

Bruksela, 18 maja 2018 r.
(OR. en)

8110/18

Międzyinstytucjonalny numer
referencyjny:
2018/0108 (COD)

JAI 323
COPEN 104
CYBER 66
DROIPEN 53
JAIEX 27
ENFOPOL 171
TELECOM 94
DAPIX 106
EJUSTICE 27
MI 269
IA 101
CODEC 577

WNIOSEK

Od:	Sekretarz Generalny Komisji Europejskiej, podpisał dyrektor Jordi AYET PUIGARNAU
Data otrzymania:	18 maja 2018 r.
Do:	Jeppe TRANHOLM-MIKKELSEN, Sekretarz Generalny Rady Unii Europejskiej
Nr dok. Kom.:	COM(2018) 225 final
Dotyczy:	Wniosek dotyczący ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY w sprawie europejskiego nakazu wydania dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych i europejskiego nakazu zabezpieczenia dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych

Delegacje otrzymują w załączeniu dokument COM(2018) 225 final.

Załącznik: COM(2018) 225 final



KOMISJA
EUROPEJSKA

Strasburg, dnia 17.4.2018
COM(2018) 225 final

2018/0108 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

**w sprawie europejskiego nakazu wydania dowodów dotyczącego elektronicznego
materiału dowodowego w sprawach karnych i europejskiego nakazu zabezpieczenia
dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych**

{SWD(2018) 118 final} - {SWD(2018) 119 final}

UZASADNIENIE

1. KONTEKST WNIOSKU

• Przyczyny i cele wniosku

W dzisiejszych czasach korzystanie z mediów społecznościowych, aplikacji webmail, usług przesyłania wiadomości oraz aplikacji do komunikacji, pracy, utrzymywania kontaktów i zdobywania informacji stało się powszechne w wielu częściach świata. Usługi te łączą ze sobą setki milionów użytkowników. Przynoszą znaczące korzyści dla dobrobytu ekonomicznego i społecznego użytkowników w całej Unii i poza nią. Mogą być jednak nadużywane jako narzędzia służące do popełniania lub ułatwiania przestępstw, w tym poważnych przestępstw takich jak ataki terrorystyczne. Gdy to się zdarza, wspomniane usługi i aplikacje często jako jedyne pozwalają służbom dochodzeniowo-śledczym znaleźć wskazówki umożliwiające ustalenie, kto popełnił przestępstwo, oraz pozyskać materiał dowodowy, który można wykorzystać w sądzie.

Ze względu na ponadgraniczny charakter internetu usługi tego rodzaju mogą być świadczone z dowolnego miejsca na świecie i niekoniecznie wymagają fizycznej infrastruktury, obecności przedsiębiorstwa lub pracowników w państwach członkowskich, w których usługi te są oferowane, czy też w ogóle obecności na rynku wewnętrznym. Ponadto nie wymagają one konkretnej lokalizacji przechowywania danych, którą usługodawca wybiera często w oparciu o uzasadnione względy, takie jak bezpieczeństwo danych, korzyści skali i szybkość dostępu. W rezultacie w przypadku coraz większej liczby spraw karnych dotyczących wszelkiego rodzaju przestępstw¹ organy państw członkowskich potrzebują dostępu do danych, które mogą być wykorzystane jako materiał dowodowy i które są przechowywane poza ich państwem lub przez usługodawców w innych państwach członkowskich lub państwach trzecich.

Na wypadek sytuacji, w których materiał dowodowy lub usługodawca zlokalizowani są gdzie indziej, kilkadziesiąt lat temu opracowano mechanizmy współpracy między państwami². Pomimo regularnego wprowadzania reform wspomniane mechanizmy współpracy poddawane są coraz większej presji spowodowanej rosnącymi potrzebami w zakresie transgranicznego dostępu do elektronicznego materiału dowodowego w odpowiednim czasie. W odpowiedzi na tę presję szereg państw członkowskich i państw trzecich ucieka się do rozbudowy swoich narzędzi krajowych. Wynikające z tego rozdrobnienie jest źródłem niepewności prawa i sprzecznych obowiązków oraz nasuwa pytania na temat ochrony praw podstawowych i gwarancji proceduralnych dla osób, których dotyczą takie żądania.

W 2016 r. Rada wezwała do podjęcia konkretnych działań opartych na wspólnym podejściu UE w celu podniesienia skuteczności wspólnej pomocy prawnej, usprawnienia współpracy pomiędzy organami państw członkowskich a usługodawcami w państwach niebędących członkami UE oraz zaproponowania rozwiązań problemów dotyczących ustalania jurysdykcji i egzekwowania przepisów³ w cyberprzestrzeni⁴. Również Parlament Europejski podkreślił

¹ Zob. sekcje 2.1.1 i 2.3 oceny skutków.

² W Unii są to mechanizmy wzajemnego uznawania, opierające się obecnie na dyrektywie w sprawie europejskiego nakazu dochodzeniowego; w przypadku państw trzecich – mechanizmy wzajemnej pomocy prawnej.

³ W niniejszym dokumencie termin „jurysdykcja wykonawcza” odnosi się do kompetencji właściwych organów do podejmowania czynności w toku postępowania przygotowawczego.

wyzwania, jakie obecnie fragmentaryczne ramy prawne mogą stwarzać dla dostawców starających się wykonać żądania organów ścigania i wezwał do zaproponowania europejskich ram prawnych obejmujących wystarczające zabezpieczenia praw i wolności wszystkich zaangażowanych podmiotów⁵.

Niniejszy wniosek dotyczy konkretnego problemu spowodowanego zmiennym charakterem cyfrowego materiału dowodowego i jego wymiarem międzynarodowym. Ma on na celu dostosowanie mechanizmów współpracy do epoki cyfrowej, udostępnienie narzędzi sądowych i narzędzi egzekwowania prawa uwzględniających dzisiejsze sposoby komunikowania się przestępców oraz zwalczanie nowoczesnych form przestępczości. Możliwość stosowania takich narzędzi zależy od objęcia ich silnymi mechanizmami ochrony praw podstawowych. Niniejszy wniosek ma na celu zwiększenie pewności prawa dla organów, usługodawców i zainteresowanych osób oraz utrzymanie wysokich standardów w odniesieniu do wniosków organów ścigania i zapewnienie w ten sposób ochrony praw podstawowych, przejrzystości i rozliczalności. Pozwala on również przyspieszyć proces zabezpieczania i pozyskiwania elektronicznego materiału dowodowego przechowywanego lub posiadanego przez usługodawców posiadających zakład w innej jurysdykcji. Niniejszy instrument będzie funkcjonować obok obecnych instrumentów współpracy wymiarów sprawiedliwości, które zachowują swoje znaczenie i w stosownych przypadkach nadal mogą być wykorzystywane przez właściwe organy. Równolegle Komisja prowadzi prace nad wzmocnieniem istniejących mechanizmów współpracy wymiarów sprawiedliwości za pomocą środków takich jak stworzenie bezpiecznej platformy umożliwiającej szybką wymianę wniosków pomiędzy organami sądowymi w UE oraz dokonanie inwestycji w wysokości 1 mln EUR mającej na celu przeszkolenie przedstawicieli zainteresowanych zawodów i organów ze wszystkich państw członkowskich UE w zakresie wzajemnej pomocy prawnej i współpracy, ze szczególnym naciskiem na Stany Zjednoczone jako państwa trzeciego otrzymującego największą liczbę wniosków z UE⁶.

W zakresie doręczania i wykonywania nakazów na podstawie niniejszego instrumentu organy powinny polegać na przedstawicielu prawnym powołanym przez usługodawców. Komisja przedstawia w dniu dzisiejszym wniosek mający na celu zapewnienie skutecznego powoływania takich przedstawicieli prawnych. Zapewnia on wspólne rozwiązanie dla całej UE na potrzeby kierowania nakazów prawnych do usługodawców za pośrednictwem przedstawiciela prawnego.

- **Spójność z istniejącymi ramami prawnymi UE w obszarze polityki oraz Konwencją Rady Europy o cyberprzestępczości**

Na obecne ramy prawne UE składają się unijne instrumenty współpracy w sprawach karnych, takie jak dyrektywa 2014/41/UE w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych⁷ (dyrektywa END), Europejska konwencja o pomocy prawnej

⁴ [Konkluzje Rady Unii Europejskiej dotyczące usprawnienia wymiaru sprawiedliwości w sprawach karnych w cyberprzestrzeni, ST9579/16.](#)

⁵ [P8_TA\(2017\)0366.](#)

⁶ https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf

⁷ [Dyrektywa 2014/41/UE](#) Parlamentu Europejskiego i Rady z dnia 3 kwietnia 2014 r. w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych, Dz.U. L 130 z 1.5.2014, s. 1.

w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej⁸, decyzja Rady 2002/187/WSiSW ustanawiająca Eurojust⁹, rozporządzenie (UE) 2016/794 w sprawie Europolu¹⁰, decyzja ramowa Rady 2002/465/WSiSW w sprawie wspólnych zespołów dochodzeniowo-śledczych¹¹, a także porozumienia dwustronne pomiędzy Unią Europejską a państwami niebędącymi członkami UE, takie jak Porozumienie między Unią Europejską a Stanami Zjednoczonymi Ameryki o wzajemnej pomocy prawnej¹² oraz Umowa między Unią Europejską a Japonią w sprawie wzajemnej pomocy prawnej w sprawach karnych¹³.

Dzięki wprowadzeniu europejskiego nakazu wydawania dowodów i europejskiego nakazu zabezpieczenia dowodów wniosek ułatwia zabezpieczenie i gromadzenie elektronicznego materiału dowodowego w postępowaniu karnym, przechowywanego lub posiadanego przez usługodawców w innej jurysdykcji. Dyrektywa w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych, która w znacznym stopniu zastąpiła Europejską konwencję o pomocy prawnej w sprawach karnych, dotyczy wszelkich czynności dochodzeniowych¹⁴, w tym dostępu do elektronicznego materiału dowodowego. Dyrektywa ta nie zawiera jednak przepisów szczegółowych dotyczących tego rodzaju dowodów¹⁵. Nowy instrument nie zastępuje europejskiego nakazu dochodzeniowego w przypadku pozyskiwania elektronicznego materiału dowodowego, lecz stanowi dodatkowe narzędzie dla organów. Mogą wystąpić sytuacje, na przykład w przypadku konieczności przeprowadzenia szeregu czynności w ramach postępowania przygotowawczego w wykonującym nakaz państwie członkowskim, w których europejski nakaz dochodzeniowy będzie preferowanym wyborem organów publicznych. Stworzenie nowego instrumentu dotyczącego elektronicznego materiału dowodowego może być lepszą alternatywą niż zmiana dyrektywy w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych ze względu na szczególne wyzwania związane z pozyskiwaniem takiego materiału dowodowego, które nie mają wpływu na inne czynności dochodzeniowo-śledcze objęte tą dyrektywą.

⁸ [Akt Rady z dnia 29 maja 2000 r.](#) ustanawiający, zgodnie z art. 34 Traktatu o Unii Europejskiej, Konwencję o wzajemnej pomocy w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej.

⁹ [Decyzja Rady 2002/187/WSiSW](#) z dnia 28 lutego 2002 r. ustanawiająca Eurojust w celu zintensyfikowania walki z poważną przestępczością. W 2013 r. Komisja przyjęła [wniosek dotyczący rozporządzenia](#) mającego na celu przeprowadzenie reformy Eurojust (wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie Agencji Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych (Eurojust), COM/2013/0535 final).

¹⁰ [Rozporządzenie \(UE\) nr 2016/794 Parlamentu Europejskiego i Rady](#) z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW.

¹¹ [Decyzja ramowa Rady 2002/465/WSiSW](#) z dnia 13 czerwca 2002 r. w sprawie wspólnych zespołów dochodzeniowo-śledczych.

¹² [Decyzja Rady 2009/820/WPZiB](#) z dnia 23 października 2009 r. w sprawie zawarcia w imieniu Unii Europejskiej Umowy o ekstradycji między Unią Europejską a Stanami Zjednoczonymi Ameryki oraz Umowy o wzajemnej pomocy prawnej między Unią Europejską a Stanami Zjednoczonymi Ameryki

¹³ [Decyzja Rady 2010/616/UE](#) z dnia 7 października 2010 r. w sprawie zawarcia Umowy między Unią Europejską a Japonią o wzajemnej pomocy prawnej w sprawach karnych.

¹⁴ Poza wspólnymi zespołami dochodzeniowo-śledczymi (zob. art. 3 dyrektywy END); nie wszystkie państwa członkowskie uczestniczą w przyjęciu i stosowaniu dyrektywy w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych (Dania, Irlandia).

¹⁵ Z wyjątkiem odniesienia w art. 10 ust. 2 lit. e) do identyfikacji osób posiadających określony adres IP, w którym to przypadku nie można powołać się na podwójną karalność jako podstawę do odmowy uznania i wykonania wniosku.

Aby usprawnić transgraniczne gromadzenie elektronicznego materiału dowodowego, nowy instrument zostanie oparty o zasadę wzajemnego uznawania. Organ w państwie, w którym zlokalizowany jest adresat nakazu, nie będzie musiał bezpośrednio brać udziału w doręczaniu i wykonaniu nakazu, z wyjątkiem sytuacji wystąpienia niezgodności, w której wymagane będzie przymuszenie do wykonania nakazu, a stroną interweniującą będzie właściwy organ w państwie, w którym zlokalizowany jest przedstawiciel. Instrument wymaga zatem wprowadzenia zestawu solidnych zabezpieczeń i przepisów, takich jak zatwierdzanie w każdym przypadku przez organ sądowy. Przykładowo europejskie nakazy wydawania dowodów dotyczących transakcji lub treści (w przeciwieństwie do danych abonenta i danych dostępu) mogą być wydawane tylko w przypadku przestępstw zagrożonych w państwie wydającym nakaz karą pozbawienia wolności o górnej granicy ustawowego zagrożenia w wysokości co najmniej trzech lat lub w przypadku konkretnych przestępstw wskazanych we wniosku, takich jak cyberprzestępstwa, przestępstwa wykorzystujące cyberprzestrzeń lub przestępstwa związane z terroryzmem.

Dane osobowe, których dotyczy niniejszy wniosek, podlegają ochronie i mogą być przetwarzane wyłącznie zgodnie z ogólnym rozporządzeniem w sprawie ochrony danych (RODO)¹⁶ oraz dyrektywą 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 oraz w sprawie swobodnego przepływu takich danych (dyrektywa o ochronie danych osobowych skierowana do policji i organów wymiaru sprawiedliwości)¹⁷. RODO będzie miało zastosowanie od dnia 25 maja 2018 r., natomiast dyrektywa o ochronie danych osobowych skierowana do policji i organów wymiaru sprawiedliwości musi zostać przetransponowana przez państwa członkowskie do dnia 6 maja 2018 r.

Konwencja Rady Europy o cyberprzestępczości (Seria Traktatów Rady Europy nr 185), ratyfikowana przez większość państw członkowskich UE, ustanawia międzynarodowe mechanizmy współpracy na rzecz walki z cyberprzestępczością¹⁸. Konwencja dotyczy przestępstw popełnianych za pośrednictwem internetu i innych sieci komputerowych. Wymaga ona również od stron wprowadzenia uprawnień i procedur umożliwiających pozyskiwanie elektronicznego materiału dowodowego oraz świadczenia sobie wzajemnej pomocy prawnej, nieograniczonej do cyberprzestępstw. W szczególności Konwencja zawiera wymóg, by strony wprowadziły nakazy wydania dowodów umożliwiające uzyskanie danych komputerowych od usługodawców na ich terytorium, a także dane abonentów od usługodawców oferujących usługi na ich terytorium. Konwencja przewiduje ponadto stosowanie nakazów zabezpieczenia, jeżeli istnieją powody, aby przypuszczać, że wspomniane dane komputerowe są szczególnie narażone na utratę lub zmianę. Doręczanie

¹⁶ [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.

¹⁷ [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 uchyłająca decyzję ramową Rady 2008/977/WSiSW.

¹⁸ W strategii bezpieczeństwa cybernetycznego Unii Europejskiej z 2013 r. Konwencję Rady Europy o cyberprzestępczości uznano za podstawowe wielostronne ramy zwalczania cyberprzestępczości – wspólny komunikat Komisji i Wysokiego Przedstawiciela Unii ds. Zagranicznych i Polityki Bezpieczeństwa w sprawie strategii bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń, JOIN(2013) 1 final.

i wykonalność krajowych nakazów wydania dowodów skierowanych do usługodawców mających zakład poza terytorium strony Konwencji rodzi kolejne problemy. W tym względzie rozważane są obecnie dalsze środki mające na celu poprawę transgranicznego dostępu do elektronicznych materiałów dowodowych¹⁹.

- **Krótki opis proponowanego rozporządzenia**

Proponowane rozporządzenie wprowadza wiążące europejskie nakazy wydania dowodów i europejskie nakazy zabezpieczenia dowodów. Oba rodzaje nakazów muszą być wydane lub zatwierdzone przez organ sądowy państwa członkowskiego. Nakaz może zostać wydany w celu zapewnienia zabezpieczenia lub wydania danych przechowywanych przez usługodawcę zlokalizowanego w innej jurysdykcji, niezbędnych do wykorzystania w charakterze materiału dowodowego w postępowaniu przygotowawczym lub procesie karnym. Nakazy te mogą być wydane tylko wówczas, gdy w państwie wydającym nakaz dostępny jest podobny środek dotyczący tego samego przestępstwa w porównywalnej sytuacji krajowej. Oba rodzaje nakazów mogą być doręczane dostawcom usług łączności elektronicznej, portali społecznościowych, internetowych platform handlowych, innym dostawcom usług hostingowych oraz dostawcom infrastruktury internetowej, takiej jak rejestry adresów IP i nazw domen, lub ich przedstawicielom prawnym, jeżeli zostali oni powołani. Europejski nakaz zabezpieczenia dowodów, podobnie jak europejski nakaz wydawania dowodów, jest skierowany do przedstawiciela prawnego spoza jurysdykcji państwa członkowskiego wydającego nakaz w celu zabezpieczenia danych z myślą o przyszłym żądaniu udostępnienia tych danych, na przykład za pośrednictwem kanałów wzajemnej pomocy prawnej w przypadku państw trzecich lub za pośrednictwem europejskiego nakazu dochodzeniowego w przypadku uczestniczących państw członkowskich. W przeciwieństwie do określonych w przepisach prawa środków nadzoru lub obowiązków w zakresie zatrzymywania danych, których nie przewidziano w niniejszym rozporządzeniu, europejski nakaz zabezpieczenia dowodów jest nakazem wydawanym lub zatwierdzanym przez organ sądowy w toku konkretnego postępowania karnego po dokonaniu indywidualnej oceny proporcjonalności i konieczności w każdym poszczególnym przypadku. Podobnie jak europejski nakaz wydania dowodów, dotyczy on konkretnych, znanych lub nieznanych, sprawców przestępstwa, które już miało miejsce. Europejski nakaz zabezpieczenia dowodów umożliwia jedynie zabezpieczenie dowodów, które były już przechowywane w momencie odbioru nakazu, nie umożliwia jednak dostępu do danych w przyszłości, po otrzymaniu europejskiego nakazu zabezpieczenia dowodów.

Oba rodzaje nakazów mogą być stosowane wyłącznie w postępowaniu karnym, od wstępnego etapu postępowania przygotowawczego do zakończenia postępowania sądowego wyrokiem lub innym orzeczeniem sądowym. Nakazy wydania dowodów dotyczące danych abonenta i danych dostępu mogą być wydawane w przypadku wszelkich przestępstw, natomiast nakazy wydania dowodów w sprawie danych dotyczących transakcji lub treści mogą być wydawane jedynie w przypadku przestępstw zagrożonych w państwie wydającym nakaz karą pozbawienia wolności o górnej granicy ustawowego zagrożenia w wysokości co najmniej trzech lat lub w przypadku konkretnych przestępstw wskazanych we wniosku, a także jeżeli

¹⁹ Na 17. posiedzeniu plenarnym (w czerwcu 2017 r.) komisja ds. Konwencji o cyberprzestępczości przyjęła zakres zadań dotyczący przygotowania drugiego protokołu dodatkowego do Konwencji („drugi protokół dodatkowy”), który ma zostać przygotowany i sfinalizowany przez tę komisję do grudnia 2019 r. Celem jest wprowadzenie zmian, dzięki którym miejsce przechowywania danych przestanie być łącznikiem decydującym.

występuje konkretne powiązanie z narzędziami elektronicznymi i przestępstwami objętymi zakresem dyrektywy (UE) 2017/541 w sprawie zwalczania terroryzmu.

Ze względu na różny stopień inwazyjności środków nakładanych w związku z niezbędnymi danymi, we wniosku określono szereg warunków i zabezpieczeń. Obejmują one obowiązek zatwierdzania *ex ante* nakazów przez organ sądowy. Wniosek niniejszy dotyczy wyłącznie danych przechowywanych. Niniejszy wniosek nie obejmuje przechwytywania przekazów telekomunikacyjnych w czasie rzeczywistym. Instrument jest ograniczony do tego, co konieczne i proporcjonalne do celów danego postępowania karnego. Umożliwia on ponadto usługodawcom zwrócenie się w razie potrzeby do organów wydających nakaz o wyjaśnienia. Jeżeli kwestie te są niemożliwe do rozwiązania i organ wydający nakaz podejmie decyzję o wszczęciu postępowania przymuszającego do wykonania nakazu, usługodawcy mogą na podstawie tych samych przesłanek sprzeciwić się temu postępowaniu przeprowadzanemu przez własne organy. Dodatkowo ustanawia się szczególną procedurę do zastosowania w sytuacjach, w których obowiązek przekazania danych pozostaje w sprzeczności z kolidującym obowiązkiem wynikającym z przepisów prawa państwa trzeciego.

Ustawodawstwo unijne chroni prawa podejrzanych i oskarżonych w postępowaniu karnym, a ponadto istnieją już przepisy przewidujące ochronę danych osobowych. W przypadku osób, których dane objęto nakazem, dodatkowe zabezpieczenia przedstawione we wniosku pozwalają jednak na ochronę praw procesowych tych osób w toku postępowania karnego lub poza nim. Obejmuje to możliwość zakwestionowania legalności, konieczności lub proporcjonalności nakazu bez ograniczania przesłanek służących do podważenia go zgodnie z prawem krajowym. Prawa przewidziane w przepisach prawa państwa wykonującego nakaz są w pełni respektowane przez zapewnienie uwzględnienia w państwie wydającym nakaz immunitetów i przywilejów chroniących dane, które mają być pozyskane w państwie członkowskim usługodawcy. Dotyczy to szczególnie sytuacji, w której przepisy prawa państwa wykonującego nakaz przewidują wyższy poziom ochrony niż przepisy prawa państwa wydającego.

Nakazy na podstawie proponowanego rozporządzenia podlegają wyegzekwowaniu w ten sam sposób, co porównywalne nakazy krajowe w jurysdykcji, w której usługodawca otrzymuje nakaz. Zgodnie z rozporządzeniem państwa członkowskie powinny wdrożyć skuteczne i proporcjonalne sankcje.

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

• Podstawa prawna

Podstawą prawną wsparcia działań w tej dziedzinie jest art. 82 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej. Art. 82 ust. 1 stanowi, że Parlament Europejski i Rada, stanowiąc zgodnie ze zwykłą procedurą ustawodawczą, przyjmują środki mające na celu ustanowienie zasad i procedur zapewniających uznawanie w całej Unii wszystkich form wyroków i orzeczeń sądowych. Przyjmowane są również środki w celu ułatwiania współpracy między organami sądowymi lub równoważnymi organami państw członkowskich w ramach ścigania karnego i wykonywania orzeczeń.

Ta podstawa prawna ma zastosowanie do mechanizmów objętych niniejszym rozporządzeniem. Art. 82 ust. 1 zapewnia wzajemne uznawanie orzeczeń sądowych, które organ sądowy w państwie wydającym nakaz kieruje do osoby prawnej w innym państwie członkowskim, a nawet za pomocą których nakłada na tę osobę prawną określone obowiązki, bez uprzedniej interwencji organu sądowego w tym innym państwie członkowskim.

Europejski nakaz wydania dowodów lub zabezpieczenia dowodów może prowadzić do interwencji organu sądowego państwa wykonującego, jeżeli jest to konieczne do wykonania takiego orzeczenia.

- **Wybór instrumentu**

Art. 82 ust. 1 TFUE daje unijnym ustawodawcom możliwość przyjmowania rozporządzeń i dyrektyw.

Ponieważ wniosek dotyczy procedur transgranicznych, w przypadku których wymagane są jednolite normy, nie jest konieczne pozostawienie państwom członkowskim pewnego marginesu swobody w ramach transpozycji tych przepisów. Rozporządzenie jest instrumentem stosowanym bezpośrednio, zapewniającym jasność i większą pewność prawa oraz pozwalającym uniknąć rozbieżnych wykładni w państwach członkowskich i innych problemów z transpozycją, których doświadczone przy decyzjach ramowych w sprawie wzajemnego uznawania wyroków i orzeczeń sądowych. Rozporządzenie umożliwia ponadto nałożenie tego samego obowiązku w całej Unii w sposób jednolity. Z tych względów rozporządzenie zostało uznane za najodpowiedniejszą formę instrumentu prawnego na potrzeby wzajemnego uznawania.

- **Pomocniczość**

Ze względu na transgraniczny wymiar poruszanych tutaj problemów środki uwzględnione we wniosku muszą zostać przyjęte na szczeblu unijnym, aby osiągnąć cele rozporządzenia. Przestępstwa, w przypadku których istnieje elektroniczny materiał dowodowy, często wiążą się z sytuacjami, w których infrastruktura służąca do przechowywania elektronicznego materiału dowodowego oraz usługodawca utrzymujący tę infrastrukturę objęci są krajowymi ramami prawnymi, w granicach Unii lub poza nią, innymi niż krajowe ramy prawne ofiary i sprawcy przestępstwa. W rezultacie uzyskanie skutecznego dostępu do elektronicznego materiału dowodowego w wymiarze transgranicznym bez wspólnych norm minimalnych może być dla właściwego państwa bardzo czasochłonne i trudne. W szczególności państwo członkowskie działające we własnym zakresie mogłoby napotkać trudności w związku z następującymi kwestiami:

- rozdrobnienie ram prawnych w państwach członkowskich, które usługodawcy dążący do spełnienia wymogów opartych na przepisach krajowych różnych państw zidentyfikowali jako główne wyzwanie;
- większa drożność współpracy wymiarów sprawiedliwości na podstawie istniejącego prawodawstwa Unii, a w szczególności dyrektywy w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych.

Ze względu na zróżnicowanie podejść prawnych, liczbę stosownych obszarów polityki (bezpieczeństwo, prawa podstawowe, w tym prawa procesowe i ochrona danych osobowych, kwestie gospodarcze) oraz dużą liczbę zainteresowanych stron ustawodawstwo na szczeblu unijnym stanowi najbardziej odpowiedni środek zaradzenia zidentyfikowanym problemom.

- **Proporcjonalność**

We wniosku określono zasady, zgodnie z którymi właściwy organ w Unii Europejskiej może nakazać usługodawcy oferującemu usługi w Unii, lecz nieposiadającemu zakładu w tym samym państwie członkowskim, przedstawienie lub zabezpieczenie elektronicznego materiału dowodowego. Najważniejsze elementy wniosku, takie jak zakres przedmiotowy

Europejskiego nakazu wydania dowodów, warunki zapewniające wzajemność, mechanizm sankcji oraz system zabezpieczeń i środków ochrony prawnej, ograniczają wniosek do zakresu koniecznego do osiągnięcia jego głównych celów. W szczególności wniosek jest ograniczony do żądań dotyczących danych przechowywanych (dane pochodzące z przechwytywania przekazów telekomunikacyjnych w czasie rzeczywistym nie są objęte zakresem proponowanego rozporządzenia) oraz nakazów wydawanych w postępowaniu karnym w odniesieniu do konkretnego przestępstwa będącego przedmiotem postępowania przygotowawczego. Nie obejmuje on zatem zapobiegania przestępczości oraz innych rodzajów postępowań lub naruszeń (takich jak postępowania administracyjne dotyczące naruszeń norm prawnych) i nie wymaga od usługodawców systematycznego gromadzenia lub przechowywania większej ilości danych niż jest to konieczne do prowadzenia przez nich działalności lub przestrzegania innych wymogów prawnych. Nakazy wydania danych abonenta i danych dostępu mogą być wydawane w przypadku wszelkich przestępstw, natomiast nakazy wydania danych dotyczących transakcji lub treści mogą być wydawane jedynie w przypadku przestępstw zagrożonych w państwie wydającym nakaz karą pozbawienia wolności o górnej granicy ustawowego zagrożenia w wysokości co najmniej trzech lat lub w przypadku konkretnych cyberprzestępstw lub przestępstw wykorzystujących cyberprzestrzeń określonych we wniosku oraz przestępstw związanych z terroryzmem. Wreszcie we wniosku wyjaśniono przepisy proceduralne i zabezpieczenia mające zastosowanie do transgranicznego dostępu do elektronicznego materiału dowodowego, nie przewidziano w nim jednak harmonizacji środków krajowych. Jest on ograniczony do tego, co konieczne i proporcjonalne w celu spełnienia potrzeb organów ścigania i organów sądowych w epoce cyfrowej.

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

• Konsultacje z zainteresowanymi stronami

Komisja prowadziła przez półtora roku konsultacje ze wszystkimi zainteresowanymi stronami w celu zidentyfikowania problemów i rozwiązań na przyszłość. Konsultacje zostały przeprowadzone za pośrednictwem ankiet – począwszy od otwartych konsultacji publicznych po ankiety skierowane do właściwych organów publicznych. Zorganizowano również spotkania ekspertów i spotkania dwustronne w celu umówienia możliwych skutków prawodawstwa UE. Konferencje, na których omawiano transgraniczny dostęp do elektronicznego materiału dowodowego, wykorzystano również do uzyskania informacji zwrotnych na temat inicjatywy.

Ogólnie rzecz biorąc, respondenci ankiet postrzegali upowszechnienie korzystania z usług informacyjnych jako wyzwanie dla właściwych organów ścigania, ponieważ są one często zbyt słabo wyposażone, by zajmować się materiałem dowodowym w internecie. Jako jedną z głównych przeszkód wskazywano również długotrwały proces pozyskiwania materiału dowodowego. Inne kluczowe kwestie, na które organy publiczne zwracały uwagę, obejmowały brak wiarygodnej współpracy z usługodawcami, brak przejrzystości, niepewność prawa w zakresie właściwej jurysdykcji, w której miałyby być prowadzone czynności w ramach postępowania przygotowawczego. Uznano, że bezpośrednia współpraca transgraniczna pomiędzy organami ścigania a dostawcami usług cyfrowych wniosłaby wartość dodaną do postępowania przygotowawczego. Usługodawcy i pewne organizacje społeczeństwa obywatelskiego wskazywali potrzebę zapewnienia pewności prawa przy współpracy z organami publicznymi oraz unikania kolizji przepisów. Ze względu na obawy dotyczące możliwego wpływu nowych przepisów UE na przysługujące prawa,

zainteresowane strony były zdania, że warunkiem koniecznym wprowadzenia jakiegokolwiek instrumentu transgranicznego jest zagwarantowanie szczególnych zabezpieczeń.

Informacje zwrotne uzyskane od początku oceny skutków dowodzą, że zdaniem zainteresowanych stron usunięcie niedociągnięć w obecnym systemie wzajemnej pomocy prawnej działałoby na rzecz poprawy jej skuteczności oraz zwiększenia pewności prawa. Niektóre organizacje społeczeństwa obywatelskiego były przeciwne uregulowaniu bezpośredniej współpracy za pomocą przepisów na szczeblu UE. Preferowały one ograniczenie działań UE do poprawy procedur wzajemnej pomocy prawnej. Koncepcji tej zostanie nadany dalszy tok w ramach praktycznych środków zatwierdzonych przez Radę w czerwcu 2016 r.

Dzięki ankiecie skierowanej do organów publicznych w państwach członkowskich stało się również jasne, że brak jest wspólnego podejścia do uzyskiwania transgranicznego dostępu do elektronicznego materiału dowodowego, ponieważ każde państwo członkowskie ma własną, krajową praktykę w tym zakresie. Również usługodawcy różnie reagują na wnioski zagranicznych organów ścigania, a terminy udzielenia odpowiedzi różnią się w zależności od wnioskującego państwa członkowskiego. Prowadzi to do niepewności prawa dla wszystkich zaangażowanych zainteresowanych stron.

Ogólnie rzecz biorąc, konsultacje z zainteresowanymi stronami wykazały, że obecne ramy prawne są rozdrobione i skomplikowane. Może to prowadzić do opóźnień na etapie wykonania oraz nieskuteczności postępowania przygotowawczego i ścigania przestępstw, w przypadku gdy konieczny jest transgraniczny dostęp do elektronicznych materiałów dowodowych.

• Ocena skutków

Rada ds. Kontroli Regulacyjnej wydała pozytywną opinię na temat oceny skutków wspierającej niniejszy wniosek²⁰ oraz przedstawiła szereg sugestii dotyczących udoskonaleń²¹. W wyniku tej opinii ocena skutków została zmieniona w celu dalszego omówienia kwestii dotyczących praw podstawowych, związanych z transgranicznym udostępnianiem danych, w szczególności związków pomiędzy poszczególnymi środkami składającymi się na preferowany wariant. Ocenę zmodyfikowano również w celu lepszego odzwierciedlenia poglądów zainteresowanych stron i państw członkowskich oraz wyjaśnienia sposobu ich uwzględnienia. Przeglądowi poddano ponadto kontekst polityczny w celu włączenia do niego dodatkowych odniesień do różnych aspektów, takich jak dyskusje w grupach ekspertów, które pomogły w kształtowaniu inicjatywy. Komplementarność poszczególnych środków (w szczególności dyrektywy w sprawie europejskiego nakazu dochodzeniowego, negocjacji w sprawie dodatkowego protokołu do Konwencji Rady Europy

²⁰ Dokument roboczy służb Komisji – Ocena skutków towarzysząca wnioskowi dotyczącemu rozporządzenia Parlamentu Europejskiego i Rady w sprawie europejskich nakazów wydania elektronicznego materiału dowodowego w sprawach karnych i europejskich nakazów zabezpieczenia w tym zakresie oraz wnioskowi dotyczącemu dyrektywy Parlamentu Europejskiego i Rady w sprawie określenia przepisów zharmonizowanych w zakresie wyznaczenia przedstawiciela prawnego do celów gromadzenia materiału dowodowego w procesie karnym, SWD(2018) 118.

²¹ Rada ds. Kontroli Regulacyjnej Komisji Europejskiej – Opinia w sprawie oceny skutków towarzyszącej wnioskowi dotyczącemu rozporządzenia Parlamentu Europejskiego i Rady w sprawie europejskich nakazów wydania elektronicznego materiału dowodowego w sprawach karnych i europejskich nakazów zabezpieczenia w tym zakresie oraz wnioskowi dotyczącemu dyrektywy Parlamentu Europejskiego i Rady w sprawie określenia przepisów zharmonizowanych w zakresie wyznaczenia przedstawiciela prawnego do celów gromadzenia materiału dowodowego w procesie karnym, SEC(2018) 199.

o cyberprzestępczości oraz wspólnego przeglądu Porozumienia pomiędzy UE a Stanami Zjednoczonymi o wzajemnej pomocy prawnej) wyjaśniono w odniesieniu do ich zakresu, czasu stosowania i dogłębności, a scenariusz odniesienia zmieniono w celu lepszego odzwierciedlenia zmian, których wystąpienie jest prawdopodobne niezależnie od przyjęcia zaproponowanych środków. Wreszcie dodano schematy blokowe w celu lepszego opisania przepływów zadań w dziedzinie udostępniania danych.

Oprócz scenariusza odniesienia (wariant O) rozważano cztery warianty polityki: szereg praktycznych środków mających na celu poprawę zarówno procedur współpracy wymiarów sprawiedliwości, jak i bezpośredniej współpracy pomiędzy organami publicznymi a usługodawcami (wariant A: o charakterze nieustawodawczym); wariant będący połączeniem środków praktycznych przewidzianych w wariantcie A i międzynarodowych rozwiązań dwustronnych i wielostronnych (wariant B: o charakterze ustawodawczym); wariant będący połączeniem wyżej opisanych środków przewidzianych w wariantcie B oraz europejskiego nakazu wydania dowodów i środka mającego na celu poprawę opartego na zapytaniach dostępu do baz danych zawierających informacje dotyczące abonentów, takich jak baza danych WHOIS z informacjami o właścicielach nazw domen (wariant C: o charakterze ustawodawczym); oraz wariant będący połączeniem wszystkich wyżej opisanych środków przewidzianych w wariantcie C z ustawodawstwem w sprawie bezpośredniego dostępu do zdalnie przechowywanych danych (wariant D: o charakterze ustawodawczym)²².

W przypadku niepodjęcia żadnych środków (wariant O) rosnąca liczba wniosków pogorszy sytuację. Wszystkie pozostałe warianty pomagają osiągnąć cele inicjatywy, jednakże w różnym stopniu. wariant A pozwoliłaby na poprawę skuteczności obecnych procesów, na przykład dzięki poprawie jakości wniosków, jednakże pole do doskonalenia byłoby ograniczone ze względu na niedociągnięcia strukturalne obecnego systemu.

Wariant B prowadziłaby do liczniejszych usprawnień, zapewniając międzynarodowo akceptowane rozwiązania, jednakże wynik tych międzynarodowych rozwiązań byłby w znacznej mierze zależny od państw trzecich. Rozwiązania te są zatem niepewne, ich skuteczność jest mało prawdopodobna i nie oferowałyby one prawdopodobnie tyle samo zabezpieczeń, co rozwiązanie unijne.

Wariant C pozwoliłaby na wniesienie wyraźnej wartości dodanej do wyżej opisanych wariantów, zapewniając ponadto wewnątrzunijny instrument bezpośredniej współpracy z usługodawcami, który umożliwiałby rozwiązanie większości zidentyfikowanych problemów, pod warunkiem istnienia usługodawcy posiadającego odpowiednie dane.

Wariant D stanowi najbardziej kompleksowy pakiet rozwiązań. Oprócz wyżej wymienionych środków obejmuje on środek ustawodawczy dotyczący bezpośredniego dostępu w sytuacjach, w których udział usługodawcy nie jest konieczny.

Niniejsza inicjatywa ustawodawcza proponowana przez Komisję opiera się na ustaleniach z oceny skutków. Ustawodawstwo to zostanie uzupełnione o środki praktyczne opisane

²² Szczegółowe informacje por. dokument roboczy służb Komisji – Ocena skutków towarzysząca wnioskowi dotyczącemu rozporządzenia Parlamentu Europejskiego i Rady w sprawie europejskich nakazów wydania elektronicznego materiału dowodowego w sprawach karnych i europejskich nakazów zabezpieczenia w tym zakresie oraz wnioskowi dotyczącemu dyrektywy Parlamentu Europejskiego i Rady w sprawie określenia przepisów zharmonizowanych w zakresie wyznaczenia przedstawiciela prawnego do celów gromadzenia materiału dowodowego w procesie karnym, SWD(2018) 118.

w ocenie skutków oraz o trwające prace nad protokołem dodatkowym do Konwencji Rady Europy o cyberprzestępczości. W oparciu o swój wniosek ustawodawczy Komisja omówi ponadto ze Stanami Zjednoczonymi i innymi państwami trzecimi możliwość przyszłych porozumień dwustronnych lub wielostronnych w sprawie transgranicznego dostępu do elektronicznego materiału dowodowego oraz zabezpieczeń w tym zakresie. W odniesieniu do środków bezpośredniego dostępu i dostępu do baz danych, stanowiących część wariantu D, Komisja nie proponuje w chwili obecnej żadnego ustawodawstwa, niemniej będzie nadal analizować najlepsze drogi postępowania w odniesieniu do tych dwóch kwestii.

Oczekuje się, że inicjatywa umożliwi bardziej skuteczne i efektywne dochodzenia i ściganie przestępstw, poprawiając jednocześnie przejrzystość i rozliczalność oraz zapewniając poszanowanie praw podstawowych. Oczekuje się również, że będzie ona sprzyjać zaufaniu na jednolitym rynku cyfrowym dzięki poprawie bezpieczeństwa i zmniejszeniu postrzeganej bezkarności w przypadku przestępstw popełnianych na urządzeniach sieciowych lub za ich pośrednictwem.

W przypadku organów publicznych oczekuje się, że inicjatywa spowoduje powstanie początkowych kosztów wdrożenia, które w długiej perspektywie czasowej zostaną skompensowane przez oszczędności w kosztach powtarzalnych. Organy krajowe musiałyby przyjąć nowe procedury i odbyć szkolenia. W dalszej perspektywie organy odniosą jednak korzyści dzięki usprawnieniu i centralizacji oraz jasnym ramom prawnym regulującym wnioski o dostęp do danych, jako że działania te powinny się przyczynić do przyrostu wydajności. Podobnie, ponieważ wariant preferowany przyczyni się do odciążenia kanałów współpracy wymiarów sprawiedliwości, państwa otrzymujące wnioski powinny odnotować zmniejszenie liczby wniosków do rozpatrzenia.

Usługodawcy będą się musieli dostosować do nowych ram prawnych, wprowadzając (nowe) procedury i szkoląc swoich pracowników. Z drugiej strony zharmonizowane ramy mogłyby odciążyć usługodawców, którzy już odpowiadają na wnioski o dane nie dotyczące treści i muszą je oceniać na podstawie różniących się od siebie przepisów prawa we wszystkich państwach członkowskich. Pewność prawa i normalizacja procedur powinny mieć również pozytywny wpływ na małe i średnie przedsiębiorstwa, zmniejszając obciążenia administracyjne i sprzyjając konkurencyjności. Ogólnie rzecz biorąc, oczekuje się również, że inicjatywa przyczyni się do osiągnięcia oszczędności przez te przedsiębiorstwa.

• **Prawa podstawowe**

Wniosek mógłby potencjalnie wpływać na szereg praw podstawowych:

- prawa osoby fizycznej, do której danych uzyskuje się dostęp: prawo do ochrony danych osobowych, prawo do poszanowania życia prywatnego i rodzinnego, prawo do wolności wypowiedzi, prawo do obrony, prawo do skutecznego środka ochrony prawnej i dostępu do bezstronnego sądu;
- prawa usługodawcy: prawo do wolności prowadzenia działalności gospodarczej, prawo do skutecznego środka ochrony prawnej;
- prawa wszystkich obywateli: prawo do wolności i bezpieczeństwa osobistego.

Do proponowanego rozporządzenia włączono, z uwzględnieniem odpowiedniego dorobku prawnego w dziedzinie ochrony danych, wystarczające i odpowiednie zabezpieczenia w celu zapewnienia ochrony praw tych osób.

Ponieważ nakazy mogą być wydawane wyłącznie w procesach karnych oraz jeżeli istnieją porównywalne rozwiązania krajowe, zarówno na etapie postępowania przygotowawczego, jak i w fazie procesu, zastosowanie mają wszystkie gwarancje proceduralne przewidziane w prawie karnym. Obejmuje to w szczególności prawo do rzetelnego procesu sądowego zawarte w art. 6 EKPC oraz w art. 47 i 48 Karty praw podstawowych Unii Europejskiej, a także odpowiednie unijne przepisy dotyczące praw proceduralnych w procesie karnym: dyrektywę 2010/64/UE w sprawie prawa do tłumaczenia ustnego i tłumaczenia pisemnego w postępowaniu karnym, dyrektywę 2012/13/UE w sprawie prawa do informacji o prawach, informacji o zarzutach i prawa dostępu do akt sprawy, dyrektywę 2013/48/UE w sprawie prawa dostępu do adwokata i prawa do porozumiewania się z krewnymi w przypadku zatrzymania i aresztowania, dyrektywę 2016/343 w sprawie wzmocnienia niektórych aspektów domniemania niewinności i prawa do obecności na rozprawie, dyrektywę 2016/800 w sprawie gwarancji procesowych dla dzieci oraz dyrektywę 2016/1919 w sprawie pomocy prawnej dla podejrzanych i oskarżonych w postępowaniu karnym oraz dla osób, których dotyczy wnioski w postępowaniu dotyczącym europejskiego nakazu aresztowania.

W szczególności uprzednia interwencja organu sądowego w przypadku wydania nakazu zapewnia możliwość sprawdzenia legalności środka oraz jego konieczności i proporcjonalności w danej sprawie. Gwarantuje to ponadto, że nakaz nie wpłynie w sposób nieuprawniony na prawa podstawowe, w tym skutki zasad prawnych takich jak poufność wymiany informacji między prawnikiem a klientem. Organ wydający nakaz ma obowiązek w każdym poszczególnym przypadku upewnić się co do konieczności i proporcjonalności środka, w tym w świetle ciężaru przestępstwa podlegającego postępowaniu przygotowawczemu. We wniosku przewidziano ponadto progi dla danych dotyczących transakcji i treści, które gwarantują, że europejski nakaz wydania dowodów stosowany będzie wyłącznie w przypadku poważniejszych przestępstw związanych z takimi danymi.

Prawo do skutecznego środka ochrony prawnej dla osób, których danych dotyczy nakaz, jest również wyraźnie omówione. Przyznane immunitety i przywileje związane z pewnymi zawodami, takimi jak zawód prawnika, a także podstawowe interesy bezpieczeństwa lub obronności państwa osoby, której nakaz dotyczy, również muszą być wzięte pod uwagę w procesie w państwie wydającym nakaz. Kontrola dokonana przez organ sądowy stanowi w tym przypadku dodatkowe zabezpieczenie.

Ponieważ nakaz jest środkiem wiążącym, ma on również wpływ na prawa usługodawców, w szczególności wolność prowadzenia działalności gospodarczej. We wniosku dotyczącym rozporządzenia uwzględniono prawo usługodawcy do wniesienia określonych roszczeń w państwie członkowskim wydającym nakaz, na przykład jeśli nakaz nie został wydany lub zatwierdzony przez organ sądowy. Jeżeli nakaz przekazuje się do wykonania do państwa wykonującego, organ przymuszający do wykonania może podjąć decyzję o nieuznaniu lub nieprzymuszaniu do wykonania nakazu, jeżeli po jego otrzymaniu spełnione są którekolwiek ze ściśle określonych przesłanek wniesienia sprzeciwu, oraz po konsultacji z organem wydającym. Dodatkowo, w przypadku wszczęcia procedury przymuszającej do wykonania, osoba, której nakaz dotyczy, będzie mogła we własnym zakresie wnieść sprzeciw wobec nakazu do organu przymuszającego do wykonania w oparciu o wszelkie takie ściśle określone przesłanki. Obejmuje to na przykład przypadki, w których jest oczywiste, że nakaz nie został wydany lub zatwierdzony przez właściwy organ, lub przypadki, w których zastosowanie się do nakazu stanowiłoby jawne pogwałcenie Karty lub miałoby wyraźnie charakter nadużycia. Powyższe nie wyklucza prawa osoby, której nakaz dotyczy, do skutecznego środka ochrony prawnej w odniesieniu do decyzji nakładającej sankcję.

Potencjalnym problemem związanym z działaniami UE w tym obszarze jest możliwość wprowadzenia przez państwa trzecie wzajemnych zobowiązań dla usługodawców z UE, niezgodnych z warunkami dotyczącymi praw podstawowych UE, w tym wysokim poziomem ochrony danych gwarantowanym przez dorobek prawny Unii. We wniosku uwzględniono tę sytuację na dwa sposoby: po pierwsze zapewniając środek zawierający solidne zabezpieczenia oraz wyraźne odesłania do warunków i zabezpieczeń właściwych dla dorobku prawnego UE, dostarczając w ten sposób model dla zagranicznego prawodawstwa; po drugie, wprowadzając specjalną klauzulę „konfliktu obowiązków”, umożliwiającą usługodawcom identyfikację sprzecznych obowiązków i powoływanie się na ich wystąpienie w celu zainicjowania kontroli sądowej. Klauzula ta ma na celu zapewnienie poszanowania zarówno ogólnych regulacji „blokujących”, takich jak np. amerykańska ustawa o prywatności w łączności elektronicznej (ECPA), która zabrania ujawniania danych dotyczących treści w przewidzianym w niej obszarze geograficznym z wyjątkiem ściśle określonych okoliczności, jak i przepisów prawa, które nie zabraniają ujawniania danych w sposób ogólny, lecz przewidują taki zakaz w poszczególnych przypadkach. W przypadku spraw związanych z ECPA dostęp do danych dotyczących treści może być obecnie w pewnych sytuacjach niemożliwy, w związku z czym wzajemna pomoc prawna powinna pozostać podstawowym narzędziem dostępu do takich danych. Niemniej zmiany wynikające z przyjęcia amerykańskiej ustawy określającej legalne wykorzystanie danych za granicą (CLOUD)²³ mogą prowadzić do zniesienia regulacji „blokujących”, jeżeli UE zawrze porozumienie ze Stanami Zjednoczonymi. Dodatkowe międzynarodowe porozumienia z kluczowymi partnerami mogą zaowocować dalszym ograniczeniem sytuacji kolizji przepisów.

W świetle tego, co powiedziano powyżej, środki przewidziane w niniejszym wniosku są zgodne z prawami podstawowymi.

4. WPLYW NA BUDŻET

Wniosek ustawodawczy dotyczący rozporządzenia nie ma wpływu na budżet Unii.

5. ELEMENTY FAKULTATYWNE

• Plany wdrożenia i monitorowanie, ocena i sprawozdania

Rozporządzenie jest bezpośrednio stosowane w Unii. Będzie ono stosowane bezpośrednio przez przedstawicieli zainteresowanych zawodów i organów, bez konieczności zmiany wewnętrznych systemów prawnych.

Komisja dokona oceny rozporządzenia i złoży Parlamentowi Europejskiemu i Radzie sprawozdanie z tej oceny nie później niż po upływie 5 lat od dnia wejścia w życie rozporządzenia. W oparciu o ustalenia zawarte w sprawozdaniu, w szczególności dotyczące tego, czy rozporządzenie pozostawia jakiegokolwiek luki istotne w praktyce, oraz z uwzględnieniem postępu technologicznego, Komisja oceni potrzebę rozszerzenia zakresu rozporządzenia. W razie potrzeby Komisja przedłoży wnioski mające na celu dostosowanie niniejszego rozporządzenia. Państwa członkowskie prześlą Komisji informacje niezbędne do przygotowania tego sprawozdania oraz zgromadzą dane niezbędne do corocznego monitorowania rozporządzenia.

²³ W dniu 23 marca 2018 r. w Stanach Zjednoczonych przyjęto ustawę określającą legalne wykorzystanie danych za granicą (CLOUD). Ustawa CLOUD dostępna jest [tutaj](#).

W razie potrzeby Komisja wyda wytyczne dla usługodawców dotyczące wywiązywania się z obowiązków przewidzianych w rozporządzeniu.

- **Szczegółowe objaśnienia poszczególnych przepisów wniosku**

	ROZPORZĄDZENIE	
	Artykuł	Motyw
I. Przedmiot, definicje i zakres	1. Przedmiot	1–15
	2. Definicje	16–23
	3. Zakres	24–27
II. Europejski nakaz wydania dowodów, europejski nakaz zabezpieczenia dowodów i zaświadczenia, przedstawiciel prawny	4. Organ wydający	30
	5. Warunki wydania europejskiego nakazu wydania dowodów	28–29, 31–35
	6. Warunki wydania europejskiego nakazu zabezpieczenia dowodów	36
	7. Adresat europejskiego nakazu wydania dowodów i europejskiego nakazu zabezpieczenia dowodów	37
	8. Zaświadczenie europejskiego nakazu wydania dowodów i zaświadczenie europejskiego nakazu zabezpieczenia dowodów	38–39
	9. Wykonanie zaświadczenia europejskiego nakazu wydania danych	40–41
	10. Wykonanie zaświadczenia europejskiego nakazu zabezpieczenia dowodów	42
	11. Poufność i informowanie użytkowników	43
	12. Zwrot kosztów	Brak
III. Sankcje i postępowanie przymuszające do wykonania nakazu	13. Sankcje	Brak
	14. Postępowanie przymuszające do wykonania nakazu	44–45, 55
IV. Środki ochrony prawnej	15 i 16. Postępowanie odwoławcze w przypadku konfliktu obowiązków wynikających z przepisów państwa trzeciego	47–53
	17. Skuteczne środki ochrony prawnej	54

	18. Zapewnienie przywilejów i immunitetów na podstawie prawa państwa wykonującego	35
V. Postanowienia końcowe	19. Monitorowanie i sprawozdawczość	58
	20. Zmiany zaświadczeń i formularzy	59–60
	21. Wykonywanie przekazanych uprawnień	60
	22. Powiadomienia	Brak
	23. Związek z europejskimi nakazami dochodzeniowymi	61
	24. Ocena	62
	25. Wejście w życie	Brak

Rozdział 1: Przedmiot, definicje i zakres

Artykuł 1: Przedmiot

W tym artykule przedstawiono ogólny zakres i cel wniosku, którym jest określenie zasad, na podstawie których właściwy organ sądowy w Unii Europejskiej może nakazać usługodawcy oferującemu usługi w Unii, na podstawie europejskiego nakazu wydania dowodów lub europejskiego nakazu zabezpieczenia dowodów, wydanie lub zabezpieczenie elektronicznego materiału dowodowego. Z instrumentów tych można korzystać wyłącznie w sytuacjach transgranicznych, czyli sytuacjach, w których usługodawca posiada zakład lub przedstawicielstwo w innym państwie członkowskim.

Niniejsze rozporządzenie zapewni dodatkowe narzędzia dla organów dochodzeniowo-sledczych, umożliwiające pozyskiwanie elektronicznego materiału dowodowego bez ograniczania uprawnień przewidzianych w prawie krajowym z myślą o przymuszaniu usługodawców mających zakład lub przedstawicielstwo na ich terytorium. Jeżeli usługodawca posiada zakład lub przedstawicielstwo w tym samym państwie członkowskim, organy tego państwa skorzystają w celu przymuszenia usługodawcy ze środków krajowych.

Dane, których wydanie zostało nakazane na podstawie europejskiego nakazu wydania dowodów, powinny być przekazane bezpośrednio tym organom bez udziału władz państwa członkowskiego, w którym usługodawca posiada zakład lub przedstawicielstwo. Rozporządzenie odchodzi również od traktowania lokalizacji danych jako decydującego łącznika, ponieważ przechowywanie danych w normalnej sytuacji nie prowadzi do kontroli ze strony państwa, na którego terytorium dane są przechowywane. Lokalizację danych określa w większości przypadków sam dostawca usług, kierując się względami gospodarczymi²⁴.

²⁴ Dalsze wyjaśnienia zawarte są w ocenie skutków.

Co więcej, rozporządzenie ma także zastosowanie, jeżeli usługodawcy nie posiadają zakładu lub przedstawicielstwa w Unii, lecz oferują usługi w Unii. Znajduje to odzwierciedlenie w art. 3 ust. 1.

Ilekoć we wniosku jest mowa o usługodawcy posiadającym zakład lub przedstawicielstwo w państwie członkowskim za pośrednictwem wyznaczonego przedstawiciela prawnego, samo wyznaczenie przedstawiciela prawnego nie przesądza, na potrzeby niniejszego rozporządzenia, o utworzeniu zakładu usługodawcy.

W art. 1 ust. 2 przypomniano, że niniejsze rozporządzenie nie powoduje skutku w postaci zmiany obowiązku poszanowania praw podstawowych i podstawowych zasad prawnych zapisanych w art. 6 TUE.

Artykuł 2: Definicje

Artykuł ten zawiera definicje, które są stosowane w całym akcie.

Zakresem rozporządzenia objęto usługodawców następujących rodzajów: dostawców usług łączności elektronicznej, dostawców usług społeczeństwa informacyjnego, w przypadku których przechowywanie danych jest elementem definiującym usługę świadczoną użytkownikowi, w tym portali społecznościowych w zakresie, w jakim nie kwalifikują się one jako usługi łączności elektronicznej, dostawców internetowych platform handlowych umożliwiających transakcje pomiędzy ich użytkownikami (takimi jak konsumenci lub przedsiębiorstwa) oraz innych dostawców usług hostingowych i dostawców usług w zakresie nazw i numeracji domen.

Zakres rozporządzenia obejmuje dostawców usług łączności elektronicznej zgodnie z definicją zawartą [w dyrektywie ustanawiającej Europejski kodeks łączności elektronicznej]. Konsumenci i przedsiębiorstwa w coraz większym stopniu zamiast na tradycyjnych usługach łączności polegają na nowych, opartych na internecie usługach umożliwiających komunikację międzyludzką, takich jak usługi telefonii internetowej (VoIP), komunikatory internetowe, usługi poczty elektronicznej przez internet. Usługi te, wraz z portalami społecznościowymi takimi jak Twitter i Facebook, umożliwiającymi użytkownikom udostępnianie treści, powinny zatem być objęte niniejszym wnioskiem.

W wielu przypadkach dane nie są już przechowywane na urządzeniu użytkownika, lecz udostępniane w infrastrukturze opartej na technologii przetwarzania w chmurze, umożliwiającej zasadniczo dostęp z dowolnego miejsca. Usługodawcy nie muszą posiadać zakładu lub serwerów w każdej jurysdykcji, lecz korzystają ze scentralizowanej administracji i zdecentralizowanych systemów do przechowywania danych i świadczenia swoich usług. Umożliwia im to optymalizację obciążenia i zmniejszenie opóźnień w odpowiadaniu na żądania użytkowników o dane. Sieci dostarczania treści (CDN) są zazwyczaj wdrażane w celu przyspieszenia dostarczania treści dzięki kopiowaniu treści na pewnej liczbie serwerów rozmieszczonych na całym świecie. Umożliwia to przedsiębiorstwom dostarczanie treści z serwera zlokalizowanego najbliżej użytkownika lub serwera, za pomocą którego można przekierować łączność przez mniej przeciążoną sieć. Aby uwzględnić to rozwiązanie, zakresem definicji objęto usługi hostingowe oparte na przetwarzaniu w chmurze i inne usługi hostingowe, które umożliwiają dostęp do różnorodnych zasobów obliczeniowych, takich jak: sieci, serwery lub inna infrastruktura, pamięć, aplikacje i usługi umożliwiające przechowywanie danych do różnych celów. Instrument ma również zastosowanie do cyfrowych platform handlowych, które umożliwiają konsumentom lub przedsiębiorstwom

zawieranie transakcji za pośrednictwem sprzedaży przez internet lub umów o świadczenie usług. Transakcje tego rodzaju są zawierane na stronie internetowej platformy handlowej lub na stronie internetowej handlowca wykorzystującego usługi obliczeniowe oferowane przez internetową platformę handlową. Platforma handlowa jest zatem w posiadaniu elektronicznego materiału dowodowego, który może być potrzebny w procesie karnym.

Usługi, w przypadku których przechowywanie danych nie jest elementem definiującym, nie są objęte niniejszym wnioskiem. Chociaż większość usług świadczonych przez usługodawców wiąże się z przechowywaniem danych, szczególnie jeżeli są to usługi świadczone przez internet na odległość, można wyróżnić usługi, w przypadku których przechowywanie danych nie jest ich podstawową cechą i w związku z tym ma jedynie charakter pomocniczy, w tym usługi prawne, architektoniczne, inżynierskie i rachunkowe świadczone przez internet na odległość.

Dane przechowywane przez dostawców usług w zakresie infrastruktury internetowej, takich jak podmioty rejestrujące i rejestry nazw domen oraz dostawcy usług prywatności i usług *proxy* lub regionalne rejestry internetowe adresów IP, mogą mieć znaczenie w postępowaniu karnym, ponieważ mogą być źródłem poszlak umożliwiających identyfikację osób fizycznych lub podmiotów zaangażowanych w działalność przestępczą.

Kategorie danych, które właściwe organy mogą pozyskać na podstawie europejskiego nakazu wydania dowodów, obejmują dane abonenta, dane dostępu, dane dotyczące transakcji (trzy kategorie danych, nazywane łącznie „danymi niedotyczącymi treści”) oraz przechowywane dane dotyczące treści. Rozróżnienie to, nie licząc danych dostępu, występuje w nakazach prawnych wielu państw członkowskich, a także w pozaunijnych ramach prawnych.

Wszystkie kategorie obejmują dane osobowe, są one zatem objęte zabezpieczeniami przewidzianymi w dorobku prawnym UE w dziedzinie ochrony danych. Intensywność oddziaływania na prawa podstawowe różni się w zależności od kategorii; szczególnie duże różnice występują pomiędzy danymi abonenta z jednej strony a danymi dotyczącymi transakcji i danymi dotyczącymi treści z drugiej. Zasadnicze znaczenie ma objęcie instrumentem wszystkich tych kategorii: dane abonenta i dane dostępu stanowią często punkt wyjścia do uzyskania w postępowaniu przygotowawczym poszlak dotyczących tożsamości podejrzanego. Natomiast dane dotyczące transakcji i dane dotyczące treści mogą się okazać najbardziej adekwatne jako materiał dowodowy. Ze względu na różne nasilenie oddziaływania na prawa podstawowe zasadne jest określenie innych warunków dla danych abonenta z jednej strony oraz danych dotyczących transakcji i treści z drugiej, czego dokonano w niektórych przepisach niniejszego rozporządzenia.

Dane dostępu należy wyodrębnić jako szczególną kategorię danych używaną w niniejszym rozporządzeniu. Dane dostępu zgodnie z zawartą tutaj definicją są pozyskiwane do tego samego celu, co dane abonenta, tj. w celu identyfikacji użytkownika, a poziom ingerencji w prawa podstawowe jest w obu przypadkach podobny. Dane dostępu powinny zatem podlegać tym samym warunkom, co dane abonenta. Stąd w niniejszym wniosku wprowadzono nową kategorię danych, którą należy traktować tak jak dane abonenta, jeżeli mają być one wykorzystane do tego samego celu.

W art. 2 określono państwa członkowskie i organy, które mogą brać udział w postępowaniu. Definicję organu wydającego zawarto w art. 4.

Sytuacje wyjątkowe to sytuacje, które regularnie wymagają reakcji ze strony usługodawcy w odpowiednim czasie oraz w przypadku których będą mieć zastosowanie szczególne warunki. Z tego powodu zdefiniowano je oddzielnie w tym artykule.

Artykuł 3: Zakres

W tym artykule przedstawiono zakres wniosku. Rozporządzenie ma zastosowanie do wszystkich usługodawców, którzy oferują usługi w Unii, w tym usługodawców nieposiadających zakładu w Unii. Aktywne oferowanie usług w Unii, ze wszystkimi czerpanymi z nich korzyściami, uzasadnia objęcie tych usługodawców zakresem rozporządzenia i pozwala stworzyć równe warunki działania dla uczestników tych samych rynków. Nieobjęcie tych usługodawców zakresem rozporządzenia prowadziłoby ponadto do powstania luki i ułatwiłoby przestępcom obejście tego zakresu.

W celu ustalenia, czy usługi są oferowane, organy muszą ocenić, czy usługodawca umożliwia osobom prawnym lub fizycznym korzystanie ze swoich usług w co najmniej jednym państwie członkowskim. Niemniej sama tylko dostępność usługi (która może też wynikać z dostępności strony internetowej usługodawcy lub pośrednika, lub adresu e-mail lub innych danych kontaktowych) nie powinna być warunkiem wystarczającym do zastosowania niniejszego rozporządzenia. Dlatego w celu stwierdzenia wystarczającego związku pomiędzy usługodawcą a terytorium, na którym oferowana jest usługa, niezbędne jest istotne powiązanie z takimi państwami członkowskimi. Takie istotne powiązanie istnieje, jeżeli usługodawca posiada zakład w co najmniej jednym państwie członkowskim. W przypadku braku zakładu w Unii spełnienie kryterium istnienia istotnego powiązania z Unią należy ocenić na podstawie istnienia znaczącej liczby użytkowników w co najmniej jednym państwie członkowskim, lub kierowania usług do co najmniej jednego państwa członkowskiego. Fakt kierowania usług do co najmniej jednego państwa członkowskiego można stwierdzić na podstawie wszelkich istotnych okoliczności, w tym czynników takich jak używanie języka lub waluty powszechnie używanych w państwie członkowskim. O kierowaniu usług do państwa członkowskiego można również wnosić na podstawie dostępności aplikacji w odpowiednim krajowym sklepie z aplikacjami, lokalnego udostępniania reklam lub udostępniania reklam w języku używanym w państwie członkowskim, używania jakichkolwiek informacji pochodzących od osób w państwach członkowskich podczas realizacji działalności usługodawcy lub zarządzania relacjami z klientem obejmującego zapewnianie obsługi klienta w języku powszechnie używanym w państwie członkowskim. Istotne powiązanie należy również zakładać, jeżeli usługodawca kieruje swoją działalność do co najmniej jednego państwa członkowskiego zgodnie z art. 17 ust. 1 lit. c) rozporządzenia nr 1215/2012 w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych.

Europejski nakaz wydania dowodów i europejski nakaz zabezpieczenia dowodów to środki dochodzeniowo-śledcze, które mogą być wydawane tylko w postępowaniu przygotowawczym lub procesie karnym w odniesieniu do konkretnych przestępstw. Związek z konkretnym postępowaniem przygotowawczym odróżnia je od środków zapobiegawczych lub obowiązków w zakresie zatrzymywania danych przewidzianych w przepisach prawa i zapewnia stosowanie praw procesowych mających zastosowanie do procesów karnych. Uprawnienie do wszczynania dochodzeń dotyczących konkretnych przestępstw jest zatem warunkiem stosowania rozporządzenia.

W ramach dodatkowego wymogu dane, które mają być pozyskane, muszą być związane z usługami oferowanymi przez usługodawcę w Unii.

Rozdział 2: Europejski nakaz wydania dowodów, europejski nakaz zabezpieczenia dowodów i zaświadczenia

Artykuł 4: Organ wydający

Przy wydawaniu europejskiego nakazu wydania dowodów lub europejskiego nakazu zabezpieczenia dowodów organ sądowy musi zawsze działać w charakterze organu wydającego lub organu zatwierdzającego. W przypadku nakazów przedstawienia danych dotyczących transakcji lub danych dotyczących treści wymagany jest udział sędziego lub sądu. W przypadku danych abonenta lub danych dostępu może to zrobić również prokurator.

Artykuł 5: Warunki wydania europejskiego nakazu wydania dowodów

W art. 5 określono warunki wydania europejskiego nakazu wydania dowodów. Muszą być one ocenione przez organ sądowy wydający nakaz.

Europejski nakaz wydania dowodów może być wydany wyłącznie wówczas, gdy jest on w danym przypadku konieczny i proporcjonalny. Co więcej, powinien być on wydany wyłącznie wówczas, gdy w państwie wydającym dostępny jest podobny środek w porównywalnej sytuacji krajowej.

Nakazy wydania dowodów dotyczące danych abonenta i danych dostępu mogą być wydawane w odniesieniu do każdego przestępstwa. Dane dotyczące transakcji i dane dotyczące treści powinny być objęte bardziej rygorystycznymi wymogami w celu odzwierciedlenia wrażliwego charakteru takich danych oraz, odpowiednio, wyższej inwazyjności nakazów dotyczących takich danych w porównaniu do danych abonenta i danych dostępu. Nakazy mogą być zatem wydawane wyłącznie w odniesieniu do przestępstw zagrożonych karą pozbawienia wolności o górnej granicy ustawowego zagrożenia w wysokości co najmniej trzech lat. Ustalenie progu w oparciu o maksymalną karę pozbawienia wolności umożliwia obranie bardziej proporcjonalnego podejścia, wraz z szeregiem innych warunków i zabezpieczeń *ex ante* i *ex post* mających na celu zapewnienie poszanowania zasady proporcjonalności i praw zainteresowanych osób.

Jednocześnie próg nie powinien osłabiać skuteczności instrumentu i utrudniać jego wykorzystania przez przedstawicieli zainteresowanych zawodów i organów. Górna granica ustawowego zagrożenia karą w państwach członkowskich jest różna w zależności od ich systemu krajowego. Krajowe kodeksy karne różnią się i nie są zharmonizowane. Dotyczy to zarówno przestępstw, jak i mających do nich zastosowanie sankcji. Krajowe kodeksy postępowania różnią się także co do progu dotyczącego pozyskiwania danych dotyczących transakcji lub treści: w niektórych państwach członkowskich nie wyznaczono żadnych konkretnych progów; w innych wprowadzono wykaz przestępstw. Próg trzyletni ogranicza zakres instrumentu do poważniejszych przestępstw, bez nadmiernego ograniczania możliwości stosowania go przez przedstawicieli zainteresowanych zawodów i organów. Próg ten wyłącza z zakresu rozporządzenia szeroką gamę przestępstw w zależności od kodeksu karnego państwa członkowskiego (na przykład w niektórych państwach członkowskich udział w działaniach zorganizowanej grupy przestępczej i uprowadzenie, ale również takie przestępstwa jak drobne kradzieże, oszustwa i napaść, w przypadku których transgraniczny nakaz wymagający przedstawienia bardziej wrażliwych danych można uznać za nieproporcjonalny). Z drugiej strony próg trzyletni pozwala na włączenie przestępstw, które wymagają bardziej skutecznego podejścia, takich jak przynależność do organizacji przestępczej, finansowanie grup terrorystycznych, wspieranie lub promowanie organizacji

przestępczej, szkolenie mające na celu popełnienie przestępstwa o charakterze terrorystycznym, niektóre przestępstwa popełnione z zamiarem terrorystycznym oraz przygotowania do popełnienia przestępstwa z zamiarem terrorystycznym, lub przygotowania do wcięcia zakładnika, które zostałyby wyłączone z zakresu rozporządzenia w przypadku zastosowania wyższego progu, w zależności od państwa członkowskiego. Próg ten został wybrany, aby w przypadku wszystkich państw członkowskich zapewnić równowagę pomiędzy skutecznością postępowania przygotowawczego a ochroną praw i proporcjonalności. Próg ma również tę zaletę, że łatwo go zastosować w praktyce.

Prócz tego nakazy przedstawienia danych dotyczących transakcji lub danych dotyczących treści mogą być wydawane w odniesieniu do konkretnych przestępstw o zharmonizowanej definicji wymienionych w niniejszym przepisie, w przypadku których materiał dowodowy jest najczęściej dostępny głównie w postaci elektronicznej. Uzasadnia to stosowanie rozporządzenia także w sytuacjach, w których górna granica ustawowego zagrożenia karą jest niższa niż opisany powyżej próg; w przeciwnym przypadku w odniesieniu do przestępstw tego rodzaju nie można by prowadzić odpowiedniego postępowania przygotowawczego, co mogłoby skutkować bezkarnością. Przestępstwa te określone są w szczegółowych przepisach: (i) decyzji ramowej Rady 2001/413/WSiSW w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi, (ii) dyrektywy 2011/93/UE w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępującej decyzję ramową Rady 2004/68/WSiSW oraz (iii) dyrektywy 2013/40/UE dotyczącej ataków na systemy informatyczne i zastępującej decyzję ramową Rady 2005/222/WSiSW. Nakazy mogą być również wydawane w odniesieniu do przestępstw wymienionych w dyrektywie 2017/541/UE w sprawie zwalczania terroryzmu i zastępującej decyzję ramową Rady 2002/475/WSiSW oraz zmieniającej decyzję Rady 2005/671/WSiSW. Niektóre z tych przestępstw są zagrożone karą pozbawienia wolności o górnej granicy ustawowego zagrożenia w wysokości co najmniej roku, inne dwóch lat, lecz żadne z nich nie jest zagrożone karą pozbawienia wolności o górnej granicy ustawowego zagrożenia w wysokości poniżej roku.

W artykule tym określono również obowiązkowe informacje, które należy włączyć do europejskiego nakazu wydania dowodów w celu umożliwienia usługodawcy identyfikacji i przedstawienia żądanych danych. W europejskim nakazie wydania dowodów powinno się znaleźć również uzasadnienie dotyczące konieczności i proporcjonalności tego środka.

Europejski nakaz wydania dowodów realizuje się w drodze wydania zaświadczenia europejskiego nakazu wydania dowodów (zob. art. 8), które zostaje przetłumaczone i przesłane usługodawcy. Zaświadczenie europejskiego nakazu wydania danych zawiera te same obowiązkowe informacje, co nakaz, z wyjątkiem uzasadnienia dotyczącego konieczności i proporcjonalności środka oraz pozostałych szczegółowych informacji dotyczących sprawy.

Jeżeli dane, które mają być pozyskane, są przechowywane lub przetwarzane w ramach infrastruktury zapewnianej spółce przez usługodawcę, co ma zazwyczaj miejsce w przypadku usług hostingowych lub usług związanych z oprogramowaniem, pierwotnym adresatem żądania ze strony organów dochodzeniowo-śledczych może być spółka. W sytuacji, w której przedsiębiorstwo nie jest usługodawcą objętym zakresem niniejszego rozporządzenia, może to wymagać zastosowania europejskiego nakazu dochodzeniowego lub procedury wzajemnej pomocy prawnej. Usługodawca może być adresatem europejskiego nakazu wydania dowodów jedynie wówczas, gdy skierowanie żądania do spółki byłoby nieodpowiednie,

w szczególności jeżeli stwarzałoby ryzyko zaszkodzenia postępowaniu przygotowawczemu, na przykład jeżeli sama spółka stanowi przedmiot postępowania przygotowawczego.

Przed wydaniem europejskiego nakazu wydania dowodów organ wydający musi również wziąć pod uwagę potencjalne immunitety i przywileje przewidziane w państwie członkowskim usługodawcy, a także wszelki wpływ na podstawowe interesy tego państwa członkowskiego, takie jak bezpieczeństwo narodowe i obrona. Celem tego przepisu jest zapewnienie, by immunitety i przywileje chroniące dane, które mają być pozyskane w państwie członkowskim usługodawcy, zostały uwzględnione w państwie wydającym, w szczególności jeżeli gwarantują one wyższy poziom ochrony niż przepisy prawa państwa wydającego.

Artykuł 6: Warunki wydania europejskiego nakazu zabezpieczenia dowodów

Europejski nakaz zabezpieczenia dowodów podlega podobnym warunkom co europejski nakaz wydania dowodów. Może on zostać wydany w przypadku wszelkich przestępstw zgodnie z pozostałymi warunkami przewidzianymi w art. 6. Jego celem jest zapobieżenie usunięciu, skasowaniu lub zmianie odpowiednich danych w sytuacji, w której doprowadzenie do wydania tych danych może zająć więcej czasu, na przykład gdy mają zostać wykorzystane kanały współpracy wymiarów sprawiedliwości. Biorąc na przykład pod uwagę, że europejski nakaz dochodzeniowy może zostać wydany co do zasady w odniesieniu do każdego przestępstwa bez ograniczeń wyznaczonych jakimikolwiek progami, europejski nakaz zabezpieczenia dowodów również nie jest ograniczony w tym zakresie. W przeciwnym przypadku instrument ten nie byłby skuteczny. Aby umożliwić organom dochodzeniowo-śledczym szybkie działanie oraz ze względu na to, że dany wniosek o wydanie danych będzie kolejnym wnioskiem, w odniesieniu do którego wszystkie warunki zostaną ponownie poddane kontroli, europejski nakaz zabezpieczenia dowodów może być wydawany lub zatwierdzany także przez prokuratora.

Artykuł 7: Adresat europejskiego nakazu wydania dowodów i europejskiego nakazu zabezpieczenia dowodów

Europejskie nakazy wydania dowodów i europejskie nakazy zabezpieczenia dowodów powinny być skierowane do przedstawiciela prawnego wyznaczonego przez usługodawcę na potrzeby gromadzenia materiału dowodowego w procesie karnym zgodnie z dyrektywą w sprawie określenia przepisów zharmonizowanych w zakresie wyznaczenia przedstawiciela prawnego do celów gromadzenia materiału dowodowego w procesie karnym. Na podstawie art. 8 pismo przyjmuje postać zaświadczenia europejskiego nakazu wydania danych („EPOC”) lub zaświadczenia europejskiego nakazu zabezpieczenia dowodów („EPOC-PR”). Przedstawiciel prawny będzie odpowiedzialny za ich odbiór oraz terminowe i pełne wykonanie. Pozostawia to usługodawcom wybór sposobu wydania danych, których żądają organy państwa członkowskiego.

W przypadku niewyznaczenia przedstawiciela prawnego nakazy mogą być skierowane do dowolnego zakładu usługodawcy w Unii. Ten wariant rezerwowy ma na celu zapewnienie skuteczności systemu, jeżeli usługodawca nie wyznaczył (jeszcze) specjalnego przedstawiciela, na przykład w sytuacji, w której wyznaczenie przedstawiciela prawnego nie jest obowiązkiem zgodnie z dyrektywą, ponieważ usługodawcy posiadają zakład i prowadzą działalność tylko w jednym państwie członkowskim, lub w przypadku, w którym obowiązek wyznaczenia przedstawiciela prawnego jeszcze nie wszedł w życie, przed upływem terminu transpozycji dyrektywy.

Jeżeli przedstawiciel prawny nie wywiązuje się z obowiązków, przewiduje się dwie sytuacje, w których organ wydający może zwrócić się do dowolnego zakładu usługodawcy w Unii: w sytuacjach nadzwyczajnych określonych w art. 9 ust. 2 oraz w sytuacjach, w których przedstawiciel prawny nie wywiązuje się z obowiązków przewidzianych w art. 9 i 10, a organ wydający uważa, że istnieje wyraźne ryzyko utraty danych.

Artykuł 8: Zaświadczenie europejskiego nakazu wydania dowodów i europejskiego nakazu zabezpieczenia dowodów

Zaświadczenia europejskiego nakazu wydania danych i zaświadczenie europejskiego nakazu zabezpieczenia dowodów służą do przekazania nakazów do adresata określonego w art. 7. Formularze obu zaświadczeń zawarte są w załącznikach I i II do rozporządzenia; muszą one zostać przetłumaczone na jeden z języków urzędowych państwa członkowskiego, w którym zlokalizowany jest adresat. Usługodawca może zadeklarować przyjmowanie nakazów również w innych językach urzędowych Unii Europejskiej. Celem zaświadczeń jest przekazanie adresatowi wszelkich niezbędnych informacji w standardowym formacie ograniczającym źródła błędów, umożliwienie łatwej identyfikacji danych i unikanie w największym możliwym stopniu tekstu dowolnego, co pozwala na obniżenie kosztów tłumaczenia. Pełne uzasadnienie wraz z przesłankami dotyczącym konieczności i proporcjonalności lub pozostałymi informacjami dotyczącymi sprawy nie są uwzględniane w zaświadczeniu, ponieważ mogłoby to zagrozić postępowaniu przygotowawczemu. Jest ono zatem potrzebne tylko w ramach samego nakazu, aby umożliwić podejrzanemu późniejsze podważenie nakazu w postępowaniu karnym.

Niektórzy usługodawcy wprowadzili już platformy służące do przekazywania wniosków przez organy ścigania. Korzystanie z tych platform nie będzie zabronione na podstawie rozporządzenia, ponieważ mają one wiele zalet, w tym oferują możliwość prostego uwierzytelnienia oraz bezpieczne przekazywanie danych. Platformy tego rodzaju muszą jednak umożliwiać przekazywanie zaświadczenia europejskiego nakazu wydania danych i zaświadczenia europejskiego nakazu zabezpieczenia dowodów w formacie przewidzianym w załącznikach I i II bez konieczności podawania dodatkowych danych dotyczących nakazu.

Platformy ustanowione przez organy państw członkowskich lub organy unijne mogą również zapewniać bezpieczne środki przekazywania danych oraz ułatwiać uwierzytelnienie nakazów i gromadzenie danych statystycznych. Należy wziąć pod uwagę potencjalne rozszerzenie platform eCodex i SIRIUS oraz uzupełnienie ich o bezpieczne połączenie z usługodawcami do celów przekazywania zaświadczeń europejskiego nakazu wydania danych i zaświadczeń europejskiego nakazu zabezpieczenia dowodów i, w stosownych przypadkach, udzielania odpowiedzi przez usługodawców.

Artykuł 9: Wykonanie zaświadczenia europejskiego nakazu wydania danych

W art. 9 nałożono na adresatów obowiązek udzielenia odpowiedzi na zaświadczenie europejskiego nakazu wydania danych i wprowadzono obowiązkowe terminy. Normalny termin na udzielenie odpowiedzi wynosi 10 dni, natomiast organy mogą wyznaczyć krótszy termin, jeżeli jest to uzasadnione. W sytuacjach nadzwyczajnych zdefiniowanych jako sytuacje, w których występuje bezpośrednie zagrożenie dla życia lub integralności cielesnej osoby lub dla infrastruktury krytycznej, termin ten wynosi 6 godzin.

Przepis ten zapewnia również możliwość dialogu pomiędzy adresatem a organem wydającym. Jeżeli zaświadczenie europejskiego nakazu wydania danych jest niekompletne, ewidentnie

błędnie wypełnione lub nie dostarcza usługodawcy wystarczających informacji do tego, aby mógł on je wykonać, w celu uzyskania wyjaśnień adresat powinien skontaktować się z organem wydającym przy użyciu załącznika III. Ponadto adresat powinien poinformować organ wydający w przypadkach, w których nie może przekazać danych ze względu na siłę wyższą lub faktyczną niemożliwość. Ma to miejsce na przykład wówczas, gdy osoba, której dane są objęte nakazem, nie jest usługobiorcą odnośnej usługi albo – na przykład ze względu na inne zobowiązania w zakresie ochrony prywatności – jej dane zostały zgodnie z prawem usunięte przez usługodawcę, zanim on lub jego przedstawiciel prawny otrzymali nakaz. Organ wydający musi mieć świadomość tych okoliczności, aby szybko zareagować, na przykład pozyskując elektroniczny materiał dowodowy od innego usługodawcy; ponadto pozwala to zapobiec wszczęciu przez organ wydający postępowania przymuszającego do wykonania nakazu w sytuacji, w której jest to bezprzedmiotowe.

Jeżeli adresat w ogóle nie przekaze informacji lub jeżeli nie przekaze ich w sposób wyczerpujący lub terminowy z innych powodów niż wymienione powyżej, musi poinformować organ wydający o tych powodach w formularzu zawartym w załączniku III. Kontaktując się z organem wydającym, adresaci mogą zatem podnosić wszelkie kwestie związane z wykonaniem zaświadczenia europejskiego nakazu wydania danych. Umożliwia to organowi wydającemu skorygowanie lub ponowne rozważenie zaświadczenia europejskiego nakazu wydania danych na wczesnym etapie, przed postępowaniem przymuszającym do wykonania.

Jeżeli dane nie zostaną przedstawione bezzwłocznie, w szczególności jeżeli uruchomiono dialog pomiędzy adresatem a organem wydającym i terminy przewidziane w art. 9 ust. 1 nie zostaną dotrzymane, po otrzymaniu zaświadczenia europejskiego nakazu wydania danych usługodawca ma obowiązek zabezpieczyć dane, aby uniknąć ich utraty, jeżeli można je zidentyfikować. Zabezpieczenie może dotyczyć wyjaśnionego zaświadczenia europejskiego nakazu wydania danych lub następującej potem procedury wzajemnej pomocy prawnej lub europejskiego nakazu dochodzeniowego przekazanego w miejsce pierwotnego zaświadczenia europejskiego nakazu wydania danych.

Artykuł 10: Wykonanie zaświadczenia europejskiego nakazu zabezpieczenia dowodów

Wykonanie zaświadczenia europejskiego nakazu zabezpieczenia dowodów wymaga zabezpieczenia danych dostępnych w momencie otrzymania nakazu. Usługodawcy powinni zabezpieczyć dane na taki okres, jaki jest konieczny, aby wydać dane na żądanie, pod warunkiem że w terminie 60 dni od wydania nakazu organ wydający potwierdzi, że wystąpił z wnioskiem o wydanie danych. Wymaga to podjęcia co najmniej pewnych oficjalnych kroków, na przykład przesłania wniosku o wzajemną pomoc prawną do przetłumaczenia.

Z drugiej strony wnioski o zabezpieczenie dowodów powinny być wydawane lub utrzymywane tylko przez taki okres, jaki jest konieczny, aby umożliwić wystąpienie z żądaniem wydania tych danych. Aby uniknąć niepotrzebnego lub zbyt długiego zabezpieczenia danych, organ, który wydał europejski nakaz zabezpieczenia dowodów, informuje adresata bezzwłocznie po podjęciu decyzji o wstrzymaniu się od wydania lub uchyleniu nakazu wydania dowodów lub wniosku o współpracę wymiarów sprawiedliwości.

Przepis ten przewiduje również możliwość dialogu pomiędzy adresatem a organem wydającym, podobnie jak przepisy zawarte w art. 9. Jeżeli zaświadczenie europejskiego nakazu zabezpieczenia dowodów jest niekompletne, ewidentnie błędnie wypełnione lub nie dostarcza usługodawcy wystarczających informacji do tego, aby mógł on je wykonać, w celu

uzyskania wyjaśnień adresat powinien skontaktować się z organem wydającym przy użyciu załącznika III. Ponadto adresat powinien poinformować organ wydający w przypadkach, w których nie może przekazać danych ze względu na okoliczności uznawane za siłę wyższą lub ze względu na faktyczną niemożliwość, lub inne powody.

Artykuł 11: Poufność i informowanie użytkowników

Poufność trwającego postępowania przygotowawczego, w tym faktu wydania nakazu w celu uzyskania określonych danych, podlega ochronie. Niniejszy artykuł jest inspirowany art. 19 dyrektywy w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych. Przewiduje on obowiązek adresata oraz, jeżeli jest to inny podmiot, usługodawcy w zakresie ochrony poufności zaświadczenia europejskiego nakazu wydania danych lub zaświadczenia europejskiego nakazu zabezpieczenia dowodów, w szczególności przez powstrzymanie się od informowania osoby, której dane są objęte nakazem, jeżeli zażąda tego organ wydający, w celu zabezpieczenia postępowania przygotowawczego zgodnie z art. 23 ogólnego rozporządzenia o ochronie danych.

Z drugiej strony poinformowanie osoby, której dane mają być pozyskane, ma istotne znaczenie, w tym w zakresie wykonania prawa do wniesienia środka ochrony prawnej. Jeżeli na żądanie organu wydającego nie uczyni tego usługodawca, organ wydający poinformuje tę osobę zgodnie z art. 13 dyrektywy o ochronie danych osobowych skierowanej do policji i organów wymiaru sprawiedliwości, kiedy nie będzie już występować ryzyko zaszkodzenia postępowaniu przygotowawczemu. Informacja ta dotyczyć będzie również dostępnych środków ochrony prawnej. Ponieważ ingerencja w prawa jest w przypadku europejskiego nakazu zabezpieczenia dowodów mniejsza, informacje te nie są przekazywane w związku z takim nakazem, lecz jedynie w przypadku europejskich nakazów wydania dowodów.

Artykuł 12: Zwrot kosztów

Jeżeli przepisy prawa krajowego państwa wydającego przewidują takie rozwiązanie w odniesieniu do krajowych nakazów w podobnych sprawach krajowych, usługodawcy mogą również domagać się od państwa wydającego zwrotu poniesionych przez siebie kosztów zgodnie z prawem krajowym państwa wydającego. Zapewnia to równe traktowanie usługodawców, do których kierowany jest nakaz krajowy, oraz usługodawców, do których kierowany jest zaświadczenie europejskiego nakazu wydania dowodów, przez to samo państwo członkowskie, jeżeli państwo to podjęło decyzję o zwrocie kosztów na rzecz pewnych usługodawców. Z drugiej strony proponowane rozporządzenie nie przewiduje harmonizacji zwrotu kosztów, ponieważ państwa członkowskie podjęły w tym zakresie rozbieżne decyzje.

O zwrot kosztów może wystąpić bezpośrednio usługodawca lub jego przedstawiciel prawny. Koszty mogą zostać zwrócone jedynie raz.

Rozdział 3: Sankcje i postępowanie przymuszające do wykonania nakazu

Artykuł 13: Sankcje

Państwa członkowskie powinny zagwarantować istnienie skutecznych, proporcjonalnych i odstraszających grzywien, które mogą być stosowane w przypadku niewywiązywania się przez usługodawców z obowiązków przewidzianych w art. 9, 10 lub 11. Powinny one pozostawać bez uszczerbku dla przepisów krajowych przewidujących nałożenie sankcji karnych w takich sytuacjach.

Artykuł 14: Postępowanie przymuszające do wykonania nakazu

W przypadku niewywiązania się z obowiązków art. 14 przewiduje postępowanie przymuszające do wykonania nakazu z pomocą państwa członkowskiego, w którym zlokalizowany jest adresat przekazanego zaświadczenia. W zależności od pierwotnego adresata będzie to państwo członkowskie usługodawcy lub przedstawiciela prawnego. Wraz z pełnym nakazem zawierającym uzasadnienie dotyczące konieczności i proporcjonalności organ wydający przekazuje zaświadczenie właściwemu organowi państwa wykonującego, a ten ostatni wszczyna postępowanie przymuszające do wykonania nakazu zgodnie z przepisami prawa krajowego, z wykorzystaniem w razie potrzeby sankcji, o których mowa w art. 13. Jeżeli nakaz przekazuje się do wykonania państwu wykonującemu, organ przymuszający do wykonania może podjąć decyzję o nieuznaniu lub niewykonaniu nakazu, jeżeli po jego otrzymaniu oraz po konsultacji z organem wydającym stwierdzi, że mają zastosowanie jakiekolwiek ściśle określone przesłanki wniesienia sprzeciwu. Dodatkowo, w przypadku wszczęcia postępowania przymuszającego do wykonania nakazu, osoba, której nakaz dotyczy, będzie mogła we własnym zakresie wnieść sprzeciw wobec nakazu do organu przymuszającego do wykonania. Adresat może wnieść sprzeciw na podstawie jakiejkolwiek z tych przesłanek z wyłączeniem immunitetów i przywilejów, ale z uwzględnieniem przypadków, w których jest oczywiste, że nakaz nie został wydany lub zatwierdzony przez właściwy organ lub zastosowanie się do niego stanowiłoby jawne pogwałcenie Karty praw podstawowych Unii Europejskiej lub miałoby wyraźnie charakter nadużycia. Przykładowo nakaz przedstawienia danych dotyczący treści związanych z nieokreśloną grupą osób na danym obszarze geograficznym lub bez związku z konkretnym procesem sądowym stanowiłby oczywiste nieuwzględnienie warunków wydania europejskiego nakazu wydania dowodów przewidzianych w niniejszym rozporządzeniu, co byłoby już jasne z treści samego zaświadczenia. Na pozostałe przesłanki może się powołać wyłącznie osoba, której dane są objęte nakazem, w środkach ochrony prawnej przysługujących jej w państwie wydającym (zob. art. 17 poniżej). Dodatkowo usługodawcom przysługuje środek odwoławczy wobec decyzji organu egzekwowania prawa nakładającej na nich karę.

Aby uniknąć dalszych opóźnień, w toku postępowania przymuszającego do wykonania nakazu przewidziano kilka terminów dla organu przymuszającego do wykonania nakazu i organu wydającego.

Rozdział 4: Środki ochrony prawnej

Artykuły 15 i 16: Postępowanie odwoławcze w przypadku konfliktu obowiązków wynikających z przepisów państwa trzeciego

Art. 15 i 16 przewidują postępowanie odwoławcze na wypadek sytuacji, w której usługodawcy posiadający zakład w państwach trzecich muszą sprostać sprzecznym ze sobą obowiązkom. Przepisy te są również szczególnie istotne dla zapewnienia ochrony praw indywidualnych oraz międzynarodowej wzajemności. Dzięki ustanowionemu wysokiemu standardowi mają one zachęcać państwa trzecie do zapewnienia podobnego poziomu ochrony. W sytuacji odwrotnej, kiedy organy państwa trzeciego chcą uzyskać informacje o obywatelu UE od europejskiego dostawcy usług, przepisy prawa unijnego lub przepisy prawa państwa członkowskiego chroniące prawa podstawowe, takie jak dorobek prawny w dziedzinie ochrony danych, mogą w podobny sposób zapobiec ujawnieniu. Unia Europejska oczekuje od państw trzecich przestrzegania takich zakazów w taki sam sposób, jak przewidziano to w niniejszym rozporządzeniu w odniesieniu do państw trzecich.

Procedurę opisaną w art. 15 może wszcząć adresat, jeżeli uczynienie zadość europejskiemu nakazowi wydania dowodów skutkowałoby naruszeniem przepisów prawa państwa trzeciego, zgodnie z którymi ujawnienie tych danych jest zabronione z uwagi na konieczność ochrony podstawowych praw zainteresowanych osób lub podstawowych interesów państwa trzeciego związanych z bezpieczeństwem narodowym lub obronnością. Adresat ma obowiązek wnieść uzasadniony sprzeciw, w którym poinformuje organ wydający o przesłankach, na podstawie których uznał, że istnieją sprzeczne ze sobą obowiązki. Uzasadniony sprzeciw nie może być oparty wyłącznie na fakcie, że podobne przepisy nie istnieją w państwie trzecim, lub jedynie na okoliczności przechowywania odnośnych danych w państwie trzecim. Uzasadniony sprzeciw wnosi się na podstawie procedury przewidzianej w art. 9 ust. 5 w odniesieniu do powiadomienia o zamiarze niezastosowania się do nakazu, przy użyciu formularza zawartego w załączniku III.

Na podstawie uzasadnionego sprzeciwu organ wydający dokonuje kontroli wydanego przez siebie nakazu. Jeżeli organ wydający podejmie decyzję o uchyleniu nakazu, postępowanie ulega zakończeniu. Jeżeli organ wydający ma zamiar utrzymać nakaz w mocy, sprawa jest przekazywana do właściwego sądu jego państwa członkowskiego. Sąd ten dokonuje oceny, na podstawie uzasadnionego sprzeciwu oraz z uwzględnieniem wszystkich istotnych okoliczności, czy prawo państwa trzeciego ma zastosowanie do rozpatrywanej sprawy oraz – jeżeli ma zastosowanie – czy w rozpatrywanej sprawie istnieją sprzeczne ze sobą obowiązki. Przeprowadzając tę ocenę, sąd powinien wziąć pod uwagę, czy przepisy prawa państwa trzeciego w oczywisty sposób nie mają na celu ochrony innych interesów niż prawa podstawowe lub podstawowe interesy państwa trzeciego związane z bezpieczeństwem narodowym lub obronnością lub czy nie mają na celu ochrony nielegalnych działań przed wnioskami organów ścigania dotyczącymi postępowania przygotowawczego.

Jeżeli sąd ustali, że konflikt z obowiązkami wynikającym z przepisów prawa chroniących prawa podstawowe osób fizycznych lub podstawowe interesy państwa trzeciego związane z bezpieczeństwem narodowym lub obronnością faktycznie występuje, sąd musi wystąpić o opinię do właściwego państwa trzeciego za pośrednictwem krajowych organów centralnych tego państwa trzeciego. Jeżeli po konsultacji państwo trzecie potwierdzi występowanie konfliktu i sprzeciwi się wykonaniu nakazu, sąd ma obowiązek uchylić nakaz.

Jeżeli konflikt wynika z innych przepisów prawa państwa trzeciego, których celem nie jest ochrona praw podstawowych osób fizycznych ani podstawowych interesów państwa trzeciego związanych z bezpieczeństwem narodowym lub obronnością, po uważnym rozważeniu wszystkich wchodzących w grę interesów sąd podejmuje decyzję o utrzymaniu w mocy nakazu lub jego uchyleniu.

Warunki określone w art. 9, w szczególności obowiązki w zakresie zabezpieczenia przewidziane w art. 9 ust. 6, mają również zastosowanie w sytuacjach, w których konflikt obowiązków wynika z przepisów prawa państwa trzeciego. Jeżeli sąd uzna, że nakaz ma być utrzymany w mocy, organ wydający i usługodawca zostaną o tym poinformowani, aby mogli przystąpić do jego wykonania. Jeżeli nakaz zostanie uchylony, możliwe jest wydanie odrębnego europejskiego nakazu zabezpieczenia dowodów, aby zapewnić dostępność danych, jeżeli można je pozyskać na podstawie wniosku w ramach wzajemnej pomocy prawnej.

Ponieważ sam europejski nakaz zabezpieczenia dowodów nie prowadzi do ujawnienia danych i w związku z tym nie budzi podobnych wątpliwości, postępowanie odwoławcze ogranicza się do europejskiego nakazu wydania dowodów.

Artykuł 17: Skuteczne środki ochrony prawnej

Ten przepis gwarantuje, że osoby, których dotyczy europejski nakaz wydania danych, mogą skorzystać ze skutecznych środków ochrony prawnej. Ze wspomnianych środków ochrony prawnej korzysta się w państwie wydającym zgodnie z prawem krajowym. Oskarżeni i podejrzani korzystają zazwyczaj ze środków ochrony prawnej w toku postępowania karnego. W odniesieniu do europejskiego nakazu zabezpieczenia dowodów nie umożliwiono wnoszenia szczególnych środków ochrony prawnej, jako że nakaz ten sam w sobie nie umożliwia ujawnienia danych, jeżeli nie zastosuje się po nim europejskiego nakazu wydania dowodów lub innego instrumentu prowadzącego do ujawnienia danych, co stanowi wówczas podstawę do skorzystania z konkretnych środków ochrony prawnej.

Osoby niebędące podejrzanymi lub oskarżonymi w procesie karnym, których dane zostały objęte nakazem, również mają prawo skorzystać ze środka ochrony prawnej w państwie wydającym. Wszystkie te prawa pozostają bez uszczerbku dla wszelkich środków ochrony prawnej dostępnych na podstawie dyrektywy o ochronie danych osobowych skierowanej do policji i organów wymiaru sprawiedliwości oraz ogólnego rozporządzenia o ochronie danych.

W odróżnieniu od przepisów dotyczących usługodawców niniejsze rozporządzenie nie ogranicza możliwych przesłanek podważenia legalności nakazu, z których mogą skorzystać wszystkie te osoby. Przesłanki te obejmują konieczność i proporcjonalność nakazu.

Skorzystanie ze środków ochrony prawnej w państwie wydającym nie obciąża zainteresowanych osób w sposób nieproporcjonalny. Tak jak w przypadku nakazów wykonywanych przy użyciu innych form współpracy wymiarów sprawiedliwości, sądy w państwie wydającym są najwłaściwszymi organami do przeprowadzenia kontroli legalności europejskiego nakazu wydania dowodów wydanego przez ich własne organy oraz oceny zgodności z ich własnym prawem krajowym. Na etapie przymuszania do wykonania nakazu adresaci mogą ponadto zgłaszać odrębne sprzeciwy wobec wykonania zaświadczenia europejskiego nakazu wydania dowodów lub zaświadczenia europejskiego nakazu zabezpieczenia dowodów w przyjmującym państwie członkowskim na podstawie przesłanek, których lista zawarta jest w rozporządzeniu (zob. art. 14 powyżej).

Artykuł 18: Zapewnienie przywilejów i immunitetów na podstawie prawa państwa wykonującego

Tak samo jak art. 5 ust. 7, przepis ten ma na celu zapewnienie, by immunitety i przywileje chroniące dane objęte nakazem w państwie członkowskim usługodawcy zostały uwzględnione w państwie wydającym – w szczególności w przypadku różnic pomiędzy tymi państwami członkowskimi – podobnie jak podstawowe interesy państwa członkowskiego usługodawcy, takie jak interesy związane z bezpieczeństwem narodowym i obronnością. Art. 18 stanowi, że sąd w państwie wydającym musi wziąć je pod uwagę w taki sam sposób, jak gdyby były przewidziane w prawie krajowym jego państwa członkowskiego. Ze względu na różnice między państwami członkowskimi pojawiające się przy dokonywaniu oceny odpowiedniości i dopuszczalności materiału dowodowego, w przepisie tym pozostawiono miejsce na pewną elastyczność działania sądów co do sposobu ich uwzględnienia.

Rozdział 5: Przepisy końcowe

Artykuł 19: Monitorowanie i sprawozdawczość

Artykuł ten wymaga od państw członkowskich przekazywania Komisji określonych informacji dotyczących stosowania rozporządzenia, aby mogła ona wykonać swoje obowiązki na podstawie art. 24. Komisja ustanowi szczegółowy program monitorowania wyników, rezultatów i skutków rozporządzenia.

Artykuł 20: Zmiany zaświadczeń i formularzy

Zaświadczenia i formularze zawarte w załącznikach I, II i III niniejszego wniosku ułatwią wykonanie zaświadczenia europejskiego nakazu wydania dowodów i zaświadczenia europejskiego nakazu zabezpieczenia dowodów. Z tego powodu niezbędne jest zapewnienie, aby w razie potrzeby w przyszłości możliwe było jak najszybsze poprawienie treści zaświadczenia i formularza. Zmiany w tych trzech załącznikach z wykorzystaniem zwykłej procedury ustawodawczej nie spełniają tego wymogu, a załączniki te stanowią elementy inne niż istotne aktów ustawodawczych. Podstawowe elementy zdefiniowano w art. 8. W art. 20 określono zatem szybszą i bardziej elastyczną procedurę wprowadzania zmian w drodze aktów delegowanych.

Artykuł 21: Wykonywanie przekazanych uprawnień

W artykule tym określono warunki dotyczące wykonywania przez Komisję uprawnień do przyjmowania aktów delegowanych w celu wprowadzenia koniecznych zmian do zaświadczenia i formularzy załączonych do wniosku. Określono w nim standardową procedurę przyjmowania takich aktów delegowanych.

Artykuł 22: Powiadomienia

Od państw członkowskich wymaga się powiadomienia Komisji o właściwych organach wydających i wykonujących oraz sądach właściwych do rozstrzygania uzasadnionych sprzeciwów usługodawców w przypadku kolizji przepisów.

Artykuł 23: Związek z europejskim nakazem dochodzeniowym

W tym przepisie wyjaśniono, że rozporządzenie nie uniemożliwia organom państw członkowskich wydawania europejskich nakazów dochodzeniowych zgodnie z dyrektywą 2014/41/UE w celu uzyskania elektronicznego materiału dowodowego.

Artykuł 24: Ocena

Przepis ten przewiduje, że Komisja przeprowadzi ocenę rozporządzenia zgodnie z wytycznymi Komisji w sprawie lepszego stanowienia prawa oraz na podstawie pkt 22 porozumienia międzyinstytucjonalnego z 13 kwietnia 2016 r.²⁵. W terminie 5 lat po wejściu w życie proponowanego rozporządzenia Komisja przedstawi Parlamentowi Europejskiemu i Radzie ustalenia pochodzące z oceny, w tym ocenę potrzeby rozszerzenia zakresu rozporządzenia o nieuwzględnione w nim dotąd usługi, które mogą się okazać bardziej właściwe dla dochodzeń.

Artykuł 25: Wejście w życie

Proponowane rozporządzenie wejdzie w życie dwudziestego dnia po jego opublikowaniu w Dzienniku Urzędowym. Rozporządzenie będzie się stosować po upływie okresu 6 miesięcy od jego wejścia w życie.

²⁵ Porozumienie międzyinstytucjonalne pomiędzy Parlamentem Europejskim, Radą Unii Europejskiej a Komisją Europejską w sprawie lepszego stanowienia prawa z dnia 13 kwietnia 2016 r.: Dz.U. L 123 z 12.5.2016, s. 1–14.

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY**w sprawie europejskiego nakazu wydania dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych i europejskiego nakazu zabezpieczenia dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych**

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 82 ust. 1,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego²⁶,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

- (1) Unia postawiła sobie za cel utrzymanie i rozwój przestrzeni wolności, bezpieczeństwa i sprawiedliwości. W celu stopniowego ustanowienia tej przestrzeni Unia przyjmie środki związane ze współpracą wymiarów sprawiedliwości w sprawach karnych w oparciu o zasadę wzajemnego uznawania wyroków i orzeczeń sądowych, która od posiedzenia Rady Europejskiej w Tampere w dniach 15 i 16 października 1999 r. jest powszechnie uważana za kamień milowy współpracy wymiarów sprawiedliwości w sprawach karnych w Unii.
- (2) Środki mające na celu pozyskanie i zabezpieczenie elektronicznego materiału dowodowego mają coraz większe znaczenie dla zapewnienia możliwości przeprowadzania dochodzeń i ścigania przestępstw w całej Unii. Skuteczne mechanizmy pozyskiwania elektronicznego materiału dowodowego mają kluczowe znaczenie dla zwalczania przestępczości, z zastrzeżeniem warunków mających na celu zapewnienie pełnej zgodności z prawami podstawowymi i zasadami uznanymi w Karcie praw podstawowych Unii Europejskiej zapisanymi w traktatach, w szczególności zasadami konieczności i proporcjonalności, sprawiedliwości proceduralnej, ochrony danych, poufności korespondencji i prywatności.
- (3) We wspólnym oświadczeniu unijnych ministrów sprawiedliwości i spraw wewnętrznych oraz przedstawicieli instytucji UE z dnia 22 marca 2016 r. w sprawie ataków terrorystycznych w Brukseli podkreślono potrzebę, nadając jej charakter priorytetowy, znalezienia sposobów szybszego i skuteczniejszego zabezpieczania i pozyskiwania elektronicznego materiału dowodowego oraz określenia konkretnych środków mających na celu zaradzenie tej kwestii.

²⁶ Dz.U. C [...], [...], s. [...].

- (4) W konkluzjach Rady z dnia 9 czerwca 2016 r. podkreślono rosnące znaczenie elektronicznego materiału dowodowego w procesach karnych oraz ochrony cyberprzestrzeni przed nadużyciami i działalnością przestępczą dla gospodarek i społeczeństw, a zatem potrzebę dysponowania przez organy ścigania i organy sądowe skutecznymi narzędziami badania i ścigania przestępstw związanych z cyberprzestrzenią.
- (5) We wspólnym komunikacie „Odporność, prewencja, obrona” z dnia 13 września 2017 r.²⁷ Komisja podkreśliła, że skuteczne badanie i ściganie przestępczości wykorzystującej cyberprzestrzeń stanowi kluczowy środek odstraszający wobec cyberataków oraz że obecne przepisy procesowe należałoby lepiej dostosować do epoki internetu. Obecne procedury niekiedy nie pozwalają mierzyć się z szybkością cyberataków, co powoduje, że sprawna współpraca transgraniczna jest szczególnie potrzebna.
- (6) Parlament Europejski przywołał te zastrzeżenia w swoim rozporządzeniu w sprawie walki z cyberprzestępczością z dnia 3 października 2017 r.²⁸, podkreślając wyzwania, które obecne rozdrobione ramy prawne mogą stwarzać dla usługodawców starających się spełniać żądania organów ścigania, i wezwał Komisję do przedstawienia unijnych ram prawnych dotyczących elektronicznego materiału dowodowego, przewidujących wystarczające zabezpieczenia dla praw i wolności wszystkich zainteresowanych stron.
- (7) Usługi oparte na sieci można świadczyć z dowolnej lokalizacji i nie wymagają one fizycznej infrastruktury, pomieszczeń ani pracowników w danym kraju. Prowadzi to do sytuacji, w których odpowiedni materiał dowodowy jest często przechowywany poza państwem prowadzącym postępowanie przygotowawcze lub przez usługodawcę posiadającego zakład poza tym państwem. Pomiędzy sprawą badaną w postępowaniu przygotowawczym w zainteresowanym państwie a państwem, w którym przechowywany jest materiał dowodowy lub w którym usługodawca ma główny zakład, często nie występuje inny związek.
- (8) Ze względu na ten brak związku wnioski w ramach współpracy wymiarów sprawiedliwości są często kierowane do państw, w których zlokalizowana jest znaczna liczba usługodawców, a które to państwa nie pozostają w innej relacji do rozpatrywanej sprawy. Ponadto liczba wniosków znacznie się zwiększyła ze względu na rosnące wykorzystanie usług sieciowych, które z natury są wolne od granic. W rezultacie pozyskanie elektronicznego materiału dowodowego z wykorzystaniem kanałów współpracy wymiarów sprawiedliwości często zabiera wiele czasu – zbyt wiele, aby ślady przestępstw pozostały dostępne. Co więcej, nie istnieją jasne ramy współpracy z usługodawcami, przy czym niektórzy usługodawcy z państw trzecich przyjmują bezpośrednio wnioski o dane nie dotyczące treści zgodnie z obowiązującymi w ich państwie przepisami prawa krajowego. W związku z powyższym wszystkie państwa członkowskie korzystają z kanału współpracy z usługodawcami, jeżeli jest on dostępny, wykorzystując różne krajowe narzędzia, warunki i procedury. Dodatkowo, w przypadku danych dotyczących treści, niektóre państwa członkowskie podjęły jednostronne działania, podczas gdy inne nadal korzystają ze współpracy wymiarów sprawiedliwości.
- (9) Rozdrobione ramy prawne stwarzają wyzwania dla usługodawców starających się stosować do wniosków organów ścigania. Istnieje zatem potrzeba zaproponowania

²⁷ JOIN(2017) 450 final.

²⁸ 2017/2068(INI).

europijskich ram prawnych dotyczących elektronicznego materiału dowodowego, aby w niniejszym instrumencie nałożyć na usługodawców obowiązek odpowiadania bezpośrednio organom ścigania bez angażowania organów sądowych w państwie członkowskim usługodawcy.

- (10) Nakazy wydawane na podstawie niniejszego rozporządzenia będą kierowane do przedstawicieli prawnych usługodawców wyznaczonych do tego celu. Jeżeli usługodawca posiadający zakład w Unii nie wyznaczył przedstawiciela prawnego, nakazy mogą być kierowane do dowolnego zakładu tego usługodawcy w Unii. Ten wariant rezerwowy ma na celu zapewnienie skuteczności systemu, jeżeli usługodawca nie wyznaczył (jeszcze) specjalnego przedstawiciela.
- (11) Mechanizm europejskiego nakazu wydania elektronicznego materiału dowodowego w sprawach karnych i europejskiego nakazu jego zabezpieczenia może działać wyłącznie w oparciu o wysokie standardy wzajemnego zaufania pomiędzy państwami członkowskimi, które stanowią kluczowy warunek konieczny prawidłowego funkcjonowania niniejszego instrumentu.
- (12) Niniejsze rozporządzenie nie narusza praw podstawowych i jest zgodne z zasadami uznanymi w szczególności w Karcie praw podstawowych Unii Europejskiej. Powyższe obejmuje prawo do wolności i bezpieczeństwa osobistego, poszanowanie życia prywatnego i rodzinnego, ochronę danych osobowych, wolność prowadzenia działalności gospodarczej, prawo do posiadania własności, prawo do skutecznego środka ochrony prawnej i dostępu do bezstronnego sądu, domniemanie niewinności, prawo do obrony, zasady legalności oraz proporcjonalności, a także prawo do niebycia sądzonym lub podlegania karze dwukrotnie w tym samym procesie karnym za to samo przestępstwo. Jeżeli państwo członkowskie dysponuje wyraźnymi przesłankami, że w innym państwie członkowskim może się toczyć równoległy proces karny, konsultuje się z organami tego państwa członkowskiego zgodnie z decyzją ramową Rady 2009/948/WSiSW²⁹.
- (13) W celu zagwarantowania pełnego poszanowania praw podstawowych w niniejszym rozporządzeniu zawarto wyraźne odwołanie do niezbędnych norm dotyczących pozyskiwania danych osobowych, przetwarzania takich danych, kontroli sądowej podejmowania przewidzianych w niniejszym instrumencie czynności w toku postępowania przygotowawczego oraz dostępnych środków ochrony prawnej.
- (14) Niniejsze rozporządzenie stosuje się bez uszczerbku dla praw procesowych w postępowaniu karnym określonych w dyrektywach 2010/64/UE³⁰, 2012/13/UE³¹, 2013/48/UE³², 2016/343³³, 2016/800³⁴ i 2016/1919³⁵ Parlamentu Europejskiego i Rady.

²⁹ [Decyzja ramowa Rady 2009/948/WSiSW](#) z dnia 30 listopada 2009 r. w sprawie zapobiegania konfliktom jurysdykcji w postępowaniu karnym i w sprawie rozstrzygania takich konfliktów (Dz.U. L 328 z 15.12.2009, s. 42).

³⁰ [Dyrektywa Parlamentu Europejskiego i Rady 2010/64/UE](#) z dnia 20 października 2010 r. w sprawie prawa do tłumaczenia ustnego i tłumaczenia pisemnego w postępowaniu karnym (Dz.U. L 280 z 26.10.2010, s. 1).

³¹ [Dyrektywa Parlamentu Europejskiego i Rady 2012/13/UE](#) z dnia 22 maja 2012 r. w sprawie prawa do informacji w postępowaniu karnym (Dz.U. L 142 z 1.6.2012, s. 1).

³² [Dyrektywa Parlamentu Europejskiego i Rady 2013/48/UE](#) z dnia 22 października 2013 r. w sprawie prawa dostępu do adwokata w postępowaniu karnym i w postępowaniu dotyczącym europejskiego nakazu aresztowania oraz w sprawie prawa do poinformowania osoby trzeciej o pozbawieniu wolności

- (15) W niniejszym instrumencie przedstawiono zasady, na podstawie których właściwy organ sądowy w Unii Europejskiej może nakazać usługodawcy oferującemu usługi w Unii, na podstawie europejskiego nakazu wydania dowodów lub europejskiego nakazu zabezpieczenia dowodów, wydanie lub zabezpieczenie elektronicznego materiału dowodowego. Niniejsze rozporządzenie ma zastosowanie we wszystkich przypadkach, w których usługodawca posiada zakład lub przedstawicielstwo w innym państwie członkowskim. W sytuacjach krajowych, w których wykorzystanie instrumentów przewidzianych w niniejszym rozporządzeniu nie jest możliwe, rozporządzenie nie powinno ograniczać uprawnień właściwych organów krajowych przewidzianych w prawie krajowym w zakresie przymuszania usługodawców posiadających zakład lub przedstawicielstwo na ich terytorium.
- (16) Usługodawcy o największym znaczeniu dla procesu karnego to dostawcy usług łączności elektronicznej oraz konkretni dostawcy usług społeczeństwa informacyjnego ułatwiający interakcje między użytkownikami. Dlatego też obie grupy należy objąć zakresem niniejszego rozporządzenia. Dostawców usług łączności elektronicznej zdefiniowano we wniosku dotyczącym dyrektywy ustanawiającej Europejski kodeks łączności elektronicznej. Obejmują one usługi umożliwiające komunikację międzyludzką, takie jak usługi telefonii internetowej (VoIP), komunikatory internetowe, usługi poczty elektronicznej przez internet. Kategorie usług społeczeństwa informacyjnego tutaj uwzględnione to kategorie, w przypadku których przechowywanie danych jest elementem definiującym usługę świadczoną użytkownikowi, i obejmują w szczególności portale społecznościowe w zakresie, w jakim nie kwalifikują się one jako usługi łączności elektronicznej, usługi oferowane przez internetowe platformy handlowe umożliwiające transakcje pomiędzy ich użytkownikami (takimi jak konsumenci lub przedsiębiorstwa) oraz inne usługi hostingowe i usługi w zakresie nazw i numeracji domen, w tym w sytuacji, w której usługa jest zapewniana za pośrednictwem przetwarzania w chmurze. Usługi społeczeństwa informacyjnego, w przypadku których przechowywanie danych nie jest elementem definiującym usługę świadczoną użytkownikowi i w związku z tym ma jedynie charakter pomocniczy, w tym usługi prawne, architektoniczne, inżynierskie i rachunkowe świadczone przez internet na odległość, należy wyłączyć z zakresu niniejszego rozporządzenia nawet wówczas, gdy spełniają one definicję usług społeczeństwa informacyjnego zawartą w dyrektywie (UE) 2015/1535.
- (17) W wielu przypadkach dane nie są już przechowywane ani przetwarzane na urządzeniu użytkownika, lecz udostępniane w infrastrukturze opartej na technologii przetwarzania w chmurze, umożliwiającej dostęp z dowolnego miejsca. Aby świadczyć takie usługi, usługodawcy nie muszą posiadać zakładu ani serwerów w określonej jurysdykcji.

i prawa do porozumiewania się z osobami trzecimi i organami konsularnymi w czasie pozbawienia wolności (Dz.U. L 294 z 6.11.2013, s. 1).

³³ [Dyrektywa Parlamentu Europejskiego i Rady \(UE\) 2016/343](#) z dnia 9 marca 2016 r. w sprawie wzmocnienia niektórych aspektów domniemania niewinności i prawa do obecności na rozprawie w postępowaniu karnym (Dz.U. L 65 z 11.3.2016, s. 1).

³⁴ [Dyrektywa Parlamentu Europejskiego i Rady \(UE\) 2016/800](#) z dnia 11 maja 2016 r. w sprawie gwarancji procesowych dla dzieci będących podejrzanymi lub oskarżonymi w postępowaniu karnym (Dz.U. L 132 z 21.5.2016, s. 1).

³⁵ [Dyrektywa Parlamentu Europejskiego i Rady \(UE\) 2016/1919](#) z dnia 26 października 2016 r. w sprawie pomocy prawnej z urzędu dla podejrzanych i oskarżonych w postępowaniu karnym oraz dla osób, których dotyczy wniosek w postępowaniu dotyczącym europejskiego nakazu aresztowania (Dz.U. L 297 z 4.11.2016, s. 1).

Dlatego stosowanie rozporządzenia nie powinno zależeć od faktycznej lokalizacji zakładu usługodawcy ani faktycznej lokalizacji przetwarzania lub przechowywania danych.

- (18) Dostawcy usług w zakresie infrastruktury internetowej związanych z przypisywaniem nazw i numeracji, takich jak podmioty rejestrujące i rejestry oraz dostawcy usług prywatności i usług *proxy*, lub regionalne rejestry internetowe adresów IP, mają szczególne znaczenie dla identyfikacji osób lub podmiotów stojących za szkodliwymi stronami internetowymi lub stronami internetowymi, które przejęto do przestępczych celów. Przechowują one dane, które są szczególnie istotne dla postępowania karnego, ponieważ umożliwiają identyfikację osoby fizycznej lub podmiotu stojącego za stroną internetową wykorzystywaną w działalności przestępczej lub ofiary działalności przestępczej w przypadku stron internetowych przejętych przez przestępców.
- (19) Niniejsze rozporządzenie reguluje gromadzenie wyłącznie danych przechowywanych, to jest danych przechowywanych przez usługodawcę w momencie otrzymania zaświadczenia europejskiego nakazu wydania dowodów lub zaświadczenia europejskiego nakazu zabezpieczenia dowodów. Nie przewiduje ono ogólnego obowiązku zatrzymywania danych ani nie upoważnia do przechwytywania przechowywanych danych w przyszłości po otrzymaniu zaświadczenia nakazu wydania dowodów lub zaświadczenia nakazu zabezpieczenia dowodów. Dane należy udostępnić bez względu na to, czy są zaszyfrowane, czy nie.
- (20) Kategorie danych objęte zakresem niniejszego rozporządzenia obejmują dane abonenta, dane dostępu, dane dotyczące transakcji (te trzy kategorie danych nazywane są dalej „danymi niedotyczącymi treści”) oraz dane dotyczące treści. Powyższe rozróżnienie, nie licząc danych dostępu, istnieje w przepisach prawnych wielu państw członkowskich, a także w obecnym ramach prawnych Stanów Zjednoczonych, umożliwiającym usługodawcom dobrowolne udostępnianie danych niedotyczących treści zagranicznym organom ścigania.
- (21) Dane dostępu należy wyodrębnić jako szczególną kategorię danych używaną w niniejszym rozporządzeniu. Dane dostępu są pozyskiwane do tego samego celu, co dane abonenta, tj. w celu identyfikacji użytkownika, którego dotyczą, a poziom ingerencji w prawa podstawowe jest w ich przypadku podobny, co w przypadku danych abonenta. Dane dostępu są w typowej sytuacji utrwalane w ramach ewidencji zdarzeń (innymi słowy w dzienniku serwera) w celu wskazania rozpoczęcia i zakończenia sesji dostępu użytkownika do usługi. Często interfejs sieciowy wykorzystywany podczas sesji dostępu można wyodrębnić dzięki indywidualnemu adresowi IP (statycznemu lub dynamicznemu) lub innemu identyfikatorowi. Jeżeli użytkownik jest nieznany, często niezbędne jest uzyskanie tego identyfikatora przed uzyskaniem od usługodawcy danych abonenta z nim związanych.
- (22) Z drugiej strony dane dotyczące transakcji pozyskuje się zasadniczo w celu zdobycia informacji na temat kontaktów i miejsca pobytu użytkownika, przy czym mogą one posłużyć do sporządzenia profilu osoby fizycznej, której sprawa dotyczy. Zarazem dane dostępu nie mogą same w sobie posłużyć do podobnego celu, jako że na przykład nie zawierają żadnych informacji na temat rozmówców związanych z użytkownikiem. Stąd w niniejszym wniosku wprowadzono nową kategorię danych, którą należy traktować podobnie jak dane abonenta, jeżeli mają być one wykorzystane do podobnego celu.
- (23) Ponieważ wszystkie kategorie danych zawierają dane osobowe, są one objęte zabezpieczeniami przewidzianymi w dorobku prawnym Unii w dziedzinie ochrony

danych osobowych; skala wpływu na prawa podstawowe jest jednak różna – duża różnica występuje w szczególności pomiędzy danymi abonenta i danymi dostępu z jednej strony a danymi dotyczącymi transakcji i danymi dotyczącymi treści z drugiej. Podczas gdy dane abonenta i dane dostępu są przydatne do uzyskania pierwszych poszlak w postępowaniu przygotowawczym umożliwiających ustalenie tożsamości podejrzanego, dane dotyczące transakcji i dane dotyczące treści są najbardziej odpowiednim materiałem dowodowym. Zasadnicze znaczenie ma zatem objęcie niniejszym instrumentem wszystkich tych kategorii danych. Ze względu na różny stopień wpływu na prawa podstawowe w odniesieniu do pozyskiwania danych abonenta i danych dostępu z jednej strony, a danych dotyczących transakcji i danych dotyczących treści z drugiej, zastosowanie mają odmienne warunki.

- (24) Europejski nakaz wydania dowodów i europejski nakaz zabezpieczenia dowodów to środki dochodzeniowo-śledcze, które należy wydawać wyłącznie w toku konkretnego postępowania karnego w odniesieniu do określonych znanych lub jeszcze nieznanymi sprawców konkretnego przestępstwa, które miało miejsce, po przeprowadzeniu indywidualnej oceny proporcjonalności i konieczności w każdym indywidualnym przypadku.
- (25) Niniejsze rozporządzenie pozostaje bez uszczerbku dla uprawnień dochodzeniowo-śledczych organów w postępowaniu cywilnym lub karnym, również w sytuacji, gdy takie procesy mogą prowadzić do nałożenia sankcji.
- (26) Niniejsze rozporządzenie powinno mieć zastosowanie wobec usługodawców oferujących usługi w Unii, a nakazy w nim przewidziane mogą być wydawane wyłącznie w odniesieniu do danych dotyczących usług oferowanych w Unii. Usługi oferowane wyłącznie poza Unią nie są objęte zakresem niniejszego rozporządzenia, nawet jeżeli usługodawca je oferujący posiada zakład w Unii.
- (27) Ustalenie, czy usługodawca oferuje usługi w Unii, wymaga przeprowadzenia oceny, czy usługodawca umożliwia osobom prawnym lub fizycznym korzystanie ze swoich usług w co najmniej jednym państwie członkowskim. Niemniej sama dostępność interfejsu internetowego – na przykład dostępności strony internetowej usługodawcy lub pośrednika, lub adresu e-mail lub innych danych kontaktowych w co najmniej jednym państwie członkowskim – nie powinna sama z siebie być warunkiem wystarczającym do zastosowania niniejszego rozporządzenia.
- (28) Istotne powiązanie z Unią powinno być również odpowiednią przesłanką przy ustaleniu zakresu stosowania niniejszego rozporządzenia. Należy przyjąć, że takie istotne powiązanie z Unią istnieje, gdy usługodawca posiada zakład w Unii. W przypadku braku takiego zakładu spełnienie kryterium istnienia istotnego powiązania z Unią należy ocenić na podstawie istnienia znaczącej liczby użytkowników w co najmniej jednym państwie członkowskim lub kierowania działalności do co najmniej jednego państwa członkowskiego. Fakt kierowania działalności do co najmniej jednego państwa członkowskiego można stwierdzić na podstawie wszelkich istotnych okoliczności, w tym czynników takich jak używanie języka lub waluty powszechnie używanych w danym państwie członkowskim lub możliwość zamówienia towarów lub usług. Przesłanką kierowania działalności do danego państwa członkowskiego może być również dostępność aplikacji w odpowiednim krajowym sklepie z aplikacjami, lokalne udostępnianie reklam lub udostępnianie reklam w języku używanym w danym państwie członkowskim lub zarządzanie relacjami z klientem obejmujące zapewnianie obsługi klienta w języku powszechnie używanym w tym państwie członkowskim. Istotne powiązanie należy

również zakładać, jeżeli usługodawca kieruje swoją działalność do co najmniej jednego państwa członkowskiego zgodnie z art. 17 ust. 1 lit. c) rozporządzenia nr 1215/2012 w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych³⁶. Z drugiej strony świadczenie usług jedynie w celu przestrzegania zakazu dyskryminowania przewidzianego w rozporządzeniu (UE) 2018/302³⁷ nie może być – na podstawie tej jedynej przesłanki – uważane za kierowanie działalności do danego terytorium w Unii.

- (29) Europejski nakaz wydania dowodów może być wydany wyłącznie wówczas, gdy jest on konieczny i proporcjonalny. W ocenie należy wziąć pod uwagę, czy nakaz jest ograniczony do tego, co jest konieczne do osiągnięcia zgodnego z prawem celu polegającego na pozyskaniu odpowiednich i niezbędnych danych przeznaczonych do wykorzystania w charakterze materiału dowodowego wyłącznie w określonej, indywidualnej sprawie.
- (30) Przy wydaniu europejskiego nakazu wydania dowodów lub europejskiego nakazu zabezpieczenia dowodów konieczny jest zawsze udział organu sądowego – czy to w procesie wydawania czy też zatwierdzenia nakazu. Ze względu na bardziej wrażliwy charakter danych dotyczących transakcji i danych dotyczących treści, wydanie lub zatwierdzenie europejskich nakazów wydania dowodów należących do tych kategorii wymaga rozpatrzenia przez sędziego. Ponieważ dane abonenta i dane dostępu są mniej wrażliwymi danymi, europejskie nakazy wydania dowodów mogą być dodatkowo wydawane lub zatwierdzane przez właściwych prokuratorów.
- (31) Z tego samego powodu należy przeprowadzić rozróżnienie dotyczące zakresu przedmiotowego niniejszego rozporządzenia: nakazy wydania dowodów będących danymi abonenta i danych dostępowych mogą być wydawane w związku z dowolnym przestępstwem, natomiast dostęp do danych dotyczących transakcji i danych dotyczących treści powinien podlegać bardziej rygorystycznym wymogom w celu odzwierciedlenia bardziej wrażliwego charakteru takich danych. Rozwiązaniem umożliwiającym obranie bardziej proporcjonalnego podejścia jest ustalenie progu, wraz z szeregiem innych warunków i zabezpieczeń *ex ante* i *ex post* zawartych w rozporządzeniu, mających na celu zapewnienie poszanowania zasady proporcjonalności i praw zainteresowanych osób. Jednocześnie próg nie powinien ograniczać skuteczności instrumentu i utrudniać jego wykorzystania przez przedstawicieli zainteresowanych zawodów i organów. Umożliwienie wydawania nakazów w związku z postępowaniem przygotowawczym w sprawie przestępstw zagrożonych karą pozbawienia wolności o górnej granicy ustawowego zagrożenia w wysokości co najmniej trzech lat ogranicza zakres instrumentu do poważniejszych przestępstw, nie oddziałując nadmiernie na możliwości jego stosowania przez przedstawicieli zainteresowanych zawodów i organów. Próg wyłącza z zakresu rozporządzenia znaczną liczbę przestępstw, które państwa członkowskie uważają za mniej poważne, co znajduje odzwierciedlenie w niższej maksymalnej karze. Ma on również tę zaletę, że łatwo go zastosować w praktyce.

³⁶ [Rozporządzenie Parlamentu Europejskiego i Rady \(UE\) nr 1215/2012](#) z dnia 12 grudnia 2012 r. w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych (Dz.U. L 351 z 20.12.2012, s. 1).

³⁷ [Rozporządzenie Parlamentu Europejskiego i Rady \(UE\) 2018/302](#) z dnia 28 lutego 2018 r. w sprawie nieuzasadnionego blokowania geograficznego oraz innych form dyskryminacji klientów ze względu na przynależność państwową, miejsce zamieszkania lub miejsce prowadzenia działalności na rynku wewnętrznym oraz w sprawie zmiany rozporządzeń (WE) nr 2006/2004 oraz (UE) 2017/2394 i dyrektywy 2009/22/WE (Dz.U. L 601 z 2.3.2018, s. 1).

- (32) Istnieją przestępstwa, w przypadku których materiał dowodowy będzie w typowej sytuacji dostępny wyłącznie w postaci elektronicznej, z natury bardzo nietrwałej. Obejmuje to przestępstwa związane z cyberprzestrzenią, również te, które mogą nie zostać uznane za poważne same w sobie, lecz mogą spowodować rozległe i znaczące szkody, w szczególności w przypadkach charakteryzujących się małym wpływem jednostkowym, ale znacznym wolumenem i wielkością ogólnych szkód. W większości przypadków, w których przestępstwo popełniono przy użyciu systemu informacyjnego, zastosowanie tego samego progu co w odniesieniu do innych rodzajów przestępstw, prowadziłoby przede wszystkim do bezkarności. Powyższe usprawiedliwia stosowanie rozporządzenia również do przestępstw zagrożonych karą pozbawienia wolności niższą niż 3 lata. W przypadku pozostałych przestępstw związanych z terroryzmem wskazanych w dyrektywie 2017/541/UE nie ma zastosowania próg górnej granicy ustawowego zagrożenia karą w wysokości co najmniej trzech lat.
- (33) Dodatkowo niezbędne jest zapewnienie, by europejski nakaz wydania dowodów mógł być wydany jedynie wówczas, gdy w państwie wydającym dostępny jest podobny środek dotyczący tego samego przestępstwa w porównywalnej sytuacji krajowej.
- (34) Jeżeli dane objęte nakazem są przechowywane lub przetwarzane w ramach infrastruktury zapewnianej przez usługodawcę na rzecz spółki lub innego podmiotu niż osoby fizyczne, co ma zazwyczaj miejsce w przypadku usług hostingowych, europejski nakaz wydania dowodów powinien być stosowany wyłącznie wówczas, gdy inne środki dochodzeniowo-śledcze skierowane do tej spółki lub podmiotu nie są właściwe, w szczególności jeżeli mogłyby zagrozić skuteczności postępowania przygotowawczego. Jest to szczególnie istotne zwłaszcza w przypadku dużych podmiotów takich jak korporacje lub instytucje rządowe, które korzystają z usług usługodawców w celu zapewniania sobie korporacyjnej infrastruktury informatycznej lub usług informatycznych, lub jednego i drugiego. Pierwszym adresatem europejskiego nakazu wydania dowodów powinna być w takich sytuacjach spółka lub wspomniany inny podmiot. Spółka lub inny podmiot nie musi być usługodawcą objętym zakresem niniejszego rozporządzenia. W przypadkach, w których skierowanie nakazu do takiego podmiotu nie jest jednak stosowne, na przykład ze względu na jego domniemany udział w odnośnej sprawie lub ze względu na przesłanki istnienia zмовy z podmiotem, wobec którego toczy się postępowanie przygotowawcze, właściwe organy powinny dysponować możliwością skierowania żądania wydania danych do usługodawcy zapewniającego rzeczoną infrastrukturę. Niniejszy przepis nie wpływa na prawo do nakazania usługodawcy zabezpieczenia odnośnych danych.
- (35) Immunitety i przywileje, które mogą dotyczyć pewnych kategorii osób (na przykład dyplomatów) lub relacje podlegające szczególnej ochronie (na przykład wymiana informacji między prawnikiem a klientem), podlegają innym instrumentom wzajemnego uznawania takim jak europejski nakaz dochodzeniowy. Ich zasięg i wpływ jest różny w zależności od mającego zastosowanie prawa krajowego, które należy wziąć pod uwagę w momencie wydawania nakazu, ponieważ organ wydający może wydać nakaz jedynie wówczas, gdy można byłoby wydać podobny nakaz w porównywalnej sytuacji krajowej. Oprócz przestrzegania tej podstawowej zasady immunitety i przywileje chroniące dane dostępu, dane dotyczące transakcji lub dane dotyczące treści w państwie członkowskim usługodawcy powinny być uwzględnione w państwie wydającym w największym możliwym stopniu – w taki sam sposób, jak gdyby były przewidziane przepisami prawa krajowego państwa wydającego. Jest to

istotne szczególnie w sytuacji, w której prawo państwa członkowskiego, w którym do usługodawcy lub jego przedstawiciela prawnego kierowany jest nakaz, zapewnia wyższy poziom ochrony niż przepisy prawa państwa wydającego. Przepis ten zapewnia ponadto uwzględnienie przypadków, w których ujawnienie danych może wpłynąć na podstawowe interesy danego państwa członkowskiego, takie jak bezpieczeństwo narodowe i obronność. W charakterze dodatkowego zabezpieczenia aspekty te powinny zostać uwzględnione nie tylko przy wydawaniu nakazu, lecz również później, przy przeprowadzaniu oceny istotności i dopuszczalności odnośnych danych na odpowiednim etapie procesu karnego, a w przypadku wszczęcia przymuszającej do wykonania nakazu, przez organ przymuszający do wykonania nakazu.

- (36) Wydanie europejskiego nakazu zabezpieczenia może nastąpić w odniesieniu do dowolnego przestępstwa. Jego celem jest zapobieżenie usunięciu, skasowaniu lub zmianie odpowiednich danych w sytuacji, w której doprowadzenie do wydania tych danych może zająć więcej czasu, na przykład gdy mają zostać wykorzystane kanały współpracy wymiarów sprawiedliwości.
- (37) Europejskie nakazy wydania dowodów i europejskie nakazy zabezpieczenia dowodów powinny być zawsze kierowane do przedstawiciela prawnego wyznaczonego przez usługodawcę. W przypadku braku przedstawiciela prawnego nakazy mogą być kierowane do dowolnego zakładu usługodawcy w Unii. Może to mieć miejsce na przykład w przypadku, gdy usługodawca nie jest prawnie zobowiązany do wyznaczenia przedstawiciela prawnego. W przypadku niewywiązania się z obowiązków przez przedstawiciela prawnego w sytuacjach wyjątkowych europejski nakaz wydania dowodów lub europejski nakaz zabezpieczenia dowodów może być również skierowany do usługodawcy równolegle do postępowania przymuszającego do wykonania pierwotnego nakazu zgodnie z art. 14 lub zamiast tego postępowania. W przypadku niewywiązania się z obowiązków przez przedstawiciela prawnego w innych sytuacjach niż sytuacje wyjątkowe, w których jednak istnieje wyraźne ryzyko utraty danych, europejski nakaz wydania dowodów lub europejski nakaz zabezpieczenia dowodów mogą być również skierowane do dowolnego zakładu usługodawcy w Unii. Ze względu na te różne możliwe scenariusze, w przepisach stosuje się ogólny termin „adresat”. Jeżeli obowiązek taki jak obowiązek zachowania poufności ma zastosowanie nie tylko do adresata, ale również do usługodawcy (kiedy nie jest on adresatem), jest to wskazane w odpowiednim przepisie.
- (38) Europejskie nakazy wydania dowodów i europejskie nakazy zabezpieczenia dowodów należy przekazać usługodawcy w formie zaświadczenia europejskiego nakazu wydania dowodów (EPOC) lub zaświadczenia europejskiego nakazu zabezpieczenia dowodów (EPOC-PR), przy czym powinny być one przetłumaczone. Zaświadczenia powinny zawierać te same obowiązkowe informacje, co nakazy, z wyjątkiem przesłanek dotyczących konieczności i proporcjonalności środka oraz pozostałych szczegółowych informacji dotyczących sprawy, w celu uniknięcia zagrożenia dla postępowania przygotowawczego. Ponieważ jednak są one częścią samego nakazu, umożliwiają podejrzanemu późniejsze podważenie nakazu w postępowaniu karnym. W razie potrzeby zaświadczenie należy również przetłumaczyć na jeden lub kilka spośród języków urzędowych państwa członkowskiego adresata, lub na inny język urzędowy akceptowany przez usługodawcę zgodnie z jego oświadczeniem.
- (39) Właściwy organ wydający powinien przekazać zaświadczenie europejskiego nakazu wydania dowodów lub zaświadczenia europejskiego nakazu zabezpieczenia dowodów bezpośrednio do adresata z wykorzystaniem wszelkich środków umożliwiających

uzyskanie dokumentu pisemnego na warunkach zapewniających usługodawcy możliwość stwierdzenia autentyczności zaświadczenia; środki te mogą obejmować przesyłkę poleconą, bezpieczną pocztę elektroniczną oraz platformy i inne zabezpieczone kanały, w tym udostępniane przez usługodawcę, zgodnie z zasadami ochrony danych osobowych.

- (40) Dane objęte nakazem powinny być przekazane organom najpóźniej w terminie 10 dni od otrzymania zaświadczenia europejskiego nakazu wydania dowodów. Usługodawca musi przestrzegać krótszego terminu w sytuacjach wyjątkowych oraz kiedy organ wydający poda inne przesłanki uzasadniające zastosowanie innego terminu niż 10 dni. Oprócz bezpośredniego ryzyka usunięcia żądanych danych przesłanki mogą obejmować okoliczności związane z trwającym postępowaniem przygotowawczym, na przykład jeśli dane objęte nakazem są związane z innymi pilnymi czynnościami dochodzeniowo-śledczymi, których nie można przeprowadzić bez brakujących danych, lub takimi, które w inny sposób od tych danych zależą.
- (41) W celu umożliwienia usługodawcom zaradzenia formalnym problemom niezbędne jest ustanowienie procedury komunikacji pomiędzy usługodawcą a organem sądowym wydającym nakaz w przypadkach, w których zaświadczenie europejskiego nakazu wydania danych może być niekompletne lub zawierać oczywiste błędy lub niewystarczające informacje do wykonania nakazu. Ponadto, jeżeli usługodawca nie przekaze informacji w sposób wyczerpujący lub terminowy z dowolnego innego powodu, na przykład ze względu na to, że jego zdaniem występuje konflikt z obowiązkiem przewidzianym w przepisach prawa państwa trzeciego, lub ze względu na to, że jego zdaniem europejski nakaz wydania dowodów nie został wydany zgodnie z warunkami przewidzianymi w niniejszym rozporządzeniu, usługodawca powinien zwrócić się do organów wydających i przedstawić stosowne uzasadnienie. Procedura komunikacji powinna zatem umożliwiać w szerokim zakresie skorygowanie lub ponowne rozpatrzenie zaświadczenia europejskiego nakazu wydania danych przez organ wydający na wczesnym etapie. W celu zagwarantowania dostępności danych usługodawca powinien zabezpieczyć dane, jeżeli jest w stanie zidentyfikować dane objęte nakazem.
- (42) Po otrzymaniu zaświadczenia europejskiego nakazu zabezpieczenia dowodów usługodawca powinien zabezpieczyć dane objęte nakazem na okres maksymalnie 60 dni, chyba że organ wydający poinformuje usługodawcę o wszczęciu postępowania na potrzeby wydania danych, w którym to przypadku zabezpieczenie powinno być kontynuowane. Okres 60 dni ma na celu umożliwienie wydania urzędowego wniosku. Wymaga to podjęcia co najmniej kilku oficjalnych kroków, na przykład skierowania wniosku o wzajemną pomoc prawną do przetłumaczenia. Po otrzymaniu tych informacji dane powinny być zabezpieczone przez wystarczająco długi okres do momentu ich wydania na podstawie kolejnego wniosku o wydanie dowodów.
- (43) Usługodawcy i ich przedstawiciele prawni powinni zapewnić poufność oraz, jeżeli zażąda tego organ wydający, powstrzymać się od informowania osoby, której dane są objęte nakazem, w celu ochrony postępowania przygotowawczego zgodnie z art. 23 rozporządzenia (UE) 2016/679³⁸. Dane użytkownika stanowią jednak kluczowy

³⁸

[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).

element umożliwiający dokonanie kontroli i dochodzenie odszkodowań na drodze sądowej i powinny zostać przekazane przez organ, jeżeli od usługodawcy zażądano powstrzymania się od informowania użytkownika, o ile nie występuje ryzyko zagrażające trwającemu postępowaniu przygotowawczemu zgodnie z krajowymi przepisami stanowiącymi transpozycję art. 13 dyrektywy (UE) 2016/680³⁹.

- (44) W przypadku niewywiązania się przez adresata z obowiązków organ wydający może przekazać pełny nakaz z uzasadnieniem dotyczącym konieczności i proporcjonalności wraz z zaświadczeniem do właściwego organu państwa członkowskiego, w którym adresat zaświadczenia ma miejsce pobytu lub ma zakład. Wspomniane państwo członkowskie powinno przymusić do wykonania nakazu zgodnie ze swoim prawem krajowym. Państwa członkowskie powinny przewidzieć nakładanie skutecznych, proporcjonalnych i odstraszających sankcji finansowych w przypadku naruszenia obowiązku przewidzianego w niniejszym rozporządzeniu.
- (45) Postępowanie przymuszające do wykonania nakazu jest postępowaniem, w ramach którego adresat może wnieść sprzeciw wobec postępowania przymuszenia do wykonania nakazu na podstawie ściśle określonych przesłanek. Organ przymuszający do wykonania nakazu może odmówić uznania i przymuszenia do wykonania nakazu na podstawie tych samych przesłanek lub jeżeli mają zastosowanie immunitety i przywileje przewidziane w jego prawie krajowym lub w sytuacji, w której ujawnienie danych może mieć wpływ na podstawowe interesy takie jak bezpieczeństwo narodowe lub obronność. Organ przymuszający do wykonania nakazu powinien skonsultować się z organem wydającym przed wydaniem odmowy uznania nakazu lub odmowy wszczęcia postępowania przymuszającego do wykonania nakazu na podstawie tych samych przesłanek. W przypadku niewywiązania się z obowiązków organy mogą nałożyć sankcje. Sankcje te powinny być proporcjonalne również ze względu na szczególne okoliczności takie jak powtarzające się lub systematyczne niewywiązanie się z obowiązków.
- (46) Niezależnie od swoich obowiązków w zakresie ochrony danych usługodawcy nie powinni być pociągani do odpowiedzialności w państwach członkowskich za działania szkodliwe dla poufności danych użytkowników lub stron trzecich wyłącznie ze względu na zastosowanie się w dobrej wierze do zaświadczenia europejskiego nakazu wydania dowodów lub zaświadczenia europejskiego nakazu zabezpieczenia dowodów.
- (47) Oprócz osób fizycznych, których dotyczą dane objęte nakazem, również usługodawcy i państwa trzecie mogą być dotknięci skutkami środka dochodzeniowo-śledczego. W celu zapewnienia wzajemności w odniesieniu do suwerennych interesów państw trzecich, a także w celu ochrony zainteresowanych osób fizycznych i zaradzenia konfliktom obowiązków nałożonych na usługodawców, w niniejszym instrumencie przewidziano specjalny mechanizm kontroli sądowej na wypadek sytuacji, w których zastosowanie się do europejskiego nakazu wydania dowodów uniemożliwiłoby usługodawcom wywiązanie się z obowiązków prawnych wynikających z przepisów prawa państwa trzeciego.

³⁹ [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 uchyłająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. L 119 z 4.5.2016, s. 89).

- (48) Jeżeli zatem adresat uzna, że europejski nakaz wydania dowodów w konkretnej sprawie wiązałby się z pogwałceniem obowiązku prawnego wynikającego z przepisów prawa państwa trzeciego, powinien poinformować organ wydający w drodze uzasadnionego sprzeciwu, przy wykorzystaniu udostępnionego formularza. Organ wydający powinien wówczas skontrolować europejski nakaz wydania dowodów w świetle uzasadnionego sprzeciwu, uwzględniając te same kryteria, których przestrzegać musiałby właściwy sąd. Jeżeli organ podejmie decyzję o utrzymaniu w mocy nakazu, postępowanie powinno zostać przeniesione do właściwego sądu powiadomionego przez odpowiednie państwo członkowskie, który dokonuje następnie kontroli nakazu.
- (49) Ustalając, czy istnieją sprzeczne obowiązki w szczególnych okolicznościach rozpatrywanej sprawy, właściwy sąd powinien korzystać, w razie potrzeby, z odpowiedniej zewnętrznej wiedzy eksperckiej, na przykład jeżeli kontrola prowadzi do wątpliwości co do wykładni przepisów prawa odnośnego państwa trzeciego. Powyższe może obejmować zwrócenie się do centralnych organów tego państwa.
- (50) Ekspertka wiedza dotycząca wykładni powinna być również w miarę możliwości zapewniona przy pomocy biegłych. Informacje i orzecznictwo dotyczące wykładni przepisów prawa państw trzecich oraz procedur rozwiązywania konfliktów w państwach członkowskich należy udostępnić na centralnej platformie takiej jak projekt SIRIUS lub Europejska Sieć Sądowa. Powyższe powinno umożliwić sądom korzystanie z doświadczenia i eksperckiej wiedzy zgromadzonych przez inne sądy w odniesieniu do tych samych lub podobnych zagadnień. Nie powinno to jednak w stosownych przypadkach uniemożliwiać ponownej konsultacji z państwem trzecim.
- (51) W przypadku występowania sprzecznych obowiązków sąd musi ustalić, czy przepisy kolizyjne państwa trzeciego zabraniają ujawnienia danych objętych nakazem z uwagi na fakt, że jest to niezbędne do ochrony podstawowych praw zainteresowanych osób lub podstawowych interesów państwa trzeciego związanych z bezpieczeństwem narodowym lub obronnością. Przeprowadzając tę ocenę, sąd powinien wziąć pod uwagę, czy przepisy prawa państwa trzeciego w oczywisty sposób nie mają na celu ochrony innych interesów niż prawa podstawowe lub podstawowe interesy państwa trzeciego związane z bezpieczeństwem narodowym lub obronnością, lub czy nie mają na celu ochrony nielegalnych działań przed wnioskami organów ścigania dotyczącymi postępowania przygotowawczego. Jeżeli sąd stwierdzi, że przepisy kolizyjne prawa państwa trzeciego zabraniają ujawniania odnośnych danych ze względu na to, że jest to niezbędne do ochrony praw podstawowych zainteresowanej osoby fizycznej lub podstawowych interesów państwa trzeciego związanych z bezpieczeństwem narodowym lub obronnością, powinien skonsultować się z tym państwem trzecim za pośrednictwem jego organów centralnych zajmujących się udzielaniem wzajemnej pomocy prawnej, które w większości krajów na świecie zostały już ustanowione. Sąd powinien wyznaczyć dla państwa trzeciego termin na wniesienie zastrzeżeń dotyczących wykonania europejskiego nakazu wydania dowodów; jeżeli organy państwa trzeciego nie udzielą odpowiedzi w (przedłużonym) terminie pomimo przypomnienia informującego o konsekwencjach nieudzielenia odpowiedzi, sąd utrzymuje nakaz w mocy. Jeżeli organy państwa trzeciego sprzeciwia się ujawnieniu danych, sąd powinien uchylić nakaz.
- (52) We wszystkich pozostałych przypadkach występowania sprzecznych obowiązków, nie dotyczących praw podstawowych osoby fizycznej lub podstawowych interesów państwa trzeciego związanych z bezpieczeństwem narodowym i obronnością, sąd powinien podjąć decyzję co do tego, czy utrzymać europejski nakaz wydania

dowodów w mocy, dokonując oceny pewnej liczby elementów służących do stwierdzenia siły powiązania z każdą z dwóch odnośnych jurysdykcji, odnośnych interesów związanych z uzyskaniem lub zapobieżeniem ujawnieniu danych oraz możliwych konsekwencji dla usługodawcy wynikających z konieczności spełnienia nakazu. Szczególnie w przypadku przestępstw związanych z cyberprzestrzenią miejsce, w którym popełniono przestępstwo, obejmuje zarówno miejsce(-a), w którym podjęto działanie, jak i miejsce(-a), w którym wystąpiły skutki przestępstwa.

- (53) Warunki określone w art. 9 mają zastosowanie również w przypadku wystąpienia sprzecznych obowiązków wynikających z przepisów prawa państwa trzeciego. Podczas tej procedury dane należy objąć ochroną. Jeżeli nakaz zostaje uchylony, możliwe jest wydanie nowego nakazu zabezpieczenia dowodów, aby umożliwić organowi wydającemu zażądanie wydania dowodów w inny sposób, na przykład w ramach wzajemnej pomocy prawnej.
- (54) Należy zadbać o to, by wszystkim osobom, których dane są objęte nakazem w postępowaniu przygotowawczym lub procesie karnym, przysługiwał skuteczny środek ochrony prawnej, zgodnie z art. 47 Karty praw podstawowych Unii Europejskiej. W przypadku podejrzanych i oskarżonych prawo do skutecznego środka ochrony prawnej powinno być wykonywane w toku postępowania karnego. Powyższe może mieć wpływ na dopuszczalność lub, w zależności od sytuacji, znaczenie w procesie materiału dowodowego uzyskanego takimi środkami. Podejrzani i oskarżeni korzystają ponadto ze wszelkich gwarancji procesowych, które mają do nich zastosowanie, takich jak prawo do informacji. Inne osoby, niebędące podejrzanymi ani oskarżonymi, również powinny mieć prawo do skutecznego środka ochrony prawnej. Dlatego, jako minimum, należy zapewnić możliwość podważenia legalności europejskiego nakazu wydania dowodów, w tym konieczności i proporcjonalności nakazu. Niniejsze rozporządzenie nie powinno ograniczać możliwych przesłanek podważenia legalności nakazu. Wspomniane środki ochrony prawnej powinny być wykonywane w państwie wydającym zgodnie z prawem krajowym. Zasady dotyczące tymczasowego zawieszenia powinny być regulowane krajowymi przepisami prawa.
- (55) Ponadto w toku postępowania przymuszającego do wykonania nakazu i następującego potem postępowania odwoławczego adresat może sprzeciwić się przymuszeniu do wykonania europejskiego nakazu wydania dowodów lub europejskiego nakazu zabezpieczenia dowodów na podstawie pewnych ściśle określonych przesłanek, w tym niewystawienia lub niezatwierdzenia nakazu przez właściwy organ lub jeżeli jest oczywiste, że nakaz narusza Kartę praw podstawowych Unii Europejskiej lub stanowi oczywiste nadużycie. Na przykład nakaz wydania dowodów dotyczących treści związanych z nieokreśloną grupą osób na obszarze geograficznym lub bez związku z konkretnym postępowaniem karnym naruszałby w sposób oczywisty warunki wydania europejskiego nakazu wydania dowodów.
- (56) Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jednym z praw podstawowych. Zgodnie z art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej i art. 16 ust. 1 TFUE każda osoba ma prawo do ochrony danych osobowych jej dotyczących. Wdrażając niniejsze rozporządzenie, państwa członkowskie powinny zapewnić, by dane osobowe objęte były ochroną i mogły być przetwarzane wyłącznie zgodnie z rozporządzeniem (UE) 2016/679 oraz dyrektywą (UE) 2016/680.

- (57) Dane osobowe uzyskane na mocy niniejszego rozporządzenia powinny być przetwarzane jedynie w razie konieczności i powinny być proporcjonalne do celów zapobiegania przestępstwom, prowadzenia w ich sprawie postępowania przygotowawczego, ich wykrywania i ścigania lub przymuszania do wykonania sankcji karnych i korzystania z prawa do obrony. W szczególności państwa członkowskie powinny zapewnić, by w odniesieniu do przekazywania danych osobowych przez właściwe organy do usługodawców na potrzeby niniejszego rozporządzenia miały zastosowanie właściwe polityki i środki ochrony danych, w tym środki mające na celu zapewnienie bezpieczeństwa tych danych. Usługodawcy powinni zapewnić te same warunki w odniesieniu do przekazywania danych osobowych do właściwych organów. Jedynie upoważnione osoby powinny mieć dostęp do informacji zawierających dane osobowe, które można uzyskać w procesach uwierzytelniania. Należy rozważyć zastosowanie mechanizmów zapewniających autentyczność, takich jak notyfikowane krajowe systemy identyfikacji elektronicznej lub usługi zaufania przewidziane w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającym dyrektywę 1999/93/WE.
- (58) Komisja powinna przeprowadzić ocenę niniejszego rozporządzenia, opartą na pięciu kryteriach: skuteczności, efektywności, zasadności, spójności i wartości dodanej dla UE oraz powinna zapewnić podstawę do przeprowadzenia oceny skutków możliwych dalszych środków. Informacje powinny być gromadzone regularnie, także w celu zapewnienia materiału do przeprowadzenia oceny niniejszego rozporządzenia.
- (59) Korzystanie z uprzednio przetłumaczonych i znormalizowanych formularzy ułatwia współpracę i wymianę informacji pomiędzy organami sądowymi a dostawcami usług, umożliwiając im zabezpieczenie i przekazanie elektronicznego materiału dowodowego szybciej i bardziej skutecznie, przy jednoczesnym spełnieniu koniecznych wymogów bezpieczeństwa w sposób przyjazny dla użytkownika. Obniżają one koszty tłumaczenia i przyczyniają się do zapewnienia wysokiego standardu jakości. Formularze odpowiedzi również powinny umożliwiać znormalizowaną wymianę informacji, w szczególności w sytuacjach, w których usługodawcy nie są w stanie wywiązać się z obowiązków, ponieważ dane konto nie istnieje lub brak jest dostępnych danych. Formularze powinny również ułatwiać gromadzenie danych statystycznych.
- (60) Aby móc skutecznie zareagować na ewentualną potrzebę poprawienia treści zaświadczenia europejskiego nakazu wydania dowodów i zaświadczenia europejskiego nakazu zabezpieczenia dowodów oraz formularza przeznaczonego do przekazania informacji na temat braku możliwości wykonania zaświadczenia europejskiego nakazu wydania dowodów lub zaświadczenia europejskiego nakazu zabezpieczenia dowodów, Komisji powinno się powierzyć uprawnienia do przyjmowania aktów delegowanych zgodnie z art. 290 Traktatu o funkcjonowaniu Unii Europejskiej w celu wprowadzenia zmian w załącznikach I, II i III niniejszego rozporządzenia. Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów, oraz aby konsultacje te prowadzone były zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym w sprawie lepszego stanowienia prawa z dnia 13 kwietnia

2016 r.⁴⁰. W szczególności, aby zapewnić udział na równych zasadach Parlamentu Europejskiego i Rady w przygotowaniu aktów delegowanych, instytucje te otrzymują wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji mogą systematycznie brać udział w posiedzeniach grup eksperckich Komisji zajmujących się przygotowaniem aktów delegowanych.

- (61) Środki oparte na niniejszym rozporządzeniu nie powinny zastępować europejskich nakazów dochodzeniowych wydanych na podstawie dyrektywy 2014/41/UE Parlamentu Europejskiego i Rady⁴¹ w celu uzyskania elektronicznego materiału dowodowego. Organy państw członkowskich powinny wybrać narzędzie najlepiej dostosowane do ich sytuacji; przy występowaniu do innego państwa członkowskiego o przeprowadzenie szeregu różnych czynności dochodzeniowo-śledczych, w tym między innymi o wydanie elektronicznego materiału dowodowego, mogą one postanowić, że wolą skorzystać z europejskiego nakazu dochodzeniowego.
- (62) Ze względu na postęp technologiczny w ciągu kilku lat bardziej powszechne mogą się stać nowe formy narzędzi komunikacji; mogą się też pojawić luki w stosowaniu niniejszego rozporządzenia. Ważną kwestią jest zatem zapewnienie dokonania przeglądu jego stosowania.
- (63) Ponieważ cele niniejszego rozporządzenia, a mianowicie uzyskanie poprawy w dziedzinie transgranicznego zabezpieczania i pozyskiwania elektronicznego materiału dowodowego, nie mogą zostać osiągnięte przez państwa członkowskie w sposób wystarczający ze względu na jego transgraniczny charakter, natomiast możliwe jest ich lepsze osiągnięcie na poziomie Unii, Unia może podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tych celów.
- (64) Zgodnie z art. 3 Protokołu w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, załączonego do Traktatu o Unii Europejskiej i do Traktatu o funkcjonowaniu Unii Europejskiej, *[Zjednoczone Królestwo / Irlandia powiadomiło(-a) o chęci uczestniczenia w przyjęciu i stosowaniu niniejszego rozporządzenia] albo [bez uszczerbku dla art. 4 tego protokołu, Zjednoczone Królestwo/Irlandia nie uczestniczy w przyjęciu niniejszego rozporządzenia, nie jest nim związane(-a) ani go nie stosuje]*.
- (65) Zgodnie z art. 1 i 2 Protokołu nr 22 w sprawie stanowiska Danii, załączonego do Traktatu o Unii Europejskiej i do Traktatu o funkcjonowaniu Unii Europejskiej, Dania nie uczestniczy w przyjęciu niniejszego rozporządzenia i nie jest nim związana ani go nie stosuje.
- (66) Zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 Parlamentu Europejskiego i Rady⁴² przeprowadzono konsultacje z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu (...) ⁴³,

⁴⁰ Dz.U. L 123 z 12.5.2016, s. 1.

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

⁴² Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.U. L 8 z 12.1.2001, s. 1).

⁴³ Dz.U. C [...], [...], s. [...].

Rozdział 1: Przedmiot, definicje i zakres

Artykuł 1 *Przedmiot*

1. W niniejszym rozporządzeniu określa się zasady, na podstawie których organ państwa członkowskiego może nakazać usługodawcy oferującemu usługi w Unii wydanie lub zabezpieczenie elektronicznego materiału dowodowego, bez względu na lokalizację danych. Niniejsze rozporządzenie pozostaje bez uszczerbku dla uprawnień organów krajowych do wymagania od usługodawców posiadających zakład lub przedstawicielstwo na ich terytorium, aby przestrzegali podobnych środków krajowych.
2. Niniejsze rozporządzenie nie ma wpływu na obowiązek poszanowania praw podstawowych i podstawowych zasad prawnych zapisanych w art. 6 TUE, w tym prawa do obrony osób, wobec których toczy się postępowanie karne, ani nie wpływa na obowiązki ciężące w tym względzie na organach ścigania i organach wymiaru sprawiedliwości.

Artykuł 2 *Definicje*

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

- 1) „europejski nakaz wydania dowodów” oznacza wiążącą decyzję podjętą przez organ wydający państwa członkowskiego wymagającą od usługodawcy oferującego usługi w Unii i posiadającego zakład lub przedstawicielstwo w innym państwie członkowskim wydania elektronicznego materiału dowodowego;
- 2) „europejski nakaz zabezpieczenia dowodów” oznacza wiążącą decyzję podjętą przez organ wydający państwa członkowskiego wymagającą od usługodawcy oferującego usługi w Unii i posiadającego zakład lub przedstawicielstwo w innym państwie członkowskim zabezpieczenia elektronicznego materiału dowodowego na potrzeby kolejnego wniosku o wydanie danych;
- 3) „usługodawca” oznacza dowolną osobę fizyczną lub prawną świadczącą usługi należące do co najmniej jednej z poniższych kategorii:
 - a) usługi łączności elektronicznej zgodnie z definicją zawartą w art. 2 ust. 4 [dyrektywy ustanawiającej Europejski kodeks łączności elektronicznej];
 - b) usługi społeczeństwa informacyjnego zgodnie z definicją zawartą w art. 1 ust. 1 lit. b) dyrektywy (UE) 2015/1535 Parlamentu Europejskiego i Rady⁴⁴, w przypadku których przechowywanie danych jest elementem definiującym usługę świadczoną na rzecz użytkownika, w tym portale społecznościowe,

⁴⁴ [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).

rynków internetowych ułatwiających transakcje pomiędzy użytkownikami oraz inni dostawcy usług hostingowych;

- c) usługi dotyczące nazw domen internetowych i numeracji IP, takie jak dostawcy adresów IP, rejestry nazw domen, podmioty rejestrujące nazwy domen i powiązane usługi prywatności i usługi *proxy*;

4) „oferowanie usług w Unii” oznacza:

- a) umożliwianie osobom prawnym lub fizycznym w co najmniej jednym państwie członkowskim korzystania z usług wymienionych w ust. 3 powyżej; oraz
- b) posiadanie istotnego powiązania z państwem członkowskim (państwami członkowskimi), o którym (których) mowa w lit. a);

5) „zakład” oznacza albo rzeczywiste prowadzenie działalności gospodarczej przez nieokreślony czas za pośrednictwem stabilnej infrastruktury, z której świadczy się usługi, albo stabilną infrastrukturę, z której działalność ta jest zarządzana;

6) „elektroniczny materiał dowodowy” oznacza materiał dowodowy przechowywany w postaci elektronicznej przez usługodawcę lub w jego imieniu w momencie otrzymania zaświadczenia nakazu wydania dowodów lub zaświadczenia nakazu zabezpieczenia dowodów, składający się z przechowywanych danych abonenta, danych dostępu, danych dotyczących transakcji i danych dotyczących treści;

7) „dane abonenta” oznaczają wszelkie dane dotyczące:

- a) tożsamości abonenta lub klienta, takie jak podane imię i nazwisko, data urodzenia, adres pocztowy lub geograficzny, dane billingowe i dane płatności, numer telefonu lub adres e-mail;
- b) rodzaju usługi i czasu jej trwania, w tym dane techniczne i dane identyfikujące powiązane środki techniczne lub interfejsy wykorzystywane przez abonenta lub klienta lub im udostępniane oraz dane związane z walidacją użycia usługi, z wyjątkiem haseł i innych środków uwierzytelnienia stosowanych zamiast hasła, podanych przez użytkownika lub utworzonych na jego prośbę;

8) „dane dostępu” oznaczają dane związane z rozpoczęciem i zakończeniem sesji dostępu użytkownika do usługi, które są ściśle niezbędne w wyłącznym celu identyfikacji użytkownika usługi, takie jak data i godzina użycia, zalogowanie do usługi i wylogowanie z niej, wraz z adresem IP przydzielonym przez dostawcę usługi dostępu do internetu użytkownikowi usługi, dane identyfikujące wykorzystywany interfejs i identyfikator użytkownika. Powyższe dane obejmują metadane pochodzące z łączności elektronicznej zgodnie z definicją zawartą w art. 4. ust. 3 lit. g) [rozporządzenia w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej];

9) „dane dotyczące transakcji” oznaczają dane związane ze świadczeniem usługi oferowanej przez usługodawcę, wykorzystywane do zapewnienia kontekstu lub dodatkowych informacji na temat tej usługi i generowane lub przetwarzane przez system informacyjny usługodawcy, takie jak dane dotyczące źródła i miejsca przeznaczenia wiadomości lub interakcji innego rodzaju, dane na temat lokalizacji urządzenia, data, godzina, czas trwania, rozmiar, trasa, format, wykorzystany protokół i typ kompresji, chyba że dane tego rodzaju stanowią dane dostępowe. Powyższe dane obejmują metadane pochodzące z łączności elektronicznej zgodnie z definicją zawartą w art. 4 ust. 3 lit. g) [rozporządzenia w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej];

- 10) „dane dotyczące treści” oznaczają wszelkie dane przechowywane w formacie cyfrowym takie jak tekst, głos, wideo, obrazy i dźwięk, inne niż dane abonenta, dane dostępu i dane dotyczące transakcji;
- 11) „system informacyjny” oznacza system informacyjny zgodnie z definicją w art. 2 lit. a) dyrektywy 2013/40/UE Parlamentu Europejskiego i Rady⁴⁵;
- 12) „państwo wydające” oznacza państwo członkowskie, w którym wydany został europejski nakaz wydania dowodów lub europejski nakaz zabezpieczenia dowodów;
- 13) „państwo wykonujące” oznacza państwo członkowskie, w którym adresat europejskiego nakazu wydania dowodów lub europejskiego nakazu zabezpieczenia dowodów ma miejsce pobytu lub zakład, do którego przekazuje się europejski nakaz wydania dowodów i zaświadczenie europejskiego nakazu wydania dowodów lub europejski nakaz zabezpieczenia dowodów i zaświadczenie europejskiego nakazu zabezpieczenia dowodów w celu ich wykonania;
- 14) „organ przymuszający do wykonania nakazu” oznacza właściwy organ w państwie wykonującym, do którego organ wydający przekazuje europejski nakaz wydania dowodów i zaświadczenie europejskiego nakazu wydania dowodów lub europejski nakaz zabezpieczenia dowodów i zaświadczenie europejskiego nakazu zabezpieczenia dowodów w celu wszczęcia postępowania przymuszającego do ich wykonania;
- 15) „sytuacje wyjątkowe” oznaczają sytuacje, w których istnieje bezpośrednie zagrożenie dla życia lub integralności cielesnej osoby lub infrastruktury krytycznej zgodnie z definicją zawartą w art. 2 lit. a) dyrektywy Rady 2008/114/WE⁴⁶.

Artykuł 3 *Zakres*

1. Niniejsze rozporządzenie stosuje się do usługodawców oferujących usługi w Unii.
2. Europejskie nakazy wydania dowodów i europejskie nakazy zabezpieczenia dowodów mogą być wydawane wyłącznie w postępowaniu karnym, zarówno na etapie postępowania przygotowawczego, jak i procesu karnego. Nakazy mogą być również wydawane w postępowaniach związanych z przestępstwami, w przypadku których osoba prawna może być pociągnięta do odpowiedzialności lub podlegać karze w państwie wydającym.
3. Nakazy przewidziane w niniejszym rozporządzeniu mogą być wydawane wyłącznie w odniesieniu do danych dotyczących usług oferowanych w Unii, zdefiniowanych w art. 2 ust. 3.

⁴⁵ [Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE](#) z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (Dz.U. L 218 z 14.8.2013, s. 8).

⁴⁶ [Dyrektywa Rady 2008/114/WE](#) z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dz.U. L 345, 23.12.2008, s. 75).

Rozdział 2: Europejski nakaz wydania dowodów, europejski nakaz zabezpieczenia dowodów i zaświadczenia

Artykuł 4 Organ wydający

1. Europejski nakaz wydania dowodów dotyczący danych abonenta i danych dostępu może być wydany przez:
 - a) sędziego, sąd, sędziego śledczego lub prokuratora właściwego w danej sprawie; lub
 - b) każdy inny właściwy organ określony przez państwo wydające i w danej sprawie pełniący funkcję organu dochodzeniowo-śledczego w postępowaniu karnym, który jest organem właściwym, by nakazać gromadzenie materiału dowodowego zgodnie z prawem krajowym. Europejski nakaz wydania dowodów podlega zatwierdzeniu przez sędziego, sąd, sędziego śledczego lub prokuratora w państwie wydającym, po zbadaniu go pod kątem zgodności z warunkami wydania europejskiego nakazu wydania dowodów określonymi w niniejszym rozporządzeniu.
2. Europejski nakaz wydania dowodów dotyczących transakcji i danych dotyczących treści może być wydany przez:
 - a) sędziego, sąd, sędziego śledczego właściwego w danej sprawie; lub
 - b) każdy inny właściwy organ określony przez państwo wydające i w danej sprawie pełniący funkcję organu dochodzeniowo-śledczego w postępowaniu karnym, który jest organem właściwym, by nakazać gromadzenie materiału dowodowego zgodnie z prawem krajowym. Europejski nakaz przedstawienia danych podlega zatwierdzeniu przez sędziego, sąd, sędziego śledczego w państwie wydającym, po zbadaniu go pod kątem zgodności z warunkami wydania europejskiego nakazu wydania dowodów określonymi w niniejszym rozporządzeniu.
3. Europejski nakaz zabezpieczenia dowodów może być wydany przez:
 - a) sędziego, sąd, sędziego śledczego lub prokuratora właściwego w danej sprawie; lub
 - b) każdy inny właściwy organ określony przez państwo wydające i w danej sprawie pełniący funkcję organu dochodzeniowo-śledczego w postępowaniu karnym, który jest organem właściwym, by nakazać gromadzenie materiału dowodowego zgodnie z prawem krajowym. Europejski nakaz zabezpieczenia podlega zatwierdzeniu przez sędziego, sąd, sędziego śledczego lub prokuratora w państwie wydającym, po zbadaniu go pod kątem zgodności z warunkami wydania europejskiego nakazu zabezpieczenia dowodów określonymi w niniejszym rozporządzeniu.
4. Jeżeli nakaz został zatwierdzony przez organ sądowy zgodnie z ustępami 1 lit. b), 2 lit. b) i 3 lit. b), organ ten może być również uważany za organ wydający na potrzeby przekazania zaświadczenia europejskiego nakazu wydania dowodów i zaświadczenia europejskiego nakazu zabezpieczenia dowodów.

Artykuł 5

Warunki wydania europejskiego nakazu wydania dowodów

1. Organ wydający może wydać europejski nakaz wydania dowodów jedynie w przypadku spełnienia warunków określonych w niniejszym artykule.
2. Europejski nakaz wydania dowodów jest konieczny i proporcjonalny do celu postępowania, o którym mowa w art. 3 ust. 2, i może być wydany jedynie w przypadku możliwości wydania podobnego środka w odniesieniu do tego samego przestępstwa w porównywalnej sytuacji krajowej w państwie wydającym.
3. Europejskie nakazy wydania dowodów dotyczących danych abonenta i danych dostępu mogą być wydawane w odniesieniu do każdego przestępstwa.
4. Europejskie nakazy wydania dowodów dotyczących transakcji lub danych dotyczących treści mogą być wydawane wyłącznie
 - a) w odniesieniu do przestępstw zagrożonych w państwie wydającym karą pozbawienia wolności o górnej granicy ustawowego zagrożenia w wysokości co najmniej trzech lat lub
 - b) w odniesieniu do następujących przestępstw, o ile popełniono je w całości lub częściowo z wykorzystaniem systemu informacyjnego:
 - przestępstw określonych w art. 3, 4 i 5 decyzji ramowej Rady 2001/413/WSiSW⁴⁷;
 - przestępstw określonych w art. 3–7 dyrektywy Parlamentu Europejskiego i Rady 2011/93/UE⁴⁸;
 - przestępstw określonych w art. 3–8 dyrektywy 2013/40/UE Parlamentu Europejskiego i Rady;
 - c) w odniesieniu do przestępstw określonych w art. 3–12 i 14 dyrektywy Parlamentu Europejskiego i Rady (UE) 2017/541⁴⁹.
5. Europejski nakaz wydania dowodów zawiera następujące informacje:
 - a) organ wydający oraz, w stosownych przypadkach, organ zatwierdzający;
 - b) adresat europejskiego nakazu wydania dowodów, o którym mowa w art. 7;
 - c) osoby, których dane są objęte nakazem, z wyjątkiem nakazów, których jedynym celem jest ustalenie tożsamości osoby;
 - d) kategoria danych objętych nakazem (dane abonenta, dane dostępu, dane dotyczące transakcji, dane dotyczące treści);

⁴⁷ [Decyzja ramowa Rady 2001/413/WSiSW](#) z dnia 28 maja 2001 r. w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi (Dz.U. L 149 z 2.6.2001, s. 1).

⁴⁸ [Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE](#) z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW (Dz.U. L 335 z 17.12.2011, s. 1).

⁴⁹ [Dyrektywa Parlamentu Europejskiego i Rady \(UE\) 2017/541](#) z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW (Dz.U. L 88 z 31.3.2017, s. 6).

- e) w stosownych przypadkach przedział czasowy, którego dotyczy nakaz przedstawienia;
 - f) mające zastosowanie przepisy prawa karnego państwa wydającego;
 - g) w przypadku sytuacji wyjątkowej lub żądania wcześniejszego ujawnienia, odpowiednie uzasadnienie;
 - h) w przypadkach, w których dane objęte nakazem są przechowywane lub przetwarzane w ramach infrastruktury zapewnianej przez usługodawcę spółce lub innemu podmiotowi niebędącemu osobą fizyczną, potwierdzenie, że nakaz jest sporządzony zgodnie z ust. 6;
 - i) przesłanki dotyczące konieczności i proporcjonalności zastosowanego środka.
6. W przypadkach, w których dane objęte nakazem są przechowywane lub przetwarzane w ramach infrastruktury zapewnianej przez usługodawcę spółce lub innemu podmiotowi niebędącemu osobą fizyczną, europejski nakaz wydania dowodów może być skierowany do usługodawcy wyłącznie w przypadku, gdy środków dochodzeniowo-śledczych nie należy kierować do danej spółki lub podmiotu, w szczególności z uwagi na fakt, że mogłoby to zagrozić postępowaniu przygotowawczemu.
7. Jeżeli organ wydający ma powody, by przypuszczać, że objęte nakazem dane dotyczące transakcji lub treści chronione są immunitetami lub przywilejami udzielonymi na podstawie przepisów prawa państwa członkowskiego, w którym skierowano nakaz do usługodawcy, lub ich ujawnienie mogłoby mieć wpływ na podstawowe interesy tego państwa członkowskiego takie jak bezpieczeństwo narodowe i obronność, organ wydający musi uzyskać wyjaśnienia przed wydaniem europejskiego nakazu wydania dowodów, w tym w drodze konsultacji z właściwymi organami zainteresowanego państwa członkowskiego, bezpośrednio lub za pośrednictwem Eurojust lub Europejskiej Sieci Sądowej. Jeżeli organ wydający uzna, że objęte nakazem dane dostępu, dane dotyczące transakcji lub dane dotyczące treści są chronione takimi immunitetami lub przywilejami lub ich ujawnienie miałoby wpływ na podstawowe interesy danego państwa członkowskiego, organ wydający nie wydaje europejskiego nakazu wydania dowodów.

Artykuł 6

Warunki wydania europejskiego nakazu zabezpieczenia dowodów

1. Organ wydający może wydać europejski nakaz zabezpieczenia dowodów jedynie w przypadku spełnienia warunków określonych w niniejszym artykule.
2. Nakaz może być wydany, jeżeli jest to konieczne i proporcjonalne w celu zapobieżenia usunięciu, skasowaniu lub modyfikacji danych, które mają być objęte przyszłym wnioskiem o wydanie tych danych przekazywanym w ramach wzajemnej pomocy prawnej, europejskiego nakazu dochodzeniowego lub europejskiego nakazu wydania dowodów. Europejskie nakazy zabezpieczenia dowodów mogą być wydawane w odniesieniu do każdego przestępstwa.
3. Europejski nakaz zabezpieczenia dowodów zawiera następujące informacje:
 - a) organ wydający oraz, w stosownych przypadkach, organ zatwierdzający;

- b) adresat europejskiego nakazu zabezpieczenia dowodów, o którym mowa w art. 7;
- c) osoby, których dane zostaną zabezpieczone, z wyjątkiem nakazów, których jedynym celem jest ustalenie tożsamości osoby;
- d) kategoria zabezpieczanych danych (dane abonenta, dane dostępu, dane dotyczące transakcji, dane dotyczące treści);
- e) w stosownych przypadkach przedział czasowy, którego dotyczy nakaz zabezpieczenia;
- f) mające zastosowanie przepisy prawa karnego państwa wydającego;
- g) przesłanki dotyczące konieczności i proporcjonalności zastosowanego środka.

Artykuł 7

Adresat europejskiego nakazu wydania dowodów i europejskiego nakazu zabezpieczenia dowodów

1. Europejski nakaz wydania dowodów i europejski nakaz zabezpieczenia dowodów są kierowane bezpośrednio do przedstawiciela prawnego powołanego przez usługodawcę do celów gromadzenia materiału dowodowego w postępowaniu karnym.
2. W przypadku niepowołania przedstawiciela prawnego europejski nakaz wydania dowodów i europejski nakaz zabezpieczenia dowodów można skierować do dowolnego zakładu usługodawcy w Unii.
3. Jeżeli przedstawiciel prawny nie stosuje się do zaświadczenia europejskiego nakazu wydania dowodów w sytuacji wyjątkowej na podstawie art. 9 ust. 2, zaświadczenie europejskiego nakazu wydania dowodów można skierować do dowolnego zakładu usługodawcy w Unii.
4. Jeżeli przedstawiciel prawny nie wywiązuje się z obowiązków przewidzianych w art. 9 lub 10 i organ wydający uzna, że istnieje poważne ryzyko utraty danych, europejski nakaz wydania dowodów lub europejski nakaz zabezpieczenia dowodów można skierować do dowolnego zakładu usługodawcy w Unii.

Artykuł 8

Zaświadczenie europejskiego nakazu wydania dowodów i europejskiego nakazu zabezpieczenia dowodów

1. Europejski nakaz wydania dowodów lub europejski nakaz zabezpieczenia dowodów przekazuje się do adresata zgodnie z definicją zawartą w art. 7 za pośrednictwem zaświadczenia europejskiego nakazu wydania dowodów lub europejskiego nakazu zabezpieczenia dowodów.

Organ wydający lub zatwierdzający wypełnia zaświadczenie europejskiego nakazu wydania dowodów zawarte w załączniku I lub zaświadczenie europejskiego nakazu zabezpieczenia dowodów zawarte w załączniku II, podpisuje je i zaświadcza, że jego treść jest prawdziwa i poprawna.

2. Zaświadczenie europejskiego nakazu wydania dowodów lub zaświadczenie europejskiego nakazu zabezpieczenia dowodów przekazuje się bezpośrednio dowolnymi środkami umożliwiającymi uzyskanie pisemnego potwierdzenia, przy spełnieniu warunków zapewniających adresatowi możliwość stwierdzenia autentyczności zaświadczenia.

Jeżeli usługodawcy, państwa członkowskie lub organy Unii Europejskiej ustanowili specjalne platformy lub inne bezpieczne kanały obsługi wniosków dotyczących danych przekazywanych przez organy ścigania i organy sądowe, organ wydający może również podjąć decyzję o przekazaniu zaświadczenia za pośrednictwem takich kanałów.
3. Zaświadczenie europejskiego nakazu zabezpieczenia dowodów zawiera informacje wymienione w art. 5 ust. 5 lit. a)–h), w tym wystarczające informacje umożliwiające adresatowi identyfikację organu wydającego i skontaktowanie się z nim. Do zaświadczenia nie włącza się przesłanek dotyczących konieczności i proporcjonalności środka lub pozostałych informacji dotyczących postępowania przygotowawczego.
4. Zaświadczenie europejskiego nakazu zabezpieczenia dowodów zawiera informacje wymienione w art. 6 ust. 3 lit. a)–f), w tym wystarczające informacje umożliwiające adresatowi identyfikację organu wydającego i kontakt z nim. Do zaświadczenia nie włącza się przesłanek dotyczących konieczności i proporcjonalności środka lub pozostałych informacji dotyczących postępowania przygotowawczego.
5. W razie potrzeby dokonuje się tłumaczenia zaświadczenia europejskiego nakazu wydania dowodów lub zaświadczenia europejskiego nakazu zabezpieczenia dowodów na język urzędowy Unii zaakceptowany przez adresata. Jeżeli nie wskazano żadnego języka, tłumaczenia zaświadczenia europejskiego nakazu wydania dowodów lub zaświadczenia europejskiego nakazu zabezpieczenia dowodów dokonuje się na jeden z języków urzędowych państwa członkowskiego, w którym przedstawiciel prawny ma miejsce pobytu lub zakład ma przedstawiciel prawny.

Artykuł 9

Wykonanie zaświadczenia europejskiego nakazu wydania dowodów

1. Po otrzymaniu zaświadczenia europejskiego nakazu wydania dowodów adresat zapewnia przekazanie danych objętych nakazem bezpośrednio do organu wydającego lub organów ścigania wskazanych w zaświadczeniu europejskiego nakazu wydania dowodów nie później niż w terminie 10 dni od otrzymania zaświadczenia europejskiego nakazu wydania dowodów, chyba że organ wydający wskaże powody uzasadniające wcześniejsze ujawnienie danych.
2. W sytuacjach wyjątkowych adresat przekazuje dane objęte nakazem bez zbędnej zwłoki, najpóźniej w terminie 6 godzin od otrzymania zaświadczenia europejskiego nakazu wydania dowodów.
3. Jeżeli adresat nie jest w stanie wywiązać się ze swoich obowiązków ze względu na to, że zaświadczenie europejskiego nakazu wydania dowodów jest niekompletne, zawiera oczywiste błędy lub nie zawiera informacji wystarczających do jego wykonania, adresat informuje bez zbędnej zwłoki organ wydający, o którym mowa w zaświadczeniu europejskiego nakazu wydania dowodów, i wnosi o wyjaśnienia z wykorzystaniem formularza zawartego w załączniku III. Adresat informuje organ

wydający, czy identyfikacja i zabezpieczenie były możliwe zgodnie z ust. 6. Organ wydający odpowiada w najkrótszym możliwym terminie, nie później niż w terminie 5 dni. Terminy określone w ust. 1 i 2 nie mają zastosowania, dopóki nie zostaną przedstawione wyjaśnienia.

4. Jeżeli adresat nie jest w stanie wywiązać się ze swojego obowiązku ze względu na siłę wyższą lub faktyczną niemożność niezawinioną przez adresata (lub usługodawcę, jeżeli jest to inny podmiot), w szczególności ze względu na to, że osoba, której dane są objęte nakazem, nie jest jego klientem, lub dane zostały usunięte przed otrzymaniem zaświadczenia europejskiego nakazu wydania dowodów, adresat informuje bez zbędnej zwłoki organ wydający wskazany w zaświadczeniu europejskiego nakazu wydania dowodów, podając wyjaśnienia przy wykorzystaniu formularza zawartego w załączniku III. W przypadku spełnienia właściwych warunków organ wydający uchyla zaświadczenie europejskiego nakazu wydania dowodów.
5. We wszystkich przypadkach, w których z innych powodów adresat nie przekazuje wymaganych informacji lub nie przekazuje ich w sposób wyczerpujący lub we wskazanym terminie, adresat informuje organ wydający bez zbędnej zwłoki, lecz nie później niż w terminach określonych w ust. 1 i 2, o powodach tego stanu rzeczy przy wykorzystaniu formularza zawartego w załączniku III. Organ wydający dokonuje kontroli nakazu w świetle informacji przekazanych przez usługodawcę i w razie potrzeby wyznacza usługodawcy nowy termin na wydanie danych.

Jeżeli adresat uzna, że zaświadczenie europejskiego nakazu wydania dowodów nie może być wykonane ze względu na to, że w oparciu o same informacje w nim zawarte jest oczywiste, że narusza ono Kartę praw podstawowych Unii Europejskiej lub stanowi oczywiste nadużycie, adresat przesyła również formularz zawarty w załączniku III do właściwego organu przymuszającego do wykonania nakazu w państwie członkowskim adresata. W takich przypadkach właściwy organ przymuszający do wykonania nakazu może wystąpić o wyjaśnienia do organu wydającego dotyczące europejskiego nakazu wydania dowodów, bezpośrednio lub za pośrednictwem Eurojust lub Europejskiej Sieci Sądowej.

6. Adresat zabezpiecza dane objęte nakazem, jeżeli nie przedstawia ich bezzwłocznie, chyba że informacje zawarte w zaświadczeniu europejskiego nakazu wydania dowodów nie pozwalają na identyfikację tych danych, w którym to przypadku adresat zwraca się o wyjaśnienia zgodnie z ust. 3. Zabezpieczenie utrzymuje się do momentu wydania danych na podstawie opatrzonego wyjaśnieniami europejskiego nakazu wydania dowodów i związanego z nim zaświadczenia lub za pośrednictwem innych kanałów takich jak wzajemna pomoc prawna. Jeżeli wydanie danych i ich zabezpieczenie nie są już konieczne, organ wydający oraz, w stosownych przypadkach przewidzianych w art. 14 ust. 8, organ przymuszający do wykonania nakazu informują o tym adresata bez zbędnej zwłoki.

Artykuł 10

Wykonanie zaświadczenia europejskiego nakazu zabezpieczenia dowodów

1. Po otrzymaniu zaświadczenia europejskiego nakazu zabezpieczenia dowodów adresat bez zbędnej zwłoki zabezpiecza dane objęte nakazem. Zabezpieczenie ustaje po upływie 60 dni, chyba że organ wydający potwierdzi, że wydano kolejny wniosek o wydanie dowodów.

2. Jeżeli organ wydający potwierdzi w terminie wskazanym w ust. 1, że wydano kolejny wniosek o wydanie dowodów, adresat jest zobowiązany do zabezpieczenia danych tak długo, jak jest to konieczne do wydania dowodów, gdy tylko doręczony zostanie kolejny wniosek o wydanie danych.
3. Jeżeli zabezpieczenie nie jest już konieczne, organ wydający informuje o tym adresata bez zbędnej zwłoki.
4. Jeżeli adresat nie jest w stanie wywiązać się ze swojego obowiązku ze względu na to, że zaświadczenie jest niekompletne, zawiera oczywiste błędy lub nie zawiera informacji wystarczających do wykonania zaświadczenia europejskiego nakazu zabezpieczenia dowodów, adresat informuje bez zbędnej zwłoki organ wydający, o którym mowa w zaświadczeniu europejskiego nakazu zabezpieczenia dowodów, i wnosi o wyjaśnienia przy użyciu formularza zawartego w załączniku III. Organ wydający udziela odpowiedzi w najkrótszym możliwym terminie, lecz nie później niż w terminie 5 dni. Adresat zapewnia po swojej stronie możliwość odbioru niezbędnych wyjaśnień, w celu wypełnienia swojego obowiązku określonego w ust. 1.
5. Jeżeli adresat nie jest w stanie wywiązać się ze swojego obowiązku ze względu na siłę wyższą lub faktyczną niemożność niezawinioną przez adresata (lub usługodawcę, jeżeli jest to inny podmiot), w szczególności ze względu na to, że osoba, której dane są objęte nakazem, nie jest jego klientem, lub dane zostały usunięte przed otrzymaniem nakazu, adresat informuje bez zbędnej zwłoki organ wydający wskazany w zaświadczeniu europejskiego nakazu zabezpieczenia dowodów, podając wyjaśnienia z wykorzystaniem formularza zawartego w załączniku III. W przypadku spełnienia tych warunków organ wydający uchyla zaświadczenia europejskiego nakazu zabezpieczenia dowodów.
6. We wszystkich przypadkach, w których adresat nie zachowuje informacji objętych nakazem z innych powodów niż wymienione w formularzu zawartym w załączniku III, adresat informuje organ wydający bez zbędnej zwłoki o powodach takiego stanu rzeczy w formularzu zawartym w załączniku III. Organ wydający dokonuje kontroli nakazu w świetle uzasadnienia przedstawionego przez usługodawcę.

Artykuł 11

Poufność i informowanie użytkowników

1. Adresaci i usługodawcy, jeżeli są to różne podmioty, podejmują wszelkie niezbędne środki w celu zapewnienia poufności zaświadczenia europejskiego nakazu wydania dowodów lub zaświadczenia europejskiego nakazu zabezpieczenia dowodów oraz wydawanych lub zabezpieczanych danych, a także, jeżeli zażąda tego organ wydający, powstrzymują się od informowania osoby, której dane są objęte zakazem, aby nie stwarzać ryzyka zakłócenia odpowiedniego postępowania karnego.
2. Jeżeli organ wydający zażądał, by adresat powstrzymał się od informowania osoby, której dane są objęte nakazem, organ wydający informuje bez zbędnej zwłoki osobę, której dane są objęte zaświadczeniem europejskiego nakazu wydania dowodów, o wydaniu danych. Przekazanie tej informacji można odłożyć tak długo, jak długo jest to konieczne i proporcjonalne, tak aby uniknąć utrudniania danego postępowania karnego.
3. Informując taką osobę, organ wydający przekazuje też informacje na temat przysługujących środków ochrony prawnej, o których mowa w art. 17.

Artykuł 12
Zwrot kosztów

Usługodawca może wystąpić o zwrot poniesionych przez siebie kosztów do państwa wydającego, jeżeli takie rozwiązanie przewidziano w przepisach prawa krajowego państwa wydającego w odniesieniu do nakazów krajowych w podobnych sytuacjach zgodnie z tymi przepisami prawa krajowego.

Rozdział 3: Sankcje i postępowanie przymuszające do wykonania nakazu

Artykuł 13
Sankcje

Bez uszczerbku dla przepisów krajowego prawa przewidujących nałożenie sankcji karnych państwa członkowskie określają zasady dotyczące kar finansowych mających zastosowanie w przypadku naruszeń obowiązków przewidzianych w art. 9, 10 i 11 niniejszego rozporządzenia i podejmują wszelkie niezbędne działania w celu zapewnienia wdrożenia tych sankcji. Przewidziane sankcje finansowe muszą być skuteczne, proporcjonalne i odstraszające. Państwa członkowskie bezzwłocznie powiadamiają Komisję o tych przepisach i środkach oraz o każdej późniejszej zmianie, która ich dotyczy.

Artykuł 14
Postępowanie przymuszające do wykonania nakazu

1. Jeżeli adresat nie zastosuje się do zaświadczenia europejskiego nakazu wydania dowodów w terminie lub nie zastosuje się do zaświadczenia europejskiego nakazu zabezpieczenia dowodów bez podania powodów akceptowanych przez organ wydający, ten ostatni może przekazać – wszelkimi środkami umożliwiającymi uzyskanie pisemnego potwierdzenia oraz przy spełnieniu warunków umożliwiających organowi przymuszającemu do wykonania nakazu stwierdzenie autentyczności – europejski nakaz wydania danych wraz z zaświadczeniem europejskiego nakazu wydania dowodów lub europejski nakaz zabezpieczenia dowodów wraz z zaświadczeniem europejskiego nakazu zabezpieczenia dowodów oraz formularz zawarty w załączniku III wypełniony przez adresata oraz wszelkie inne właściwe dokumenty do właściwego organu w państwie wykonującym w celu wszczęcia postępowania przymuszającego do wykonania nakazu. W tym celu organ wydający dokonuje tłumaczenia nakazu, formularza oraz wszelkich innych dokumentów towarzyszących na jeden z języków urzędowych tego państwa członkowskiego i informuje adresata o przekazaniu dokumentów.
2. Po ich otrzymaniu, organ przymuszający do wykonania nakazu uznaje europejski nakaz wydania dowodów lub europejski nakaz zabezpieczenia dowodów bez dodatkowych formalności, zgodnie z art. 1, i podejmuje wszelkie niezbędne działania mające na celu przymuszenie do jego wykonania, chyba że organ ten uzna, że ma zastosowanie jedna z przesłanek przewidzianych w ust. 4 lub 5 lub że odnośne dane są chronione immunitetem lub przywilejem na podstawie przepisów prawa krajowego jego państwa lub ich ujawnienie może mieć wpływ na podstawowe

interesy tego państwa takie jak bezpieczeństwo narodowe i obrona. Organ przymuszający do wykonania nakazu podejmuje decyzję o uznaniu nakazu bez zbędnej zwłoki, lecz nie później niż w terminie 5 dni roboczych od otrzymania nakazu.

3. Jeżeli organ przymuszający do wykonania nakazu uzna nakaz, występuje do adresata z oficjalnym wnioskiem o zastosowanie się do właściwego obowiązku, informując adresata o możliwości wniesienia sprzeciwu wobec postępowania przymuszającego do wykonania nakazu przez powołanie się na przesłanki wymienione w ust. 4 lub 5 oraz o sankcjach mających zastosowanie w przypadku niewywiązania się z obowiązku, i ustala termin na wywiązanie się z obowiązku lub wniesienie sprzeciwu.
4. Adresat może wnieść sprzeciw wobec postępowania przymuszającego do wykonania europejskiego nakazu wydania dowodów jedynie ze względu na następujące przesłanki:
 - a) europejski nakaz wydania dowodów nie został wydany lub zatwierdzony przez organ wydający na zasadach określonych w art. 4;
 - b) europejski nakaz przedstawienia danych nie został wydany w związku z przestępstwem określonym w art. 5 ust. 4;
 - c) adresat nie mógł zastosować się do zaświadczenia europejskiego nakazu wydania dowodów z powodu faktycznej niemożności lub siły wyższej, lub ze względu na oczywiste błędy zawarte w zaświadczeniu europejskiego nakazu wydania dowodów;
 - d) europejski nakaz wydania dowodów nie dotyczy danych przechowywanych przez usługodawcę lub w jego imieniu w momencie otrzymania zaświadczenia europejskiego nakazu wydania dowodów;
 - e) usługa nie jest objęta zakresem niniejszego rozporządzenia;
 - f) same informacje zawarte w zaświadczeniu europejskiego nakazu wydania dowodów wskazują na to, że zaświadczenie europejskiego nakazu wydania dowodów w sposób oczywisty narusza przepisy Karty praw podstawowych lub ma charakter oczywistego nadużycia.
5. Adresat może wnieść sprzeciw wobec postępowania przymuszającego do wykonania europejskiego nakazu zabezpieczenia dowodów jedynie ze względu na następujące przesłanki:
 - a) europejski nakaz zabezpieczenia dowodów nie został wydany lub zatwierdzony przez organ wydający na zasadach określonych w art. 4;
 - b) usługodawca nie mógł zastosować się do zaświadczenia europejskiego nakazu zabezpieczenia dowodów z powodu faktycznej niemożności lub siły wyższej, lub ze względu na oczywiste błędy zawarte w zaświadczeniu europejskiego nakazu zabezpieczenia dowodów;
 - c) europejski nakaz zabezpieczenia dowodów nie dotyczy danych przechowywanych przez usługodawcę lub w jego imieniu w momencie otrzymania zaświadczenia europejskiego nakazu zabezpieczenia dowodów;
 - d) usługa nie jest objęta zakresem niniejszego rozporządzenia;

- e) same informacje zawarte w zaświadczeniu europejskiego nakazu zabezpieczenia dowodów wskazują na to, że zaświadczenie europejskiego nakazu zabezpieczenia dowodów w sposób oczywisty narusza przepisy Karty praw podstawowych lub ma charakter oczywistego nadużycia.
6. W przypadku sprzeciwu adresata organ przymuszający do wykonania nakazu podejmuje decyzję, czy wszcząć postępowanie przymuszające do wykonania nakazu na podstawie informacji przekazanych przez adresata oraz, w stosownych przypadkach, informacji uzupełniających uzyskanych od organu wydającego zgodnie z ust. 7.
7. Przed podjęciem decyzji o nieuznaniu lub nieprzymuszaniu do wykonania nakazu zgodnie z ust. 2 i ust. 6 organ przymuszający do wykonania nakazu konsultuje się z organem wydającym przy użyciu dowolnych właściwych środków. W stosownych przypadkach organ przymuszający do wykonania nakazu występuje o dalsze informacje do organu wydającego. Organ wydający udziela odpowiedzi na wszelkie takie wnioski w terminie 5 dni roboczych.
8. O wszystkich decyzjach informuje się bezzwłocznie organ wydający oraz adresata przy użyciu środków umożliwiających uzyskanie pisemnego potwierdzenia.
9. Jeżeli organ przymuszający do wykonania nakazu uzyska dane od adresata, przekazuje je do organu wydającego w terminie 2 dni roboczych, chyba że dane te są chronione immunitetem lub przywilejem na podstawie przepisów prawa krajowego organu przymuszającego do wykonania nakazu lub mają wpływ na podstawowe interesy jego państwa takie jak bezpieczeństwo narodowe i obronność. W takim przypadku organ przymuszający do wykonania nakazu informuje organ wydający o powodach nieprzekazania danych.
10. Jeżeli adresat nie wywiązuje się z obowiązku przewidzianego w uznanym nakazie, którego wykonalność potwierdził organ przymuszający do wykonania nakazu, ten ostatni nakłada karę finansową zgodnie z przepisami prawa krajowego swojego państwa. Wobec decyzji o nałożeniu kary powinien przysługiwać skuteczny środek ochrony prawnej.

Rozdział 4: Środki ochrony prawnej

Artykuł 15

Postępowanie odwoławcze w przypadku konfliktu obowiązków w oparciu o prawa podstawowe lub podstawowe interesy państwa trzeciego

1. Jeżeli w opinii adresata zastosowanie się do europejskiego nakazu wydania dowodów pozostawałoby w konflikcie z mającymi zastosowanie przepisami prawa państwa trzeciego zabraniającymi ujawniania odnośnych danych na tej podstawie, że jest to niezbędne do ochrony praw podstawowych zainteresowanych osób fizycznych lub podstawowych interesów tego państwa trzeciego związanych z bezpieczeństwem narodowymi lub obronnością, adresat informuje organ wydający o powodach niewykonania europejskiego nakazu wydania dowodów zgodnie z procedurą opisaną w art. 9 ust. 5.
2. Taki uzasadniony sprzeciw powinien zawierać wszelkie właściwe informacje na temat przepisów prawa państwa trzeciego, ich stosowności do odnośnej sprawy oraz charakteru sprzecznych obowiązków. Nie może on opierać się na faktach, że

podobne przepisy dotyczące warunków, formalności i procedur związanych z wydaniem nakazu wydania dowodów nie istnieją w mających zastosowanie przepisach prawa tego państwa trzeciego ani wyłącznie na okoliczności, że dane te są przechowywane w państwie trzecim..

3. Organ wydający dokonuje kontroli europejskiego nakazu wydania dowodów na podstawie uzasadnionego sprzeciwu. Jeżeli organ wydający zamierza utrzymać europejski nakaz wydania dowodów w mocy, wnioskuję o dokonanie kontroli przez właściwy sąd swojego państwa członkowskiego. Wykonanie nakazu zawiesza się do ukończenia postępowania odwoławczego.

Właściwy sąd ocenia w pierwszej kolejności, czy konflikt istnieje, w oparciu o analizę, czy

- a) przepisy prawa państwa trzeciego mają zastosowanie do szczególnych okoliczności rozpatrywanej sprawy, a jeśli tak jest,
 - b) czy przepisy prawa państwa trzeciego zastosowane do szczególnych okoliczności rozpatrywanej sprawy zabraniają ujawniania odnośnych danych.
4. Przeprowadzając tę ocenę, sąd powinien wziąć pod uwagę to, czy przepisy prawa państwa trzeciego w oczywisty sposób nie mają na celu ochrony innych interesów niż podstawowych praw lub podstawowych interesów państwa trzeciego związanych z bezpieczeństwem narodowym lub obronnością, lub czy nie mają na celu ochrony nielegalnych działań przed żądaniem organów ścigania w ramach postępowania przygotowawczego.
 5. Jeżeli właściwy sąd uzna, że nie występuje odnośny konflikt w rozumieniu ust. 1 i ust. 4, utrzymuje nakaz w mocy. Jeżeli właściwy sąd stwierdzi występowanie odnośnego konfliktu w rozumieniu ust. 1 i ust. 4, przekazuje wszelkie właściwe informacje dotyczące stanu faktycznego i prawnego dotyczące sprawy, w tym swoją ocenę, do organów centralnych w zainteresowanym państwie trzecim za pośrednictwem organu centralnego swojego państwa, z wyznaczeniem 15-dniowego terminu na odpowiedź. Na podstawie uzasadnionego wniosku przekazanego przez organ centralny państwa trzeciego wspomniany termin może zostać przedłużony do 30 dni.
 6. Jeżeli organ centralny państwa trzeciego poinformuje w wyznaczonym terminie właściwy sąd o swoim sprzeciwie wobec wykonania europejskiego nakazu wydania dowodów w danej sprawie, właściwy sąd uchyla nakaz i informuje organ wydający oraz adresata. Jeżeli w (przedłużonym) terminie właściwy sąd nie otrzyma sprzeciwu, przesyła przypomnienie wyznaczające organowi centralnemu państwa trzeciego 5 dodatkowych dni na odpowiedź oraz informujące ten organ o konsekwencjach nieudzielenia odpowiedzi. W przypadku nieotrzymania sprzeciwu w tym dodatkowym terminie sąd utrzymuje nakaz w mocy.
 7. Jeżeli właściwy sąd stwierdzi, że nakaz ma być utrzymany w mocy, informuje organ wydający i adresata, który przystępuje do wykonania nakazu.

Artykuł 16

Postępowanie odwoławcze w przypadku konfliktu obowiązków na podstawie innych przesłanek

1. Jeżeli adresat uzna, że zastosowanie się do europejskiego nakazu wydania dowodów pozostawałoby w konflikcie z mającymi zastosowanie przepisami prawa państwa trzeciego zabraniającymi ujawniania odnośnych danych ze względu na inne przesłanki niż przesłanki wskazane w art. 15, adresat informuje organ wydający o powodach niewykonania europejskiego nakazu wydania dowodów zgodnie z procedurą opisaną w art. 9 ust. 5.
2. Uzasadniony sprzeciw musi zawierać wszelkie właściwe informacje na temat przepisów prawa państwa trzeciego, ich stosowności do odnośnej sprawy oraz charakteru sprzecznych obowiązków. Nie może on opierać się na fakcie, że podobne przepisy dotyczące warunków, formalności i procedur związanych z wydaniem nakazu wydania dowodów nie istnieją w mających zastosowanie przepisach prawa tego państwa trzeciego ani wyłącznie na okoliczności, że dane te są przechowywane w państwie trzecim.
3. Organ wydający dokonuje kontroli europejskiego nakazu wydania dowodów na podstawie uzasadnionego sprzeciwu. Jeżeli organ wydający zamierza utrzymać europejski nakaz wydania dowodów w mocy, wnioskuję o dokonanie kontroli przez właściwy sąd swojego państwa członkowskiego. Wykonanie nakazu zawiesza się do ukończenia postępowania odwoławczego.
4. Właściwy sąd ocenia w pierwszej kolejności, czy konflikt istnieje, w oparciu o analizę, czy
 - a) przepisy prawa państwa trzeciego mają zastosowanie do szczególnych okoliczności rozpatrywanej sprawy, a jeśli tak jest,
 - b) czy przepisy prawa państwa trzeciego zastosowane do szczególnych okoliczności rozpatrywanej sprawy zabraniają ujawniania odnośnych danych.
5. Jeżeli właściwy sąd uzna, że nie występuje odnośny konflikt w rozumieniu ust. 1 i ust. 4, utrzymuje nakaz w mocy. Jeżeli właściwy sąd stwierdzi, że przepisy prawa państwa trzeciego zastosowane do szczególnych okoliczności rozpatrywanej sprawy zabraniają ujawniania odnośnych danych, właściwy sąd ustala, czy utrzymać w mocy, czy też uchylić nakaz, w szczególności w oparciu o następujące czynniki:
 - a) interesy chronione przez właściwe przepisy prawa państwa trzeciego, w tym interes państwa trzeciego związany z zapobieżeniem ujawnieniu odnośnych danych;
 - b) stopień powiązania sprawy karnej, w której wydano nakaz, z każdą z dwóch jurysdykcji, między innymi na podstawie:
 - lokalizacji, przynależności państwowej i miejsca pobytu osoby, której dane objęte są nakazem, lub ofiary (ofiary),
 - miejsca popełnienia odnośnego przestępstwa;
 - c) stopnia powiązania pomiędzy usługodawcą a państwem trzecim, którego sprawa dotyczy; w tym kontekście sama lokalizacja przechowywania danych nie wystarczy do stwierdzenia istotnego stopnia powiązania;
 - d) interesy państwa prowadzącego postępowanie przygotowawcze związane z uzyskaniem odnośnego materiału dowodowego w oparciu o wagę

przestępstwa i znaczenie uzyskania materiału dowodowego w najbliższym możliwym terminie;

e) możliwe konsekwencje dla adresata lub usługodawcy związane z wykonaniem europejskiego nakazu przedstawienia danych, w tym możliwe sankcje.

6. Jeżeli właściwy sąd podejmie decyzję o uchyleniu nakazu, informuje organ wydający i adresata. Jeżeli właściwy sąd stwierdzi, że nakaz ma być utrzymany w mocy, informuje organ wydający i adresata, który przystępuje do wykonania nakazu.

Artykuł 17

Skuteczne środki ochrony prawnej

1. Osoby podejrzane i oskarżone, których dane uzyskano na podstawie europejskiego nakazu wydania dowodów, są uprawnione do skorzystania ze skutecznych środków ochrony prawnej w związku z europejskim nakazem wydania dowodów w toku postępowania karnego, którego dotyczy nakaz, bez uszczerbku dla środków ochrony prawnej dostępnych na podstawie dyrektywy (UE) 2016/680 i rozporządzenia (UE) 2016/679.
2. Jeżeli osoba, której dane uzyskano, nie jest podejrzanym ani oskarżonym w postępowaniu karnym, w odniesieniu do którego wydano nakaz, osobie tej przysługuje prawo do skutecznych środków ochrony prawnej w związku z europejskim nakazem wydania dowodów w państwie wydającym, bez uszczerbku dla środków ochrony prawnej dostępnych na podstawie dyrektywy (UE) 2016/680 i rozporządzenia (UE) 2016/679.
3. Wspomniane prawo do skutecznego środka ochrony prawnej wykonuje się przed sądem w państwie wydającym zgodnie z jego prawem krajowym, przy czym obejmuje ono możliwość podważenia legalności środka, w tym jego konieczności i proporcjonalności.
4. Bez uszczerbku dla art. 11 organ wydający podejmuje właściwe środki mające na celu zapewnienie przekazania informacji na temat możliwości przewidzianych w przepisach krajowego prawa dotyczących środków ochrony prawnej, a także zapewnienie możliwości ich skutecznego zastosowania.
5. W niniejszym przypadku zastosowanie mają te same terminy lub pozostałe warunki korzystania ze środka ochrony prawnej, co w przypadku podobnych sytuacji krajowych – w sposób gwarantujący zainteresowanym osobom skuteczne zastosowanie tych środków ochrony prawnej.
6. Bez uszczerbku dla krajowych przepisów procesowych państwa członkowskie zapewniają przestrzeganie w postępowaniu karnym w państwie wydającym prawa do obrony i do rzetelnego postępowania przy ocenie materiału dowodowego uzyskanego za pomocą europejskiego nakazu wydania dowodów.

Artykuł 18

Zapewnienie przywilejów i immunitetów na podstawie prawa państwa wykonującego

Jeżeli dane dotyczące transakcji lub dane dotyczące treści uzyskane za pośrednictwem europejskiego nakazu wydania dowodów są chronione immunitetami lub przywilejami udzielonymi na podstawie przepisów prawa państwa członkowskiego adresata lub mają wpływ na podstawowe interesy tego państwa członkowskiego takie jak bezpieczeństwo

narodowe i obronność, sąd w tym państwie członkowskim zapewnia przy ocenie odpowiedniości i dopuszczalności odnośnego materiału dowodowego w toku postępowania karnego, w odniesieniu do którego wydano nakaz, uwzględnienie tych przesłanek w taki sam sposób, jak gdyby były one przewidziane w przepisach prawa jego państwa. Sąd może skonsultować się z organami właściwego państwa członkowskiego, Europejską Siecią Sądową w sprawach karnych lub Eurojust.

Rozdział 5: Przepisy końcowe

Artykuł 19

Monitorowanie i sprawozdawczość

1. Najpóźniej do *[data rozpoczęcia stosowania niniejszego rozporządzenia]* Komisja ustanowi szczegółowy program monitorowania wyników, rezultatów i skutków niniejszego rozporządzenia. Program monitorowania określa środki służące do gromadzenia danych i innych niezbędnych dowodów, a także przedziały czasowe, w jakich będą one gromadzone. Wskazane są w nim również działania podejmowane przez Komisję i przez państwa członkowskie w celu gromadzenia i analizowania danych oraz innych dowodów.
2. W każdym przypadku państwa członkowskie systematycznie gromadzą i utrzymują kompleksowe dane statystyczne uzyskiwane od właściwych organów. Zgromadzone dane przesyła się do Komisji każdego roku do dnia 31 marca za poprzedni rok kalendarzowy i obejmują one:
 - a) liczbę wydanych zaświadczeń europejskiego nakazu wydania dowodów i zaświadczeń europejskiego nakazu zabezpieczenia dowodów w podziale na rodzaje danych objętych nakazem, usługodawców, do których skierowano nakaz, i charakter sytuacji (sytuacja wyjątkowa lub nie);
 - b) liczbę wykonanych i niewykonanych zaświadczeń europejskiego nakazu wydania dowodów w podziale na rodzaje danych objętych nakazem, usługodawców, do których skierowano nakaz, i charakter sytuacji (sytuacja wyjątkowa lub nie);
 - c) w przypadku wykonanych zaświadczeń europejskiego nakazu zabezpieczenia dowodów – średni czas wymagany na uzyskanie danych objętych nakazem od momentu wydania zaświadczenia europejskiego nakazu zabezpieczenia dowodów do momentu uzyskania danych, w podziale na rodzaje danych objętych nakazem, usługodawców, do których skierowano nakaz, i charakter sytuacji (sytuacja wyjątkowa lub nie);
 - d) liczbę europejskich nakazów wydania dowodów przekazanych do celów postępowania przymuszającego do wykonania do państwa wykonującego i przez nie otrzymanych w podziale na rodzaje danych objętych nakazem, usługodawców, do których skierowano nakaz, i charakter sytuacji (sytuacja wyjątkowa lub nie) oraz liczbę wykonanych nakazów;
 - e) liczbę środków ochrony prawnej wniesionych w przypadku europejskich nakazów wydania dowodów w państwie wydającym i państwie wykonującym według rodzaju danych objętych nakazem.

Artykuł 20
Zmiany zaświadczeń i formularzy

Komisja przyjmuje akty delegowane zgodnie z art. 21 w celu wprowadzenia zmian w załącznikach I, II i III, by skutecznie zrealizować ewentualną potrzebę poprawienia treści formularzy zaświadczenia europejskiego nakazu wydania dowodów i zaświadczenia europejskiego nakazu zabezpieczenia dowodów oraz formularzy wykorzystywanych do przekazywania informacji na temat niemożliwości wykonania zaświadczenia europejskiego nakazu wydania dowodów lub zaświadczenia europejskiego nakazu zabezpieczenia dowodów.

Artykuł 21
Wykonywanie przekazanych uprawnień

1. Powierzenie Komisji uprawnień do przyjęcia aktów delegowanych podlega warunkom określonym w niniejszym artykule.
2. Uprawnienia do przyjęcia aktów delegowanych, o których mowa w art. 20, powierza się na czas nieokreślony od dnia *[data rozpoczęcia stosowania niniejszego rozporządzenia]*.
3. Przekazanie uprawnień, o którym mowa w art. 20, może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna od następnego dnia po jej opublikowaniu w Dzienniku Urzędowym Unii Europejskiej lub w określonym w tej decyzji późniejszym terminie. Nie wpływa ona na ważność jakichkolwiek już obowiązujących aktów delegowanych.
4. Przed przyjęciem aktu delegowanego Komisja konsultuje się z ekspertami wyznaczonymi przez każde państwo członkowskie zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym w sprawie lepszego stanowienia prawa z dnia 13 kwietnia 2016 r.⁵⁰.
5. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie.
6. Akt delegowany przyjęty na podstawie art. 20 wchodzi w życie tylko wówczas, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie dwóch miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie, lub gdy, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o dwa miesiące z inicjatywy Parlamentu Europejskiego lub Rady.

Artykuł 22
Powiadomienia

1. Do *[data rozpoczęcia obowiązywania niniejszego rozporządzenia]* każde państwo członkowskie przekazuje Komisji poniższe informacje:
 - a) organy, które – zgodnie z przepisami prawa krajowego danego państwa członkowskiego – są organami właściwymi zgodnie z art. 4 do wydawania lub

⁵⁰ Dz.U. L 123 z 12.5.2016, s. 13.

zatwierdzania europejskich nakazów wydania dowodów i europejskich nakazów zabezpieczenia dowodów;

b) organ lub organy przymuszające do wykonania nakazu właściwe w zakresie postępowania przymuszającego do wykonania europejskich nakazów wydania dowodów i europejskich nakazów zabezpieczenia dowodów w imieniu innego państwa członkowskiego;

c) sądy właściwe do rozpatrywania uzasadnionych sprzeciwów adresatów na podstawie art. 15 i 16.

2. Komisja publicznie udostępnia informacje otrzymane na podstawie niniejszego artykułu na specjalnej stronie internetowej lub na stronie internetowej Europejskiej Sieci Sądowej, o której mowa w art. 9 decyzji Rady 2008/976/WSiSW⁵¹.

Artykuł 23

Związek z europejskim nakazem dochodzeniowym

Organy państw członkowskich mogą nadal wydawać europejskie nakazy dochodzeniowe zgodnie z dyrektywą 2014/41/UE na potrzeby gromadzenia materiału dowodowego, który objęty byłby również zakresem niniejszego rozporządzenia.

Artykuł 24

Ocena

Najpóźniej do dnia [5 lat od daty rozpoczęcia stosowania niniejszego rozporządzenia] Komisja przeprowadzi ocenę rozporządzenia i przedstawi Parlamentowi Europejskiemu i Radzie sprawozdanie na temat funkcjonowania niniejszego rozporządzenia, które będzie obejmować ocenę potrzeby rozszerzenia zakresu rozporządzenia. W razie konieczności do sprawozdania załącza się wnioski legislacyjne. Ocena zostanie przeprowadzona zgodnie z wytycznymi Komisji dotyczącymi lepszego stanowienia prawa. Państwa członkowskie przekazują Komisji informacje niezbędne do przygotowania tego sprawozdania.

Artykuł 25

Wejście w życie

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

Rozporządzenie stosuje się od dnia [6 miesięcy po wejściu w życie].

⁵¹ Decyzja Rady 2008/976/WSiSW z dnia 16 grudnia 2008 r. w sprawie Europejskiej Sieci Sądowej (Dz.U. L 348 z 24.12.2008, s. 130).

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane w państwach członkowskich zgodnie z Traktatami.

Sporządzono w Brukseli dnia r.

*W imieniu Parlamentu Europejskiego
Przewodniczący*

*W imieniu Rady
Przewodniczący*