C/2023/1054

20.11.2023

Streszczenie opinii Europejskiego Inspektora Ochrony Danych na temat wniosku dotyczącego rozporządzenia w sprawie ram dostępu do danych finansowych

(C/2023/1054)

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

28 czerwca 2023 r. Komisja Europejska przedstawiła wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ram dostępu do danych finansowych oraz zmiany rozporządzeń (UE) nr 1093/2010, (UE) nr 1094/2010, (UE) nr 1095/2010 i (UE) 2022/2554 („wniosek"). Celem wniosku jest wspieranie rozwoju usług i produktów finansowych opartych na danych poprzez zapewnienie konsumentom i firmom lepszej kontroli nad dostępem do ich danych finansowych.

EIOD z zadowoleniem przyjmuje fakt, że celem wniosku jest umożliwienie klientom – w tym osobom, których dane dotyczą – decydowania, w jaki sposób i przez kogo są wykorzystywane ich dane. Zauważa jednak, że definicja „danych klienta" jest szczególnie szeroka i potencjalnie obejmuje dane osobowe o bardzo wrażliwym charakterze. Kategorie danych osobowych, które mają być udostępniane na podstawie wniosku, powinny być jasno określone, a przy ich określeniu należy uwzględnić ryzyko dla osób fizycznych, których dane osobowe byłyby dostępne i wykorzystywane. Europejski Inspektor Ochrony Danych zaleca również wyraźne wyłączenie z definicji „danych klienta" danych utworzonych w wyniku profilowania.

EIOD z zadowoleniem przyjmuje fakt, że wniosek przewiduje nałożenie szeregu obowiązków na posiadaczy danych i użytkowników danych, co mogłoby mieć pozytywny wpływ na poziom ochrony danych osobowych. Aby osiągnąć ten cel, użytkownicy danych powinni być zobowiązani do jasnego określenia, w odniesieniu do każdego zapytania, konkretnych kategorii danych klientów, do których to danych chcą uzyskać dostęp. We wniosku należałoby także zawrzeć zakaz odmowy świadczenia usług finansowych klientom, którzy nie zainstalują panelu do zarządzania zezwoleniami i nie skorzystają z niego ani w inny sposób nie umożliwią udostępniania danych przez posiadaczy danych użytkownikom danych w sposób przewidziany we wniosku.

EIOD uważa, że wyraźne wyznaczenie i zdecydowane egzekwowanie dozwolonego zakresu wykorzystania danych jest niezbędne do określenia stosownych sposobów wykorzystania danych osobowych i ochrony konsumentów podatnych na zagrożenia. W tym względzie EIOD z zadowoleniem przyjmuje fakt, że wniosek przewiduje, że Europejski Urząd Nadzoru Bankowego i Europejski Urząd Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych przygotują wytyczne we współpracy z Europejską Radą Ochrony Danych (EROD). Aby zapewnić pełną zgodność tych wytycznych z przepisami o ochronie danych, EIOD uważa, że konieczne są formalne konsultacje z EROD. EIOD zaleca również rozszerzenie zakresu przyszłych wytycznych na inne odpowiednie produkty i usługi finansowe, takie jak umowy o kredyt hipoteczny, usługi płatnicze, inne produkty ubezpieczeniowe, produkty inwestycyjne i produkty emerytalne. W wytycznych należy także wypracować, w stosownych przypadkach, ograniczenia dotyczące łączenia „danych klienta" z innymi rodzajami danych osobowych, takimi jak dane osobowe uzyskane ze źródeł zewnętrznych (np. mediów społecznościowych lub przedsiębiorstw pośredniczących w obrocie danymi).

EIOD zaleca zapewnienie ścisłej współpracy między właściwymi organami w rozumieniu wniosku a organami nadzorującymi ochronę danych, aby zapewnić spójność między stosowaniem i egzekwowaniem wniosku a unijnym prawem ochrony danych. Tego rodzaju ścisłej współpracy sprzyjałoby doprecyzowanie, w jakich okolicznościach właściwe organy mogą konsultować się z organami ochrony danych i wymieniać się z nimi informacjami.

1. Wprowadzenie

1. 28 czerwca 2023 r. Komisja Europejska przedstawiła wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ram dostępu do danych finansowych oraz zmiany rozporządzeń (UE) nr 1093/2010, (UE) nr 1094/2010, (UE) nr 1095/2010 i (UE) 2022/2554 ([1]) („wniosek").

2. Celem wniosku jest wspieranie rozwoju usług i produktów finansowych opartych na danych poprzez zapewnienie konsumentom i firmom lepszej kontroli dostępu do ich danych finansowych ([2]). Dzięki temu wniosek umożliwiłby konsumentom i przedsiębiorstwom korzystanie z produktów i usług finansowych nieograniczonych do płatności, które to produkty i usługi są dostosowane do ich potrzeb na podstawie istotnych dla nich danych. Jednocześnie wniosek ma na celu przeciwdziałanie zagrożeniom, które są nieodłącznie wpisane w prowadzone na większą skalę udostępnianie danych finansowych i szerszy dostęp do nich ([3]).

([1]) COM(2023) 360 final.
([2]) COM(2023) 360 final, s. 1.
([3]) COM(2023) 360 final, s. 1.

3. Wniosek stanowi element sektorowy, który wpisuje się w szerszą europejską strategię w zakresie danych i umożliwia udostępnianie danych w ramach sektora finansowego i z innymi sektorami ([4]). Ma on bezpośredni związek z jednym z priorytetów strategii Komisji dla UE w zakresie finansów cyfrowych, zwłaszcza tworzeniem europejskiej przestrzeni danych finansowych w celu wspierania innowacji wykorzystujących potencjał danych w oparciu o europejską strategię w zakresie danych ([5]), w tym zwiększenie dostępu do danych i udostępniania danych w sektorze finansowym ([6]).

4. Zasadniczo wniosek zakłada:

   a. ustanowienie zasad, zgodnie z którymi określone kategorie „danych klientów" – w tym dane osobowe – w finansach ([7]) mogłyby być udostępniane i wykorzystywane przez instytucje finansowe i dostawców usług z zakresu informacji finansowych – „uprawnione podmioty" ([8]) – występujące w charakterze posiadaczy danych ([9]) lub użytkowników danych ([10]);

   b. zapewnienie klientowi – który może być osobą fizyczną lub prawną ([11]) – prawa do żądania od posiadacza danych, aby udostępnił te dane użytkownikowi danych w celach i na warunkach uzgodnionych między użytkownikiem danych a klientem ([12]);

   c. nałożenie pewnych obowiązków na użytkowników danych otrzymujących dane na wniosek klientów i określenie pewnych granic tego, w jaki sposób można wykorzystywać dane klientów ([13]);

   d. upoważnienie Europejskiego Urzędu Nadzoru Bankowego („EUNB") i Europejskiego Urzędu Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych („EIOPA") – działających we współpracy z Europejską Radą Ochrony Danych („EROD") – do opracowania ukierunkowanych wytycznych dotyczących obszarów, w których udostępnianie danych i dostęp do danych w sposób przewidziany we wniosku mogłyby wiązać się z większym ryzykiem wykluczenia klientów ([14]), co oznaczałoby tym samym wyznaczenie „zakresu wykorzystania danych" ([15]);

   e. umożliwienie klientom monitorowania zezwoleń dostępu do danych i zarządzania tymi zezwoleniami, udzielonymi przez nich użytkownikom danych za pośrednictwem paneli do zarządzania zezwoleniami w ramach otwartych finansów (które mają być obowiązkowo konfigurowane przez posiadaczy danych) ([16]); oraz

   f. wprowadzenie wymogów dotyczących tworzenia systemów udostępniania danych finansowych i zarządzania systemami udostępniania danych finansowych, których stronami byliby posiadacze danych, użytkownicy danych i organizacje konsumenckie, w celu opracowania (między innymi) standardów danych i interfejsów oraz wspólnych standaryzowanych ram umownych regulujących dostęp do określonych zbiorów danych ([17]).

([4]) COM(2023) 360 final, s. 3.
([5]) Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów zatytułowany „Europejska strategia w zakresie danych" (COM(2020) 66 final, 19.2.2020).
([6]) Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie strategii dla UE w zakresie finansów cyfrowych (COM(2020) 591 final, 24.9.2020, s. 3 i 4).
([7]) Wymienione w art. 2 ust. 1 wniosku.
([8]) Wymienione w art. 2 ust. 2 wniosku.
([9]) Artykuł 3 pkt 5 wniosku. „»posiadacz danych« oznacza instytucję finansową inną niż dostawca świadczący usługę dostępu do informacji o rachunku, która gromadzi, przechowuje i w inny sposób przetwarza dane wymienione w art. 2 ust. 1".
([10]) Artykuł 3 pkt 6 wniosku: „»użytkownik danych« oznacza dowolny z podmiotów wymienionych w art. 2 ust. 2, który – po uzyskaniu zgody klienta – ma zgodny z prawem dostęp do danych klienta wymienionych w art. 2 ust. 1".
([11]) Artykuł 3 pkt 2 wniosku.
([12]) Artykuł 5 wniosku.
([13]) Artykuł 6 wniosku.
([14]) W szczególności produkty i usługi związane z punktową oceną kredytową konsumentów oraz oceną ryzyka, a także ustalaniem cen dla konsumentów w przypadku produktów związanych z ubezpieczeniem na życie, ubezpieczeniem zdrowotnym i chorobowym. Zob. również motyw 18 wniosku.
([15]) Artykuł 7 wniosku.
([16]) Artykuł 8 wniosku.
([17]) Tytuły IV i V wniosku.

5. Niniejszą opinię EIOD wydano w odpowiedzi na konsultacje przeprowadzone przez Komisję Europejską 29 czerwca 2023 r. zgodnie z art. 42 ust. 1 rozporządzenia ([18]) 2018/1725. EIOD z zadowoleniem przyjmuje odniesienie się do tych konsultacji w motywie 54 wniosku. W tym względzie EIOD z zadowoleniem zauważa również, że uprzednio przeprowadzono już z nim nieformalne konsultacje, zgodnie z motywem 60 rozporządzenia 2018/1725.

8. **Wnioski**

54. W świetle powyższego EIOD zaleca, co następuje:

(1) doprecyzowanie w motywie 48, że przetwarzanie danych osobowych w kontekście rozporządzenia, którego dotyczy wniosek, powinno odbywać się zgodnie z RODO ([19]), rozporządzeniem 2018/1725 oraz dyrektywą o e-prywatności ([20]);

(2) wyraźne określenie kategorii danych osobowych zawartych w art. 2 ust. 1 wniosku, z uwzględnieniem charakteru usług i produktów finansowych oferowanych przez kwalifikujące się podmioty wymienione w art. 2 ust. 2 wniosku oraz ryzyka dla osób fizycznych, których dane osobowe byłyby dostępne i wykorzystywane przez użytkowników danych;

(3) wyraźne wyłączenie z definicji „danych klienta", zawartej w art. 3 pkt 3 wniosku, danych utworzonych w wyniku profilowania;

(4) dla uniknięcia wszelkich niejasności między terminem „zezwolenie" w rozumieniu wniosku a podstawą prawną przetwarzania na podstawie RODO – dodatkowe wyjaśnienie w motywie 48, że zezwolenia nie należy rozumieć jako „zgody" ani „wyraźnej zgody", ani „niezbędności do wykonania umowy" w rozumieniu definicji zawartych w RODO;

(5) wprowadzenie do części normatywnej wniosku przepisu, który zakazywałby odmowy świadczenia usług finansowych wymienionych w art. 2 ust. 2 wniosku klientom, którzy nie zainstalują panelu do zarządzania zezwoleniami przewidzianego w art. 8 wniosku i nie skorzystają z niego ani w inny sposób nie umożliwią udostępniania danych przez posiadaczy danych użytkownikom danych w sposób przewidziany we wniosku;

(6) włączenie do art. 6 wniosku wymogu, aby użytkownicy danych wyraźnie określali w swoich wnioskach o dostęp do danych klientów konkretne kategorie danych klientów, do których to danych chcą uzyskać dostęp;

(7) dokonanie zmiany brzmienia art. 6 ust. 2 wniosku w następujący sposób: „Użytkownik danych składa wniosek o udostępnienie danych i uzyskuje dostęp do danych klienta udostępnionych na podstawie art. 5 ust. 1, przy czym dostęp ten jest adekwatny, stosowny i niezbędny, wyłącznie do celów i na warunkach, w związku z którymi dany klient udzielił zezwolenia";

(8) doprecyzowanie, że użytkownik danych może kontaktować się z klientami w celach marketingu bezpośredniego wyłącznie za ich uprzednią zgodą lub z ofertami produktów lub usług podobnych do tych, w odniesieniu do których uzyskał dostęp do danych klientów, oraz na warunkach określonych w art. 13 ust. 2 dyrektywy o e-prywatności;

(9) włączenie do art. 7 wniosku wyraźnego odniesienia do konieczności przestrzegania istniejących unijnych przepisów i wytycznych sektorowych dotyczących dostępu do danych osobowych i ich wykorzystywania do celów świadczenia usług i dostarczania produktów finansowych objętych zakresem wniosku;

(10) zapewnienie przeprowadzenia zarówno przez EUNB, jak i EIOPA formalnych konsultacji z EROD podczas opracowywania proponowanych wytycznych w sprawie zakresu wykorzystania danych – poprzez dodanie w art. 7 ust. 4 po słowach „ściśle współpracują" sformułowania „i przeprowadzają formalne konsultacje";

(11) zapewnienie przyjęcia wytycznych, o których mowa w art. 7, po przeprowadzeniu formalnych konsultacji z EROD w najwcześniejszym możliwym terminie, biorąc pod uwagę datę rozpoczęcia stosowania wniosku;

([18]) 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 oraz w sprawie swobodnego przepływu takich osób danych oraz uchylające rozporządzenie (WE) nr 45/2001 i decyzję nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39).

([19]) 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).

([20]) Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (Dyrektywa o prywatności i łączności elektronicznej) (Dz.U. L 201 z 31.7.2002, s. 37).

(12) rozszerzenie zakresu wytycznych, o których mowa w art. 7, na inne ważne produkty i usługi finansowe objęte zakresem wniosku;

(13) doprecyzowanie, że wytyczne, o których mowa w art. 7, powinny dotyczyć także, w stosownych przypadkach, ograniczeń w łączeniu „danych klientów" uzyskanych w sposób przewidziany we wniosku z innymi rodzajami danych osobowych;

(14) zobowiązanie użytkowników danych na podstawie art. 8 ust. 4 lit. b) do informowania posiadaczy danych również o rachunku klienta, produkcie finansowym lub usłudze finansowej, do których chcą uzyskać dostęp;

(15) zobowiązanie użytkowników danych na podstawie art. 8 ust. 4 lit. b) do informowania posiadaczy danych o podstawie prawnej określonej w art. 6 ust. 1 RODO oraz (w stosownych przypadkach) wyjątku przewidzianym w art. 9 ust. 2 RODO, na którym będą się opierać, aby uzyskać dostęp do danych osobowych zawartych w zbiorze danych klienta;

(16) doprecyzowanie w art. 8 wniosku, że panel do zarządzania zezwoleniami nie powinien być zaprojektowany w sposób, który zachęcałby klienta do udzielania lub wycofywania zezwoleń lub wywierał na niego nienależyty wpływ;

(17) zobowiązanie użytkowników danych do wykazania posiadaczom danych w odpowiedni sposób, że uzyskali od klienta zezwolenie na dostęp do danych klienta będących w posiadaniu posiadacza danych;

(18) jeżeli użytkownicy danych mogą wystąpić z wnioskiem o dostęp do danych klienta w imieniu klienta – zobowiązanie posiadaczy danych do żądania (a użytkowników danych do dostarczenia) dowodu uprawnień do reprezentowania klienta udzielonych przez klienta;

(19) dokonanie zmiany art. 14 ust. 7 wniosku w celu doprecyzowania, że właściwe organy mogą cofnąć zezwolenie, którego udzieliły dostawcy usług z zakresu informacji finansowych, jeżeli organy nadzorcze w rozumieniu RODO stwierdzą, że dostawca usług z zakresu informacji finansowych naruszył swoje obowiązki wynikające z unijnych przepisów o ochronie danych;

(20) wprowadzenie definicji „usług z zakresu informacji finansowych" do art. 3 wniosku;

(21) zobowiązanie systemów udostępniania danych finansowych do określenia minimalnych środków technicznych i organizacyjnych, które członkowie tego systemu powinni wdrożyć, aby zapewnić odpowiedni poziom bezpieczeństwa danych osobowych będących przedmiotem wymiany;

(22) zastąpienie zwrotu „podobnych do tych przygotowywanych przez administratorów i podmioty przetwarzające na podstawie art. 40 rozporządzenia (UE) 2016/679" po słowach „sporządzania kodeksów postępowania" w motywie 25 wniosku zwrotem „zgodnie z art. 40 RODO";

(23) doprecyzowanie, że organy nadzorcze w rozumieniu RODO należą do „[innych] odpowiednich organów publicznych" lub „innych właściwych organów", z którymi zgodnie z art. 14 ust. 1 i art. 10 ust. 6 wniosku mają konsultować się właściwe organy; oraz

(24) uwzględnienie w art. 18 ust. 3 wniosku wyraźnego odniesienia do organów nadzorczych w rozumieniu RODO.

Bruksela, 22 sierpnia 2023 r.

Wojciech Rafał WIEWIÓROWSKI