EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Streszczenie opinii Europejskiego Inspektora Ochrony Danych na temat wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniającego rozporządzenie (UE) 2019/1020

(2022/C 452/07)

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

15 września 2022 r. Komisja Europejska przedstawiła wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniającego rozporządzenie (UE) 2019/1020 ([1]) (zwany dalej „wnioskiem").

EIOD z zadowoleniem przyjmuje wniosek i w pełni popiera jego ogólny cel, jakim jest poprawa funkcjonowania rynku wewnętrznego poprzez ustanowienie jednolitych ram prawnych w zakresie zasadniczych wymogów cyberbezpieczeństwa dotyczących wprowadzania do obrotu w Unii produktów z elementami cyfrowymi.

EIOD przypomina, że zgodnie z art. 5 ust. 1 lit. f) RODO bezpieczeństwo jest jedną z głównych zasad związanych z przetwarzaniem danych osobowych. W art. 32 RODO doprecyzowano ten obowiązek, który odnosi się zarówno do administratorów, jak i podmiotów przetwarzających, w celu zapewnienia odpowiedniego poziomu bezpieczeństwa. W związku z tym EIOD z zadowoleniem przyjmuje fakt, że zasady bezpieczeństwa i minimalizacji danych są już zawarte w zasadniczych wymogach cyberbezpieczeństwa wymienionych w załączniku I do wniosku. Ponadto EIOD stanowczo zaleca włączenie zasady uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych do podstawowych wymogów w zakresie cyberbezpieczeństwa produktów z elementami cyfrowymi.

Motyw 17 zawiera bardzo ważne przepisy dotyczące zarządzania, które nie znajdują odzwierciedlenia w części operacyjnej wniosku. W związku z tym w części operacyjnej wniosku EIOD zaleca określenie wszystkich aspektów związanych ze stworzeniem synergii zarówno w zakresie normalizacji, jak i certyfikacji cyberbezpieczeństwa, a także synergii między niniejszym wnioskiem a unijnym prawem o ochronie danych w obszarze nadzoru rynku i egzekwowania przepisów. Ponadto EIOD uznaje, że konieczne jest doprecyzowanie, 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 instrumentami.

EIOD z zadowoleniem przyjmuje fakt, że przepis ten uznaje przetwarzanie danych osobowych jako funkcję krytyczną i wrażliwą i może w związku z tym wymagać uzyskania europejskiego certyfikatu cyberbezpieczeństwa w ramach europejskiego programu certyfikacji cyberbezpieczeństwa odpowiednich produktów wysoce krytycznych z elementami cyfrowymi. Jednocześnie EIOD zaleca wyjaśnienie w motywie wniosku, że uzyskanie europejskiej certyfikacji cyberbezpieczeństwa na podstawie wniosku nie gwarantuje zgodności z RODO.

Ponadto EIOD z zadowoleniem przyjmuje proponowane sankcje, które są podobne do sankcji przewidzianych w RODO za naruszenie art. 32 RODO dotyczącego bezpieczeństwa przetwarzania, gdzie maksymalna grzywna wynosi 2,5 % światowego rocznego obrotu. W związku z tym wniosek mógłby służyć jako kolejny rodzaj ochrony osób fizycznych mieszkających w państwach członkowskich UE, w powiązaniu z przepisami RODO.

1. WPROWADZENIE

1. 15 września 2022 r. Komisja Europejska przedstawiła wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniającego rozporządzenie (UE) 2019/1020.

([1]) COM/2022/454 final.

2. Wniosek ma na celu poprawę funkcjonowania rynku wewnętrznego poprzez ustanowienie jednolitych ram prawnych w zakresie zasadniczych wymogów cyberbezpieczeństwa dotyczących wprowadzania do obrotu w Unii produktów z elementami cyfrowymi ([2]). W szczególności wniosek ma na celu określenie warunków brzegowych dla rozwoju bezpiecznych produktów z elementami cyfrowymi poprzez zapewnienie, aby sprzęt i oprogramowanie były wprowadzane do obrotu z mniejszą liczbą podatności, a także aby producenci poważnie traktowali bezpieczeństwo w całym cyklu życia produktu. Jego celem jest również stworzenie warunków umożliwiających użytkownikom uwzględnianie cyberbezpieczeństwa przy wyborze produktów z elementami cyfrowymi i korzystaniu z nich ([3]).

3. W związku z powyższym wniosek zawiera ([4]):

— przepisy dotyczące wprowadzania do obrotu produktów z elementami cyfrowymi w celu zapewnienia cyberbezpieczeństwa takich produktów;

— zasadnicze wymogi dotyczące projektowania, opracowywania i produkcji produktów z elementami cyfrowymi oraz obowiązki podmiotów gospodarczych w odniesieniu do tych produktów w zakresie cyberbezpieczeństwa;

— zasadnicze wymogi dotyczące procedur postępowania w przypadku wykrycia podatności wprowadzonych przez producentów w celu zapewnienia cyberbezpieczeństwa produktów z elementami cyfrowymi w całym cyklu życia oraz obowiązki podmiotów gospodarczych w odniesieniu do tych procedur;

— przepisy dotyczące nadzoru rynku i egzekwowania wyżej wymienionych przepisów i wymogów.

4. Ramy UE obejmują szereg horyzontalnych aktów prawnych, które obejmują niektóre aspekty związane z cyberbezpieczeństwem z różnych punktów widzenia (produkty, usługi, zarządzanie kryzysowe i przestępstwa). W 2013 r. weszła w życie dyrektywa dotycząca ataków na systemy informatyczne ([5]), w której dokonano harmonizacji kar za niektóre przestępstwa dotyczące systemów informatycznych. W sierpniu 2016 r. dyrektywa (UE) 2016/1148 ([6]) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa NIS) weszła w życie jako pierwszy ogólnounijny akt prawny dotyczący cyberbezpieczeństwa. Rewizja tego aktu zaowocowała przyjęciem dyrektywy NIS2 i zawiesiła jeszcze wyżej poprzeczkę, jeśli chodzi o cyberbezpieczeństwo usług ICT. W 2019 r. wszedł w życie unijny akt dotyczący cyberbezpieczeństwa ([7]), którego celem jest zwiększenie bezpieczeństwa produktów ICT, usług ICT i procesów ICT poprzez wprowadzenie dobrowolnych europejskich ram certyfikacji cyberbezpieczeństwa.

5. Niniejszą opinię EIOD wydano w odpowiedzi na konsultacje przeprowadzone przez Komisję Europejską dnia 15 września 2022 r. zgodnie z art. 42 ust. 1 EUDPR. Europejski Inspektor Ochrony Danych z zadowoleniem przyjmuje odniesienie się do tych konsultacji w motywie 71 wniosku. W tym względzie EIOD z zadowoleniem zauważa, że uprzednio przeprowadzono już z nim nieformalne konsultacje, zgodnie z motywem 60 EUDPR.

3. WNIOSKI

31. W świetle powyższego EIOD wydaje następujące zalecenia:

(1) uwzględnienie ochrony danych w fazie projektowania oraz domyślnej ochrony danych w kluczowych wymogach cyberbezpieczeństwa produktów z elementami cyfrowymi;

([2]) Motyw 1 wniosku.
([3]) Motyw 2 wniosku.
([4]) Artykuł 1 wniosku
([5]) Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (Dz.U. L 218 z 14.8.2013, s. 8).
([6]) 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).
([7]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.U. L 151, 7.6.2019, s.15).

(2) wyjaśnienie w preambule znaczenia produktów z elementami cyfrowymi, które wykonują operacje kryptograficzne – w tym szyfrowanie odpowiednich danych odłożonych i danych przesyłanych oraz pseudonimizację – które są niezbędne do zapewnienia skutecznego bezpieczeństwa informacji, cyberbezpieczeństwa, ochrony danych i prywatności;

(3) dodanie do załącznika II materialnych i niematerialnych produktów z elementami cyfrowymi do przeprowadzania operacji kryptograficznych;

(4) usunięcie rozporządzenia (UE) 2017/745 ([8]) z wykazu aktów prawnych wyłączonych ze stosowania wniosku;

(5) wyraźne wyjaśnienie we wniosku elementów zasadniczych wymagań, o których mowa w art. 3 ust. 3 lit. e) dyrektywy 2014/53/UE ([9]) w sprawie danych osobowych i prywatności;

(6) określenie w części operacyjnej wniosku praktycznych aspektów związanych z tworzeniem synergii zarówno w zakresie normalizacji, jak i certyfikacji cyberbezpieczeństwa, a także synergii między niniejszym wnioskiem a unijnymi przepisami prawa o ochronie danych w dziedzinie nadzoru rynku i egzekwowania przepisów;

(7) doprecyzowanie, 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;

(8) dodanie odpowiednich definicji „bezpłatnego oprogramowania", „otwartego oprogramowania" oraz „bezpłatnego i otwartego oprogramowania";

(9) wyjaśnienie w motywie wniosku, że uzyskanie europejskiej certyfikacji cyberbezpieczeństwa na podstawie wniosku nie gwarantuje zgodności z RODO.

Bruksela, 9 listopada 2022 r.

Wojciech Rafał WIEWIÓROWSKI

([8]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/745 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych, zmiany dyrektywy 2001/83/WE, rozporządzenia (WE) nr 178/2002 i rozporządzenia (WE) nr 1223/2009 oraz uchylenia dyrektyw Rady 90/385/EWG i 93/42/EWG (Dz.U. L 117 z 5.5.2017, s. 1).

([9]) Dyrektywa Parlamentu Europejskiego i Rady 2014/53/UE z dnia 16 kwietnia 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do udostępniania na rynku urządzeń radiowych i uchylająca dyrektywę 1999/5/WE (Dz.U. L 153, 22.5.2014, s. 62).