Streszczenie opinii Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 oraz (UE) nr 909/2014

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

(2021/C 229/05)

Komisja Europejska przyjęła w dniu 24 września 2020 r. wniosek dotyczący rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 oraz (UE) nr 909/2014 („Wniosek"). Wniosek wprowadza kompleksowe ramy operacyjnej odporności cyfrowej dla podmiotów sektora finansowego UE w oparciu o pięć kluczowych obszarów, a mianowicie: zarządzanie ryzykiem związanym z ICT (rozdział II), zarządzanie incydentami, ich klasyfikację i zgłaszanie (rozdział III), testowanie operacyjnej odporności cyfrowej (rozdział IV), zarządzanie ryzykiem i regulacje dotyczące zewnętrznych dostawców krytycznych usług ICT (rozdział V) oraz wymianę informacji (rozdział VI).

Europejski Inspektor Ochrony Danych z zadowoleniem przyjmuje cele wniosku i uważa, że dla stabilności rynku finansowego Unii Europejskiej zasadnicze znaczenie ma to, by instytucje finansowe posiadały solidne, kompleksowe i dobrze udokumentowane ramy zarządzania ryzykiem w zakresie ICT.

Podkreśla konieczność zapewnienia, by wszelkie operacje przetwarzania danych w kontekście działalności podmiotów finansowych opierały się na jednej z podstaw prawnych określonych w art. 6 RODO ([1]). Zaznacza też, jak ważne dla podmiotów finansowych jest włączenie do ich ram operacyjnej odporności cyfrowej silnego mechanizmu zarządzania ochroną danych, w którym wyraźnie określa się role i obowiązki administratora i podmiotu przetwarzającego, a także czynności przetwarzania, które zostaną przeprowadzone.

W odniesieniu do międzynarodowego przekazywania danych zewnętrznym dostawcom usług ICT mającym siedzibę w państwie trzecim Europejski Inspektor Ochrony Danych przypomina, że wszelkie międzynarodowe operacje przekazywania danych osobowych muszą spełniać wymogi rozdziału V RODO zgodnie z wykładnią zawartą w orzecznictwie TSUE, w tym w wyroku w sprawie *Schrems II*.

Odnosząc się do ustaleń dotyczących wymiany informacji wywiadowczych i informacji o cyberzagrożeniach między podmiotami finansowymi, Inspektor podkreśla, że ochrona danych osobowych nie stanowi przeszkody dla wymiany informacji wywiadowczych w sektorze finansowym. Wymogi dotyczące ochrony danych powinny być raczej postrzegane jako podstawowy warunek, który należy spełnić, aby zapewnić ochronę praw osób fizycznych. W tym kontekście EIOD zachęca do przyjęcia również w sektorze finansowym kodeksów postępowania zgodnie z art. 40 RODO, w szczególności po to, aby jasno określić role głównych zainteresowanych stron w przetwarzaniu danych osobowych, a także zapewnić uczciwe i przejrzyste przetwarzanie.

EIOD zaleca, aby w odniesieniu do publikacji grzywien administracyjnych wśród kryteriów branych pod uwagę przez właściwy organ uwzględnić ryzyko dla ochrony danych osobowych osób fizycznych. Przypomina też, że zasada ograniczenia przechowywania danych wymaga, by były one przechowywane nie dłużej niż jest to konieczne do celów, dla których dane te są przetwarzane.

Inspektor podkreśla w odniesieniu do zgłaszania przypadków naruszenia danych, że brzmienie motywu 42 wniosku jest niezgodne z art. 33 RODO. W związku z tym zaleca usunięcie odniesienia do organów ochrony danych z motywu 42 wniosku, jak również nieznaczną zmianę art. 17 wniosku zgodnie z zaleceniami zawartymi w niniejszej opinii.

1. KONTEKST

1. Komisja Europejska przyjęła w dniu 24 września 2020 r. wniosek dotyczący rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniającego rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 oraz (UE) nr 909/2014 („**Wniosek**"). Wniosek wprowadza kompleksowe ramy operacyjnej odporności cyfrowej dla podmiotów sektora finansowego UE w oparciu o pięć kluczowych obszarów, a mianowicie: zarządzanie ryzykiem związanym z ICT (rozdział II), zarządzanie incydentami, ich klasyfikację i zgłaszanie (rozdział III), testowanie operacyjnej odporności cyfrowej (rozdział IV), zarządzanie ryzykiem i regulacje dotyczące zewnętrznych dostawców krytycznych usług ICT (rozdział V) oraz wymianę informacji (rozdział VI).

2. Niniejszy wniosek jest częścią pakietu, który obejmuje również wniosek dotyczący rozporządzenia w sprawie tworzenia rynków kryptoaktywów ([2]) („**rozporządzenie MICA**"), wniosek w sprawie systemu pilotażowego dla infrastruktur rynkowych opartych na DLT ([3]) raz wniosek mający na celu wyjaśnienie lub zmianę niektórych powiązanych przepisów UE dotyczących usług finansowych ([4]). Przeprowadzono konsultacje z Europejskim Inspektorem Ochrony Danych w sprawie wniosku dotyczącego systemu pilotażowego dla infrastruktur rynkowych opartych na DLT i wydał on swoją opinię w dniu 23 kwietnia 2021 r. ([5]) Zwrócono się do niego również w sprawie rozporządzenia MiCA w dniu 29 kwietnia 2021 r. i wyda on swoją opinię zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([6]).

3. W dniu 15 marca 2021 r. Komisja Europejska zwróciła się do Europejskiego Inspektora Ochrony Danych („EIOD") o wydanie opinii w sprawie wniosku, zgodnie z art. 42 ust. 1 rozporządzenia (UE) 2018/1725. Uwagi te ograniczają się do przepisów wniosku, które są istotne z punktu widzenia ochrony danych.

4. WNIOSKI

W związku z powyższym EIOD:

— Podkreśla znaczenie zapewnienia, by wszelkie operacje przetwarzania danych w kontekście działalności podmiotów finansowych **opierały się na jednej z podstaw prawnych określonych w art. 6 RODO**, oraz wskazuje art. 6 ust. 1 lit. c), e) i f) RODO jako możliwe podstawy prawne do rozważenia przez podmioty finansowe.

— Zaznacza też, jak ważne jest dla podmiotów finansowych włączenie do ich ram operacyjnej odporności cyfrowej **silnego mechanizmu zarządzania** ochroną danych, w którym wyraźnie określa się role i obowiązki administratora i podmiotu przetwarzającego, a także czynności przetwarzania, które zostaną przeprowadzone.

— EIOD przypomina, że **wszelkie międzynarodowe transfery danych osobowych przez podmioty finansowe** do zewnętrznego dostawcy usług ICT mającego siedzibę w państwie trzecim **muszą być zgodne z wymogami rozdziału V GDPR**, a w przypadku ich dokonywania muszą podlegać odpowiednim zabezpieczeniom zgodnie z ramami ochrony danych i orzecznictwem TSUE, w szczególności w sprawie Schrems II. Takie podmioty finansowe mogą odwoływać się do standardowych klauzul umownych, ponieważ wydaje się, że jest to najbardziej odpowiednie narzędzie transferu.

— EIOD podkreśla**, że ochrona danych osobowych nie stanowi przeszkody dla innowacji, w szczególności dla rozwoju nowych technologii w sektorze finansowym**. Wymogi dotyczące ochrony danych powinny być raczej postrzegane jako podstawowy warunek, który należy spełnić, aby zapewnić ochronę praw osób fizycznych w ramach cyfrowej odporności operacyjnej podmiotów finansowych.

— EIOD **zachęca do przyjęcia również w sektorze finansowym kodeksów postępowania** zgodnie z art. 40 RODO, zwłaszcza w celu jasnego określenia roli głównych zainteresowanych stron w przetwarzaniu danych osobowych, jak również zapewnienia uczciwego i przejrzystego przetwarzania.

— Odnosząc się do **publikacji sankcji administracyjnych**, EIOD zaleca uwzględnienie wśród kryteriów branych pod uwagę przez właściwy organ **ryzyka związanego z ochroną danych osobowych osób fizycznych**.

— Zgodnie z zasadą ograniczenia przechowywania EIOD zachęca, aby podmioty finansowe przyjęły środki zapewniające **usunięcie informacji o grzywnach administracyjnych z ich strony internetowej po upływie pięciu lat lub wcześniej**, jeżeli nie są one już potrzebne.

— EIOD podkreśla, że **sformułowanie motywu 42 wniosku jest niezgodne z art. 33 RODO**. EIOD zaleca zatem usunięcie odniesienia do organów ochrony danych z motywu 42 wniosku, jak również zmianę art. 17 wniosku w celu włączenia odniesienia do obowiązku powiadamiania odpowiednich organów ochrony danych o naruszeniach ochrony danych.

— EIOD zaleca zmianę art. 23 ust. 2 wniosku, aby zagwarantować, że testowanie, rozwój produktów lub badania systemów TIK nie mogą być przeprowadzane na działających systemach produkcyjnych zawierających dane osobowe klientów.

Bruksela, dnia 10 maja 2021 r.

Wojciech Rafał WIEWIÓROWSKI

(1) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

(2) *Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie rynków kryptoaktywów oraz zmieniającego dyrektywę (UE) 2019/1937, COM/2020/593 final. Dostępny pod adresem: EUR-Lex – 52020PC0593 – PL – EUR-Lex (europa.eu).*

(3) *Wniosek dotyczący ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY w sprawie systemu pilotażowego na potrzeby infrastruktur rynkowych opartych na technologii rozproszonego rejestru COM/2020/594 final, dostępny pod adresem:EUR-Lex – 52020PC0593 – PL – EUR-Lex (europa.eu)*

(4) *Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady zmieniającej dyrektywy 2006/43/WE, 2009/65/WE, 2009/138/WE, 2011/61/UE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366 i (UE) 2016/2341, COM/2020/596 final. Dostępny pod adresem: EUR-Lex – 52020PC0596 – PL – EUR-Lex (europa.eu).*

(5) *Opinia 6/2021 w sprawie wniosku dotyczącego systemu pilotażowego dla infrastruktur rynkowych opartych na technologii rozproszonego rejestru, dostępna pod adresem 2021-0219_d0912_opinion_6_2021_en_0.pdf (europa.eu)*

(6) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1727 z dnia 14 listopada 2018 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych (Eurojust) oraz zastąpienia i uchylenia decyzji Rady 2002/187/WSiSW (Dz.U. L 295 z 21.11.2018, s. 138).