech Rafał WIEWIÓROWSKI