Dziennik Urzędowy
Unii Europejskiej

PL
Seria L

2025/2050

9.10.2025

ROZPORZĄDZENIE DELEGOWANE KOMISJI (UE) 2025/2050

z dnia 1 lipca 2025 r.

uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 poprzez ustanowienie warunków technicznych i procedur, zgodnie z którymi dostawcy bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych mają udostępniać dane zweryfikowanym badaczom

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE ([1]), w szczególności jego art. 40 ust. 13,

a także mając na uwadze, co następuje:

(1) W art. 40 rozporządzenia (UE) 2022/2065 ustanowiono zasady dostępu do danych, który ma być udzielany przez dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych. W szczególności umożliwia on badaczom, którzy pomyślnie przeszli proces wykazania, że spełniają warunki określone w ust. 8 tego artykułu („zweryfikowani badacze"), aby uzyskać taki dostęp.

(2) Zgodnie z art. 40 ust. 4 rozporządzenia (UE) 2022/2065 zweryfikowanym badaczom zapewnia się dostęp do danych, aby pomóc im w badaniu ryzyka systemowego w Unii i ocenie skuteczności środków służących ograniczeniu tego ryzyka. Ich ustalenia mogą stanowić cenny wkład w egzekwowanie rozporządzenia (UE) 2022/2065 i sprzyjać rozliczalności dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych. Celem niniejszego rozporządzenia jest określenie warunków technicznych i procedur niezbędnych do umożliwienia takiego dostępu w sposób bezpieczny i skuteczny, spójny dla wszystkich koordynatorów ds. usług cyfrowych oraz zapewniający równe traktowanie badaczy i dostawców danych.

(3) Aby zapewnić spójność procesu dostępu do danych przez wszystkich koordynatorów ds. usług cyfrowych oraz aby proces ten był jasny i przejrzysty dla wszystkich, konieczne jest stworzenie specjalnej infrastruktury cyfrowej („portal dostępu do danych na potrzeby DSA"). Portal dostępu do danych na potrzeby DSA powinien umożliwiać badaczom, dostawcom danych i koordynatorom ds. usług cyfrowych udział w procesie dostępu do danych, dostęp do odpowiednich informacji, takich jak dane specjalnych punktów kontaktowych, oraz ich rozpowszechnianie, a także komunikowanie się ze sobą. Portalu dostępu do danych na potrzeby DSA nie należy uznawać za jedną z form dostępu wykorzystywanych do zapewnienia dostępu do danych na uzasadniony wniosek.

(4) Dostawcy danych i badacze pragnący uczestniczyć w procesie dostępu do danych powinni w tym celu utworzyć konto na portalu dostępu do danych na potrzeby DSA. Aby zapewnić koordynatorom ds. usług cyfrowych możliwość dostępu do informacji przekazywanych za pośrednictwem portalu dostępu do danych na potrzeby DSA bez konieczności tworzenia odrębnego konta w portalu, portal dostępu do danych na potrzeby DSA powinien być interoperacyjny z systemem wymiany informacji AGORA ustanowionym w rozporządzeniu wykonawczym Komisji (UE) 2024/607 ([2]).

(5) Aby zapewnić przejrzystość procesu dostępu do danych przez wszystkie zaangażowane strony oraz monitorować skuteczność i efektywność procesu dostępu do danych oraz zgodność z art. 40 ust. 4 rozporządzenia (UE) 2022/2065 i niniejszym rozporządzeniem, portal dostępu do danych na potrzeby DSA powinien generować automatyczne powiadomienia dotyczące różnych etapów i aktualizacji procesu.

([1]) Dz.U. L 277 z 27.10.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj.

([2]) Rozporządzenie wykonawcze Komisji (UE) 2024/607 z dnia 15 lutego 2024 r. w sprawie ustaleń praktycznych i operacyjnych na potrzeby funkcjonowania systemu wymiany informacji na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 (akt o usługach cyfrowych) (Dz.U. L, 2024/607, 16.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/607/oj).

(6) Aby zapewnić badaczom spójne informacje na temat procesu dostępu do danych, koordynatorzy ds. usług cyfrowych powinni udostępniać w ramach swoich interfejsów internetowych informacje dotyczące procesu dostępu do danych, w tym linki do portalu dostępu do danych na potrzeby DSA, i zapewnić do nich łatwy dostęp. Aby uniknąć tworzenia zbędnych obciążeń administracyjnych, zwiększyć skuteczność i ułatwić komunikację między wszystkimi stronami zaangażowanymi w proces dostępu do danych, zachęca się koordynatorów ds. usług cyfrowych, by ułatwiali zarządzanie informacjami związanymi z procesem dostępu do danych, również z perspektywy językowej.

(7) Z myślą o umożliwieniu badaczom identyfikacji odpowiednich danych do celów określonych w art. 40 ust. 4 rozporządzenia (UE) 2022/2065 dostawcy danych powinni udostępniać katalogi danych DSA na potrzeby swoich usług. Należy zapewnić możliwość łatwego znalezienia takich katalogów i ich łatwą dostępność w ramach interfejsów internetowych dostawców danych oraz powinny one zawierać opis dostępnych zasobów danych, ich struktury danych i metadanych, do których dostęp można uzyskać na podstawie art. 40 ust. 4 rozporządzenia (UE) 2022/2065. Udostępniając katalogi danych DSA, dostawcy danych powinni brać pod uwagę zagrożenia dla poufności, bezpieczeństwa danych lub ochrony danych osobowych, które mogą wynikać z publicznego udostępnienia takich informacji.

(8) Aby przyczynić się do rozwoju istotnych projektów badawczych do celów określonych w art. 40 ust. 4 rozporządzenia (UE) 2022/2065, katalogi danych DSA powinny zawierać w szczególności dane dotyczące ryzyka systemowego w Unii, które dostawcy danych zidentyfikowali w swoich rocznych ocenach ryzyka zgodnie z art. 34 tego rozporządzenia, a także dane dotyczące wszelkich środków zmniejszających ryzyko, o których mowa w art. 35 tego rozporządzenia. Aby zapewnić adekwatność i aktualność katalogów danych DSA, katalogi te powinny być regularnie aktualizowane z należytym uwzględnieniem nowo rozpoznanego ryzyka systemowego i ewolucji ryzyka systemowego. Na przykład powinny one odzwierciedlać pojawiające się ryzyka zidentyfikowane w wyniku doraźnej oceny ryzyka zgodnie z art. 34 rozporządzenia (UE) 2022/2065 lub w następstwie sprawozdania z audytu na podstawie art. 37 tego rozporządzenia. Aby zminimalizować obciążenia proceduralne dla dostawców danych, w stosownych przypadkach takie katalogi mogą opierać się na istniejących zasobach dokumentacji danych wykorzystywanych do innych celów i dla innych odbiorców, takich jak reklama, tworzenie treści lub opracowywanie aplikacji przez osoby trzecie. Katalogi danych DSA nie muszą być wyczerpujące i w związku z tym nie powinny ograniczać ani wiązać badaczy w kontekście wniosków o udzielenie dostępu do danych.

(9) Aby ułatwić koordynatorowi ds. usług cyfrowych właściwemu dla miejsca siedziby określenie sposobów dostępu oraz zmniejszyć ogólne obciążenie związane z procesem dostępu do danych dla wszystkich zaangażowanych podmiotów, dostawcy danych powinni publikować swoje proponowane sposoby dostępu do danych opisanych w katalogach danych DSA. Te proponowane sposoby dostępu powinny być proporcjonalne do stopnia wrażliwości danych i obejmować informacje na temat możliwych warunków technicznych, organizacyjnych i prawnych uznanych przez dostawców danych za odpowiednie do umożliwienia dostępu do danych. Sposoby dostępu proponowane przez dostawców danych nie powinny być wiążące dla koordynatorów ds. usług cyfrowych właściwych dla miejsca siedziby, którzy powinni zachować kompetencje w zakresie określania odpowiednich sposobów dostępu.

(10) Aby zapewnić równe traktowanie wniosków o udzielenie dostępu do danych, niezależnie od koordynatora ds. usług cyfrowych, do którego złożono wniosek o udzielenie dostępu do danych lub od którego pochodzi uzasadniony wniosek, należy określić ramy czasowe składania uzasadnionych wniosków, aby zapewnić spójność działań wszystkich koordynatorów ds. usług cyfrowych. Jeżeli sformułowanie uzasadnionego wniosku wymaga dodatkowego czasu, koordynator ds. usług cyfrowych właściwy dla miejsca siedziby powinien powiadomić głównego badacza i podać przyczyny opóźnienia. Takie powody mogą obejmować potrzebę przeprowadzenia dodatkowych weryfikacji przez koordynatora ds. usług cyfrowych organizacji badawczej lub właściwego dla miejsca siedziby, na przykład w przypadku gdy wnioski o udzielenie dostępu do danych wiążą się z międzynarodowym przekazywaniem danych lub gdy koordynator ds. usług cyfrowych właściwy dla miejsca siedziby zidentyfikował potencjalne zagrożenia dla bezpieczeństwa Unii w przypadku udostępnienia danych. W celu ujednolicenia również etapów procesu dostępu do danych poprzedzających sformułowanie uzasadnionych wniosków, w tym oceny wniosków o udzielenie dostępu do danych i przyznania statusu zweryfikowanego badacza, koordynatorów ds. usług cyfrowych zachęca się do opracowania spójnego i skoordynowanego sposobu pracy, w tym wspólnych kryteriów operacyjnych, w ramach Europejskiej Rady ds. Usług Cyfrowych.

(11) Aby usprawnić procedury formułowania uzasadnionych wniosków, wszyscy koordynatorzy ds. usług cyfrowych właściwi dla miejsca siedziby powinni być zobowiązani do sprawdzenia, czy we wnioskach o udzielenie dostępu do danych zostały należycie uwzględnione określone wspólne elementy procesu dostępu do danych. W tym celu koordynatorzy ds. usług cyfrowych właściwi dla miejsca siedziby powinni sprawdzić, czy wszyscy badacze wymienieni we wniosku o udzielenie dostępu do danych wykazali swoją przynależność do organizacji badawczej, na przykład przez przedstawienie dokumentów potwierdzających umowę o pracę lub inną formę prawnego powiązania z organizacją badawczą. Koordynatorzy ds. usług cyfrowych właściwi dla miejsca siedziby powinni również sprawdzić, czy badacze składający wnioski wykazali swoją niezależność od interesów komercyjnych, na przykład w drodze stosownego oświadczenia.

(12) Koordynator ds. usług cyfrowych właściwy dla miejsca siedziby powinien sprawdzić, czy finansowanie projektu badawczego, na potrzeby którego wnioskuje się o dane, zostało ujawnione we wniosku o udzielenie dostępu do danych. Informacje przekazywane przez badaczy składających wnioski powinny obejmować szczegółowe informacje dotyczące wkładu, takie jak podmiot finansujący, kwota, charakter i czas trwania wkładu, w tym informację, czy finansowanie zostało już przyznane, czy też wniosek o finansowanie jest nadal rozpatrywany, a także, w stosownych przypadkach, odpowiednie odniesienia do projektów finansowanych przez Unię. W miarę dostępności wniosek o udzielenie dostępu do danych powinien również zawierać wyniki ocen przeprowadzonych przez podmiot lub podmioty zapewniające finansowanie.

(13) Koordynator ds. usług cyfrowych właściwy dla miejsca siedziby powinien sprawdzić, czy we wniosku o udzielenie dostępu do danych opisano sposób wyboru danych i formatu danych, w odniesieniu do wymogów dotyczących konieczności i proporcjonalności do celu planowanych badań. W przypadku gdy wnioskowane dane są również dostępne za pośrednictwem innych źródeł, koordynator ds. usług cyfrowych właściwy dla miejsca siedziby powinien ocenić, czy wniosek o udostępnienie takich danych zawarty we wniosku o udzielenie dostępu do danych jest należycie uzasadniony, biorąc pod uwagę informacje zawarte we wniosku o dostęp do danych. Możliwe uzasadnienia mogą obejmować dowody niskiej jakości lub niewiarygodności takich danych pochodzących z innych źródeł lub nieodpowiedniość formatu, w jakim dane te mogą być pozyskane z innych źródeł do celów projektu badawczego, co utrudniałoby realizację projektu badawczego. Dane, których można zażądać w celu badania ryzyka systemowego lub jego zmniejszenia w Unii, mogą w przyszłości ewoluować. Obecne przykłady takich danych obejmują dane dotyczące użytkowników usług, takie jak informacje profilowe, sieci kontaktów, ekspozycja treści na poziomie indywidualnym oraz historia zaangażowania; dane dotyczące interakcji, takie jak komentarze lub inna aktywność; dane związane z rekomendacjami treści, w tym dane wykorzystywane do personalizacji rekomendacji; dane związane z targetowaniem reklam i profilowaniem, w tym koszty za kliknięcie i inne miary cen reklam; dane związane z testowaniem nowych funkcji przed ich wdrożeniem, w tym wyniki testów A/B; dane związane z moderowaniem treści i zarządzaniem nimi, takie jak dane dotyczące algorytmicznych lub innych systemów i procesów moderowania treści, w tym dzienniki zmian, archiwa lub repozytoria dokumentujące moderowane treści, w tym konta, a także dane dotyczące cen, ilości i cech towarów lub usług dostarczanych przez dostawcę danych lub za jego pośrednictwem.

(14) Koordynator ds. usług cyfrowych właściwy dla miejsca siedziby powinien sprawdzić, czy wniosek o udzielenie dostępu do danych zawiera wystarczające informacje potwierdzające, że badacz jest w stanie spełnić szczególne wymogi dotyczące poufności, bezpieczeństwa i ochrony danych osobowych w odniesieniu do danych, których dotyczy wniosek, identyfikuje możliwe ryzyko wynikające z dostępu do takich danych i ich przetwarzania do celów badań, a także dokumentuje wszelkie proponowane sposoby dostępu, w tym warunki prawne, organizacyjne i techniczne, które zostaną wprowadzone w celu zminimalizowania zidentyfikowanego ryzyka, na przykład w drodze pisemnego zobowiązania ze strony organizacji badawczej potwierdzającego dostęp do środków, które mogą stanowić odpowiednie zabezpieczenia, lub innych dokumentów potwierdzających.

(15) W przypadku wniosku o udostępnienie danych osobowych koordynator ds. usług cyfrowych właściwy dla miejsca siedziby powinien sprawdzić, czy wniosek o udzielenie dostępu do danych zawiera informacje na temat podstawy prawnej przetwarzania danych osobowych, w tym w stosownych przypadkach szczególnych kategorii danych osobowych, oraz czy taka podstawa prawna jest zgodna z art. 6 ust. 1 lit. e) lub f) oraz, w stosownych przypadkach, art. 9 ust. 2 lit. g) lub j) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 ([3]). Ponadto koordynator ds. usług cyfrowych właściwy dla miejsca siedziby powinien sprawdzić, czy wniosek o udzielenie dostępu do danych zawiera wystarczające wskazania, że badacze ocenili ryzyko dla ochrony danych osobowych. Można to wykazać na przykład przez ocenę skutków dla ochrony danych w rozumieniu art. 35 tego rozporządzenia. Aby zapewnić dostęp do danych osobowych zgodnie z rozporządzeniem (UE) 2016/679, koordynatorzy ds. usług cyfrowych powinni mieć możliwość konsultowania się z odpowiednimi organami nadzorczymi ustanowionymi na podstawie art. 51 tego rozporządzenia, które pozostają właściwe do oceny zgodności z rozporządzeniem (UE) 2016/679.

([3]) 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(16) Aby ułatwić formułowanie uzasadnionego wniosku i zachować integralność informacji zawartych we wniosku o udzielenie dostępu do danych, koordynator ds. usług cyfrowych właściwy dla miejsca siedziby powinien sprawdzić, czy wniosek o udzielenie dostępu do danych obejmuje streszczenie. Takie streszczenie powinno zawierać przegląd informacji, które będą stanowić część uzasadnionego wniosku, publikowanego na portalu dostępu do danych na potrzeby DSA, w przypadkach gdy ocena wniosku o udzielenie dostępu do danych prowadzi do sformułowania uzasadnionego wniosku.

(17) Aby zagwarantować, że sposoby dostępu określone przez koordynatora ds. usług cyfrowych właściwego dla miejsca siedziby są odpowiednie w odniesieniu do wrażliwości konkretnych danych, o które wnioskowano we wniosku o udzielenie dostępu do danych, koordynator ds. usług cyfrowych właściwy dla miejsca siedziby powinien przeprowadzać indywidualną ocenę każdego przypadku na podstawie informacji zawartych we wniosku o udzielenie dostępu do danych. Sposoby dostępu określone w uzasadnionym wniosku powinny być odpowiednie do spełnienia wymogów bezpieczeństwa danych, poufności danych i ochrony danych osobowych, a jednocześnie umożliwiać osiągnięcie celów badawczych projektu badawczego. Dostęp do danych może mieć miejsce na przykład przez przekazywanie danych zweryfikowanym badaczom za pośrednictwem odpowiedniego interfejsu i odpowiedniego systemu przechowywania danych; przekazywanie danych do bezpiecznego środowiska przetwarzania danych i przechowywanie ich w tym środowisku, zarządzanym przez dostawcę danych lub przez stronę trzecią, do którego dostęp mają zweryfikowani badacze, ale gdzie nie odbywa się przekazywanie danych do zweryfikowanych badaczy, lub inne sposoby dostępu, które zostaną ustalone lub ułatwione przez dostawcę danych. Określając sposoby dostępu, koordynator ds. usług cyfrowych właściwy dla miejsca siedziby powinien również wymienić wszelkie warunki prawne, techniczne lub organizacyjne, którym ma podlegać dostęp. W przypadkach gdy zapewnienie dostępu wiąże się z przekazaniem danych osobowych do państw trzecich lub organizacji międzynarodowych w rozumieniu rozdziału V rozporządzenia (UE) 2016/679, sposoby dostępu powinny również obejmować informacje na temat potrzeby wprowadzenia odpowiedniego mechanizmu przekazywania danych, aby zapewnić podjęcie przez dostawcę danych niezbędnych działań w celu zapewnienia zgodności z tym rozporządzeniem.

(18) Aby dopilnować, żeby sposoby dostępu do danych były odpowiednie do uwzględnienia szczególnych kwestii wrażliwych w zakresie ochrony danych, bezpieczeństwa danych lub poufności, koordynator ds. usług cyfrowych właściwy dla miejsca siedziby powinien mieć możliwość, na podstawie informacji otrzymanych we wniosku o udzielenie dostępu do danych, zażądania, aby dostęp do danych był zapewniony za pośrednictwem bezpiecznych środowisk przetwarzania danych. W takich przypadkach koordynator ds. usług cyfrowych właściwy dla miejsca siedziby powinien zapewnić, aby wybrane środowisko działało zgodnie z najbardziej odpowiednią technologią i umożliwiało zweryfikowanym badaczom osiągnięcie celów ich badań.

(19) Aby zapewnić spójność informacji przekazywanych dostawcom danych przez koordynatorów ds. usług cyfrowych właściwych dla miejsca siedziby, konieczne jest określenie treści uzasadnionych wniosków.

(20) W celu ochrony interesów dostawców danych i z czasem ograniczenia częstotliwości składania wniosków o zmianę, a także ułatwienia badaczom składania odpowiednich wniosków o udzielenie dostępu do danych, koordynator ds. usług cyfrowych właściwy dla miejsca siedziby, który wydał odpowiednie uzasadnione wnioski, powinien podawać do wiadomości publicznej na portalu dostępu do danych na potrzeby DSA przegląd każdego uzasadnionego wniosku, w tym wszelkich jego zmian i aktualizacji.

(21) W celu zapewnienia koordynatorowi ds. usług cyfrowych właściwemu dla miejsca siedziby dostępu do informacji istotnych dla oceny wniosku o zmianę oraz ułatwienia jednolitego podejścia do oceny wniosków o zmianę, dostawca danych powinien być zobowiązany do podania powodów złożenia takiego wniosku, zgodnie z art. 40 ust. 5 rozporządzenia (UE) 2022/2065. Dokładniej rzecz ujmując, podczas oceny wniosku o zmianę złożonego na podstawie braku dostępu dostawcy danych do danych, koordynator ds. usług cyfrowych właściwy dla miejsca siedziby powinien być w stanie zbadać, czy domniemana niemożność jest należycie uzasadniona, na przykład nieistnieniem żądanych danych lub ograniczeniami technicznymi, takimi jak szyfrowanie, oraz powinien dysponować informacjami niezbędnymi do ustalenia, czy brak dostępu ma charakter stały czy tymczasowy. W tym kontekście należy jasno stwierdzić, że względy komercyjne nie powinny stanowić podstawy do automatycznej odmowy dostępu do żądanych danych, ale raczej podstawę do zmiany sposobu zapewnienia dostępu do danych, co może skutkować nałożeniem dodatkowych wymogów w zakresie bezpieczeństwa i poufności danych.

(22) Aby zapewnić skuteczne rozstrzyganie sporów i zachęcić do znalezienia rozwiązania możliwego do zaakceptowania przez obie strony, po złożeniu wniosku o zmianę dostawcy danych powinni mieć możliwość zwrócenia się do koordynatorów ds. usług cyfrowych właściwych dla miejsca siedziby o udział w mediacji. Taki udział powinien być dobrowolny w trakcie całego procesu mediacji i nie powinien skutkować żadnym wiążącym wynikiem dla koordynatora ds. usług cyfrowych właściwego dla miejsca siedziby, który pozostaje właściwy do podejmowania decyzji w sprawie wniosków o zmianę. Wszystkie strony uczestniczące w procesie mediacji powinny działać w dobrej wierze i dążyć do osiągnięcia sprawiedliwego i wzajemnie akceptowalnego porozumienia.

(23) Aby uniknąć sytuacji, w której mediacja przedłuża proces dostępu do danych w nieskończoność, przekazanie pisemnego wniosku o mediację, wybór mediatora oraz sam proces mediacji powinny odbywać się w określonych terminach. Koordynatorzy ds. usług cyfrowych właściwi dla miejsca siedziby powinni wyznaczyć termin na przeprowadzenie procesu mediacji w odniesieniu do danego uzasadnionego wniosku, a mediator powinien być uprawniony do zakończenia postępowania mediacyjnego w szczególnych okolicznościach.

(24) W celu utrzymania wzajemnego zaufania między stronami zaangażowanymi w mediację, koordynator ds. usług cyfrowych właściwy dla miejsca siedziby powinien zapewnić, aby proponowany mediator spełniał wymogi bezstronności, niezależności i posiadał odpowiednią wiedzę fachową na temat przedmiotu mediacji.

(25) W celu ułatwienia świadomego i skutecznego podejmowania decyzji w odniesieniu do procesu dostępu do danych koordynatorzy ds. usług cyfrowych powinni mieć możliwość zwracania się o opinie ekspertów na temat konkretnych elementów procesu dostępu do danych, takich jak określenie sposobów dostępu, w tym odpowiednich interfejsów, sformułowanie uzasadnionego wniosku i wszelkich wniosków o zmianę złożonych przez dostawcę danych. Eksperci, z którymi prowadzone są konsultacje, powinni posiadać udokumentowaną wiedzę fachową na temat sprawy, co do której zwrócono się do nich o opinię, i powinni być niezależni. W szczególności nie powinni oni pozostawać w konflikcie interesów wynikającym na przykład z jakichkolwiek powiązań z badaczami składającymi wnioski lub z dostawcą danych.

(26) Aby zwiększyć przejrzystość i umożliwić koordynatorom ds. usług cyfrowych wykorzystanie wiedzy fachowej zdobytej w miarę upływu czasu, każdy wniosek o konsultacje z ekspertami i wynikające z niego działania następcze powinny być rejestrowane w systemie AGORA.

(27) Aby ułatwić skuteczny nadzór nad przestrzeganiem warunków określonych w uzasadnionym wniosku, dostawca danych powinien powiadomić koordynatora ds. usług cyfrowych właściwego dla miejsca siedziby w terminie trzech dni roboczych od dnia udzielenia dostępu zweryfikowanym badaczom i od dnia zakończenia dostępu.

(28) Aby umożliwić zweryfikowanym badaczom wykorzystanie wnioskowanych danych do celów badań oraz zapewnić odpowiednie informacje kontekstowe, dostawcy danych powinni dostarczyć zweryfikowanym badaczom odpowiednie metadane i dokumentację opisującą udostępnione dane, takie jak książki kodów, dzienniki zmian i dokumentacja architektury.

(29) Aby ułatwić zweryfikowanym badaczom przeprowadzenie rzetelnych badań, również przez umożliwienie łączenia żądanych danych z danymi dostępnymi za pośrednictwem innych źródeł, dostawcy danych nie powinni nakładać żadnych ograniczeń na narzędzia analityczne stosowane przez zweryfikowanych badaczy, w tym odpowiednie biblioteki oprogramowania, i nie powinni nakładać wymogów dotyczących archiwizacji, przechowywania, odświeżania i usuwania danych, chyba że są one wyraźnie wymienione w warunkach dostępu określonych w uzasadnionym wniosku.

(30) W przypadku gdy dane przekazane zweryfikowanym badaczom obejmują dane osobowe w rozumieniu art. 4 rozporządzenia (UE) 2016/679, dostawca danych powinien przestrzegać przepisów określonych w tym rozporządzeniu. W szczególności art. 40 ust. 4 rozporządzenia (UE) 2022/2065 nakłada obowiązek prawny w rozumieniu art. 6 ust. 1 lit. c) rozporządzenia (UE) 2016/679 w odniesieniu do przetwarzania danych osobowych niezbędnego do zapewnienia przez dostawcę danych dostępu do danych określonych w uzasadnionym wniosku. W przypadku przetwarzania szczególnych kategorii danych osobowych w rozumieniu art. 9 rozporządzenia (UE) 2016/679 niniejsze rozporządzenie spełnia wymóg określony w art. 9 ust. 2 lit. g) rozporządzenia (UE) 2016/679.

(31) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([4]) skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię 4 grudnia 2024 r.

(32) Po konsultacji z Europejską Radą ds. Usług Cyfrowych zgodnie z art. 40 ust. 13 rozporządzenia (UE) 2022/2065 i po zatwierdzeniu przez nią,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

PRZEPISY OGÓLNE

Artykuł 1

Przedmiot

W niniejszym rozporządzeniu ustanawia się procedury i warunki techniczne dotyczące zapewniania zweryfikowanym badaczom dostępu do danych będących w posiadaniu dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych, zgodnie z art. 40 ust. 4 rozporządzenia (UE) 2022/2065, w szczególności:

a) warunki techniczne rozwoju i funkcjonowania portalu dostępu do danych;

b) procedury i warunki techniczne zarządzania procesem dostępu do danych przez koordynatorów ds. usług cyfrowych i dostawców danych;

c) wymogi dotyczące formułowania uzasadnionych wniosków i oceny wniosków o zmianę;

d) warunki techniczne udzielania dostępu do danych przez dostawców danych.

Artykuł 2

Definicje

Do celów niniejszego rozporządzenia stosuje się definicje zawarte w art. 4 rozporządzenia (UE) 2016/679 i w art. 3 rozporządzenia (UE) 2018/1725. Stosuje się również następujące definicje:

1) „wniosek o udzielenie dostępu do danych" oznacza informacje i odpowiednią dokumentację przedłożone przez badaczy ubiegających się o dostęp do danych koordynatorowi ds. usług cyfrowych właściwemu dla miejsca siedziby lub koordynatorowi ds. usług cyfrowych państwa członkowskiego organizacji badawczej, z którą powiązany jest główny badacz, w celu uzyskania statusu „zweryfikowanego badacza", o którym mowa w art. 40 ust. 8 akapit pierwszy rozporządzenia (UE) 2022/2065, na potrzeby konkretnego projektu badawczego obejmującego dostęp do danych od dostawcy danych;

2) „proces dostępu do danych" oznacza etapy i procedury, które mogą prowadzić do udzielenia dostępu do danych, o czym mowa w art. 40 ust. 4 rozporządzenia (UE) 2022/2065;

3) „badacz ubiegający się o dostęp do danych" oznacza każdą osobę fizyczną ubiegającą się o dostęp do danych, o którym mowa w art. 40 ust. 4 rozporządzenia (UE) 2022/2065, indywidualnie, grupowo lub jako część podmiotu;

4) „główny badacz" oznacza badacza ubiegającego się o dostęp do danych, który składa wniosek o udzielenie dostępu do danych we własnym imieniu lub w imieniu podmiotu lub grupy badaczy ubiegających się o dostęp do danych;

5) „dostawca danych" oznacza dostawcę bardzo dużej platformy internetowej lub bardzo dużej wyszukiwarki internetowej wskazanych jako takie zgodnie z art. 33 ust. 4 rozporządzenia (UE) 2022/2065, do którego może zostać skierowany uzasadniony wniosek;

([4]) 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

6) „uzasadniony wniosek" oznacza uzasadniony wniosek o dostęp do danych na podstawie art. 40 ust. 4 rozporządzenia (UE) 2022/2065;

7) „wniosek o zmianę" oznacza wniosek o zmianę na podstawie art. 40 ust. 5 rozporządzenia (UE) 2022/2065 złożony przez dostawcę danych do koordynatora ds. usług cyfrowych właściwego dla miejsca siedziby po otrzymaniu uzasadnionego wniosku;

8) „bezpieczne środowisko przetwarzania" oznacza bezpieczne środowisko przetwarzania, o którym mowa w art. 2 pkt 20 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/868 ([5]).

ROZDZIAŁ II

OBOWIĄZKI INFORMACYJNE I OBOWIĄZKI DOTYCZĄCE KONTAKTÓW

Artykuł 3

Portal dostępu do danych na potrzeby DSA

1. Komisja ustanawia i obsługuje portal dostępu do danych na potrzeby aktu o usługach cyfrowych (DSA).

2. Portal dostępu do danych na potrzeby DSA pełni następujące funkcje:

a) wspieranie i usprawnianie zarządzania procesem dostępu do danych na potrzeby badaczy, dostawców danych i koordynatorów ds. usług cyfrowych;

b) pełnienie funkcji centralnego cyfrowego punktu informacji na temat procesu dostępu do danych i ułatwienie wymiany informacji na podstawie niniejszego rozporządzenia między badaczami ubiegającymi się o dostęp do danych, zweryfikowanymi badaczami, dostawcami danych i koordynatorami ds. usług cyfrowych.

3. Portal dostępu do danych na potrzeby DSA jest interoperacyjny z systemem wymiany informacji AGORA ustanowionym na mocy rozporządzenia wykonawczego (UE) 2024/607. W systemie AGORA koordynatorzy ds. usług cyfrowych mają dostęp do informacji przekazywanych za pośrednictwem portalu dostępu do danych na potrzeby DSA.

4. Dostawcy danych posiadają konto w portalu dostępu do danych na potrzeby DSA.

5. Aby uczestniczyć w procesie dostępu do danych, badacze ubiegający się o dostęp do danych posiadają konto w portalu dostępu do danych na potrzeby DSA.

Artykuł 4

Role i obowiązki w zakresie przetwarzania danych osobowych w portalu dostępu do danych na potrzeby DSA

1. Koordynatorzy ds. usług cyfrowych są odrębnymi administratorami w odniesieniu do przetwarzania danych osobowych w celu zarządzania procesem dostępu do danych i publikacji istotnych informacji.

2. Komisja jest podmiotem przetwarzającym dane osobowe w ramach portalu dostępu do danych na potrzeby DSA.

3. Obowiązki Komisji jako podmiotu przetwarzającego w odniesieniu do czynności przetwarzania danych na portalu dostępu do danych na potrzeby DSA określono w załączniku.

([5]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z dnia 30 maja 2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724 (akt w sprawie zarządzania danymi) (Dz.U. L 152 z 3.6.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/868/oj).

Artykuł 5

Przetwarzanie danych osobowych w portalu dostępu do danych na potrzeby DSA

1. W przypadku gdy dane osobowe są rejestrowane i wymieniane za pośrednictwem portalu dostępu do danych na potrzeby DSA, przetwarzanie odbywa się wyłącznie w zakresie, w jakim jest to proporcjonalne i niezbędne do celów procesu dostępu do danych i publikacji odpowiednich informacji.

2. Przetwarzanie danych osobowych w portalu dostępu do danych na potrzeby DSA odbywa się wyłącznie w odniesieniu do następujących kategorii osób, których dane dotyczą:

a) osoby fizyczne posiadające konto w portalu dostępu do danych na potrzeby DSA;

b) osoby fizyczne, których dane osobowe znajdują się w portalu dostępu do danych na potrzeby DSA lub w jakiejkolwiek innej wymianie na podstawie niniejszego rozporządzenia dotyczącej procesu dostępu do danych.

3. Przetwarzanie danych osobowych w portalu dostępu do danych na potrzeby DSA odbywa się wyłącznie w odniesieniu do następujących kategorii danych osobowych:

a) dane dotyczące tożsamości, takie jak imię i nazwisko, identyfikator użytkownika;

b) dane kontaktowe, takie jak adres, adres e-mail, dane kontaktowe;

c) dane osobowe zawarte w dokumentacji wykazującej przynależność do organizacji badawczej oraz wszelkie inne informacje osobowe uznane za niezbędne do celów uczestnictwa w procesie dostępu do danych.

4. Przetwarzanie danych osobowych, o których mowa w ust. 1, odbywa się z wykorzystaniem infrastruktury informatycznej znajdującej się na terytorium Europejskiego Obszaru Gospodarczego.

Artykuł 6

Punkty kontaktowe i informacje publiczne na temat procesu dostępu do danych

1. Każdy koordynator ds. usług cyfrowych i każdy dostawca danych ustanawiają specjalny punkt kontaktowy, którego zadaniem jest udzielanie informacji i wsparcia w zakresie procesu dostępu do danych.

2. Koordynatorzy ds. usług cyfrowych i dostawcy danych niezwłocznie informują Komisję o swoich punktach kontaktowych. Komisja publikuje szczegółowe informacje dotyczące punktów kontaktowych, o których mowa w ust. 1, w publicznym interfejsie portalu dostępu do danych na potrzeby DSA.

3. W swoim interfejsie internetowym każdy koordynator ds. usług cyfrowych udostępnia łatwe do wyszukania szczegółowe informacje dotyczące punktu kontaktowego ustanowionego na podstawie ust. 1 wraz z linkiem do portalu dostępu do danych na potrzeby DSA.

4. Dostawcy danych udostępniają następujące, łatwe do wyszukania informacje w swoich interfejsach internetowych:

a) dane punktu kontaktowego ustanowionego przez nich zgodnie z ust. 1;

b) link do portalu dostępu do danych na potrzeby DSA;

c) katalog danych DSA, w którym opisano zasoby danych, do których można uzyskać dostęp do celów określonych w art. 40 ust. 4 rozporządzenia (UE) 2022/2065, a także ich strukturę danych i metadane;

d) proponowane sposoby dostępu do danych w katalogu zgodnie z lit. c), odpowiednie do poziomu wrażliwości poszczególnych zasobów danych.

5. Informacje, o których mowa w ust. 4 lit. c) i d), są regularnie aktualizowane, w szczególności w celu odzwierciedlenia danych związanych z ocenami ryzyka przeprowadzonymi na podstawie art. 34 rozporządzenia (UE) 2022/2065 i audytami przeprowadzonymi na podstawie art. 37 tego rozporządzenia.

ROZDZIAŁ III

WYMOGI DOTYCZĄCE FORMUŁOWANIA I PRZETWARZANIA UZASADNIONYCH WNIOSKÓW

Artykuł 7

Sformułowanie uzasadnionego wniosku

1. W ciągu 80 dni roboczych od złożenia wniosku o udzielenie dostępu do danych koordynator ds. usług cyfrowych właściwy dla miejsca siedziby, należycie uwzględniając warunki wstępne określone w art. 8 oraz, w stosownych przypadkach, każdą inną ocenę istotną do tych celów, podejmuje decyzję, czy można sformułować uzasadniony wniosek, i podejmuje jedno z następujących działań:

a) formułuje uzasadniony wniosek, przedkłada go dostawcy danych i powiadamia głównego badacza o złożeniu uzasadnionego wniosku;

b) informuje głównego badacza o powodach, dla których nie można było sformułować uzasadnionego wniosku.

2. Jeżeli w należycie uzasadnionych przypadkach koordynator ds. usług cyfrowych właściwy dla miejsca siedziby potrzebuje dodatkowego czasu na sformułowanie uzasadnionego wniosku, jak najszybciej powiadamia o tym głównego badacza i wskazuje przyczyny opóźnienia, a także nowy termin na podjęcie działań, o których mowa w ust. 1.

Artykuł 8

Warunki wstępne do sformułowania uzasadnionego wniosku

1. Koordynator ds. usług cyfrowych właściwy dla miejsca siedziby decyduje, czy można sformułować uzasadniony wniosek, uwzględniając następujące elementy:

a) w odniesieniu do każdego badacza ubiegającego się o dostęp do danych:

   (i) potwierdzenie członkostwa w organizacji badawczej zdefiniowanej w art. 2 pkt 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/790 ([6]);

   (ii) oświadczenie o niezależności od interesów komercyjnych związanych z konkretnym projektem, którego dotyczy wniosek o udostępnienie danych;

   (iii) zobowiązanie do bezpłatnego publicznego udostępniania wyników badań;

b) informacje na temat finansowania projektu badawczego, którego dotyczy wniosek o udzielenie dostępu do danych;

c) opis żądanych danych, w tym wskazanie ich formatu, zakresu oraz, w miarę możliwości, konkretnych atrybutów, odpowiednich metadanych i dokumentacji danych, z uwzględnieniem również informacji udostępnionych zgodnie z art. 6 ust. 4 niniejszego rozporządzenia;

d) informacje na temat konieczności i proporcjonalności dostępu do danych oraz informacje na temat ram czasowych badań, których dotyczy wniosek o udostępnienie danych;

e) informacje na temat zidentyfikowanych zagrożeń w zakresie poufności, bezpieczeństwa danych i ochrony danych osobowych związanych z danymi, do których uzyskano by dostęp, opis środków technicznych, prawnych i organizacyjnych, które zostaną wprowadzone, w tym, w miarę możliwości, proponowane sposoby dostępu, aby ograniczyć takie ryzyko podczas przetwarzania żądanych danych;

f) opis działań badawczych, które mają być prowadzone z wykorzystaniem żądanych danych;

g) streszczenie wniosku o udzielenie dostępu do danych zawierające następujące elementy:

   (i) tematykę badań;

   (ii) dostawcę danych, od którego żąda się danych;

   (iii) opis żądanych danych, o których mowa w lit. c).

([6]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790 z dnia 17 kwietnia 2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE (Dz.U. L 130 z 17.5.2019, s. 92, ELI: http://data.europa.eu/eli/dir/2019/790/oj).

Artykuł 9

Warunki dostępu

1. Koordynator ds. usług cyfrowych właściwy dla miejsca siedziby określa sposoby, w tym środki techniczne, prawne i organizacyjne, które dostawca danych ma stosować w celu zapewnienia dostępu do danych zweryfikowanym badaczom.

2. Koordynatorom ds. usług cyfrowych zezwala się na konsultację z odpowiednimi organami nadzorczymi ustanowionymi na podstawie art. 51 rozporządzenia (UE) 2016/679.

3. Przy określaniu sposobów dostępu koordynator ds. usług cyfrowych właściwy dla miejsca siedziby bierze pod uwagę informacje podane we wniosku o udzielenie dostępu do danych, w szczególności informacje, o których mowa w art. 8 lit. e), uwzględniając również prawa i interesy zainteresowanych dostawców danych i odbiorców danej usługi, w tym ochronę informacji poufnych, tajemnic przedsiębiorstwa oraz utrzymanie bezpieczeństwa ich usługi i informacji udostępnianych przez dostawców danych zgodnie z art. 6 ust. 4 lit. d).

4. Oprócz elementów, o których mowa w ust. 3, koordynator ds. usług cyfrowych właściwy dla miejsca siedziby przy określaniu sposobów dostępu określa następujące elementy:

a) jeżeli dostęp wiąże się z przetwarzaniem danych osobowych:

   (i) ocenę ryzyka związanego z przetwarzaniem danych osobowych, o której mowa w art. 8 lit. e), w tym, w stosownych przypadkach, ocenę skutków dla ochrony danych w rozumieniu art. 35 rozporządzenia (UE) 2016/679;

   (ii) planowane środki techniczne i organizacyjne przedłożone zgodnie z art. 8 lit. e);

b) odpowiednie środki bezpieczeństwa sieci, szyfrowanie, mechanizmy kontroli dostępu, polityki tworzenia kopii zapasowych, mechanizmy integralności danych, plany reagowania na incydenty;

c) w stosownych przypadkach informacje na temat planowanego okresu przechowywania i odpowiednich planów zniszczenia danych;

d) wszelkie środki organizacyjne, takie jak procedury przeglądu wewnętrznego, ograniczenia praw dostępu i wymiana informacji;

e) wszelkie proponowane klauzule umowne, takie jak umowy o zachowaniu poufności, umowy dotyczące danych i wszelkie inne rodzaje pisemnych oświadczeń, określające ewentualne warunki dostępu i przetwarzania między głównym badaczem a dostawcą danych;

f) prowadzenie szkoleń w zakresie bezpieczeństwa danych i ochrony danych osobowych otrzymanych przez badaczy ubiegających się o dostęp do danych;

g) czy do przetwarzania danych niezbędne są bezpieczne środowiska przetwarzania.

5. W przypadku gdy koordynator ds. usług cyfrowych właściwy dla miejsca siedziby uzna, że do zapewnienia dostępu do żądanych danych należy wykorzystać bezpieczne środowisko przetwarzania, koordynator ds. usług cyfrowych miejsca siedziby wymaga dokumentacji potwierdzającej, że operator tego środowiska:

a) określa warunki dostępu do bezpiecznego środowiska przetwarzania w celu zminimalizowania ryzyka nieuprawnionego odczytu, kopiowania, zmiany lub usunięcia danych przechowywanych w bezpiecznym środowisku przetwarzania;

b) zapewnia zweryfikowanym badaczom dostęp wyłącznie do danych objętych uzasadnionym wnioskiem z wykorzystaniem indywidualnych i niepowtarzalnych identyfikatorów użytkownika oraz poufnych trybów dostępu;

c) przechowuje możliwe do zidentyfikowania logi dostępu do bezpiecznego środowiska przetwarzania przez okres niezbędny do zweryfikowania i skontrolowania wszystkich operacji przetwarzania w tym środowisku;

d) zapewnia, aby moc obliczeniowa do dyspozycji zweryfikowanych badaczy była odpowiednia i wystarczająca do celów projektu badawczego;

e) monitoruje skuteczność środków wymienionych w lit. a)–d).”.

Artykuł 10

Treść uzasadnionego wniosku

1. Uzasadniony wniosek zawiera co najmniej następujące elementy:

a) datę udzielenia przez dostawcę danych dostępu do żądanych danych oraz datę zakończenia takiego dostępu;

b) sposoby dostępu określone zgodnie z art. 9;

c) streszczenie wniosku o udzielenie dostępu do danych, o którym mowa w art. 8 lit. g).

2. Koordynator ds. usług cyfrowych właściwy dla miejsca siedziby może zawrzeć w uzasadnionym wniosku nazwiska i dane kontaktowe wszystkich zweryfikowanych badaczy wymienionych we wniosku o udzielenie dostępu do danych, jeżeli jest to konieczne do umożliwienia dostępu do żądanych danych, zgodnie ze sposobami dostępu określonymi w uzasadnionym wniosku.

3. Jeżeli udzielenie dostępu wiąże się z przekazaniem danych osobowych do państwa trzeciego lub organizacji międzynarodowej w rozumieniu rozdziału V rozporządzenia (UE) 2016/679, uzasadniony wniosek zawiera informacje na temat potrzeby wprowadzenia odpowiedniego mechanizmu przesyłania danych lub odniesienia się do takiego mechanizmu w celu zapewnienia zgodności z rozporządzeniem (UE) 2016/679.

Artykuł 11

Publikacja przeglądu uzasadnionego wniosku na portalu dostępu do danych na potrzeby DSA

1. Po złożeniu uzasadnionego wniosku koordynator ds. usług cyfrowych właściwy dla miejsca siedziby publikuje przegląd uzasadnionego wniosku w publicznym interfejsie portalu dostępu do danych na potrzeby DSA. W przeglądzie uwzględnia się wszystkie następujące elementy:

a) streszczenie wniosku o udzielenie dostępu do danych, o którym mowa w art. 8 lit. g);

b) sposoby dostępu określone zgodnie z art. 9.

2. Przegląd, o którym mowa w ust. 1, jest aktualizowany w celu odzwierciedlenia wszelkich zmian wynikających ze zmiany co najmniej jednego elementu po rozpatrzeniu wniosku o zmianę lub wyniku mediacji zgodnie z art. 13.

Artykuł 12

Procedury rozpatrywania wniosków o zmianę

1. Po otrzymaniu wniosku o zmianę na podstawie art. 40 ust. 5 rozporządzenia (UE) 2022/2065 koordynator ds. usług cyfrowych właściwy dla miejsca siedziby informuje o tym głównego badacza, którego to dotyczy.

2. Przy podejmowaniu decyzji w sprawie wniosku o zmianę złożonego na podstawie art. 40 ust. 5 lit. a) rozporządzenia (UE) 2022/2065 koordynator ds. usług cyfrowych właściwy dla miejsca siedziby uwzględnia następujące elementy:

a) czy powody domniemanego braku dostępu do danych są należycie uzasadnione;

b) czy ten brak dostępu do danych ma charakter stały czy tymczasowy.

3. Przy podejmowaniu decyzji w sprawie wniosku o zmianę złożonego na podstawie art. 40 ust. 5 lit. b) rozporządzenia (UE) 2022/2065 koordynator ds. usług cyfrowych właściwy dla miejsca siedziby uwzględnia wszystkie następujące elementy:

a) czy domniemane luki w zakresie bezpieczeństwa i ich znaczenie są należycie uzasadnione;

b) prawdopodobieństwo i dotkliwość szkody wynikającej z tych domniemanych znacznych luk w zakresie bezpieczeństwa;

c) zakres, w jakim sposoby dostępu określone w uzasadnionym wniosku skutecznie ograniczają ryzyko wystąpienia takiej szkody.

4. W dowolnym momencie oceny wniosku o zmianę koordynator ds. usług cyfrowych właściwy dla miejsca siedziby może zwrócić się do dostawcy danych lub głównego badacza o wszelkie dodatkowe informacje, które uzna za niezbędne do zakończenia oceny.

5. Taki wniosek o dodatkowe informacje składa się jak najszybciej, aby zapewnić dostawcy danych lub głównemu badaczowi wystarczająco dużo czasu na udzielenie odpowiedzi, a w każdym razie nie może mieć to wpływu na termin określony w art. 40 ust. 6 akapit drugi rozporządzenia (UE) 2022/2065. W przypadku gdy dostawca danych lub główny badacz nie dostarczą żądanych informacji w ogóle lub w terminie określonym przez koordynatora ds. usług cyfrowych właściwego dla miejsca siedziby lub przedstawią częściowe informacje, koordynator ds. usług cyfrowych właściwy dla miejsca siedziby podejmuje decyzję w terminie określonym w art. 40 ust. 6 rozporządzenia (UE) 2022/2065 na podstawie informacji, które zostały mu udostępnione w rozsądnym terminie.

Artykuł 13

Mediacja

1. Jeżeli dostawca danych nie zgadza się z decyzją koordynatora ds. usług cyfrowych właściwego dla miejsca siedziby w sprawie wniosku o zmianę, może on, w terminie pięciu dni roboczych od powiadomienia przez koordynatora ds. usług cyfrowych właściwego dla miejsca siedziby na podstawie art. 40 ust. 6 akapit drugi rozporządzenia (UE) 2022/2065, zwrócić się na piśmie do koordynatora ds. usług cyfrowych właściwego dla miejsca siedziby o uczestnictwo w mediacji.

2. Koordynator ds. usług cyfrowych właściwy dla miejsca siedziby nie jest zobowiązany do uczestnictwa w procesie mediacji.

3. Pisemny wniosek, o którym mowa w ust. 1, zawiera zwięzły opis konkretnych elementów decyzji przekazanych przez koordynatora ds. usług cyfrowych właściwego dla miejsca siedziby na podstawie art. 40 ust. 6 akapit drugi rozporządzenia (UE) 2022/2065, wobec których dostawca danych wystosował sprzeciw.

4. Koordynator ds. usług cyfrowych właściwy dla miejsca siedziby i dostawca danych uzgadniają wyznaczenie mediatora i rozpoczynają mediację w terminie 20 dni roboczych od złożenia wniosku o mediację zgodnie z ust. 3.

5. Przed wyrażeniem zgody na wyznaczenie mediatora koordynator ds. usług cyfrowych właściwy dla miejsca siedziby sprawdza, czy mediator jest bezstronny i niezależny oraz czy posiada odpowiednią wiedzę fachową w danej sprawie, jak opisano w pisemnym wniosku, o którym mowa w ust. 1.

6. Dostawca danych ponosi wszystkie koszty mediacji.

7. Koordynator ds. usług cyfrowych właściwy dla miejsca siedziby bez zbędnej zwłoki informuje głównego badacza o wniosku o mediację, o którym mowa w ust. 1, i może podjąć decyzję o zaproszeniu głównego badacza do przystąpienia do mediacji jako strona. W przypadku gdy wniosek o udzielenie dostępu do danych przedłożono koordynatorowi ds. usług cyfrowych organizacji badawczej, koordynator ds. usług cyfrowych właściwy dla miejsca siedziby może zaprosić koordynatora ds. usług cyfrowych organizacji badawczej do uczestnictwa w procesie mediacji. Żadna ze stron zaproszonych do uczestnictwa w mediacji przez koordynatora ds. usług cyfrowych właściwego dla miejsca siedziby nie jest zobowiązana do uczestnictwa w procesie mediacji.

8. Uczestnictwo w mediacji nie wpływa na prawo stron do wszczęcia postępowania sądowego w dowolnym momencie przed mediacją, w jej trakcie lub po jej zakończeniu.

9. Koordynator ds. usług cyfrowych właściwy dla miejsca siedziby wyznacza termin mediacji, który nie może przekraczać 40 dni roboczych od dnia rozpoczęcia mediacji zgodnie z ust. 4.

10. Mediator może zakończyć mediację wcześniej w jednej z następujących sytuacji:

a) jedna ze stron wyraźnie wnosi o zakończenie mediacji;

b) staje się jasne, że ze względu na postępowanie stron w trakcie mediacji, w tym brak działania w dobrej wierze, osiągnięcie porozumienia jest mało prawdopodobne.

11. W przypadku gdy mediacja prowadzi do porozumienia między stronami, koordynator ds. usług cyfrowych właściwy dla miejsca siedziby uwzględnia takie porozumienie, w stosownych przypadkach, zmienia uzasadniony wniosek i informuje głównego badacza o zmianie.

12. Jeżeli strony nie osiągną porozumienia, koordynator ds. usług cyfrowych właściwy dla miejsca siedziby powiadamia dostawcę danych, że decyzję koordynatora ds. usług cyfrowych właściwego dla miejsca siedziby w sprawie wniosku o zmianę, ostatnio przekazaną na podstawie art. 40 ust. 6 akapit drugi rozporządzenia (UE) 2022/2065, uznaje się za ważną i stanowi ona odpowiednią podstawę dalszych kroków w tym procesie oraz informuje głównego badacza.

13. Koordynator ds. usług cyfrowych właściwy dla miejsca siedziby rejestruje w systemie AGORA skrócony protokół z mediacji przygotowany przez mediatora i podpisany przez wszystkie strony. Protokół musi zawierać następujące informacje:

a) datę pisemnego wniosku o mediację złożonego przez dostawcę danych;

b) tożsamość i dane kontaktowe stron;

c) datę rozpoczęcia i datę zakończenia mediacji;

d) wynik mediacji, w tym osiągnięte porozumienie lub powód zakończenia mediacji.

Artykuł 14

Konsultacje z niezależnymi ekspertami

1. Przed złożeniem uzasadnionego wniosku lub podjęciem decyzji w sprawie wniosku o zmianę koordynator ds. usług cyfrowych może podjąć decyzję o przeprowadzeniu konsultacji z ekspertami.

2. Eksperci są niezależni i bezstronni oraz posiadają odpowiednią wiedzę fachową i udokumentowane umiejętności oraz dysponują zdolnościami i zasobami umożliwiającymi im niezwłoczne wykonanie określonego zadania.

3. W celu poświadczenia bezstronności eksperci podpisują oświadczenie potwierdzające, że:

a) nie mają powiązań finansowych ani osobistych z dostawcą danych lub badaczami ubiegającymi się o dostęp do danych;

b) nie mają interesu w wyniku procesu dostępu do danych;

c) są wolni od wszelkich konfliktów interesów.

4. Koordynator ds. usług cyfrowych bez zbędnej zwłoki wprowadza do systemu AGORA wszelkie konsultacje przeprowadzone na podstawie ust. 1 wraz z opinią eksperta otrzymaną w odpowiedzi na konsultacje.

ROZDZIAŁ IV

WARUNKI PRZEKAZYWANIA ŻĄDANYCH DANYCH ZWERYFIKOWANYM BADACZOM

Artykuł 15

Udostępnianie danych i dokumentacja danych

1. Dostawcy danych powiadamiają koordynatora ds. usług cyfrowych właściwego dla miejsca siedziby w terminie trzech dni roboczych o tym, że:

a) dostęp do żądanych danych został zapewniony zweryfikowanym badaczom zgodnie z uzasadnionym wnioskiem;

b) dostęp zweryfikowanych badaczy został zakończony.

2. Dostawcy danych przekazują zweryfikowanym badaczom wszelkie dodatkowe informacje niezbędne do uzyskania dostępu do żądanych danych i ich zrozumienia, takie jak książki kodów, dzienniki zmian i dokumentacja architektury. W przypadkach gdy przekazanie takich informacji może prowadzić do znacznej luki w zakresie bezpieczeństwa usługi dostawcy danych, dostawca danych powiadamia o tym ryzyku koordynatora ds. usług cyfrowych właściwego dla miejsca siedziby i, w miarę możliwości, proponuje alternatywne informacje.

3. Zapewniając dostęp do danych, dostawcy danych nie nakładają na zweryfikowanych badaczy wymogów w zakresie zarządzania danymi, takich jak wymogi dotyczące archiwizacji, przechowywania, odświeżania i usuwania danych, ani ograniczeń w stosowaniu standardowych narzędzi analitycznych, które mogą utrudniać prowadzenie odpowiednich badań, chyba że takie wymogi lub ograniczenia są wyraźnie wymienione w uzasadnionym wniosku.

4. W przypadku przetwarzania danych osobowych dostawcy danych nie nakładają na zweryfikowanych badaczy żadnych warunków związanych z przetwarzaniem udostępnianych danych osobowych innych niż warunki określone w uzasadnionym wniosku.

ROZDZIAŁ V

PRZEPISY KOŃCOWE

Artykuł 16

Wejście w życie

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 1 lipca 2025 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN

ZAŁĄCZNIK

Obowiązki Komisji jako podmiotu przetwarzającego w odniesieniu do czynności przetwarzania danych w kontekście portalu dostępu do danych na potrzeby aktu o usługach cyfrowych (DSA)

1. Komisja tworzy i zapewnia bezpieczną oraz niezawodną infrastrukturę informatyczną, portal dostępu do danych na potrzeby DSA, w imieniu koordynatorów ds. usług cyfrowych w celu wspierania i usprawnienia zarządzanie procesem dostępu do danych dla badaczy, organizacji badawczych, dostawców danych i koordynatorów ds. usług cyfrowych.

2. Aby wypełnić swoje obowiązki jako podmiot przetwarzający na rzecz koordynatorów ds. usług cyfrowych, Komisja może korzystać z osób trzecich działających w charakterze podwykonawców przetwarzania. W takim przypadku administratorzy upoważniają Komisję do korzystania z podwykonawców przetwarzania lub zastąpienia w razie potrzeby podwykonawców przetwarzania. Komisja informuje administratorów o takim skorzystaniu z podwykonawców przetwarzania lub zastąpieniu ich, dając tym samym administratorom możliwość zgłoszenia sprzeciwu wobec wszelkich takich zmian. Komisja zapewnia, aby do podwykonawców przetwarzania zastosowanie miały takie same obowiązki dotyczące ochrony danych jak obowiązki określone w niniejszym rozporządzeniu.

3. Komisja przetwarza dane osobowe wyłącznie w takim zakresie, w jakim jest to niezbędne do:

   a) uwierzytelniania i kontroli dostępu w odniesieniu do wszystkich użytkowników portalu dostępu do danych na potrzeby DSA;

   b) zatwierdzenia realizacji wniosków użytkowników portalu dostępu do danych na potrzeby DSA o utworzenie, aktualizację i usunięcie wszelkich informacji zawartych we wniosku w portalu dostępu do danych na potrzeby DSA;

   c) otrzymywania danych osobowych, o których mowa w art. 5 ust. 3 niniejszego rozporządzenia, przesłanych przez użytkowników portalu dostępu do danych na potrzeby DSA;

   d) przechowywania danych osobowych w portalu dostępu do danych na potrzeby DSA;

   e) usuwania danych osobowych z datą ich wygaśnięcia lub na polecenie administratora;

   f) po zakończeniu świadczenia usług w ramach portalu dostępu do danych na potrzeby DSA, usuwania wszelkich pozostałych danych osobowych, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie takich danych osobowych.

4. Komisja wprowadza wszelkie najnowocześniejsze organizacyjne, fizyczne i logiczne środki bezpieczeństwa w celu zapewnienia funkcjonowania portalu dostępu do danych na potrzeby DSA. W tym celu Komisja:

   a) wyznacza podmiot odpowiedzialny za zarządzanie bezpieczeństwem portalu dostępu do danych na potrzeby DSA, przekazuje administratorom dane kontaktowe tego podmiotu oraz zapewnia jego dostępność w celu reagowania na zagrożenia dla bezpieczeństwa;

   b) przyjmuje odpowiedzialność za bezpieczeństwo portalu dostępu do danych na potrzeby DSA, w tym za regularne przeprowadzanie testów, ocen i badań środków bezpieczeństwa;

5. Komisja wprowadza wszystkie niezbędne środki bezpieczeństwa, aby nie dopuścić do zakłócenia sprawnego funkcjonowania portalu dostępu do danych na potrzeby DSA. Środki te obejmują:

   a) procedury oceny ryzyka, by wykryć i oszacować potencjalne zagrożenia dla portalu dostępu do danych na potrzeby DSA;

   b) procedurę audytu i przeglądu w celu:

      (i) sprawdzania zgodności między wprowadzonymi środkami bezpieczeństwa a mającą zastosowanie polityką bezpieczeństwa;

      (ii) przeprowadzania regularnych kontroli integralności portalu dostępu do danych na potrzeby DSA, parametrów bezpieczeństwa i przyznanych zezwoleń;

      (iii) wykrywania naruszeń bezpieczeństwa i wtargnięć do portalu dostępu do danych na potrzeby DSA;

(iv) wdrażania zmian, których celem jest ograniczenie istniejących uchybień w zakresie bezpieczeństwa w portalu dostępu do danych na potrzeby DSA;

(v) określania warunków w zakresie upoważniania, w tym na wniosek administratorów, do przeprowadzania niezależnych audytów, w tym kontroli, i przeglądów środków bezpieczeństwa, oraz wnoszenia wkładu w przeprowadzanie tych audytów, kontroli i przeglądów, z zastrzeżeniem warunków, które są zgodne z Protokołem (nr 7) do Traktatu o funkcjonowaniu Unii Europejskiej w sprawie przywilejów i immunitetów Unii Europejskiej;

c) zmianę procedury kontroli, by udokumentować i zmierzyć wpływ zmiany przed jej wdrożeniem oraz na bieżąco informować administratorów o wszelkich zmianach, które mogą wpłynąć na łączność z portalem dostępu do danych na potrzeby DSA lub na bezpieczeństwo portalu dostępu do danych na potrzeby DSA;

d) ustanowienie procedury konserwacji i naprawy, by określić zasady i warunki, których należy przestrzegać w przypadku konieczności przeprowadzenia konserwacji lub naprawy portal dostępu do danych na potrzeby DSA;

e) ustanowienie procedury dotyczącej cyberincydentów na potrzeby określenia systemu zgłaszania i eskalacji, bezzwłocznego informowania administratorów, których to dotyczy, bezzwłocznego informowania administratorów, aby mogli zgłosić krajowym organom nadzorczym odpowiedzialnym za ochronę danych wszelkie naruszenia ochrony danych osobowych, a także na potrzeby określenia procesu dyscyplinarnego w przypadku naruszeń zasad bezpieczeństwa w portalu dostępu do danych na potrzeby DSA.

6. Komisja wprowadza najnowocześniejsze fizyczne lub logiczne środki bezpieczeństwa w odniesieniu do obiektów, w których znajduje się portal dostępu do danych na potrzeby DSA, oraz w odniesieniu do kontroli dostępu do danych i bezpiecznego dostępu. W tym celu Komisja:

a) egzekwuje bezpieczeństwo fizyczne, by ustanowić wyraźne granice bezpieczeństwa i umożliwić wykrywanie naruszeń w portalu dostępu do danych na potrzeby DSA;

b) kontroluje dostęp do obiektów portalu dostępu do danych na potrzeby DSA;

c) zapewnia, aby sprzętu nie można było dodać, wymienić ani usunąć bez uprzedniej zgody wyznaczonych odpowiedzialnych podmiotów;

d) kontroluje dostęp do portalu dostępu do danych na potrzeby DSA;

e) zapewnia uwierzytelnienie użytkowników portalu dostępu do danych na potrzeby DSA, którzy mają dostęp do portalu dostępu do danych na potrzeby DSA;

f) dokonuje przeglądu uprawnień do udzielania zezwoleń na dostęp do portalu dostępu do danych na potrzeby DSA w przypadku wykrycia naruszenia bezpieczeństwa mającego wpływ na działanie portalu dostępu do danych na potrzeby DSA;

g) zachowuje integralność informacji przekazywanych za pośrednictwem portalu dostępu do danych na potrzeby DSA;

h) wprowadza techniczne i organizacyjne środki bezpieczeństwa, by zapobiec nieuprawnionemu dostępowi do danych osobowych w portalu dostępu do danych na potrzeby DSA;

i) wdraża, w razie potrzeby, środki mające na celu zablokowanie nieuprawnionego dostępu do portalu dostępu do danych na potrzeby DSA (tj. zablokowanie lokalizacji/adresu IP).

7. Komisja:

a) podejmuje działania w celu ochrony swojej domeny obejmujące zerwanie połączeń, w przypadku znacznych odstępstw od zasad i koncepcji jakości i bezpieczeństwa;

b) utrzymuje plan zarządzania ryzykiem związany ze swoim zakresem odpowiedzialności;

c) monitoruje – w czasie rzeczywistym – wydajność wszystkich komponentów usług w ramach portalu dostępu do danych na potrzeby DSA, tworzy regularne statystyki i prowadzi rejestry;

d) zapewnia wsparcie dla użytkowników portalu dostępu do danych na potrzeby DSA w języku angielskim;

e) wspiera administratorów za pośrednictwem odpowiednich środków technicznych i organizacyjnych w wywiązywaniu się ze spoczywającego na administratorze obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III rozporządzenia (UE) 2016/679;

f) wspiera administratorów poprzez przekazywanie im informacji na temat portalu dostępu do danych na potrzeby DSA w celu realizacji obowiązków przewidzianych w art. 32, 33, 34, 35 i 36 rozporządzenia (UE) 2016/679;

g) zapewnia, aby dane przetwarzane w ramach portalu dostępu do danych na potrzeby DSA były niemożliwe do odczytania dla każdej osoby, która nie jest uprawniona do uzyskania do nich dostępu;

h) wprowadza wszelkie stosowne środki, aby zapobiec nieuprawnionemu dostępowi do przekazywanych danych osobowych za pośrednictwem portalu dostępu do danych na potrzeby DSA;

i) wprowadza środki w celu ułatwienia komunikacji między administratorami;

j) prowadzi rejestr czynności przetwarzania dokonywanych w imieniu administratorów zgodnie z art. 31 ust. 2 rozporządzenia (UE) 2018/1725.