ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2018/1807

z dnia 14 listopada 2018 r.

w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej

(Tekst mający znaczenie dla EOG)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 114,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego ([1]),

po konsultacji z Komitetem Regionów,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą ([2]),

a także mając na uwadze, co następuje:

(1) Cyfryzacja gospodarki postępuje coraz szybciej. Technologie informacyjno-komunikacyjne nie stanowią już specyficznego sektora, lecz są podstawą wszystkich nowoczesnych, innowacyjnych systemów gospodarczych i społeczeństw. Dane elektroniczne znajdują się w centrum tych systemów i mogą przynieść ogromne korzyści, jeżeli podda się je analizie lub połączy z usługami i produktami. Jednocześnie szybki rozwój gospodarki opartej na danych oraz nowo powstające technologie, takie jak sztuczna inteligencja, produkty i usługi internetu rzeczy, systemy autonomiczne i sieci 5G, stwarzają nowe wyzwania prawne dotyczące kwestii dostępu do danych i ich ponownego wykorzystywania, odpowiedzialności, etyki i solidarności. Należy rozważyć działania w kwestii odpowiedzialności, w szczególności w drodze wdrożenia kodeksów samoregulacji i innych wzorcowych praktyk, uwzględniając zalecenia, decyzje i działania podejmowane bez udziału człowieka w całym łańcuchu wartości przetwarzania danych. Działania takie mogłyby również uwzględniać odpowiednie mechanizmy ustalania odpowiedzialności, przenoszenia odpowiedzialności między uzupełniającymi się usługami, ubezpieczenia oraz kontroli.

(2) Łańcuchy wartości danych opierają się na różnych działaniach w zakresie danych: tworzenia i gromadzenia danych; agregacji i organizacji danych; przetwarzania danych; analizy danych, obrotu danymi i dystrybucji danych; wykorzystywania i ponownego wykorzystywania danych. Skuteczne i efektywne funkcjonowanie przetwarzania danych stanowi podstawowy element budowy każdego łańcucha wartości danych. Jednakże skuteczne i efektywne funkcjonowanie przetwarzania danych oraz rozwój gospodarki opartej na danych w Unii utrudniają w szczególności dwa rodzaje przeszkód w mobilności danych i tworzeniu rynku wewnętrznego: wymogi dotyczące lokalizacji danych wprowadzone przez organy państw członkowskich oraz uzależnienie od jednego dostawcy w sektorze prywatnym.

(3) Zgodnie z Traktatem o funkcjonowaniu Unii Europejskiej (zwanym dalej „TFUE") swoboda przedsiębiorczości i swoboda świadczenia usług mają zastosowanie do usług przetwarzania danych. Świadczenie tych usług jest jednak utrudnione, a czasem nawet niemożliwe ze względu na niektóre wymogi krajowe, regionalne lub lokalne dotyczące lokalizacji danych na określonym terytorium.

(4) Takie przeszkody dla swobodnego przepływu usług przetwarzania danych oraz dla swobody przedsiębiorczości w przypadku dostawców usług wynikają z wymogów w przepisach państw członkowskich, zgodnie z którymi dane muszą być zlokalizowane na określonym obszarze geograficznym lub określonym terytorium do celów ich przetwarzania. Równoważny skutek mają inne przepisy lub praktyki administracyjne, które nakładają szczególne wymogi utrudniające przetwarzanie danych poza określonym obszarem geograficznym lub określonym terytorium w Unii, takie jak wymogi stosowania rozwiązań technologicznych, które zostały certyfikowane lub zatwierdzone w danym państwie członkowskim. Brak pewności prawa co do zakresu uzasadnionych i nieuzasadnionych wymogów dotyczących lokalizacji danych w jeszcze większym stopniu ogranicza uczestnikom rynku i podmiotom sektora publicznego możliwości wyboru w odniesieniu do miejsca przetwarzania danych. Niniejsze rozporządzenie w żaden sposób nie ogranicza swobody przedsiębiorstw w zakresie zawierania umów określających lokalizację danych. Celem niniejszego rozporządzenia jest jedynie zagwarantowanie tej swobody w drodze zapewnienia, aby uzgodniona lokalizacja mogła znajdować się w dowolnym miejscu w Unii.

([1]) Dz.U. C 227 z 28.6.2018, s. 78.

([2]) Stanowisko Parlamentu Europejskiego z dnia 4 października 2018 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z dnia 6 listopada 2018 r.

(5) Jednocześnie mobilność danych w Unii hamują również ograniczenia w sektorze prywatnym: kwestie prawne, umowne i techniczne utrudniające lub uniemożliwiające użytkownikom usług przetwarzania danych przenoszenie ich danych od jednego dostawcy usług do innego lub z powrotem do ich własnych systemów informatycznych, także po rozwiązaniu przez użytkowników umowy z dostawcą usług.

(6) Połączenie tych przeszkód doprowadziło do braku konkurencji między dostawcami usług w chmurze w Unii, różnych problemów z uzależnieniem od jednego dostawcy oraz poważnego braku mobilności danych. Podobnie polityki dotyczące lokalizacji danych ograniczyły zdolność przedsiębiorstw badawczo-rozwojowych do ułatwiania współpracy między firmami, uczelniami oraz innymi organizacjami badawczymi celem pobudzania innowacyjności.

(7) Mając na uwadze pewność prawa oraz z uwagi na potrzebę zapewnienia równych warunków działania w Unii jednolity zestaw przepisów dla wszystkich uczestników rynku stanowi element o kluczowym znaczeniu dla funkcjonowania rynku wewnętrznego. Aby wyeliminować bariery w handlu i zakłócenia konkurencji wynikające z różnic między przepisami krajowymi oraz zapobiec pojawianiu się kolejnych możliwych barier w handlu i znaczących zakłóceń konkurencji, konieczne jest przyjęcie jednolitych przepisów mających zastosowanie we wszystkich państwach członkowskich.

(8) Niniejsze rozporządzenie nie ma wpływu na ramy prawne w zakresie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych oraz w zakresie poszanowania życia prywatnego i ochrony danych osobowych w łączności elektronicznej, w szczególności na rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 ([1]) oraz dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 ([2]) i 2002/58/WE ([3]).

(9) Rozwijający się internet rzeczy, sztuczna inteligencja oraz uczenie się maszyn stanowią duże źródło danych nieosobowych, na przykład w konsekwencji stosowania ich w zautomatyzowanych procesach produkcji przemysłowej. Konkretnym przykładem danych nieosobowych są zagregowane i zanonimizowane zbiory danych wykorzystywane do celów analizy dużych zbiorów danych, dane związane z rolnictwem precyzyjnym ułatwiające monitorowanie i optymalizację zużycia pestycydów i wody lub dane dotyczące potrzeb związanych z konserwacją maszyn przemysłowych. Jeżeli rozwój technologiczny umożliwia przekształcanie zanonimizowanych danych w dane osobowe, takie dane należy traktować jako dane osobowe i stosować odpowiednio rozporządzenie (UE) 2016/679.

(10) Zgodnie z rozporządzeniem (UE) 2016/679 państwa członkowskie nie mogą ograniczać ani zakazywać swobodnego przepływu danych osobowych w Unii z powodów związanych z ochroną osób fizycznych w związku z przetwarzaniem danych osobowych. W niniejszym rozporządzeniu ustanawia się tę samą zasadę swobodnego przepływu w Unii w odniesieniu do danych nieosobowych, z wyjątkiem sytuacji, w których ograniczenie lub zakaz są uzasadnione ze względów bezpieczeństwa publicznego. Rozporządzenie (UE) 2016/679 oraz niniejsze rozporządzenie stanowią spójny zbiór przepisów dotyczących swobodnego przepływu różnych rodzajów danych. Ponadto niniejsze rozporządzenie nie nakłada obowiązku oddzielnego przechowywania różnych rodzajów danych.

(11) W celu stworzenia ram swobodnego przepływu danych nieosobowych w Unii oraz podstaw do rozwoju gospodarki opartej na danych i zwiększenia konkurencyjności unijnego przemysłu, niezbędne jest ustanowienie jasnych, kompleksowych i przewidywalnych ram prawnych w zakresie przetwarzania danych innych niż dane osobowe na rynku wewnętrznym. Podejście oparte na zasadach przewidujące współpracę między państwami członkowskimi, a także samoregulacja, powinny zapewnić wystarczającą elastyczność ram, aby umożliwić uwzględnianie w nich zmieniających się potrzeb użytkowników, dostawców usług i organów krajowych w Unii. Aby uniknąć ryzyka pokrywania się z istniejącymi mechanizmami, a tym samym uniknąć zwiększenia obciążeń zarówno dla państw członkowskich, jak i podmiotów gospodarczych, nie należy ustanawiać szczegółowych przepisów technicznych.

(12) Niniejsze rozporządzenie nie powinno mieć wpływu na przetwarzanie danych w zakresie, w jakim to przetwarzanie danych stanowi część działalności, która wykracza poza zakres prawa Unii. Należy w szczególności przypomnieć, że zgodnie z art. 4 Traktatu o Unii Europejskiej (zwanego dalej „TUE") bezpieczeństwo narodowe pozostaje w zakresie wyłącznej odpowiedzialności każdego państwa członkowskiego.

([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]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. L 119 z 4.5.2016, s. 89).

([3]) 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).

(13) Swobodny przepływ danych w Unii odegra ważną rolę w osiąganiu wzrostu i innowacji opartych na danych. Podobnie jak przedsiębiorstwa i konsumenci, również organy publiczne i podmioty prawa publicznego państw członkowskich mogą skorzystać na większej swobodzie wyboru dostawców usług opartych na danych, bardziej konkurencyjnych cenach i większej skuteczności świadczenia usług obywatelom. Zważywszy na to, że organy publiczne i podmioty prawa publicznego zajmują się dużą ilością danych, niezwykle ważne jest, aby dawały one przykład i korzystały z usług przetwarzania danych oraz aby, korzystając z takich usług, powstrzymywały się od wprowadzania jakichkolwiek ograniczeń w zakresie lokalizowaniu danych. Zatem organy publiczne i podmioty prawa publicznego powinny zostać objęte zakresem stosowania niniejszego rozporządzenia. W związku z tym zasada swobodnego przepływu danych nieosobowych przewidziana w niniejszym rozporządzeniu powinna mieć zastosowanie również do powszechnych i spójnych praktyk administracyjnych oraz do innych wymogów dotyczących lokalizacji danych w dziedzinie zamówień publicznych, bez uszczerbku dla dyrektywy Parlamentu Europejskiego i Rady 2014/24/UE ([1]).

(14) Podobnie jak w przypadku dyrektywy 2014/24/UE, niniejsze rozporządzenie pozostaje bez uszczerbku dla przepisów ustawowych, wykonawczych i administracyjnych, które dotyczą wewnętrznej organizacji państw członkowskich i które przyznają organom publicznym i podmiotom prawa publicznego uprawnienia i obowiązki w zakresie przetwarzania danych bez wynikającego ze stosunku umownego wynagrodzenia na rzecz podmiotów prawa prywatnego, a także dla przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich przewidujących zasady wykonywania tych uprawnień i obowiązków. Chociaż organy publiczne i podmioty prawa publicznego zachęca się do rozważenia korzyści ekonomicznych i innych korzyści wynikających z outsourcingu zewnętrznym usługodawcom, mogłyby one mieć uzasadnione powody wyboru świadczenia takich usług we własnym zakresie lub insourcingu. W związku z powyższym żaden przepis niniejszego rozporządzenia nie zobowiązuje państw członkowskich do zlecania na zewnątrz lub eksternalizowania świadczenia usług, które chcą świadczyć we własnym zakresie lub organizować w sposób inny niż w drodze zamówień publicznych.

(15) Niniejsze rozporządzenie powinno mieć zastosowanie do osób fizycznych lub prawnych, które świadczą usługi przetwarzania danych na rzecz użytkowników mających miejsce zamieszkania lub siedzibę w Unii, w tym do dostawców usług, którzy świadczą usługi przetwarzania danych w Unii, ale nie mają siedziby na jej terytorium. Niniejsze rozporządzenie nie powinno zatem mieć zastosowania do usług przetwarzania danych poza Unią ani do wymogów dotyczących lokalizacji danych w odniesieniu do takich danych.

(16) Niniejsze rozporządzenie nie ustanawia przepisów dotyczących ustalania prawa właściwego w sprawach handlowych i w związku z tym pozostaje bez uszczerbku dla rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 593/2008 ([2]). W szczególności w zakresie, w jakim prawo właściwe dla umowy nie zostało wybrane na podstawie tego rozporządzenia, umowa o świadczenie usług podlega co do zasady prawu państwa, w którym dostawca usług ma miejsce zwykłego pobytu.

(17) Niniejsze rozporządzenie powinno mieć zastosowanie do jak najszerzej rozumianego przetwarzania danych, obejmującego wykorzystanie wszelkiego rodzaju systemów informatycznych, niezależnie od tego, czy są one zlokalizowane w pomieszczeniach użytkownika czy też są zlecane w ramach outsourcingu na rzecz dostawcy usług. Zakres tego pojęcia powinien obejmować różne stopnie intensywności przetwarzania danych, od przechowywania danych (infrastruktura jako usługa, ang. Infrastructure-as-a-Service, IaaS) po przetwarzanie danych na platformach (platforma jako usługa, ang. Platform-as-a-Service, PaaS) lub w aplikacjach (oprogramowanie jako usługa, ang. Software-as-a-Service, SaaS).

(18) Wymogi dotyczące lokalizacji danych stanowią niewątpliwą przeszkodę dla swobody świadczenia usług przetwarzania danych w Unii oraz dla rozwoju rynku wewnętrznego. Powinny one zatem zostać zakazane, chyba że są uzasadnione względami bezpieczeństwa publicznego, zdefiniowanego w prawie Unii, w szczególności w rozumieniu art. 52 TFUE, oraz zgodne z zasadą proporcjonalności zapisaną w art. 5 TUE. W celu wdrożenia zasady transgranicznego swobodnego przepływu danych nieosobowych, zapewnienia szybkiego zniesienia istniejących wymogów dotyczących lokalizacji danych oraz umożliwienia, do celów operacyjnych, przetwarzania danych w wielu lokalizacjach w całej Unii, a także w związku z tym, że w niniejszym rozporządzeniu przewidziano środki służące zapewnieniu dostępności danych do celów kontroli regulacyjnej, państwa członkowskie powinny mieć możliwość powoływania się jedynie na bezpieczeństwo publiczne jako uzasadnienie wymogów lokalizacji danych.

(19) Pojęcie „bezpieczeństwa publicznego" w rozumieniu art. 52 TFUE i zgodnie z wykładnią Trybunału Sprawiedliwości obejmuje zarówno bezpieczeństwo wewnętrzne, jak i zewnętrzne danego państwa członkowskiego, a także kwestie ochrony publicznej, w szczególności w celu ułatwienia prowadzenia postępowań przygotowawczych, wykrywania i ścigania przestępstw. Zakłada ono istnienie rzeczywistego i wystarczająco poważnego zagrożenia dla jednego z podstawowych interesów społecznych, takiego jak zagrożenie dla funkcjonowania instytucji i podstawowych usług publicznych oraz życia ludności, a także ryzyko poważnego zakłócenia stosunków zagranicznych lub pokojowego współistnienia narodów, lub zagrożenie dla interesów wojskowych. Zgodnie z zasadą proporcjonalności wymogi dotyczące lokalizacji danych, które uzasadnione są względami bezpieczeństwa publicznego, powinny być odpowiednie do zamierzonego celu oraz nie powinny wykraczać poza to, co jest niezbędne do realizacji tego celu.

([1]) Dyrektywa Parlamentu Europejskiego i Rady 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych, uchylająca dyrektywę 2004/18/WE (Dz.U. L 94 z 28.3.2014, s. 65).

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 593/2008 z dnia 17 czerwca 2008 r. w sprawie prawa właściwego dla zobowiązań umownych (Rzym I) (Dz.U. L 177 z 4.7.2008, s. 6).

(20) Aby zapewnić skuteczne stosowanie zasady swobodnego transgranicznego przepływu danych nieosobowych oraz zapobiec pojawianiu się nowych przeszkód dla sprawnego funkcjonowania rynku wewnętrznego, państwa członkowskie powinny niezwłocznie zgłaszać Komisji każdy projekt aktu, który wprowadza nowe lub zmienia istniejące wymogi dotyczące lokalizacji danych. Te projekty aktów powinny być przedkładane i oceniane zgodnie z dyrektywą (UE) 2015/1535 Parlamentu Europejskiego i Rady ([1]).

(21) Ponadto, w celu wyeliminowania możliwych istniejących przeszkód, w okresie przejściowym trwającym 24 miesiące od dnia rozpoczęcia stosowania niniejszego rozporządzenia, państwa członkowskie powinny dokonać przeglądu istniejących przepisów ustawowych, wykonawczych lub administracyjnych o charakterze ogólnym, ustanawiających wymogi dotyczące lokalizacji danych oraz zgłosić Komisji wszelkie takie wymogi dotyczące lokalizacji danych, uznane przez nie za zgodne z niniejszym rozporządzeniem, wraz z uzasadnieniem. Powinno to umożliwić Komisji zbadanie zgodności wszelkich utrzymanych w mocy wymogów dotyczących lokalizacji danych. W stosownych przypadkach Komisja powinna mieć możliwość przedstawiania uwag danemu państwu członkowskiemu. Takie uwagi mogłyby obejmować zalecenie zmiany lub uchylenia wymogu dotyczącego lokalizacji danych.

(22) Ustanowione w niniejszym rozporządzeniu obowiązki zgłaszania Komisji istniejących wymogów dotyczących lokalizacji danych oraz projektów aktów powinny mieć zastosowanie do wymogów regulacyjnych dotyczących lokalizacji i projektów aktów o charakterze ogólnym, lecz nie powinny mieć zastosowania do decyzji skierowanych do konkretnej osoby fizycznej lub prawnej.

(23) W celu zapewnienia, aby wymogi dotyczące lokalizacji danych w państwach członkowskich, ustanowione w przepisach ustawowych, wykonawczych lub administracyjnych o charakterze ogólnym, były przejrzyste dla osób fizycznych i prawnych, takich jak dostawcy usług i użytkownicy usług przetwarzania danych, państwa członkowskie powinny publikować informacje na temat takich wymogów na stronie krajowego centralnego internetowego punktu informacyjnego, oraz regularnie je aktualizować. Jako alternatywne rozwiązanie państwa członkowskie powinny przekazywać aktualne informacje na temat takich wymogów centralnemu punktowi informacyjnemu ustanowionemu na mocy innego aktu Unii. Do celów odpowiedniego informowania osób fizycznych i prawnych o wymogach dotyczących lokalizacji danych w całej Unii państwa członkowskie powinny przekazywać Komisji informacje o adresach takich centralnych punktów informacyjnych. Komisja powinna opublikować te informacje na swojej stronie internetowej wraz z regularnie aktualizowanym skonsolidowanym wykazem wszystkich wymogów dotyczących lokalizacji danych obowiązujących w państwach członkowskich, w tym również podsumowanie informacji na temat tych wymogów.

(24) Wymogi dotyczące lokalizacji danych wynikają często z braku zaufania do transgranicznych usług przetwarzania danych, który wywodzi się z założenia, że właściwe organy państw członkowskich nie miałyby dostępu do tych danych do takich celów jak inspekcje i audyty w ramach kontroli regulacyjnej lub nadzorczej. Taki brak zaufania nie może zostać przezwyciężony wyłącznie w drodze unieważnienia warunków umowy zakazujących właściwym organom zgodnego z prawem dostępu do danych na potrzeby wykonywania ich obowiązków urzędowych. W związku z tym w niniejszym rozporządzeniu należy wyraźnie określić, że nie ma ono wpływu na uprawnienia właściwych organów do żądania lub uzyskiwania dostępu do danych zgodnie z prawem Unii lub prawem krajowym, oraz że właściwym organom nie można odmówić dostępu do danych z uwagi na fakt, że dane są przetwarzane w innym państwie członkowskim. Właściwe organy mogłyby nakładać wymogi funkcjonalne w celu uzyskania dostępu do danych, takie jak wymóg przechowywania opisów systemu w danym państwie członkowskim.

(25) Osoby fizyczne lub prawne, które podlegają obowiązkom przekazywania danych właściwym organom, mogą wywiązać się z tych obowiązków przez udzielenie i zagwarantowanie tym organom skutecznego i terminowego dostępu do danych drogą elektroniczną, niezależnie od państwa członkowskiego, na którego terytorium dane są przetwarzane. Dostęp taki można zapewnić przez sprecyzowanie konkretnych warunków w umowach zawieranych między osobą fizyczną lub prawną podlegającą obowiązkowi udzielenia dostępu a dostawcą usług.

(26) W przypadku gdy osoba fizyczna lub prawna podlegająca obowiązkowi przekazywania danych nie wywiąże się z niego, właściwy organ powinien mieć możliwość zwrócenia się o pomoc do właściwych organów innych państw członkowskich. W takich przypadkach właściwe organy powinny korzystać ze specjalnych instrumentów współpracy przewidzianych w prawie Unii lub umowach międzynarodowych, w zależności od przedmiotu

([1]) Dyrektywa (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz.U. L 241 z 17.9.2015, s. 1).

sprawy, takich jak, w obszarze współpracy organów ścigania i wymiaru sprawiedliwości w sprawach cywilnych lub karnych albo w sprawach administracyjnych, odpowiednio: decyzja ramowa Rady 2006/960/WSiSW ([1]), dyrektywa Parlamentu Europejskiego i Rady 2014/41/UE ([2]), Konwencja Rady Europy o cyberprzestępczości ([3]), rozporządzenie Rady (WE) nr 1206/2001 ([4]), dyrektywa Rady 2006/112/WE ([5]) oraz rozporządzenie Rady (UE) nr 904/2010 ([6]). W przypadku braku takich specjalnych mechanizmów współpracy właściwe organy powinny ze sobą współpracować w celu udzielenia dostępu do żądanych danych za pośrednictwem wyznaczonych centralnych punktów kontaktowych.

(27) W przypadku gdy wniosek o pomoc pociąga za sobą konieczność uzyskania przez organ, do którego wniosek jest skierowany, dostępu do jakichkolwiek pomieszczeń osoby fizycznej lub prawnej, w tym do jakichkolwiek urządzeń lub środków służących do przetwarzania danych, uzyskanie takiego dostępu musi odbywać się zgodnie z prawem Unii lub krajowym prawem procesowym, w tym z wszelkimi wymogami dotyczącymi uzyskania uprzedniej zgody organu sądowego.

(28) Niniejsze rozporządzenie nie powinno umożliwiać użytkownikom podejmowania prób obejścia zastosowania prawa krajowego. Należy zatem przewidzieć nakładanie przez państwa członkowskie skutecznych, proporcjonalnych i odstraszających sankcji na użytkowników, którzy uniemożliwiają właściwym organom uzyskanie dostępu do swoich danych niezbędnych do wykonywania przez właściwe organy obowiązków urzędowych wynikających z prawa Unii i prawa krajowego. W pilnych przypadkach, gdy użytkownik nadużywa przysługujących mu praw, państwa członkowskie powinny mieć możliwość nałożenia ściśle proporcjonalnych środków tymczasowych. Wszelkie środki tymczasowe wymagające relokalizacji danych na okres dłuższy niż 180 dni od relokalizacji stanowiłyby odejście od zasady swobodnego przepływu danych przez znaczący okres czasu i w związku z tym należy je zgłosić Komisji do celów zbadania ich zgodności z prawem Unii.

(29) Możliwość przenoszenia danych bez przeszkód jest jednym z kluczowych czynników ułatwiających dokonywanie wyboru przez użytkowników oraz rozwój skutecznej konkurencji na rynkach usług przetwarzania danych. Rzeczywiste trudności w transgranicznym przenoszeniu danych lub kwestie postrzegane jako takie trudności podważają również zaufanie użytkowników profesjonalnych do korzystania z ofert transgranicznych, a co za tym idzie, ich zaufanie do rynku wewnętrznego. Podczas gdy indywidualni konsumenci korzystają z istniejących przepisów prawa Unii, brak jest ułatwień dla tych użytkowników, którzy chcą zmienić dostawcę usług w ramach swojej działalności gospodarczej lub zawodowej. Spójność wymogów technicznych w całej Unii, dotyczących harmonizacji technicznej, wzajemnego uznawaniu czy też dobrowolnej harmonizacji, przyczynia się także do rozwoju konkurencyjnego rynku wewnętrznego usług przetwarzania danych.

(30) Aby móc w pełni czerpać z korzyści, jakie płyną z konkurencji na rynku, użytkownicy profesjonalni powinni móc dokonywać świadomych wyborów i łatwo porównywać poszczególne elementy różnych oferowanych na rynku wewnętrznym usług przetwarzania danych, w tym warunki umowne przenoszenia danych po rozwiązaniu umowy. W celu uwzględnienia potencjału innowacyjnego rynku oraz doświadczenia i wiedzy fachowej dostawców usług raz profesjonalnych użytkowników usług przetwarzania danych, uczestnicy rynku powinni opracować szczegółowe informacje i wymagania operacyjne dotyczące przenoszenia danych – poprzez samoregulację wspieraną, ułatwianą i monitorowaną przez Komisję – w formie unijnych kodeksów postępowania, co mogłoby obejmować określenie wzorca warunków umownych.

(31) Takie kodeksy postępowania – aby były one skuteczne oraz ułatwiały zmianę dostawcy usług i przenoszenie danych – powinny być kompleksowe i obejmować co najmniej kluczowe aspekty istotne w procesie przenoszenia danych, takie jak: procesy tworzenia zapasowych kopii danych i lokalizację takich kopii; dostępne formaty i nośniki danych; wymaganą konfigurację systemów informatycznych i minimalną szerokość pasma sieciowego; czas wymagany przed rozpoczęciem procesu przenoszenia danych i okres, przez który dane będą nadal dostępne do celów ich przeniesienia; a także gwarancje dostępu do danych w przypadku upadłości dostawcy usług. Kodeksy postępowania powinny również wyraźnie stanowić, że uzależnienie od jednego dostawcy nie jest dopuszczalną praktyką handlową, powinny przewidywać stosowanie technologii zwiększających zaufanie oraz powinny być regularnie aktualizowane, aby nadążać za rozwojem technologicznym. Podczas całego procesu Komisja powinna zapewniać konsultacje z wszystkimi zainteresowanymi stronami, w tym małymi i średnimi przedsiębiorstwami (zwanymi dalej „MŚP") oraz przedsiębiorstwami typu start-up, użytkownikami oraz dostawcami usług w chmurze. Komisja powinna przeprowadzić ocenę opracowywania i skuteczności wdrażania takich kodeksów postępowania.

([1]) Decyzja ramowa Rady 2006/960/WSiSW z dnia 18 grudnia 2006 r. w sprawie uproszczenia wymiany informacji i danych wywiadowczych między organami ścigania państw członkowskich Unii Europejskiej (Dz.U. L 386 z 29.12.2006, s. 89).

([2]) Dyrektywa Parlamentu Europejskiego i Rady nr 2014/41/UE z dnia 3 kwietnia 2014 r. w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych (Dz.U. L 130 z 1.5.2014, s. 1).

([3]) Konwencja Rady Europy o cyberprzestępczości (CETS nr 185).

([4]) Rozporządzenie Rady (WE) nr 1206/2001 z dnia 28 maja 2001 r. w sprawie współpracy między sądami państw członkowskich przy przeprowadzaniu dowodów w sprawach cywilnych lub handlowych (Dz.U. L 174 z 27.6.2001, s. 1).

([5]) Dyrektywa 2006/112/WE Rady z dnia 28 listopada 2006 r. w sprawie wspólnego systemu podatku od wartości dodanej (Dz.U. L 347 z 11.12.2006, s. 1).

([6]) Rozporządzenie Rady (UE) nr 904/2010 z dnia 7 października 2010 r. w sprawie współpracy administracyjnej oraz zwalczania oszustw w dziedzinie podatku od wartości dodanej (Dz.U. L 268 z 12.10.2010, s. 1).

(32) W przypadku gdy właściwy organ jednego z państw członkowskich zwraca się do innego państwa członkowskiego o pomoc w uzyskaniu dostępu do danych na podstawie niniejszego rozporządzenia, powinien on złożyć, za pośrednictwem wyznaczonego centralnego punktu kontaktowego, należycie uzasadniony wniosek do wyznaczonego centralnego punktu kontaktowego tego innego państwa członkowskiego, wraz z pisemnym wyjaśnieniem powodów i podstaw prawnych ubiegania się o dostęp do danych. Centralny punkt kontaktowy wyznaczony przez państwo członkowskie, do którego skierowany jest wniosek, powinien ułatwiać przekazanie wniosku do właściwego organu w państwie członkowskim, do którego wniosek jest skierowany. W celu zapewnienia skutecznej współpracy organ, któremu wniosek został przekazany, powinien bez zbędnej zwłoki udzielić pomocy w odpowiedzi na dany wniosek lub dostarczyć informacji na temat trudności w wykonaniu takiego wniosku o pomoc lub podać powody odmowy wykonania takiego wniosku.

(33) Zwiększenie zaufania do bezpieczeństwa transgranicznego przetwarzania danych powinno zmniejszyć skłonność uczestników rynku i podmiotów sektora publicznego do traktowania lokalizacji danych jako zastępczej gwarancji bezpieczeństwa danych. Powinno to również zapewnić przedsiębiorstwom większą pewność prawa w odniesieniu do spełniania wymogów w zakresie bezpieczeństwa mających zastosowanie do zlecania przetwarzania danych w ramach outsourcingu dostawcom usług, w tym również dostawcom w innych państwach członkowskich.

(34) Wymogi w zakresie bezpieczeństwa dotyczące przetwarzania danych, które są stosowane w sposób uzasadniony i proporcjonalny na podstawie prawa Unii lub prawa krajowego zgodnego z prawem Unii w państwie członkowskim miejsca zamieszkania osób fizycznych lub siedziby osób prawnych, których danych to dotyczy, powinny mieć nadal zastosowanie do przetwarzania tych danych w innym państwie członkowskim. Te osoby fizyczne lub prawne powinny mieć możliwość spełniania takich wymogów samodzielnie albo za pośrednictwem klauzul umownych w umowach z dostawcami usług.

(35) Wymogi w zakresie bezpieczeństwa ustanowione na poziomie krajowym powinny być konieczne i proporcjonalne do ryzyka, na jakie narażone jest bezpieczeństwo przetwarzania danych w zakresie stosowania prawa krajowego, w którym wymogi te określono.

(36) W dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/1148 ([1]) przewidziano środki prawne w celu zwiększenia ogólnego poziomu cyberbezpieczeństwa w Unii. Usługi przetwarzania danych stanowią jedną z kategorii usług cyfrowych objętych zakresem stosowania tej dyrektywy. Zgodnie z tą dyrektywą państwa członkowskie mają obowiązek zapewnić, aby dostawcy usług cyfrowych określali i podejmowali odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zarządzania ryzykiem, na jakie narażone są wykorzystywane przez nich sieci i systemy informatyczne. Środki takie powinny zapewniać poziom bezpieczeństwa odpowiedni do istniejącego ryzyka oraz uwzględniać bezpieczeństwo systemów i obiektów, postępowanie w przypadku incydentu, zarządzanie ciągłością działania, monitorowanie, audyt i testowanie oraz zgodność z normami międzynarodowymi. Elementy te mają zostać określone bardziej szczegółowo w aktach wykonawczych, które Komisja ma przyjąć na podstawie tej dyrektywy.

(37) Komisja powinna przedłożyć sprawozdanie z wykonania niniejszego rozporządzenia, w szczególności w celu określenia, czy istnieje potrzeba wprowadzenia zmian w świetle postępu technologicznego i zmian na rynku. Sprawozdanie to powinno w szczególności oceniać niniejsze rozporządzenie, zwłaszcza jego stosowanie do zbiorów danych obejmujących zarówno dane osobowe, jak i nieosobowe, a także oceniać stosowanie wyjątku dotyczącego bezpieczeństwa publicznego. Przed rozpoczęciem stosowania niniejszego rozporządzenia, Komisja powinna również opublikować wskazówki na temat tego, jak postępować ze zbiorami danych obejmującymi zarówno dane osobowe, jak i nieosobowe, tak aby te przedsiębiorstwa, w tym MŚP, mogły lepiej zrozumieć wzajemne powiązania między niniejszym rozporządzeniem a rozporządzeniem (UE) 2016/679 oraz aby zapewnić przestrzeganie obu rozporządzeń.

(38) Niniejsze rozporządzenie nie narusza praw podstawowych i jest zgodne z zasadami uznanymi w szczególności w Karcie praw podstawowych Unii Europejskiej, oraz powinno być interpretowane i stosowane zgodnie z tymi prawami i zasadami, w tym prawem do ochrony danych osobowych wolnością wypowiedzi i informacji oraz wolnością prowadzenia działalności gospodarczej.

(39) Ponieważ cel niniejszego rozporządzenia, a mianowicie zapewnienie swobodnego przepływu danych innych niż osobowe w Unii, nie może zostać osiągnięty w sposób wystarczający przez państwa członkowskie, natomiast ze względu na jego rozmiary i skutki możliwe jest lepsze jego osiągnięcie na poziomie Unii, Unia może podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 TUE. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tego celu,

([1]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194 z 19.7.2016, s. 1).

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Przedmiot

Celem niniejszego rozporządzenia jest zapewnienie na terytorium Unii swobodnego przepływu danych innych niż dane osobowe poprzez ustanowienie przepisów odnoszących się do wymogów dotyczących lokalizacji danych, dostępności danych dla właściwych organów i przenoszenia danych przez użytkowników profesjonalnych.

Artykuł 2

Zakres stosowania

1. Niniejsze rozporządzenie ma zastosowanie do przetwarzania elektronicznych danych innych niż dane osobowe w Unii, które jest:

a) świadczone jako usługa na rzecz użytkowników mających miejsce zamieszkania lub siedzibę w Unii, niezależnie od tego, czy dostawca usługi ma swoją siedzibę w Unii czy poza nią; lub

b) prowadzone na potrzeby własne przez osobę fizyczną mającą miejsce zamieszkania w Unii lub osobę prawną mającą siedzibę w Unii.

2. W przypadku zbiorów danych obejmujących zarówno dane osobowe, jak i nieosobowe niniejsze rozporządzenie ma zastosowanie do części zbioru złożonej z danych nieosobowych. W przypadku gdy w zbiorze danych dane osobowe i nieosobowe są nierozerwalnie związane, niniejsze rozporządzenie pozostaje bez uszczerbku dla stosowania rozporządzenia (UE) 2016/679.

3. Niniejsze rozporządzenie nie ma zastosowania do działalności, która wykracza poza zakres stosowania prawa Unii.

Niniejsze rozporządzenie pozostaje bez uszczerbku dla przepisów ustawowych, wykonawczych i administracyjnych dotyczących wewnętrznej organizacji państw członkowskich, przyznających organom publicznym i podmiotom prawa publicznego zdefiniowanym w art. 2 ust. 1 pkt 4 dyrektywy 2014/24/UE uprawnienia i obowiązki w zakresie przetwarzania danych bez wynikającego ze stosunku umownego wynagrodzenia na rzecz podmiotów prywatnych, jak również dla przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich, które przewidują zasady wykonywania tych uprawnień i obowiązków.

Artykuł 3

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „dane" oznaczają dane inne niż dane osobowe zdefiniowane w art. 4 pkt 1 rozporządzenia (UE) 2016/679;

2) „przetwarzanie" oznacza każdą operację lub zestaw operacji wykonywanych na danych lub zbiorach danych w formie elektronicznej w sposób zautomatyzowany lub niezautomatyzowany, takie jak gromadzenie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie przez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

3) „projekt aktu" oznacza tekst sporządzony w celu wprowadzenia go w życie jako przepisu ustawowego, wykonawczego lub administracyjnego o charakterze ogólnym, który jest na etapie przygotowań, na którym to etapie wciąż jeszcze można dokonywać zmian merytorycznych;

4) „dostawca usług" oznacza osobę fizyczną lub prawną świadczącą usługi przetwarzania danych;

5) „wymóg dotyczący lokalizacji danych" oznacza każdy obowiązek, zakaz, warunek, ograniczenie lub innego rodzaju wymóg określony w przepisach ustawowych, wykonawczych lub administracyjnych państwa członkowskiego lub wynikający z powszechnych i spójnych praktyk administracyjnych w państwie członkowskim i w podmiotach prawa publicznego, w tym w dziedzinie zamówień publicznych, bez uszczerbku dla dyrektywy 2014/24/UE, który narzuca wymóg przetwarzania danych na terytorium danego państwa członkowskiego lub utrudnia przetwarzanie danych w jakimkolwiek innym państwie członkowskim;

6) „właściwy organ" oznacza organ państwa członkowskiego lub jakikolwiek inny podmiot uprawniony na mocy prawa krajowego do wykonywania funkcji publicznej lub sprawowania władzy publicznej, i który jest uprawniony do uzyskania dostępu do danych przetwarzanych przez osobę fizyczną lub prawną, do celów wykonywania swoich obowiązków urzędowych, stosownie do prawa Unii lub prawa krajowego;

7) „użytkownik" oznacza osobę fizyczną lub prawną, w tym organ publiczny lub podmiot prawa publicznego, korzystającą lub ubiegającą się o skorzystanie z usługi przetwarzania danych;

8) „użytkownik profesjonalny" oznacza osobę fizyczną lub prawną, w tym organ publiczny lub podmiot prawa publicznego, korzystającą lub ubiegającą się o skorzystanie z usługi przetwarzania danych do celów związanych z jej działalnością handlową, gospodarczą, rzemieślniczą, zawodową lub wykonywanym zadaniem.

Artykuł 4

Swobodny przepływ danych w Unii

1. Zakazuje się nakładania wymogów dotyczących lokalizacji danych, chyba że są one uzasadnione względami bezpieczeństwa publicznego zgodnie z zasadą proporcjonalności.

Akapit pierwszy pozostaje bez uszczerbku dla ust. 3 oraz dla wymogów dotyczących lokalizacji danych określonych na podstawie istniejących przepisów prawa Unii.

2. Państwa członkowskie niezwłocznie zgłaszają Komisji każdy projekt aktu, w którym wprowadza się nowe wymogi dotyczące lokalizacji danych lub zmiany w istniejących wymogach dotyczących lokalizacji danych, zgodnie z procedurami określonymi w art. 5, 6 i 7 dyrektywy (UE) 2015/1535.

3. Do dnia 30 maja 2021 r. państwa członkowskie zapewnią uchylenie wszelkich istniejących wymogów dotyczących lokalizacji danych ustanowionych w przepisach ustawowych, wykonawczych lub administracyjnych o charakterze ogólnym, które nie są zgodne z ust. 1 niniejszego artykułu.

Do dnia 30 maja 2021 r., jeżeli państwo członkowskie uzna, że istniejący środek zawierający wymóg dotyczący lokalizacji danych jest zgodny z ust. 1 niniejszego artykułu i w związku z tym może zostać utrzymany w mocy, zgłasza ten środek Komisji, wraz z uzasadnieniem utrzymania go w mocy. Bez uszczerbku dla art. 258 TFUE Komisja, w terminie sześciu miesięcy od dnia otrzymania takiego zgłoszenia, bada zgodność tego środka z ust. 1 niniejszego artykułu oraz w stosownych przypadkach przedstawia uwagi państwu członkowskiemu, w tym w razie konieczności zalecenie zmiany lub uchylenia tego środka.

4. Państwa członkowskie publicznie udostępniają informacje o wszelkich mających zastosowanie na ich terytorium wymogach dotyczących lokalizacji danych określonych w przepisach ustawowych, wykonawczych lub administracyjnych o charakterze ogólnym, za pośrednictwem krajowego centralnego internetowego punktu informacyjnego, oraz je aktualizują, lub przekazują aktualne informacje na temat takich wymogów dotyczących lokalizacji centralnemu punktowi informacyjnemu ustanowionemu na mocy innego aktu Unii.

5. Państwa członkowskie przekazują Komisji informację o adresie swojego centralnego punktu informacyjnego, o którym mowa w ust. 4. Komisja publikuje na swojej stronie internetowej linki do stron takich punktów wraz ze skonsolidowanym i regularnie aktualizowanym wykazem wszystkich wymogów dotyczących lokalizacji danych, o których mowa w ust. 4, w tym również podsumowanie informacji na temat tych wymogów.

Artykuł 5

Dostęp właściwych organów do danych

1. Niniejsze rozporządzenie nie ma wpływu na uprawnienia właściwych organów do żądania lub uzyskiwania dostępu do danych na potrzeby wykonywania ich obowiązków urzędowych zgodnie z prawem Unii lub prawem krajowym. Właściwym organom nie można odmówić dostępu do danych z uwagi na fakt, że dane są przetwarzane w innym państwie członkowskim.

2. W przypadku gdy po złożeniu wniosku o dostęp do danych użytkownika właściwy organ nie uzyskał dostępu oraz jeśli brak jest specjalnych mechanizmów współpracy przewidzianych w prawie Unii lub umowach międzynarodowych umożliwiających wymianę danych między właściwymi organami różnych państw członkowskich, ten właściwy organ może zwrócić się z wnioskiem o pomoc do właściwego organu innego państwa członkowskiego zgodnie z procedurą określoną w art. 7.

3. W przypadku gdy wniosek o pomoc pociąga za sobą konieczność uzyskania przez organ, do którego wniosek jest skierowany, dostępu do jakichkolwiek pomieszczeń osoby fizycznej lub prawnej, w tym do jakichkolwiek urządzeń lub środków służących do przetwarzania danych, uzyskanie takiego dostępu musi odbywać się zgodnie z prawem Unii lub krajowym prawem procesowym.

4. Państwa członkowskie mogą nakładać skuteczne, proporcjonalne i odstraszające sankcje za nieprzestrzeganie obowiązku przekazywania danych, zgodnie z prawem Unii i prawem krajowym.

W przypadku nadużycia praw przez użytkownika państwo członkowskie może, w przypadku gdy jest to uzasadnione koniecznością uzyskania pilnego dostępu do danych oraz przy uwzględnieniu interesów zainteresowanych stron, nałożyć ściśle proporcjonalne środki tymczasowe na tego użytkownika,. Jeżeli środek tymczasowy nakłada obowiązek relokalizacji danych na okres dłuższy niż 180 dni od dnia relokalizacji, zgłaszany jest Komisji w ciągu tych 180 dni. Komisja w najkrótszym możliwym czasie bada środek i jego zgodność z prawem Unii oraz w stosownych przypadkach podejmuje niezbędne środki. Komisja wymienia się informacjami dotyczącymi doświadczenia nabytego w tym zakresie z centralnymi punktami kontaktowymi państw członkowskich, o których mowa w art. 7.

Artykuł 6

Przenoszenie danych

1. Aby przyczynić się do rozwoju konkurencyjnej gospodarki opartej na danych, Komisja wspiera i ułatwia opracowywanie samoregulacyjnych kodeksów postępowania na poziomie Unii (zwanych dalej „kodeksami postępowania"), opartych na zasadzie przejrzystości i interoperacyjności oraz należycie uwzględniających otwarte standardy, obejmujące między innymi następujące aspekty:

a) najlepsze praktyki w zakresie ułatwiania zmiany dostawcy usług i przenoszenia danych z wykorzystaniem formatów ustrukturyzowanych, powszechnie używanych i nadających się do odczytu maszynowego, w tym formatów opartych na otwartych standardach, gdy jest to wymagane przez dostawcę usług otrzymującego dane lub gdy zwraca się on z takim wnioskiem;

b) minimalne wymogi informacyjne mające na celu zapewnienie użytkownikom profesjonalnym, przed zawarciem umowy o przetwarzanie danych, wystarczająco dokładnych, jasnych i przejrzystych informacji na temat następujących kwestii: procesów, wymogów technicznych, ram czasowych i opłat, które mają zastosowanie w przypadku, gdy użytkownik profesjonalny chce zmienić dostawcę usług lub przenieść dane z powrotem do własnych systemów informatycznych;

c) podejścia w zakresie systemów certyfikacji ułatwiających porównywanie produktów i usług związanych z przetwarzaniem danych dla użytkowników profesjonalnych, z uwzględnieniem przyjętych krajowych lub międzynarodowych norm, w celu ułatwienia porównywalności tych produktów i usług. Podejścia takie mogą obejmować między innymi zarządzanie jakością, zarządzanie bezpieczeństwem informacji, zarządzanie ciągłością działania i zarządzanie środowiskowe;

d) plany działania w zakresie komunikacji z wielodyscyplinarnym podejściem do upowszechniania wiedzy o kodeksach postępowania wśród właściwych zainteresowanych stron.

2. Komisja zapewnia, aby kodeksy postępowania były opracowywane w ścisłej współpracy ze wszystkimi właściwymi zainteresowanymi stronami, w tym stowarzyszeniami MŚP oraz przedsiębiorstwami typu start-up, użytkownikami i dostawcami usług w chmurze.

3. Komisja zachęca dostawców usług do zakończenia prac nad kodeksami postępowania do dnia 29 listopada 2019 r. oraz do ich skutecznego wdrożenia do dnia 29 maja 2020 r.

Artykuł 7

Procedura współpracy między organami

1. Każde państwo członkowskie wyznacza centralny punkt kontaktowy, który współpracuje z centralnymi punktami kontaktowymi innych państw członkowskich i z Komisją w odniesieniu do stosowania niniejszego rozporządzenia. Państwa członkowskie powiadamiają Komisję o wyznaczonych centralnych punktach kontaktowych oraz o wszelkich późniejszych zmianach w tym zakresie.

2. W przypadku gdy właściwy organ w jednym z państw członkowskich zwraca się do innego państwa członkowskiego z wnioskiem o pomoc, na podstawie art. 5 ust. 2, w celu uzyskania dostępu do danych, składa on w centralnym punkcie kontaktowym wyznaczonym przez to inne państwo członkowskie należycie uzasadniony wniosek. Wniosek musi zawierać pisemne wyjaśnienie powodów i podstaw prawnych ubiegania się o dostęp do danych.

3. Centralny punkt kontaktowy ustala, który organ jego państwa członkowskiego jest właściwy, oraz przekazuje temu organowi wniosek otrzymany zgodnie z ust. 2.

4. Właściwy organ, który otrzymał taki wniosek, bez zbędnej zwłoki oraz w terminie proporcjonalnym do pilności wniosku, przekazuje odpowiedź, podając żądane dane lub informując właściwy organ występujący z wnioskiem, że uważa, że warunki uzasadniające wniosek o pomoc na podstawie niniejszego rozporządzenia nie zostały spełnione.

5. Wszelkie informacje wymieniane w ramach pomocy, o którą zwrócono się z wnioskiem, i udzielanej na podstawie w art. 5 ust. 2 mogą być wykorzystywane jedynie w odniesieniu do sprawy, w której o nie wnioskowano.

6. Centralne punkty kontaktowe udostępniają użytkownikom ogólne informacje na temat niniejszego rozporządzenia, w tym na temat kodeksów postępowania.

Artykuł 8

Ocena i wytyczne

1. Nie później niż w dniu 29 listopada 2022 r. Komisja przedłoży Parlamentowi Europejskiemu, Radzie i Europejskiemu Komitetowi Ekonomiczno-Społecznemu sprawozdanie z oceny wykonania niniejszego rozporządzenia, w szczególności w odniesieniu do:

a) stosowania niniejszego rozporządzenia, zwłaszcza w odniesieniu do zbiorów danych obejmujących zarówno dane osobowe, jak i nieosobowe, w świetle zmian na rynku i rozwoju technologicznego, które mogłyby zwiększyć możliwości deanonimizacji danych;

b) wykonywania przez państwa członkowskie art. 4 ust. 1, w szczególności wyjątku dotyczącego bezpieczeństwa publicznego; oraz

c) opracowania i skutecznego wdrażania kodeksów postępowania oraz skutecznego przekazywania informacji przez dostawców usług.

2. Państwa członkowskie przekazują Komisji wszelkie informacje niezbędne do przygotowania sprawozdania, o którym mowa w ust. 1.

3. Do dnia 29 maja 2019 r. Komisja opublikuje wskazówki na temat wzajemnych powiązań niniejszego rozporządzenia i rozporządzenia (UE) 2016/679, w szczególności w odniesieniu do zbiorów danych obejmujących zarówno dane osobowe, jak i nieosobowe.

Artykuł 9

Przepisy końcowe

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

Niniejsze rozporządzenie stosuje się po upływie sześciu miesięcy od jego opublikowania.

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

Sporządzono w Strasburgu dnia 14 listopada 2018 r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
A. TAJANI	K. EDTSTADLER
Przewodniczący	*Przewodnicząca*