Rada
Unii Europejskiej

Bruksela, 7 lipca 2025 r.
(OR. en)

11312/25
ADD 1

MI 511
COMPET 695
IND 249
TELECOM 237
CONSOM 131
JAI 1040
CT 91
PI 146
AUDIO 65
DELACT 95

PISMO PRZEWODNIE

Od:	Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)
Data otrzymania:	2 lipca 2025 r.
Do:	Thérèse BLANCHET, sekretarz generalna Rady Unii Europejskiej
Nr dok. Kom.:	C(2025) 4340 final - ANNEX
Dotyczy:	ZAŁĄCZNIK do rozoprządzenia delegowanego Komisji (UE) .../... uzupełniającego 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

Delegacje otrzymują w załączeniu dokument C(2025) 4340 final - ANNEX.

Zał.: C(2025) 4340 final - ANNEX

KOMISJA
EUROPEJSKA

Bruksela, dnia 1.7.2025 r.
C(2025) 4340 final

ANNEX

ZAŁĄCZNIK

do rozoprządzenia delegowanego Komisji (UE) .../...

uzupełniającego 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

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:

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

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

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

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

e) 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.