KOMISJA
EUROPEJSKA

Bruksela, dnia 13.9.2017 r.
COM(2017) 495 final

2017/0228 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej

{SWD(2017) 304 final}
{SWD(2017) 305 final}

UZASADNIENIE

1. KONTEKST WNIOSKU

• Przyczyny i cele wniosku

Nowe technologie cyfrowe, takie jak przetwarzanie w chmurze, duże zbiory danych, sztuczna inteligencja i internet rzeczy (IoT) zaprojektowane są tak, aby w jak największym stopniu zwiększyć wydajność oraz umożliwić osiągnięcie korzyści skali i rozwój nowych usług. Technologie te mają wiele zalet z punktu widzenia użytkownika, takich jak większa elastyczność, produktywność, szybkość wdrażania i autonomia, np. dzięki zdolności maszyn do uczenia się[1].

Jak wskazano w komunikacie z 2017 r. zatytułowanym „Budowa europejskiej gospodarki opartej na danych”[2], wartość unijnego rynku danych oszacowano w 2016 r. na kwotę niemal 60 mld EUR, co oznacza wzrost o 9,5 % w porównaniu z rokiem 2015. Zgodnie z wynikami badania w tym zakresie unijny rynek danych mógłby potencjalnie osiągnąć wartość ponad 106 mld EUR w 2020 r.[3].

Aby uwolnić ten potencjał, we wniosku dąży się do osiągnięcia następujących celów:

- poprawa transgranicznej mobilności danych nieosobowych na jednolitym rynku, utrudnionej obecnie w wielu państwach członkowskich ograniczeniami dotyczącymi lokalizacji lub brakiem pewności prawa na rynku;
- zapewnienie, by właściwe organy zachowały pełne uprawnienia do żądania i uzyskiwania dostępu do danych na potrzeby kontroli regulacyjnej, w tym na potrzeby inspekcji i audytów; oraz
- ułatwienie profesjonalnym użytkownikom usług przechowywania lub innego rodzaju przetwarzania danych dokonania zmiany dostawcy usług i przeniesienia swoich danych, nie stwarzając przy tym nadmiernego obciążenia dla dostawców usług ani nie powodując zakłóceń na rynku.

W ramach przeglądu śródokresowego realizacji strategii jednolitego rynku cyfrowego[4] zapowiedziano przedłożenie wniosku ustawodawczego dotyczącego ram współpracy w zakresie swobodnego przepływu danych w UE.

Ogólnym celem strategicznym niniejszej inicjatywy jest osiągnięcie bardziej konkurencyjnego i zintegrowanego rynku wewnętrznego usług przechowywania oraz innego rodzaju przetwarzania danych i działalności w tym zakresie poprzez podjęcie działań w wymienionych wyżej obszarach. W niniejszym wniosku przechowywanie i innego rodzaju przetwarzanie danych pojmowane jest szeroko i obejmuje wykorzystanie wszelkiego rodzaju systemów informatycznych, niezależnie od tego, czy są one zlokalizowane

---

[1] Uczenie się maszyn to jedno z zastosowań sztucznej inteligencji (AI), oznaczające zdolność systemów do automatycznego uczenia się i doskonalenia na podstawie doświadczeń, bez bezpośredniej ingerencji programisty.

[2] COM(2017) 9: „Budowa europejskiej gospodarki opartej na danych”, komunikat z dnia 10 stycznia 2017 r.; zob. także dokument roboczy służb Komisji towarzyszący temu komunikatowi, SWD(2017) 2 z dnia 10 stycznia 2017 r.

[3] IDC and Open Evidence, European Data Market (Europejski rynek danych), sprawozdanie końcowe z dnia 1 lutego 2017 r. (SMART 2013/0063).

[4] Komunikat Komisji przyjęty w dniu 10 maja 2017 r. (COM(2017) 228 final).

w pomieszczeniach użytkownika czy też są przedmiotem outsourcingu na rzecz dostawcy usług przechowywania lub innego rodzaju przetwarzania danych[5].

- **Spójność z przepisami obowiązującymi w tej dziedzinie polityki**

Wniosek służy realizacji celów określonych w strategii jednolitego rynku cyfrowego[6], niedawnym śródokresowym przeglądzie tej strategii, a także w wytycznych politycznych na obecną kadencję Komisji Europejskiej zatytułowanych „Nowy początek dla Europy: Mój program na rzecz zatrudnienia, wzrostu, sprawiedliwości oraz zmian demokratycznych”[7].

W niniejszym wniosku skupiono się na kwestiach dotyczących świadczenia usług hostingu (przechowywania) i innego rodzaju przetwarzania danych, a wniosek jest spójny z **obowiązującymi instrumentami prawnymi**. Inicjatywa ta służy stworzeniu skutecznie funkcjonującego jednolitego rynku takich usług w UE. Jest zatem spójna z **dyrektywą o handlu elektronicznym[8]**, której celem jest stworzenie kompleksowego i skutecznie funkcjonującego jednolitego rynku unijnego dla szerszej kategorii usług społeczeństwa informacyjnego, oraz z dyrektywą usługową[9], która przyczynia się do pogłębienia jednolitego rynku usług w UE w pewnych sektorach.

Kilka istotnych sektorów celowo wyłączono z zakresu stosowania wspomnianych aktów prawnych (tj. dyrektywy o handlu elektronicznym i dyrektywy usługowej), tak aby tylko ogólne przepisy traktatu miały zastosowanie do całości usług hostingu (przechowywania) i innego rodzaju przetwarzania danych. Istniejących barier dla tych usług nie można jednak skutecznie usunąć, polegając wyłącznie na bezpośrednim stosowaniu art. 49 i 56 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), ponieważ, z jednej strony, rozwiązywanie problemu każdej z tych barier osobno w ramach postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego byłoby niezwykle skomplikowane dla instytucji krajowych i unijnych, a z drugiej strony zniesienie wielu barier równocześnie wymaga szczegółowych przepisów prowadzących do wyeliminowania barier nie tylko w sektorze publicznym, ale i prywatnym, a także rodzi potrzebę ustanowienia współpracy administracyjnej. Ponadto wynikające z tego zwiększanie pewności prawa wydaje się szczególnie ważne dla użytkowników nowych technologii[10].

Ponieważ niniejszy wniosek dotyczy elektronicznych danych innych niż dane osobowe, nie ma on wpływu na unijne ramy prawne w zakresie ochrony danych osobowych, w szczególności rozporządzenie (UE) 2016/679 (ogólne rozporządzenie o ochronie danych)[11], dyrektywę (UE) 2016/680 (dyrektywa w sprawie przetwarzania danych przez policję)[12]

---

5 Inne usługi przetwarzania danych obejmują usługi oparte na danych, takie jak analiza danych, systemy zarządzania danymi itp.

6 COM(2015) 0192 final.

7 Przemówienie inauguracyjne wygłoszone podczas sesji plenarnej Parlamentu Europejskiego w Strasburgu dnia 22 października 2014 r.

8 Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego („dyrektywa o handlu elektronicznym”) (Dz.U. L 178 z 17.7.2000, s. 1).

9 Dyrektywa 2006/123/WE Parlamentu Europejskiego i Rady z dnia 12 grudnia 2006 r. dotycząca usług na rynku wewnętrznym (Dz.U. L 376 z 27.12.2006, s. 36).

10 Badanie LE Europe (SMART 2015/0016) i badanie IDC (SMART 2013/0063).

11 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).

12 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

i dyrektywę 2002/58/WE (dyrektywa o prywatności i łączności elektronicznej)[13], które zapewniają wysoki poziom ochrony danych osobowych oraz swobodny przepływ danych osobowych w Unii. Wraz z tymi ramami prawnymi wniosek służy ustanowieniu kompleksowych i spójnych ram unijnych umożliwiających swobodny przepływ danych na jednolitym rynku.

We wniosku zawarto wymaganie powiadamiania o projektach środków dotyczących lokalizacji danych na podstawie dyrektywy (UE) 2015/1535 w sprawie przejrzystości[14], aby umożliwić ocenę, czy takie ograniczenia dotyczące lokalizacji są uzasadnione.

W kwestii współpracy między właściwymi organami i udzielania sobie przez nie wzajemnej pomocy we wniosku przewidziano stosowanie wszelkich odnośnych mechanizmów. Na wypadek braku mechanizmów współpracy we wniosku wprowadzono środki w celu umożliwienia właściwym organom wymiany i dostępu do danych przechowywanych lub w inny sposób przetwarzanych w innych państwach członkowskich.

- **Spójność z innymi politykami Unii**

W myśl strategii jednolitego rynku cyfrowego inicjatywa ta służy zmniejszeniu barier dla rozwoju w Europie konkurencyjnej gospodarki opartej na danych. Zgodnie z komunikatem w sprawie przeglądu śródokresowego realizacji strategii jednolitego rynku cyfrowego Komisja bada oddzielnie kwestie dostępności oraz ponownego wykorzystania danych publicznych i publicznie finansowanych oraz prywatnych danych istotnych z punktu widzenia interesu publicznego, a także odpowiedzialności w przypadkach szkód spowodowanych przez produkty w znacznym stopniu korzystające z danych[15].

Przy opracowywaniu niniejszego wkładu w ten obszar polityki czerpano również ze strategicznego pakietu w sprawie **cyfryzacji europejskiego przemysłu**, obejmującego **europejską inicjatywę dotyczącą przetwarzania w chmurze**[16], służącą wdrożeniu rozwiązań opartych na wykorzystaniu chmur o dużej pojemności do przechowywania, udostępniania i ponownego wykorzystywania danych naukowych. Niniejszą inicjatywę oparto również na wynikach przeglądu **europejskich ram interoperacyjności**[17], których celem jest poprawa współpracy cyfrowej między administracjami publicznymi w Europie i którym swobodny przepływ danych przyniesie bezpośrednie korzyści. Przyczynia się ona do realizacji podjętego przez UE zobowiązania do wspierania **otwartego internetu**[18].

---

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).

[13] 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).

[14] 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).

[15] COM(2017) 228 final.

[16] COM(2016) 178 final: „Europejska inicjatywa dotycząca przetwarzania w chmurze – budowanie w Europie konkurencyjnej gospodarki opartej na danych i wiedzy", z dnia 19 kwietnia 2016 r.

[17] COM(2017) 134 final: „Europejskie ramy interoperacyjności – strategia wdrażania", z dnia 23 marca 2017 r.

[18] COM(2014) 72 final: „Polityka wobec internetu i zarządzanie internetem. Rola Europy w kształtowaniu przyszłości zarządzania internetem", http://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:52014DC0072

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

• Podstawa prawna

Niniejszy wniosek wchodzi w zakres kompetencji dzielonych zgodnie z art. 4 ust. 2 lit. a) TFUE. Służy on osiągnięciu bardziej konkurencyjnego i zintegrowanego rynku wewnętrznego usług przechowywania i innego rodzaju przetwarzania danych poprzez zapewnienie swobodnego przepływu danych w obrębie Unii. We wniosku określono przepisy dotyczące wymogów dotyczących lokalizacji danych, dostępności danych dla właściwych organów i przenoszenia danych przez użytkowników profesjonalnych. Wniosek jest oparty na art. 114 TFUE, który stanowi podstawę prawną przyjęcia takich przepisów.

• Pomocniczość

Wniosek jest zgodny z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej (TUE). Celem niniejszego wniosku jest zapewnienie sprawnego funkcjonowania rynku wewnętrznego wyżej wymienionych usług, który nie jest ograniczony do terytorium jednego państwa członkowskiego, ponadto działania państw członkowskich na szczeblu krajowym nie wystarczą do osiągnięcia swobodnego przepływu danych nieosobowych w obrębie Unii, ponieważ podstawowym problemem jest transgraniczna mobilność danych.

Państwa członkowskie dysponują możliwością zmniejszenia liczby i zakresu własnych ograniczeń dotyczących lokalizacji danych, prawdopodobnie dokonywałyby tego jednak w różnym stopniu, na różnych warunkach lub w ogóle nie skorzystałyby z tej możliwości.

Odmienne podejście w poszczególnych państwach członkowskich prowadziłoby jednak do mnożenia wymogów regulacyjnych na jednolitym rynku UE, a także do powstania wymiernych dodatkowych kosztów dla przedsiębiorstw, w szczególności małych i średnich przedsiębiorstw (MŚP).

• Proporcjonalność

Wniosek jest zgodny z zasadą proporcjonalności określoną w art. 5 TUE, ponieważ przewidziano w nim skuteczne ramy, które nie wykraczają poza to, co jest konieczne do rozwiązania stwierdzonych problemów, i są proporcjonalne do zakładanych w nim celów.

Aby usunąć przeszkody w swobodnym przepływie danych nieosobowych w obrębie Unii, ograniczanym wymogami dotyczącymi lokalizacji, i zwiększyć zaufanie do transgranicznych przepływów danych, a także usług przechowywania i innego rodzaju przetwarzania danych, wniosek oparto w dużej mierze na wykorzystaniu istniejących instrumentów i ram unijnych: dyrektywy w sprawie przejrzystości – do celów powiadamiania o projektach środków przewidujących wymogi dotyczące lokalizacji danych, a także różnych ram zapewniających dostępność danych na potrzeby kontroli regulacyjnej prowadzonej przez państwa członkowskie. Mechanizm współpracy ustanowiony we wniosku będzie wykorzystywany do rozwiązywania kwestii dostępności danych dla właściwych organów krajowych jedynie w przypadku braku innych mechanizmów współpracy oraz wyczerpania innych środków dostępu.

Proponowane podejście do przepływu danych przez granice państw członkowskich i między dostawcami usług/wewnętrznymi systemami informatycznymi ma zapewnić równowagę między uregulowaniami unijnymi a względami bezpieczeństwa publicznego państw członkowskich, a także równowagę między uregulowaniami unijnymi a samoregulacją rynku.

W szczególności, w celu zmniejszenia trudności, z jakimi borykają się użytkownicy profesjonalni pragnący zmienić dostawcę usług i przenieść swoje dane, niniejsza inicjatywa stwarza bodźce do samoregulacji w postaci kodeksów postępowania dotyczących informacji, które mają być dostarczane użytkownikom korzystającym z usług przechowywania lub

innego rodzaju przetwarzania danych. Ponadto kwestia trybów zmiany dostawcy i przenoszenia danych powinna zostać rozwiązana w drodze samoregulacji w celu określenia najlepszych praktyk.

We wniosku przypomniano o konieczności stosowania się również do wymogów w zakresie bezpieczeństwa ustanowionych w przepisach krajowych i prawie Unii, w sytuacjach gdy osoby fizyczne lub prawne zlecają w ramach outsourcingu przechowywanie swoich danych lub innego rodzaju ich przetwarzanie, w tym w innym państwie członkowskim. Przywołano w nim również uprawnienia wykonawcze powierzone Komisji na mocy dyrektywy w sprawie bezpieczeństwa sieci i informacji w celu określenia wymogów w zakresie bezpieczeństwa, które również przyczynią się do sprawnego funkcjonowania niniejszego rozporządzenia. Wniosek wprawdzie pociąga za sobą konieczność podjęcia działań przez organy publiczne państw członkowskich z uwagi na wymagania dotyczące zgłaszania/przeglądu, wymagania dotyczące przejrzystości oraz współpracę administracyjną, jednak przepisy sformułowano tak, by ograniczyć wymagane działania do najistotniejszych potrzeb w zakresie współpracy, a tym samym uniknąć zbędnego obciążenia administracyjnego.

Poprzez ustanowienie jasnych ram wraz z towarzyszącymi im mechanizmami współpracy między państwami członkowskimi i z tymi państwami, a także poprzez samoregulację, niniejszy wniosek służy zwiększeniu pewności prawa i poziomu zaufania, a jednocześnie zapewnieniu istotności i skuteczności przepisów w perspektywie długoterminowej, dzięki elastyczności ram współpracy, w oparciu o centralne punkty kontaktowe w państwach członkowskich.

Komisja zamierza powołać grupę ekspertów, którzy będą doradzać jej w kwestiach objętych niniejszym rozporządzeniem.

- **Wybór instrumentu**

Komisja przedkłada wniosek w formie rozporządzenia, które może zapewnić stosowanie jednolitych przepisów w zakresie swobodnego przepływu danych nieosobowych na całym terytorium Unii w tym samym czasie. Ma to szczególne znaczenie w usuwaniu istniejących i zapobieganiu wprowadzaniu przez państwa członkowskie nowych ograniczeń, w zagwarantowaniu pewności prawa dostawcom usług i użytkownikom objętym tymi przepisami, a tym samym zwiększaniu zaufania do transgranicznych przepływów danych, a także do usług przechowywania i innego rodzaju przetwarzania danych.

3. WYNIKI OCEN *EX POST*, KONSULTACJI Z ZAINTERESOWANYMI STRONAMI I OCEN SKUTKÓW

- **Konsultacje z zainteresowanymi stronami**

Podczas **pierwszej tury gromadzenia danych** w 2015 r. przeprowadzono **konsultacje publiczne** dotyczące środowiska regulacyjnego w odniesieniu do platform, pośredników internetowych, przetwarzania danych i przetwarzania w chmurze oraz gospodarki współpracy. Dwie trzecie respondentów – reprezentujących w równych proporcjach wszystkie grupy zainteresowanych stron, w tym MŚP – stwierdziło, że ograniczenia dotyczące lokalizacji danych miały wpływ na ich strategię biznesową[19]. Pozostała działalność służąca gromadzeniu informacji obejmowała spotkania i wydarzenia, ukierunkowane warsztaty z udziałem

[19] W celu pozyskania dodatkowych danych ekonomicznych przeprowadzono badanie ekonomicznego wpływu chmury obliczeniowej w Europie (SMART 2014/0031, Deloitte, „Measuring the economic impact of cloud computing in Europe” (Badanie ekonomicznego wpływu przetwarzania w chmurze w Europie), 2016).

kluczowych zainteresowanych stron (takich jak np. Cloud Select Industry Group) i specjalne warsztaty w kontekście badań.

W ramach **drugiej rundy gromadzenia danych**, od końca 2016 r. do drugiej połowy 2017 r., przeprowadzono między innymi **konsultacje publiczne zainicjowane w następstwie komunikatu Komisji „Budowa europejskiej gospodarki opartej na danych”** z dnia 10 stycznia 2017 r. Z odpowiedzi otrzymanych w ramach konsultacji publicznych wynika, iż według 61,9 % zainteresowanych stron ograniczenia dotyczące lokalizacji danych powinny zostać usunięte. Większość zainteresowanych stron biorących udział w konsultacjach (55,3 % respondentów) uważa, że działania legislacyjne są najbardziej odpowiednim instrumentem rozwiązania kwestii nieuzasadnionych ograniczeń dotyczących lokalizacji, a pewna ich liczba zaapelowała o przyjęcie w tej kwestii właśnie rozporządzenia[20]. Dostawcy usług w zakresie technologii informatycznych, niezależnie od wielkości ich przedsiębiorstwa, zarówno ci mający siedzibę w UE, jak i ci spoza UE, wyrazili największe poparcie dla działań regulacyjnych. Zainteresowane strony wskazały również negatywne skutki ograniczeń w zakresie lokalizacji danych. Oprócz wzrostu kosztów dla przedsiębiorstw wymieniono także negatywny wpływ na świadczenie usług na rzecz podmiotów prywatnych lub publicznych (69,6 % wszystkich zainteresowanych stron, które udzieliły odpowiedzi, uznało ten wpływ za „duży”) lub na zdolność wejścia na nowy rynek (73,9 % zainteresowanych stron, które udzieliły odpowiedzi, uznało ten wpływ za „duży”). Zainteresowane strony ze wszystkich środowisk w podobny sposób odpowiadały na te pytania. Wyniki internetowych konsultacji publicznych również wskazują na to, że problemy ze zmianą dostawcy są powszechne, ponieważ 56,8 % respondentów reprezentujących MŚP podało, iż napotkali oni trudności przy próbie zmiany dostawcy.

Spotkania w formie zorganizowanych dialogów z państwami członkowskimi ułatwiły osiągnięcie jednakowego zrozumienia wyzwań u wszystkich stron. W piśmie skierowanym do przewodniczącego Donalda Tuska 16 państw członkowskich wyraźnie zaapelowało o przedłożenie wniosku ustawodawczego.

W niniejszym wniosku uwzględniono pewną liczbę uwag zgłaszanych przez państwa członkowskie i przedstawicieli sektora, w szczególności potrzebę: ustanowienia przekrojowej zasady swobodnego przepływu danych zapewniającej pewność prawa; poczynienia postępu w zakresie dostępności danych do celów regulacyjnych; ułatwienia użytkownikom profesjonalnym dokonywania zmiany dostawcy usług przechowywania lub innego rodzaju przetwarzania danych i przenoszenia danych do nowego dostawcy, poprzez zachęcanie dostawców usług do zwiększenia przejrzystości stosowanych procedur i warunków umów, lecz bez narzucania im na tym etapie konkretnych norm lub obowiązków.

- **Gromadzenie i wykorzystanie wiedzy eksperckiej**

Przy opracowywaniu szeregu aspektów mobilności danych, w tym wymogów dotyczących lokalizacji danych[21], zmiany dostawcy / przenoszenia danych[22] oraz bezpieczeństwa danych[23],

---

[20] Na zadane w ramach konsultacji publicznych pytania wielokrotnego wyboru odpowiedzi udzieliło 289 zainteresowanych stron. Respondentów nie pytano o *rodzaj* działania legislacyjnego, ale 12 zainteresowanych stron z własnej inicjatywy skorzystało z okazji, by w uwagach pisemnych wyraźnie zaapelować o przyjęcie rozporządzenia. Grupa zainteresowanych stron była zróżnicowana, w jej skład weszli przedstawiciele 2 państw członkowskich, 3 stowarzyszeń przedsiębiorców, 6 dostawców usług w zakresie technologii informatycznych oraz przedstawiciel firmy prawniczej.

[21] SMART 2015/0054, TimeLex, Spark i Tech4i „Cross-border Data Flow in the Digital Single Market: Study on Data Location Restrictions” (Transgraniczny przepływ danych na jednolitym rynku cyfrowym: Badanie na temat ograniczeń dotyczących lokalizacji danych), D5. Sprawozdanie końcowe (w opracowaniu) [Badanie TimeLex (SMART 2015/0054)]; SMART 2015/0016, London Economics Europe, Carsa i Charles

opierano się na analizach prawnych i ekonomicznych. Zlecono także przeprowadzenie badań na temat wpływu przetwarzania w chmurze[24] i korzystania z chmur obliczeniowych[25], jak również na temat europejskiego rynku danych[26]. Ponadto przeprowadzono badania w celu analizy działań współ- lub samoregulacyjnych w sektorze usług przetwarzania w chmurze[27]. Komisja korzystała w swych pracach również z dodatkowych źródeł zewnętrznych, w tym przeglądów rynku i statystyk (np. statystyk Eurostatu).

- **Ocena skutków**

W odniesieniu do niniejszego wniosku przeprowadzono ocenę skutków. W ocenie tej rozważono następujący zestaw wariantów: scenariusz odniesienia (brak działań na szczeblu politycznym) oraz trzy warianty strategiczne. Wariant 1 polegał na wykorzystaniu wytycznych lub samoregulacji do rozwiązania poszczególnych stwierdzonych problemów i pociągał za sobą surowsze egzekwowanie przepisów w odniesieniu do różnych kategorii nieuzasadnionych lub nieproporcjonalnych ograniczeń dotyczących lokalizacji danych, nakładanych przez państwa członkowskie. W wariancie 2 przewidziano ustanowienie zasad prawnych dotyczących poszczególnych stwierdzonych problemów oraz wyznaczenie przez państwa członkowskie centralnych punktów kontaktowych i powołanie grupy ekspertów, której zadaniem byłoby omawianie wspólnych podejść i praktyk, a także doradzanie w kwestiach zasad wprowadzonych w ramach tego wariantu. Rozważono także podwariant 2a, aby umożliwić ocenę połączenia środków w postaci przepisów ustanawiających ramy swobodnego przepływu danych, centralnych punktów kontaktowych i powołania grupy ekspertów ze środkami samoregulacji dotyczącymi przenoszenia danych. Wariant 3 obejmował szczegółową inicjatywę ustawodawczą w celu wprowadzenia, między innymi, z góry określonych (zharmonizowanych) kryteriów oceny tego, czy dane ograniczenie dotyczące lokalizacji danych jest (nie)uzasadnione i (nie)proporcjonalne, oraz ustanowienia nowego prawa dotyczącego przenoszenia danych.

Russell Speechlys „Facilitating cross border data flow in the Digital Single Market" (Ułatwianie transgranicznego przepływu danych na jednolitym rynku cyfrowym), 2016 (w toku) [Badanie LE Europe (SMART 2015/0016)].

[22] SMART 2016/0032, IDC i Arthur's Legal „Switching between Cloud Service Providers" (Zmienianie dostawców usług przetwarzania w chmurze), 2017 (w toku) [Badanie IDC i Arthur'Legal (SMART 2016/0032)].

[23] SMART 2016/0029 (w trakcie realizacji), Tecnalia „Certification Schemes for Cloud Computing" (Systemy certyfikacji dla przetwarzania w chmurze), D6.1, sprawozdanie wstępne.

[24] SMART 2014/0031, Deloitte „Measuring the economic impact of cloud computing in Europe" (Badanie ekonomicznego wpływu przetwarzania w chmurze w Europie), 2016 [Badanie Deloitte (SMART 2014/0031)].

[25] SMART 2013/43, IDC „Uptake of Cloud in Europe. Follow-up of IDC Study on Quantitative estimates of the demand for Cloud computing in Europe and the likely barriers to take-up" (Wprowadzanie usług przetwarzania w chmurze w Europie. Badanie stanowiące aktualizację badania na temat szacunkowych danych ilościowych dotyczących popytu na usługi przetwarzania w chmurze obliczeniowej w Europie i możliwych barier dla ich wprowadzania), 2014, dostępne na stronie internetowej: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=9742; SMART 2011/0045, IDC „Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Uptake" (Szacunkowe dane ilościowe dotyczące popytu na usługi przetwarzania w chmurze obliczeniowej w Europie i możliwych barier dla ich wprowadzania), lipiec 2012.

[26] SMART 2013/0063, IDC i Open Evidence „European Data Market. Data ownership and Access to Data – Key Emerging Issues" (Europejski rynek danych. Własność danych i dostęp do nich – kluczowe wyłaniające się kwestie), 1 lutego 2017 [Badanie IDC Study (SMART 2013/0063)].

[27] SMART 2015/0018, TimeLex, Spark „Clarification of Applicable Legal Framework for Full, Co- or Self-Regulatory Actions in the Cloud Computing Sector" (Wyjaśnienie obowiązujących ram prawnych w zakresie działań czysto regulacyjnych, a także współ- i samoregulacyjnych w sektorze usług przetwarzania w chmurze) (w trakcie realizacji).

W dniu 28 września 2016 r. Rada ds. Kontroli Regulacyjnej wydała swoją pierwszą opinię na temat oceny skutków, wnosząc o poprawienie tej oceny i jej ponowne przedłożenie. Ocena została następnie zrewidowana i ponownie przedłożona Radzie ds. Kontroli Regulacyjnej w dniu 11 sierpnia 2017 r. W swojej drugiej opinii Rada ds. Kontroli Regulacyjnej uwzględniła fakt, że rozszerzono zakres oceny, w następstwie komunikatu Komisji COM(2017) 9 w sprawie budowy europejskiej gospodarki opartej na danych, jak również uzupełniono ją o dodatkowe informacje na temat poglądów zainteresowanych stron i słabych punktów obecnych ram. Mimo to w dniu 25 sierpnia 2017 r. Rada wydała drugą negatywną opinię, zwracając w szczególności uwagę na brak dowodów na poparcie koncepcji wprowadzenia nowego prawa dotyczącego przenoszenia danych w ramach usług przetwarzania w chmurze. Zgodnie ze swoją praktyką operacyjną Rada uznała swoją opinię za ostateczną.

Komisja uznała za stosowne przedłożenie wniosku, dokonując jednocześnie dalszej poprawy analizy w ocenie skutków w celu uwzględnienia uwag zgłoszonych przez Radę ds. Kontroli Regulacyjnej w drugiej opinii. Zakres niniejszego wniosku jest ograniczony do swobodnego przepływu danych nieosobowych w Unii Europejskiej. Ponadto mając na uwadze stwierdzenie Rady, że dowody wydają się przemawiać za mniej rygorystycznym wariantem w odniesieniu do przenoszenia danych, w ocenie skutków odstąpiono od pierwotnie preferowanego wariantu polegającego na nałożeniu na dostawców usług obowiązku ułatwienia użytkownikom zmiany dostawcy lub przenoszenia danych. Zamiast tego Komisja zachowała mniej uciążliwy wariant, w którym przewidziano samoregulację przy wsparciu Komisji. Proponowane środki są proporcjonalne i mniej rygorystyczne, ponieważ nie obejmują nowego prawa dotyczącego przenoszenia danych między dostawcami usług przechowywania lub innego rodzaju przetwarzania danych, oparte zostały natomiast na samoregulacji w celu osiągnięcia przejrzystości w zakresie warunków technicznych i operacyjnych dotyczących przenoszenia danych.

We wniosku uwzględniono także opinię Rady, aby zapobiec nakładaniu się lub powielaniu proponowanych działań z działaniami w ramach przeglądu mandatu Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) i ustanawiania europejskich ram w zakresie bezpieczeństwa cybernetycznego technologii informacyjno-komunikacyjnych.

Z oceny skutków wynika, że wariant preferowany, podwariant 2a, umożliwiłby skuteczne zniesienie obecnych nieuzasadnionych ograniczeń dotyczących lokalizacji i skuteczne zapobieżenie nowym ograniczeniom w przyszłości, dzięki jasnej zasadzie prawnej w połączeniu z systemem przeglądów, mechanizmami zgłaszania i zapewnieniem przejrzystości, a jednocześnie zwiększyłby pewność prawa i zaufanie do rynku. Obciążenie organów publicznych państw członkowskich byłoby umiarkowane i wyrażałoby się w kwocie około 33 000 EUR rocznie stanowiącej wydatki na zasoby ludzkie w celu utrzymania centralnych punktów kontaktowych, a także rocznym koszcie w wysokości od 385 do 1 925 EUR za przygotowywanie zgłoszeń.

Wniosek będzie miał pozytywny wpływ na konkurencyjność, ponieważ stworzy bodźce do wprowadzania innowacyjnych rozwiązań w usługach przechowywania lub innego rodzaju przetwarzania danych, zachęci większą liczbę użytkowników do korzystania z tych usług i znacznie ułatwi, w szczególności nowym i małym przedsiębiorstwom będącym dostawcami usług, wchodzenie na nowe rynki. Wniosek przyczyni się również do zwiększenia transgranicznego i międzysektorowego korzystania z usług przechowywania lub innego rodzaju przetwarzania danych oraz do rozwoju rynku danych. W związku z powyższym

niniejszy wniosek pomoże w przekształcaniu społeczeństwa i gospodarki oraz otworzy nowe możliwości dla europejskich obywateli, przedsiębiorstw i administracji publicznej.

- **Sprawność regulacyjna i uproszczenie**

Wniosek ma zastosowanie do obywateli, administracji krajowych oraz do wszystkich przedsiębiorstw, w tym mikroprzedsiębiorstw i MŚP. Wszystkie przedsiębiorstwa odniosą korzyść z przepisów eliminujących przeszkody dla mobilności danych. Proponowane środki przyniosą korzyści w szczególności MŚP, ponieważ swobodny przepływ danych nieosobowych przyniesie bezpośrednie ograniczenie ich kosztów i pomoże im w uzyskaniu bardziej konkurencyjnej pozycji na rynku. Wyłączenie MŚP z zakresu obowiązywania proponowanych przepisów mogłoby podważyć skuteczność tych uregulowań, ponieważ MŚP stanowią istotną część dostawców usług przechowywania lub innego rodzaju przetwarzania danych i są siłą napędową innowacji na rynkach tych usług. Kolejnym argumentem przemawiającym za niewyłączaniem mikroprzedsiębiorstw lub MŚP z zakresu stosowania przepisów jest to, że koszty wynikające z tych przepisów prawdopodobnie nie będą zbyt wysokie.

- **Prawa podstawowe**

Proponowane rozporządzenie nie narusza praw podstawowych i jest zgodne z zasadami uznanymi w Karcie praw podstawowych Unii Europejskiej. Proponowane rozporządzenie powinno mieć pozytywny wpływ na wolność prowadzenia działalności gospodarczej (art. 16), ponieważ przyczyni się do wyeliminowania nieuzasadnionych lub nieproporcjonalnych barier w korzystaniu i świadczeniu usług związanych z danymi, takich jak usługi przetwarzania w chmurze, a także w konfigurowaniu wewnętrznych systemów informatycznych, oraz do zapobiegania powstawaniu takich barier.

4. WPŁYW NA BUDŻET

Proponowane środki pociągną za sobą umiarkowane obciążenie administracyjne dla organów publicznych państw członkowskich, wynikające z konieczności przydzielenia zasobów ludzkich do celów współpracy między państwami członkowskimi za pośrednictwem „centralnych punktów kontaktowych” oraz zapewnienia zgodności z przepisami dotyczącymi powiadamiania, przeglądu i przejrzystości.

5. ELEMENTY FAKULTATYWNE

- **Plany wdrożenia i monitorowanie, ocena i sprawozdania**

Pięć lat po rozpoczęciu stosowania przepisów przeprowadzona zostanie kompleksowa ocena ich skuteczności i proporcjonalności. Ocena ta zostanie przeprowadzona zgodnie z wytycznymi dotyczącymi lepszego stanowienia prawa.

W jej ramach konieczne będzie w szczególności zbadanie, czy rozporządzenie przyczyniło się do ograniczenia liczby i zakresu ograniczeń dotyczących lokalizacji danych oraz do zwiększenia pewności prawa i przejrzystości utrzymanych w mocy (uzasadnionych i proporcjonalnych) wymogów. Niezbędne będzie również ocenienie, czy inicjatywa polityczna przyczyniła się do poprawy zaufania do swobodnego przepływu danych nieosobowych, czy państwa członkowskie mają sensowną możliwość uzyskania – do celów kontroli regulacyjnej – dostępu do danych przechowywanych za granicą oraz czy rozporządzenie doprowadziło do poprawy przejrzystości warunków dotyczących przenoszenia danych.

Zaplanowano wykorzystanie centralnych punktów kontaktowych państw członkowskich jako cennego źródła informacji na etapie oceny *ex post* przepisów.

Do pomiaru postępów w tych obszarach posłużono by się szczegółowymi wskaźnikami (zaproponowanymi w ocenie skutków). Planuje się także wykorzystanie danych Eurostatu oraz indeksu gospodarki cyfrowej i społeczeństwa cyfrowego. Rozważane jest również przeprowadzenie do tych celów specjalnego badania Eurobarometr.

- **Szczegółowe objaśnienia poszczególnych przepisów wniosku**

W **art. 1–3** określono **przedmiot** wniosku, **zakres stosowania** rozporządzenia i **definicje** stosowane do celów rozporządzenia.

W **art. 4** ustanawia się **zasadę swobodnego przepływu danych nieosobowych** w Unii. Zgodnie z tą zasadą zakazane są wszelkie wymogi dotyczące lokalizacji danych, chyba że są one uzasadnione względami bezpieczeństwa publicznego. Ponadto w artykule tym przewidziano przegląd istniejących wymogów, obowiązek powiadamiania Komisji o wymogach utrzymanych w mocy lub nowych, a także środki w zakresie przejrzystości.

Celem **art. 5** jest zapewnienie **dostępności danych na potrzeby kontroli regulacyjnej prowadzonej przez właściwe organy**. W tym celu określono, iż użytkownicy nie mogą odmówić udzielenia właściwym organom dostępu do danych, podając jako przyczynę odmowy fakt, że dane te są przechowywane lub w inny sposób przetwarzane w innym państwie członkowskim. W przypadku gdy właściwy organ wyczerpał wszystkie stosowne środki w celu uzyskania dostępu do danych, **organ ten może zwrócić się o pomoc** do organu w innym państwie członkowskim, jeżeli brak jest mechanizmu współpracy w tym zakresie.

Zgodnie z **art. 6** Komisja ma zachęcać **dostawców usług i użytkowników profesjonalnych do opracowywania i wdrażania kodeksów postępowania**, zawierających szczegółowe informacje na temat warunków przenoszenia danych (w tym wymagań technicznych i operacyjnych), które dostawcy usług powinni formułować wystarczająco szczegółowo, jasno i przejrzyście i przed zawarciem umowy udostępniać użytkownikom profesjonalnym. Komisja dokona przeglądu opracowywania i skutecznego wdrażania takich kodeksów w terminie dwóch lat po rozpoczęciu stosowania niniejszego rozporządzenia.

Zgodnie z **art. 7** każde państwo członkowskie ma obowiązek wyznaczyć jeden **centralny punkt kontaktowy** do celów współpracy z punktami kontaktowymi innych państw członkowskich i z Komisją w kwestiach stosowania niniejszego rozporządzenia. W art. 7 określono również warunki proceduralne mające zastosowanie do udzielania sobie wzajemnie przez właściwe organy pomocy przewidzianej w art. 5.

Zgodnie z **art. 8** Komisję wspomagać ma Komitet ds. Swobodnego Przepływu Danych będący komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.

W **art. 9** przewidziano dokonanie **przeglądu** w ciągu pięciu lat po rozpoczęciu stosowania rozporządzenia.

W **art. 10** ustanowiono, iż niniejsze rozporządzenie zacznie obowiązywać po upływie sześciu miesięcy od dnia jego opublikowania.

2017/0228 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej

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[28],

uwzględniając opinię Komitetu Regionów[29],

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) Cyfryzacja gospodarki postępuje coraz szybciej. Technologie informacyjno-komunikacyjne (ICT) nie stanowią już osobnego sektora, lecz leżą u podłoża wszystkich nowoczesnych, innowacyjnych systemów gospodarczych i społeczeństw. Dane elektroniczne są rdzeniem tych systemów i mogą przynieść wielkie korzyści, jeżeli podda się je analizie lub połączy z usługami i produktami.

(2) Łańcuchy wartości danych złożone są z różnych działań w zakresie danych: tworzenia i gromadzenia danych; agregacji i organizacji danych; przechowywania i przetwarzania danych; analizy danych, obrotu danymi i dystrybucji danych; wykorzystywania i ponownego wykorzystywania danych. Skuteczne i wydajne funkcjonowanie przechowywania i innego rodzaju przetwarzania danych stanowi podstawowy element budowy każdego łańcucha wartości danych. Osiągnięcie takiego skutecznego i wydajnego funkcjonowania oraz rozwój gospodarki opartej na danych w Unii utrudniają jednak w szczególności dwa rodzaje przeszkód w mobilności danych i tworzeniu rynku wewnętrznego.

(3) Zgodnie z Traktatem o funkcjonowaniu Unii Europejskiej swoboda przedsiębiorczości i swoboda świadczenia usług mają zastosowanie do usług przechowywania lub innego rodzaju przetwarzania danych. Świadczenie takich usług jest jednak utrudnione, a czasem nawet niemożliwe ze względu na pewne wymogi krajowe dotyczące lokalizacji danych na określonym terytorium.

(4) Takie przeszkody dla swobodnego świadczenia usług przechowywania lub innego rodzaju przetwarzania danych oraz dla swobody przedsiębiorczości dostawców usług przechowywania lub innego rodzaju przetwarzania danych wynikają z wymogów w przepisach krajowych państw członkowskich, zgodnie z którymi dane muszą być zlokalizowane na określonym obszarze geograficznym lub określonym terytorium, aby

[28] Dz.U. C [...] z [...], s. [...].
[29] Dz.U. C [...] z [...], s. [...].

móc je przechowywać lub przetwarzać. Podobny skutek wywołują inne przepisy lub praktyki administracyjne, w których nakłada się określone wymogi utrudniające przechowywanie lub innego rodzaju przetwarzanie danych poza określonym obszarem geograficznym lub określonym terytorium w obrębie 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 dalszym stopniu ogranicza ilość opcji dostępnych dla uczestników rynku i podmiotów sektora publicznego przy wyborze miejsca przechowywania lub innego rodzaju przetwarzania danych.

(5) Jednocześnie rozwój mobilności danych w Unii hamowany jest również ograniczeniami w sektorze prywatnym: kwestie prawne, umowne i techniczne utrudniają lub uniemożliwiają użytkownikom usług przechowywania lub innego rodzaju 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) Z uwagi na pewność prawa oraz 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 rozbieżności między przepisami w poszczególnych państwach oraz zapobiec pojawianiu się nowych możliwych barier w handlu i znaczących zakłóceń konkurencji, konieczne jest zatem przyjęcie jednolitych przepisów mających zastosowanie we wszystkich państwach członkowskich.

(7) W celu stworzenia ram swobodnego przepływu danych nieosobowych w Unii oraz podstaw do rozwoju gospodarki opartej na danych i zwiększenia konkurencyjności europejskiego przemysłu, konieczne jest ustanowienie jasnych, kompleksowych i przewidywalnych ram prawnych w zakresie przechowywania lub innego rodzaju przetwarzania danych innych niż dane osobowe na rynku wewnętrznym. Podejście oparte na zasadach przewidujące współpracę między państwami członkowskimi, a także samoregulacja powinny zapewnić elastyczność takich ram, umożliwiającą 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.

(8) Niniejsze rozporządzenie powinno mieć zastosowanie do osób fizycznych lub prawnych, które świadczą usługi przechowywania lub innego rodzaju przetwarzania danych na rzecz użytkowników mających miejsce zamieszkania lub siedzibę na terytorium Unii, w tym do dostawców usług, którzy świadczą usługi w Unii, ale nie mają na jej terytorium siedziby.

(9) Niniejsze rozporządzenie nie powinno mieć wpływu na ramy prawne w zakresie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych,

w szczególności na rozporządzenie (UE) 2016/679[30], dyrektywę (UE) 2016/680[31] i dyrektywę 2002/58/WE[32].

(10) Zgodnie z rozporządzeniem (UE) 2016/679 państwa członkowskie nie mogą ograniczać ani zakazywać swobodnego przepływu danych osobowych w Unii z powodów odnoszących się do ochrony 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 byłyby uzasadnione ze względów bezpieczeństwa.

(11) Niniejsze rozporządzenie powinno mieć zastosowanie do przechowywania i innego rodzaju przetwarzania danych pojmowanego jak najszerzej i obejmującego wykorzystanie wszelkiego rodzaju systemów informatycznych, niezależnie od tego, czy są one zlokalizowane w pomieszczeniach użytkownika czy też są przedmiotem outsourcingu na rzecz dostawcy usług przechowywania lub innego rodzaju przetwarzania danych. 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). Te różne usługi powinny wejść w zakres stosowania niniejszego rozporządzenia, chyba że przechowywanie danych lub inny rodzaj ich przetwarzania ma charakter wyłącznie pomocniczy w ramach usług innego typu, takich jak oferowanie internetowej platformy handlowej pośredniczącej między dostawcami usług a konsumentami lub przedsiębiorstwami.

(12) Wymogi dotyczące lokalizacji danych stanowią niewątpliwą przeszkodę dla swobodnego świadczenia usług przechowywania lub innego rodzaju przetwarzania danych w obrębie Unii oraz dla rozwoju rynku wewnętrznego. Powinny one zatem zostać zasadniczo zakazane, chyba że są uzasadnione względami bezpieczeństwa publicznego w rozumieniu prawa Unii, w szczególności art. 52 Traktatu o funkcjonowaniu Unii Europejskiej, i zgodne z zasadą proporcjonalności, zapisaną w art. 5 Traktatu o Unii Europejskiej. W celu wprowadzenia w życie zasady swobodnego przepływu danych nieosobowych przez granice, zapewnienia szybkiego zniesienia istniejących wymogów dotyczących lokalizacji danych oraz umożliwienia, do celów operacyjnych, przechowywania lub innego rodzaju przetwarzania danych w wielu lokalizacjach na terytorium UE, a także w związku z tym, że w niniejszym rozporządzeniu określono środki służące zapewnieniu dostępności danych do celów

---

30 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).

31 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).

32 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).

kontroli regulacyjnej, państwa członkowskie nie powinny mieć możliwości powoływania się w uzasadnieniach na względy inne niż bezpieczeństwo publiczne.

(13) Aby zapewnić skuteczne stosowanie zasady swobodnego przepływu danych nieosobowych przez granice oraz zapobiec pojawianiu się nowych przeszkód dla sprawnego funkcjonowania rynku wewnętrznego, państwa członkowskie powinny powiadamiać Komisję o każdym projekcie aktu, który zawiera nowe lub zmienia obowiązujące wymogi dotyczące lokalizacji danych. Powiadomienia te powinny być przekazywane i oceniane zgodnie z procedurą określoną w dyrektywie (UE) 2015/1535[33].

(14) Ponadto, w celu wyeliminowania możliwych istniejących przeszkód, w okresie przejściowym trwającym 12 miesięcy państwa członkowskie powinny dokonać przeglądu istniejących krajowych wymogów dotyczących lokalizacji danych i powiadomić Komisję o wszelkich wymogach w tym zakresie uznanych przez nie za zgodne z niniejszym rozporządzeniem, przekazując również uzasadnienie. Powiadomienia te powinny umożliwić Komisji ocenę zgodności wszelkich utrzymanych w mocy wymogów dotyczących lokalizacji danych.

(15) W celu zapewnienia, by wymogi dotyczące lokalizacji danych obowiązujące w państwach członkowskich były przejrzyste dla osób fizycznych i prawnych, takich jak dostawcy i użytkownicy usług przechowywania lub innego rodzaju przetwarzania danych, państwa członkowskie powinny publikować informacje o takich środkach na stronie centralnego internetowego punktu informacyjnego, jednego na kraj, i regularnie je aktualizować. W celu należytego informowania osób fizycznych i prawnych o wymogach dotyczących lokalizacji danych na całym terytorium Unii państwa członkowskie powinny przekazać Komisji informację o adresach takich punktów internetowych. Komisja powinna opublikować tę informację na swojej stronie internetowej.

(16) Wymogi dotyczące lokalizacji danych wynikają często z braku zaufania do transgranicznych usług przechowywania lub innego rodzaju przetwarzania danych, wywodzącego 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. W związku z tym w niniejszym rozporządzeniu należy wyraźnie określić, że nie narusza ono uprawnień właściwych organów do żądania i uzyskiwania dostępu do danych zgodnie z prawem Unii lub prawem krajowym, oraz że właściwym organom nie można odmówić dostępu do danych, podając jako przyczynę odmowy fakt, że dane są przechowywane lub w inny sposób przetwarzane w innym państwie członkowskim.

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

[33] 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).

(18) Jeżeli osoba fizyczna lub prawna podlegająca obowiązkom dostarczenia danych nie wywiąże się z nich oraz pod warunkiem że właściwy organ wyczerpał wszystkie stosowne środki w celu uzyskania dostępu do danych, organ ten 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 przedmiotowej kwestii, takich jak, w obszarze współpracy organów ścigania i wymiaru sprawiedliwości w sprawach cywilnych lub karnych albo w sprawach administracyjnych, odpowiednio: decyzja ramowa 2006/960/WSiSW[34], dyrektywa Parlamentu Europejskiego i Rady 2014/41/UE[35], Konwencja Rady Europy o cyberprzestępczości[36], rozporządzenie Rady (WE) nr 1206/2001[37], dyrektywa Rady 2006/112/WE[38] oraz rozporządzenie Rady (UE) nr 904/2010[39]. W przypadku braku takich specjalnych mechanizmów współpracy właściwe organy powinny ze sobą współpracować w celu umożliwienia dostępu do danych będących przedmiotem wniosku, za pośrednictwem wyznaczonych centralnych punktów kontaktowych, chyba że naruszałoby to porządek publiczny państwa członkowskiego, do którego skierowany jest wniosek o dostęp.

(19) Jeżeli wniosek o pomoc pociąga za sobą konieczność uzyskania przez organ, do którego wniosek ten jest skierowany, dostępu do jakichkolwiek pomieszczeń osoby fizycznej lub prawnej, w tym do jakichkolwiek urządzeń lub środków służących do przechowywania lub innego rodzaju przetwarzania danych, uzyskanie takiego dostępu musi odbywać się zgodnie z prawem procesowym Unii lub państwa członkowskiego, w tym z wszelkimi wymogami dotyczącymi uzyskania najpierw zgody organu sądowego.

(20) Możliwość przenoszenia danych bez przeszkód jest jednym z kluczowych czynników ułatwiających dokonywanie wyboru przez użytkowników i rozwój skutecznej konkurencji na rynkach usług przechowywania lub innego rodzaju przetwarzania danych. Rzeczywiste trudności w transgranicznym przenoszeniu danych lub kwestie postrzegane jako takie problemy podważają również zaufanie użytkowników profesjonalnych do korzystania z ofert transgranicznych, a co za tym idzie, ich zaufanie do rynku wewnętrznego. Obowiązujące przepisy unijne zapewniają stosowne prawa użytkownikom będącym osobami fizycznymi i konsumentami, natomiast brak jest przepisów ułatwiających zmianę dostawcy usług użytkownikom chcącym tego dokonać w ramach swojej działalności gospodarczej lub zawodowej.

(21) Aby móc w pełni czerpać z korzyści, jakie płyną z konkurencji na rynku, użytkownicy profesjonalni powinni móc dokonywać świadomych wyborów i łatwo porównywać

---

[34] 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).

[35] 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).

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

[37] 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).

[38] 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).

[39] 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).

poszczególne elementy różnych oferowanych na rynku wewnętrznym usług przechowywania lub innego rodzaju przetwarzania danych, w tym umowne warunki przenoszenia danych po rozwiązaniu umowy. W celu uwzględnienia potencjału innowacyjnego rynku oraz doświadczenia i wiedzy fachowej dostawców usług raz profesjonalnych użytkowników usług przechowywania lub innego rodzaju przetwarzania danych, uczestnicy rynku powinni opracować szczegółowe informacje i wymagania operacyjne dotyczące przenoszenia danych – w ramach samoregulacji wspieranej i ułatwianej przez Komisję – w formie unijnych kodeksów postępowania, co może obejmować określenie wzorca warunków umownych. Jeżeli jednak takie kodeksy postępowania nie zostaną opracowane i skutecznie wdrożone w rozsądnym czasie, Komisja powinna dokonać przeglądu sytuacji.

(22) Aby przyczynić się do sprawnej współpracy między państwami członkowskimi, każde państwo członkowskie powinno wyznaczyć jeden centralny punkt kontaktowy do współpracy z punktami kontaktowymi innych państw członkowskich i z Komisją w kwestiach stosowania niniejszego rozporządzenia. 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 w centralnym punkcie kontaktowym wyznaczonym przez to państwo członkowskie należycie uzasadniony wniosek, wraz z pisemnym wyjaśnieniem swojego uzasadnienia i podstaw prawnych wnioskowania o dostęp do danych. Centralny punkt kontaktowy wyznaczony przez państwo członkowskie, do którego skierowany jest wniosek o pomoc, powinien ułatwiać wzajemne udzielanie sobie pomocy przez organy poprzez ustalenie właściwego organu w państwie członkowskim wykonującym wniosek i przekazanie mu wniosku. W celu zapewnienia skutecznej współpracy organ, któremu wniosek został przekazany, powinien bez zbędnej zwłoki udzielić pomocy w odpowiedzi na dany wniosek bądź informacji na temat trudności w wykonaniu wniosku o pomoc lub podać uzasadnienie swojej odmowy wykonania takiego wniosku.

(23) W celu zapewnienia skutecznego stosowania procedury udzielania sobie nawzajem pomocy przez właściwe organy państw członkowskich Komisja może przyjmować akty wykonawcze określające standardowe formularze wniosków, ich języki, terminy lub inne szczegóły procedur wnioskowania o udzielenie pomocy. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011[40].

(24) Zwiększenie zaufania do bezpieczeństwa transgranicznego przechowywania lub innego rodzaju 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 co do wymogów w zakresie bezpieczeństwa mających zastosowanie do zlecania przechowywania lub innych czynności przetwarzania danych w ramach outsourcingu, w tym dostawcom usług z innych państw członkowskich.

(25) Wymogi w zakresie bezpieczeństwa dotyczące przechowywania lub innego rodzaju przetwarzania danych, które są stosowane w sposób uzasadniony i proporcjonalny na

[40] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.U. L 55 z 28.2.2011, s. 13).

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 przechowywania lub innego rodzaju przetwarzania danych w innym państwie członkowskim. Wspomniane osoby fizyczne lub prawne powinny być w stanie spełnić takie wymogi samodzielnie albo za pośrednictwem klauzul umownych w umowach z dostawcami usług.

(26) Wymogi w zakresie bezpieczeństwa ustanowione na szczeblu krajowym powinny być nieodzowne i proporcjonalne do ryzyka, na jakie narażone jest bezpieczeństwo przechowywania lub innego rodzaju przetwarzania danych w tym obszarze w zakresie prawa krajowego, w którym wymogi te określono.

(27) W dyrektywie 2016/1148[41] przewidziano środki prawne w celu zwiększenia ogólnego poziomu bezpieczeństwa cybernetycznego w Unii. Usługi przechowywania lub innego rodzaju przetwarzania danych stanowią jedną z kategorii usług cyfrowych objętych zakresem tej dyrektywy. Zgodnie z jej art. 16 państwa członkowskie mają obowiązek zapewnić, aby dostawcy usług cyfrowych określali i podejmowali odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zarządzania ryzykami, na jakie narażone są wykorzystywane przez nich sieci i systemy informatyczne. Środki te 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.

(28) Komisja powinna okresowo dokonywać przeglądu niniejszego rozporządzenia, w szczególności w celu określenia, czy istnieje potrzeba wprowadzenia zmian w świetle postępu technologicznego i zmian na rynku.

(29) Niniejsze rozporządzenie nie narusza praw podstawowych i jest zgodne z zasadami uznanymi w szczególności w Karcie praw podstawowych Unii Europejskiej, a zatem powinno być interpretowane i stosowane zgodnie z tymi prawami i zasadami, w tym prawem do ochrony danych osobowych (art. 8), wolnością prowadzenia działalności gospodarczej (art. 16) oraz wolnością wypowiedzi i informacji (art. 11).

(30) Ponieważ cel niniejszego rozporządzenia, to jest zapewnienie swobodnego przepływu danych nieosobowych w Unii, nie może zostać osiągnięty w sposób wystarczający przez państwa członkowskie, natomiast ze względu na jego skalę i skutki możliwe jest lepsze jego osiągnięcie na poziomie Unii, Unia może przyjąć środki zgodnie z zasadą pomocniczości, określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną we wspomnianym artykule niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tego celu,

[41] 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 w zakresie 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 przechowywania lub innego rodzaju 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 lub prawną posiadającą miejsce zamieszkania lub siedzibę w Unii.

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

Artykuł 3
Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1. „dane” oznaczają dane inne niż dane osobowe, o których mowa w art. 4 pkt 1 rozporządzenia (UE) 2016/679;

2. „przechowywanie danych” oznacza jakiekolwiek przechowywanie danych w formie elektronicznej;

3. „projekt aktu” oznacza tekst sformułowany w celu doprowadzenia do wprowadzenia go w życie jako przepis ustawowy, wykonawczy lub administracyjny o charakterze ogólnym, który jest na etapie przygotowań, na którym powiadamiające o nim państwo członkowskie może wciąż dokonywać zmian merytorycznych;

4. „dostawca” oznacza osobę fizyczną lub prawną świadczącą usługi przechowywania lub innego rodzaju przetwarzania danych;

5. „wymóg dotyczący lokalizacji danych” oznacza każdy obowiązek, zakaz, warunek, ograniczenie lub innego rodzaju wymóg określony w przepisach ustawowych, wykonawczych lub administracyjnych państw członkowskich, który narzuca lokalizację przechowywania lub innego rodzaju przetwarzania danych na terytorium danego państwa członkowskiego lub utrudnia przechowywanie lub innego rodzaju przetwarzanie danych w innym państwie członkowskim;

6. „właściwy organ” oznacza organ państwa członkowskiego uprawniony do uzyskania dostępu do danych przechowywanych lub przetwarzanych przez osobę fizyczną lub prawną, do celów wykonywania swoich obowiązków urzędowych, jak przewidziano w prawie krajowym lub prawie Unii;

7. „użytkownik” oznacza osobę fizyczną lub prawną korzystającą lub pragnącą skorzystać z usługi przechowywania lub innego rodzaju przetwarzania danych;

8. „użytkownik profesjonalny” oznacza osobę fizyczną lub prawną, w tym podmiot sektora publicznego, korzystającą lub pragnącą skorzystać z usługi przechowywania lub innego rodzaju przetwarzania danych do celów związanych z jej działalnością handlową, gospodarczą, rzemieślniczą, zawodową lub wykonywanym zadaniem.

Artykuł 4
Swobodny przepływ danych na terytorium Unii

1. Lokalizacji danych będących przedmiotem przechowywania lub innego rodzaju przetwarzania na terytorium Unii nie ogranicza się do terytorium określonego państwa członkowskiego, a przechowywanie lub innego rodzaju przetwarzanie danych w innym państwie członkowskim nie może być zakazywane ani ograniczane, chyba że jest to uzasadnione względami bezpieczeństwa publicznego.

2. Państwa członkowskie powiadamiają Komisję o każdym projekcie aktu, w którym wprowadza się nowe wymogi dotyczące lokalizacji danych lub zmiany w istniejących wymogach dotyczących lokalizacji danych, zgodnie z procedurami określonymi w przepisach krajowych wdrażających dyrektywę (UE) 2015/1535.

3. W terminie 12 miesięcy po rozpoczęciu stosowania niniejszego rozporządzenia państwa członkowskie zapewniają uchylenie wszelkich wymogów dotyczących lokalizacji danych, które nie są zgodne z ust. 1. Jeżeli państwo członkowskie uzna, że wymóg dotyczący lokalizacji danych jest zgodny z ust. 1 i może w związku z tym zostać utrzymany w mocy, powiadamia o tym środku Komisję, przedkładając również uzasadnienie utrzymania go w mocy.

4. Państwa członkowskie podają i aktualizują informacje o wszelkich mających zastosowanie na ich terytorium wymogach dotyczących lokalizacji danych, udostępniając je publicznie w internecie za pośrednictwem centralnego punktu informacyjnego, jednego na kraj.

5. Państwa członkowskie przekazują Komisji informację o adresie ich centralnego punktu informacyjnego, o którym mowa w ust. 4. Komisja publikuje na swojej stronie internetowej linki do stron takich punktów.

Artykuł 5
Zapewnienie właściwym organom dostępu do danych

1. Niniejsze rozporządzenie nie narusza uprawnień właściwych organów do żądania i uzyskiwania dostępu do danych na potrzeby wykonywania swoich obowiązków urzędowych zgodnie z prawem Unii lub prawem krajowym. Właściwym organom nie można odmówić dostępu do danych, podając jako przyczynę odmowy fakt, że dane są przechowywane lub w inny sposób przetwarzane w innym państwie członkowskim.

2. W przypadku gdy właściwy organ wyczerpał wszystkie stosowne środki w celu uzyskania dostępu do danych, może on zwrócić się z wnioskiem o pomoc do właściwego organu w innym państwie członkowskim zgodnie z procedurą przewidzianą w art. 7, a organ, do którego zwrócono się o pomoc, udziela jej zgodnie z procedurą przewidzianą w art. 7, chyba że naruszałoby to porządek publiczny państwa członkowskiego, do którego skierowano wniosek o pomoc.

3. Jeżeli wniosek o pomoc pociąga za sobą konieczność uzyskania przez organ, do którego wniosek ten jest skierowany, dostępu do jakichkolwiek pomieszczeń osoby fizycznej lub prawnej, w tym do jakichkolwiek urządzeń lub środków służących do przechowywania lub innego rodzaju przetwarzania danych, uzyskanie takiego dostępu musi odbywać się zgodnie z prawem procesowym Unii lub państwa członkowskiego.

4. Ust. 2 stosuje się wyłącznie w przypadku, gdy w prawie Unii lub umowach międzynarodowych nie przewidziano żadnego szczególnego mechanizmu współpracy do celów wymiany danych między właściwymi organami różnych państw członkowskich.

Artykuł 6
Przenoszenie danych

1. Komisja wspiera i ułatwia opracowywanie w ramach samoregulacji kodeksów postępowania na szczeblu Unii, w celu określenia wytycznych dotyczących najlepszych praktyk w zakresie ułatwiania zmiany dostawcy oraz w celu zapewnienia, aby przed zawarciem umowy o przechowywanie i przetwarzanie danych dostawcy dostarczali użytkownikom profesjonalnym dostatecznie szczegółowych, jasnych i przejrzystych informacji dotyczących następujących kwestii:

   a) procesy, wymagania techniczne, ramy czasowe i opłaty, które mają zastosowanie w przypadku gdy użytkownik profesjonalny chce zmienić dostawcę na innego lub przenieść dane z powrotem do własnych systemów informatycznych, w tym procesy tworzenia kopii zapasowych danych i lokalizacja takich kopii, dostępne formaty i nośniki danych, wymagana konfiguracja systemów informatycznych i minimalna 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; oraz

   b) wymagania operacyjne obowiązujące przy zmianie dostawcy lub przenoszeniu danych, przedstawione w sposób uporządkowany, w powszechnie używanym formacie nadającym się do przetwarzania automatycznego, zapewniające użytkownikowi wystarczająco dużo czasu na zmianę dostawcy lub przeniesienie danych.

2. Komisja zachęca dostawców do skutecznego wdrożenia kodeksów postępowania, o których mowa w ust. 1, w ciągu roku od daty rozpoczęcia stosowania niniejszego rozporządzenia.

3. Nie później niż dwa lata po rozpoczęciu stosowania niniejszego rozporządzenia Komisja dokonuje przeglądu opracowywania i skutecznego wdrażania takich kodeksów postępowania, a także skutecznego dostarczania informacji przez dostawców.

Artykuł 7
Centralne punkty kontaktowe

1. Każde państwo członkowskie wyznacza jeden centralny punkt kontaktowy, który współpracuje z centralnymi punktami kontaktowymi innych państw członkowskich i z Komisją w kwestiach stosowania niniejszego rozporządzenia. Państwa

członkowskie powiadamiają Komisję o wyznaczonych centralnych punktach kontaktowych oraz o wszelkich późniejszych zmianach w tym zakresie.

2. Państwa członkowskie zapewniają, by centralne punkty kontaktowe posiadały zasoby niezbędne do stosowania niniejszego rozporządzenia.

3. W przypadku gdy właściwy organ jednego z państw członkowskich zwraca się do innego państwa członkowskiego o pomoc w uzyskaniu dostępu do danych na podstawie art. 5 ust. 2, składa on w centralnym punkcie kontaktowym wyznaczonym przez to państwo członkowskie należycie uzasadniony wniosek, wraz z pisemnym wyjaśnieniem swojego uzasadnienia i podstaw prawnych wnioskowania o dostęp do danych.

4. Centralny punkt kontaktowy ustala, który organ jego państwa członkowskiego jest właściwy, i przekazuje temu organowi wniosek otrzymany zgodnie z ust. 3. Organ, który otrzymał taki wniosek, bez zbędnej zwłoki:

   a) udziela odpowiedzi wnioskującemu właściwemu organowi i informuje o tej odpowiedzi centralny punkt kontaktowy; oraz

   b) informuje centralny punkt kontaktowy i wnioskujący właściwy organ o wszelkich trudnościach lub, w przypadku odmowy bądź tylko częściowego wykonania wniosku, o powodach takiej odmowy bądź częściowego wykonania.

5. Wszelkie informacje wymieniane w ramach pomocy wnioskowanej i udzielanej na podstawie w art. 5 ust. 2 są wykorzystywane jedynie w odniesieniu do kwestii, w której o nie wnioskowano.

6. Komisja może przyjmować akty wykonawcze określające standardowe formularze wniosków, ich języki, terminy lub inne szczegóły procedur wnioskowania o udzielenie pomocy. Takie akty wykonawcze przyjmuje się zgodnie z procedurą, o której mowa w art. 8.

Artykuł 8
Komitet

1. Komisję wspiera Komitet ds. Swobodnego Przepływu Danych. Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.

2. W przypadku odesłania do niniejszego ustępu stosuje się art. 5 rozporządzenia (UE) nr 182/2011.

Artykuł 9
Przegląd

1. Nie później niż dnia [5 lat po dacie wymienionej w art. 10 ust. 2] r. Komisja dokonuje przeglądu niniejszego rozporządzenia i przedkłada Parlamentowi Europejskiemu, Radzie i Europejskiemu Komitetowi Ekonomiczno-Społecznemu sprawozdanie zawierające główne wyniki tego przeglądu.

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

Artykuł 10
Przepisy końcowe

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

2. 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 Brukseli dnia r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodniczący	*Przewodniczący*