

**ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2023/1543****z dnia 12 lipca 2023 r.****w sprawie europejskich nakazów wydania i europejskich nakazów zabezpieczenia dowodów elektronicznych w postępowaniu karnym oraz w postępowaniu karnym wykonawczym w związku z wykonaniem kar pozbawienia wolności**

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-Społecznego <sup>(1)</sup>,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą <sup>(2)</sup>,

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 takiej przestrzeni, Unia przyjmuje 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 dowodów elektronicznych mają coraz większe znaczenie dla prowadzenia postępowań przygotowawczych i ścigania przestępstw w całej Unii. Skuteczne mechanizmy pozyskiwania dowodów elektronicznych mają kluczowe znaczenie dla zwalczania przestępczości, przy czym takie mechanizmy powinny podlegać warunkom i zabezpieczeniom mającym na celu zapewnienie pełnej zgodności z prawami podstawowymi i zasadami uznanymi w art. 6 Traktatu o Unii Europejskiej (TUE) i w Kartce praw podstawowych Unii Europejskiej (zwana dalej „Kartą”), w szczególności zasadami konieczności i proporcjonalności, sprawiedliwości proceduralnej, ochrony prywatności i danych osobowych oraz poufności komunikacji.
- (3) We wspólnym oświadczeniu unijnych ministrów sprawiedliwości i spraw wewnętrznych oraz przedstawicieli instytucji UE z dnia 24 marca 2016 r. w sprawie zamachów terrorystycznych w Brukseli podkreślono potrzebę, nadając jej charakter priorytetowy, szybszego i skuteczniejszego zabezpieczenia i pozyskiwania dowodów cyfrowych oraz określenia konkretnych środków do osiągnięcia tego celu.
- (4) W konkluzjach Rady z dnia 9 czerwca 2016 r. podkreślono rosnące znaczenie dowodów elektronicznych w postępowaniu karnym oraz znaczenie ochrony cyberprzestrzeni przed nadużyciami i działalnością przestępczą dla gospodarek i społeczeństw, a zatem potrzebę dysponowania przez organy ścigania i organy sądowe skutecznymi narzędziami prowadzenia postępowań przygotowawczych oraz ścigania przestępstw związanych z cyberprzestrzenią.
- (5) We wspólnym komunikacie Komisji oraz Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa do Parlamentu Europejskiego i Rady z dnia 13 września 2017 r. pt. „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej”, Komisja podkreśliła, że skuteczne prowadzenie dochodzeń i ściganie przestępczości wykorzystującej cyberprzestrzeń jest kluczowym czynnikiem prewencji wobec ataków cybernetycznych oraz że obecne ramy proceduralne wymagają lepszego dostosowania do potrzeb ery internetu. Szybkość ataków cybernetycznych może czasami okazywać się zbyt duża dla obecnych procedur, co stwarza specyficzne potrzeby w zakresie sprawnej współpracy transgranicznej.
- (6) W rezolucji Parlamentu Europejskiego z dnia 3 października 2017 r. w sprawie walki z cyberprzestępczością <sup>(3)</sup>, Parlament Europejski podkreślił potrzebę znalezienia sposobów szybszego zabezpieczenia i uzyskiwania dowodów elektronicznych, a także znaczenie ścisłej współpracy między organami ścigania, państwami trzecimi i dostawcami usług działającymi na terytorium europejskim, zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 <sup>(4)</sup> i dyrektywą Parlamentu Europejskiego i Rady

<sup>(1)</sup> Dz.U. C 367 z 10.10.2018, s. 88.

<sup>(2)</sup> Stanowisko Parlamentu Europejskiego z dnia 13 czerwca 2023 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z dnia 27 czerwca 2023 r.

<sup>(3)</sup> Dz.U. C 346 z 27.9.2018, s. 29.

<sup>(4)</sup> 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).

(UE) 2016/680<sup>(5)</sup> oraz obowiązującymi umowami o wzajemnej pomocy prawnej. W rezolucji tej Parlament Europejski podkreślił również, że obecnie fragmentaryczne ramy prawne mogą utrudniać dostawcom wykonanie żądań organów ścigania, i wezwał Komisję do przedstawienia unijnych ram prawnych dotyczących dowodów elektronicznych z wystarczającymi zabezpieczeniami praw i wolności wszystkich zaangażowanych podmiotów, a jednocześnie z zadowoleniem przyjął trwające w Komisji prace nad platformą współpracy obejmującą bezpieczny kanał komunikacji dla cyfrowych wymian informacji w sprawie europejskich nakazów dochodzeniowych (END) w celu gromadzenia dowodów elektronicznych i odpowiedzi między unijnymi organami sądowymi.

- (7) Usługi oparte na sieci można świadczyć z dowolnej lokalizacji i nie wymagają one fizycznej infrastruktury, pomieszczeń ani pracowników w kraju, gdzie oferowana jest dana usługa. W związku z tym odpowiednie dowody elektroniczne są często przechowywane poza państwem prowadzącym postępowanie przygotowawcze lub przez usługodawcę mającego siedzibę poza tym państwem, co stwarza wyzwania związane z gromadzeniem dowodów elektronicznych w postępowaniu karnym.
- (8) Ze względu na sposób, w jaki świadczone są usługi oparte na sieci, wnioski w ramach współpracy wymiarów sprawiedliwości są często kierowane do państw, w których zlokalizowana jest znaczna liczba usługodawców. Ponadto liczba wniosków znacznie się zwiększyła ze względu na fakt, że coraz częściej korzysta się z usług opartych na sieci. Dyrektywa Parlamentu Europejskiego i Rady nr 2014/41/UE<sup>(6)</sup> przewiduje możliwość wydania END do celów gromadzenia dowodów w innym państwie członkowskim. Ponadto Konwencja, ustanowiona przez Radę zgodnie z artykułem 34 Traktatu o Unii Europejskiej, o pomocy prawnej w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej<sup>(7)</sup> (zwana dalej „konwencją o pomocy prawnej w sprawach karnych”) również przewiduje możliwość wystąpienia o dowody do innego państwa członkowskiego. Jednak procedury i terminy przewidziane w dyrektywie 2014/41/UE ustanawiającej END i w konwencji o pomocy prawnej w sprawach karnych mogłyby nie być odpowiednie dla dowodów elektronicznych, które są mniej trwałe oraz mogą być łatwiej i szybciej usuwane. Pozyskanie dowodów elektronicznych z wykorzystaniem kanałów współpracy wymiarów sprawiedliwości często zabiera wiele czasu, co prowadzi do sytuacji, w których ślady przestępstw mogą już nie być dostępne. Co więcej, nie istnieją zharmonizowane ramy współpracy z usługodawcami, podczas gdy niektórzy usługodawcy z państw trzecich przyjmują bezpośrednie wnioski o dane inne niż dane dotyczące treści zgodnie z ich mającym zastosowanie prawem krajowym. W związku z powyższym państwa członkowskie w coraz większym stopniu korzystają z bezpośrednich dobrowolnych kanałów współpracy z usługodawcami, jeżeli są one dostępne, i stosują różne krajowe narzędzia, warunki i procedury. W przypadku danych dotyczących treści, niektóre państwa członkowskie podjęły jednostronne działania, podczas gdy inne nadal korzystają ze współpracy wymiarów sprawiedliwości.
- (9) Rozdrobnione ramy prawne stwarzają wyzwania dla organów ścigania, organów sądowych, a także dla usługodawców starających się stosować do przewidzianych prawem wniosków dotyczących dowodów elektronicznych, ponieważ mierzą się oni coraz częściej z niepewnością prawa i możliwą kolizją przepisów. Istnieje zatem potrzeba ustanowienia szczegółowych przepisów dotyczących transgranicznej współpracy sądowej w zakresie zabezpieczania i wydawania dowodów elektronicznych, które to przepisy uwzględniają szczególny charakter dowodów elektronicznych. Przepisy takie powinny obejmować obowiązek usługodawców objętych zakresem stosowania niniejszego rozporządzenia do bezpośredniego odpowiadania na wnioski organów w innym państwie członkowskim. Niniejsze rozporządzenie uzupełni zatem obowiązujące prawo unijne i doprecyzuje przepisy mające zastosowanie do organów ścigania i organów sądowych, a także do usługodawców, w dziedzinie dowodów elektronicznych, przy jednoczesnym zapewnieniu pełnej zgodności z prawami podstawowymi.
- (10) Niniejsze rozporządzenie nie narusza praw podstawowych i jest zgodne z zasadami uznanymi w art. 6 TUE i w Karcie, w prawie międzynarodowym i umowach międzynarodowych, których stronami są Unia lub wszystkie państwa członkowskie, w tym w europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności oraz w konstytucjach państw członkowskich we właściwych im obszarach zastosowania. Takie prawa i zasady obejmują w szczególności prawo do wolności i bezpieczeństwa osobistego, poszanowanie życia prywatnego i rodzinnego, ochronę danych osobowych, wolność prowadzenia działalności gospodarczej, prawo własności, prawo do skutecznego środka prawnego i dostępu do bezstronnego sądu, domniemanie niewinności i prawo do obrony, zasady legalności oraz proporcjonalności, a także zakaz ponownego sądenia lub karnia w postępowaniu karnym za ten sam czyn zabroniony pod groźbą kary.

<sup>(5)</sup> 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).

<sup>(6)</sup> Dyrektywa Parlamentu Europejskiego i Rady nr 2014/41/UE z dnia 3 kwietnia 2014 r. w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych (Dz.U. L 130 z 1.5.2014, s. 1).

<sup>(7)</sup> Konwencja, ustanowiona przez Radę zgodnie z artykułem 34 Traktatu o Unii Europejskiej, o pomocy prawnej w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej (Dz.U. C 197 z 12.7.2000, s. 3).

- (11) Żadnego z przepisów niniejszego rozporządzenia nie należy interpretować jako zakazującego odmowy realizacji europejskiego nakazu wydania dowodów przez organ przymuszający do wykonania nakazu, jeżeli na podstawie obiektywnych przesłanek można sądzić, że europejski nakaz wydania dowodów wydano w celu ścigania lub ukarania osoby ze względu na jej płeć, pochodzenie rasowe lub etniczne, religię, orientację seksualną lub tożsamość płciową, narodowość, język lub poglądy polityczne albo że jej sytuacja mogłaby ulec pogorszeniu z którejkolwiek z tych przyczyn.
- (12) Mechanizm europejskiego nakazu wydania dowodów i europejskiego nakazu zabezpieczenia dowodów elektronicznych w postępowaniu karnym opiera się na zasadzie wzajemnego zaufania pomiędzy państwami członkowskimi oraz na domniemaniu przestrzegania przez państwa członkowskie prawa Unii, zasady państwa prawnego, a w szczególności praw podstawowych, które stanowią kluczowe elementy unijnej przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Taki mechanizm umożliwia właściwym organom krajowym wysyłanie takich nakazów bezpośrednio do usługodawców.
- (13) Poszanowanie życia prywatnego i rodzinnego oraz ochrona osób fizycznych w związku z przetwarzaniem danych osobowych stanowią prawa podstawowe. Zgodnie z art. 7 i art. 8 ust. 1 Karty każda osoba ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się oraz do ochrony dotyczących jej danych osobowych.
- (14) Wdrażając niniejsze rozporządzenie, państwa członkowskie powinny zapewnić, by dane osobowe były objęte ochroną i były przetwarzane wyłącznie zgodnie z rozporządzeniem (UE) 2016/679 i dyrektywą (UE) 2016/680, a także dyrektywą 2002/58/WE<sup>(8)</sup> Parlamentu Europejskiego i Rady, w tym w razie dalszego wykorzystania, przesyłania lub dalszego przekazywania pozyskanych danych.
- (15) Dane osobowe pozyskane na mocy niniejszego rozporządzenia powinny być przetwarzane jedynie w razie konieczności i w sposób proporcjonalny do celów zapobiegania przestępstwom, prowadzenia w ich sprawie postępowania przygotowawczego, ich wykrywania i ścigania lub wykonywania kar i korzystania z prawa do obrony. W szczególności państwa członkowskie powinny zapewnić, by w odniesieniu do przekazywania danych osobowych przez odpowiednie organy usługodawcom na potrzeby niniejszego rozporządzenia miały zastosowanie właściwe procedury i środki ochrony danych, w tym środki mające na celu zapewnienie bezpieczeństwa tych danych. Usługodawcy powinni zapewnić, by te same gwarancje miały zastosowanie do przekazywania danych osobowych odpowiednim organom. Jedynie upoważnione osoby powinny mieć dostęp do informacji zawierających dane osobowe, które można uzyskać w procesach uwierzytelniania.
- (16) Prawa procesowe w postępowaniu karnym określone w dyrektywach Parlamentu Europejskiego i Rady 2010/64/UE<sup>(9)</sup>, 2012/13/UE<sup>(10)</sup>, 2013/48/UE<sup>(11)</sup>, (UE) 2016/343<sup>(12)</sup>, (UE) 2016/800<sup>(13)</sup> i (UE) 2016/1919<sup>(14)</sup> powinny mieć zastosowanie – w ramach zakresu stosowania tych dyrektyw – w postępowaniach karnych objętych niniejszym rozporządzeniem w odniesieniu do państw członkowskich związanych tymi dyrektywami. Zastosowanie powinny mieć również gwarancje proceduralne przewidziane w Karcie.
- (17) Aby zagwarantować pełne poszanowanie praw podstawowych, wartość dowodowa materiału dowodowego zgromadzonego dzięki zastosowaniu niniejszego rozporządzenia powinna być oceniana przez właściwy organ sądowy podczas procesu, zgodnie z prawem krajowym i w szczególności z poszanowaniem prawa do rzetelnego procesu sądowego i prawa do obrony.

<sup>(8)</sup> Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. L 201 z 31.7.2002, s. 37).

<sup>(9)</sup> 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).

<sup>(10)</sup> 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).

<sup>(11)</sup> 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 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).

<sup>(12)</sup> 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).

<sup>(13)</sup> 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).

<sup>(14)</sup> 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 wnioski w postępowaniu dotyczącym europejskiego nakazu aresztowania (Dz.U. L 297 z 4.11.2016, s. 1).

- (18) W niniejszym rozporządzeniu określono zasady, na podstawie których właściwy organ sądowy w Unii może – w postępowaniu karnym, w tym w postępowaniu przygotowawczym, lub w postępowaniu karnym wykonawczym w związku z wykonaniem kary pozbawienia wolności lub środka zabezpieczającego polegającego na pozbawieniu wolności zgodnie z niniejszym rozporządzeniem – nakazać usługodawcy oferującemu usługi w Unii, na podstawie europejskiego nakazu wydania dowodów lub europejskiego nakazu zabezpieczenia dowodów, wydanie lub zabezpieczenie dowodów elektronicznych. Niniejsze rozporządzenie powinno mieć zastosowanie we wszystkich sprawach transgranicznych, jeżeli usługodawca ma wyznaczony zakład lub przedstawiciela prawnego w innym państwie członkowskim. Niniejsze rozporządzenie pozostaje bez uszczerbku dla uprawnień organów krajowych do zwracania się do usługodawców posiadających zakład lub przedstawiciela na ich terytorium, aby przestrzegali podobnych środków krajowych.
- (19) Niniejsze rozporządzenie powinno regulować gromadzenie wyłącznie danych przechowywanych przez usługodawcę w momencie otrzymania europejskiego nakazu wydania dowodów lub europejskiego nakazu zabezpieczenia dowodów. Nie powinno ono ustanawiać ogólnego obowiązku zatrzymywania danych przez usługodawców i nie powinno skutkować ogólnym i niezróżnicowanym zatrzymywaniem danych. Niniejsze rozporządzenie nie powinno również upoważniać do przechwytywania danych ani pozyskiwania danych przechowywanych po otrzymaniu europejskiego nakazu wydania dowodów lub europejskiego nakazu zabezpieczenia dowodów.
- (20) Stosowanie niniejszego rozporządzenia nie powinno mieć wpływu na stosowanie szyfrowania przez usługodawców lub ich użytkowników. Dane, których zażądano poprzez europejski nakaz wydania dowodów lub europejski nakaz zabezpieczenia dowodów, należy wydać lub zabezpieczyć niezależnie od tego, czy są one zaszyfrowane, czy też nie. Niniejsze rozporządzenie nie powinno jednak nakładać na usługodawców obowiązku odszyfrowywania danych.
- (21) W wielu przypadkach dane nie są już przechowywane ani przetwarzane w inny sposób 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. Dlatego stosowanie rozporządzenia nie powinno zależeć od faktycznej lokalizacji zakładu usługodawcy ani faktycznej lokalizacji przetwarzania lub przechowywania danych.
- (22) Niniejsze rozporządzenie pozostaje bez uszczerbku dla uprawnień organów w postępowaniu cywilnym lub administracyjnym do prowadzenia postępowań wyjaśniających, również w sytuacji, gdy takie postępowania mogą prowadzić do nałożenia sankcji.
- (23) Ponieważ procedurę wzajemnej pomocy prawnej można by uznać za postępowanie karne zgodne z prawem krajowym mającym zastosowanie w państwach członkowskich, należy sprecyzować, że europejskie nakazy wydania dowodów ani europejskie nakazy zabezpieczenia dowodów nie powinny być wydawane w celu udzielenia wzajemnej pomocy prawnej innemu państwu członkowskiemu lub państwu trzeciemu. W takich przypadkach należy wystosować wniosek o wzajemną pomoc prawną do państwa członkowskiego lub państwa trzeciego, które mogą udzielić wzajemnej pomocy prawnej na mocy swojego prawa krajowego.
- (24) W ramach postępowań karnych europejski nakaz wydania dowodów i europejski nakaz zabezpieczenia dowodów należy wydawać wyłącznie w toku konkretnego postępowania karnego dotyczącego konkretnego przestępstwa, które miało miejsce, po przeprowadzeniu indywidualnej oceny konieczności i proporcjonalności tych nakazów w każdym indywidualnym przypadku, z uwzględnieniem praw podejrzanego lub oskarżonego.
- (25) Niniejsze rozporządzenie powinno mieć również zastosowanie do postępowań karnych wykonawczych wszczętych przez organ wydający, aby zlokalizować skazanego, który ukrywa się przed wymiarem sprawiedliwości, w celu wykonania kary pozbawienia wolności lub środka zabezpieczającego polegającego na pozbawieniu wolności. Jednakże w przypadku gdy wyrok skazujący na karę pozbawienia wolności lub orzeczenie o zastosowaniu środka zabezpieczającego polegającego na pozbawieniu wolności zostały wydane zaocznie, nie powinno być możliwości wydania europejskiego nakazu wydania dowodów ani europejskiego nakazu zabezpieczenia dowodów, gdyż w zakresie orzeczeń wydawanych zaocznie przepisy krajowe państw członkowskich w Unii znacznie się różnią.
- (26) Niniejsze rozporządzenie powinno mieć zastosowanie wobec usługodawców oferujących usługi w Unii, a wydanie nakazów przewidzianych w niniejszym rozporządzeniu powinno być możliwe wyłącznie w odniesieniu do danych dotyczących usług oferowanych w Unii. Usługi oferowane wyłącznie poza Unią nie powinny być objęte zakresem stosowania niniejszego rozporządzenia, nawet jeżeli usługodawca je oferujący ma siedzibę w Unii. W związku z tym niniejsze rozporządzenie nie powinno umożliwiać dostępu do danych innych niż dane związane z usługami oferowanymi użytkownikowi w Unii przez tych usługodawców.
- (27) Kluczowymi usługodawcami z punktu widzenia gromadzenia dowodów w postępowaniu karnym są dostawcy usług łączności elektronicznej oraz konkretni dostawcy usług społeczeństwa informacyjnego, którzy stwarzają użytkownikom warunki do interakcji. Dlatego też obie grupy należy objąć zakresem niniejszego rozporządzenia. Usługi łączności elektronicznej zdefiniowano w dyrektywie Parlamentu Europejskiego i Rady (UE) 2018/1972<sup>(15)</sup> i obejmują

<sup>(15)</sup> Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (Dz.U. L 321 z 17.12.2018, s. 36).

one usługi umożliwiające komunikację międzyludzką, takie jak usługi telefonii internetowej (VoIP), komunikatory internetowe i usługi poczty elektronicznej. Niniejsze rozporządzenie powinno mieć zastosowanie także do dostawców usług społeczeństwa informacyjnego w rozumieniu dyrektywy (UE) 2015/1535<sup>(16)</sup> Parlamentu Europejskiego i Rady, którzy nie zaliczają się do dostawców usług łączności elektronicznej, lecz oferują użytkownikom możliwość komunikowania się ze sobą lub oferują im usługi, które mogą być wykorzystywane do przechowywania lub przetwarzania w inny sposób danych w ich imieniu. Byłoby to zgodne z terminami stosowanymi w Konwencji Rady Europy o cyberprzestępczości (ETS nr 185) sporządzonej w Budapeszcie w dniu 23 listopada 2001 r. (zwaną dalej „konwencją o cyberprzestępczości”). Przetwarzanie danych należy rozumieć w sensie technicznym, jako tworzenie danych lub operowanie danymi, co oznacza techniczne operacje wytwarzania lub modyfikacji danych za pomocą mocy obliczeniowej komputerów. Kategorie usługodawców objęte niniejszym rozporządzeniem powinny uwzględniać na przykład internetowe platformy handlowe umożliwiające konsumentom i przedsiębiorstwom komunikowanie się ze sobą oraz inne usługi hostingowe, w tym w sytuacji, w której usługa jest zapewniana za pośrednictwem przetwarzania w chmurze, a także internetowe platformy gier komputerowych i gier losowych. Jeśli dostawca usług społeczeństwa informacyjnego nie umożliwia użytkownikom komunikowania się między sobą, lecz jedynie z nim samym, lub nie umożliwia przechowywania ani przetwarzania w inny sposób danych, lub w sytuacji, gdy przechowywanie danych nie jest elementem definiującym, czyli zasadniczą częścią usługi świadczonej użytkownikom, tak jak w przypadku usług prawnych, architektonicznych, inżynierskich i rachunkowych świadczonych przez internet na odległość, nie powinien on być objęty zakresem definicji „usługodawcy” określonej w niniejszym rozporządzeniu, nawet wówczas, gdy usługi świadczone przez tego usługodawcę odpowiadają definicji usług społeczeństwa informacyjnego w rozumieniu dyrektywy (UE) 2015/1535.

- (28) Dostawcy usług w zakresie infrastruktury internetowej związanych z przypisywaniem nazw i numeracji, takich jak rejestry nazw domen internetowych i rejestratorzy nazw domen internetowych oraz dostawcy usług prywatności i usług proxy, lub regionalne rejestry internetowe adresów protokołu internetowego (IP), mają szczególne znaczenie dla identyfikacji osób lub podmiotów stojących za szkodliwymi stronami internetowymi lub stronami internetowymi, które przejęto do przestępczych celów. Przechowują oni dane, które mogłyby umożliwić identyfikację osoby fizycznej lub podmiotu stojącego za stroną internetową wykorzystywaną w działalności przestępczej lub umożliwić identyfikację ofiary działalności przestępczej.
- (29) Ustalenie, czy usługodawca oferuje usługi w Unii, wymaga przeprowadzenia oceny, aby stwierdzić czy usługodawca umożliwia osobom fizycznym lub prawnym korzystanie ze swoich usług w co najmniej jednym państwie członkowskim. Niemniej sama dostępność interfejsu internetowego w Unii, jak na przykład dostępność strony internetowej lub adresu e-mail lub innych danych kontaktowych usługodawcy lub pośrednika, nie powinna sama z siebie być uznawana za wystarczającą do ustalenia, że usługodawca oferuje usługi w Unii w rozumieniu niniejszego rozporządzenia.
- (30) Istotny związek z Unią powinien być również znaczącą przesłanką przy ustalaniu, czy usługodawca oferuje usługi w Unii. Należy przyjąć, że taki istotny związek z Unią istnieje, gdy usługodawca posiada zakład w Unii. W przypadku braku takiego zakładu spełnienie kryterium istnienia istotnego związku powinno mieć za podstawę konkretne, oparte na faktach kryteria, takie jak istnienie znacznej liczby użytkowników w co najmniej jednym państwie członkowskim lub kierowanie działalności do co najmniej jednego państwa członkowskiego. Fakt kierowania działalności do co najmniej jednego państwa członkowskiego należy 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. Kierowanie działalności do danego państwa członkowskiego może być również stwierdzone na podstawie dostępności aplikacji w danym krajowym sklepie z aplikacjami, obecności reklam na rynku lokalnym lub posługiwania się w reklamach językiem powszechnie używanym w tym państwie członkowskim, lub utrzymywania kontaktów z klientami, takich jak w ramach obsługi klientów, w języku powszechnie używanym w tym państwie członkowskim. Należy uznać, że istotny związek występuje również w przypadku, gdy usługodawca kieruje swoją działalność do co najmniej jednego państwa członkowskiego jak określono w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 1215/2012<sup>(17)</sup>. Z drugiej strony, świadczenie usługi jedynie w celu przestrzegania zakazu dyskryminacji ustanowionego w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2018/302<sup>(18)</sup> nie powinno, bez dodatkowych podstaw, być uważane za kierowanie działalności do danego terytorium w Unii. To samo dotyczy ustalenia, czy dany usługodawca oferuje usługi w danym państwie członkowskim.

<sup>(16)</sup> 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).

<sup>(17)</sup> 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).

<sup>(18)</sup> 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 60 I z 2.3.2018, s. 1).

- (31) Niniejsze rozporządzenie powinno obejmować następujące kategorie danych: dane abonenta, dane o ruchu i dane dotyczące treści. Takie kategorie są zgodne z prawem wielu państw członkowskich i prawem Unii, takim jak dyrektywa 2002/58/WE, oraz orzecznictwem Trybunału Sprawiedliwości, a także z prawem międzynarodowym, w szczególności konwencją o cyberprzestępczości.
- (32) Adresy IP, a także numery dostępu i powiązane informacje mogą stanowić kluczowy punkt wyjścia dla postępowań przygotowawczych, w których tożsamość podejrzanego nie jest znana. Są one zazwyczaj ujęte w ewidencji zdarzeń, zwanej również dziennikiem serwera, która wskazuje rozpoczęcie i zakończenie sesji dostępu użytkownika do usługi. Często interfejs sieciowy wykorzystywany podczas sesji dostępu można wyodrębnić dzięki indywidualnemu adresowi IP, czy to statycznemu, czy dynamicznemu, lub innemu identyfikatorowi. Potrzebne są powiązane informacje na temat rozpoczęcia i zakończenia sesji dostępu użytkownika do usługi, takie jak informacje dotyczące portów źródłowych oraz znacznika czasu, ponieważ adresy IP są często wymieniane między użytkownikami, na przykład w przypadku translacji adresów sieciowych klasy operatorskiej (CGN) lub jej odpowiedników technicznych. Jednak zgodnie z dorobkiem prawnym Unii adresy IP uznaje się za dane osobowe i muszą one być objęte pełną ochroną na mocy unijnego dorobku prawnego w zakresie ochrony danych. Ponadto w pewnych okolicznościach adresy IP można uznać za dane o ruchu. Co więcej, w niektórych państwach członkowskich za dane o ruchu uznaje się numery dostępu i powiązane informacje. Jednakże do celów konkretnego postępowania przygotowawczego organy ścigania mogą potrzebować zażądać podania adresu IP, a także numerów dostępu i powiązanych informacji wyłącznie w celu identyfikacji użytkownika, zanim można zażądać od usługodawcy danych abonenta związanych z tym identyfikatorem. W takich przypadkach właściwe jest stosowanie takiego samego systemu jak dla danych abonenta, zdefiniowanych w niniejszym rozporządzeniu.
- (33) W przypadku gdy adresów IP, numerów dostępu i powiązanych informacji nie zażądano wyłącznie w celu identyfikacji użytkownika w konkretnym postępowaniu przygotowawczym, zazwyczaj żąda się ich, by uzyskać informacje bardziej naruszające prywatność, takie jak dane kontaktowe i miejsce pobytu użytkownika. Mogą one służyć ustanowieniu kompleksowego profilu danej osoby fizycznej, przy czym można je łatwiej przetwarzać i analizować niż dane dotyczące treści, ponieważ są przedstawiane w ustrukturyzowanym i znormalizowanym formacie. Istotne jest zatem, aby w takich sytuacjach adresy IP, numery dostępu i powiązane informacje, o które nie zwrócono się wyłącznie w celu identyfikacji użytkownika w konkretnym postępowaniu przygotowawczym, były traktowane jako dane o ruchu a żądania o ich wydanie były wystosowywane w ramach takiego samego systemu, jak stosowany w odniesieniu do danych dotyczących treści w rozumieniu niniejszego rozporządzenia.
- (34) Ponieważ wszystkie kategorie danych zawierają dane osobowe, są one objęte zabezpieczeniami przewidzianymi w dorobku prawnym Unii w dziedzinie ochrony danych osobowych. Jednak skala wpływu na prawa podstawowe różni się w zależności od kategorii, w szczególności między danymi abonenta i danymi, których zażądano wyłącznie w celu identyfikacji użytkownika zdefiniowanymi w niniejszym rozporządzeniu, z jednej strony, a danymi o ruchu – z wyjątkiem danych, których zażądano wyłącznie w celu identyfikacji użytkownika zdefiniowanych w niniejszym rozporządzeniu – i danymi dotyczącymi treści, z drugiej strony. Podczas gdy dane abonenta, jak również adresy IP, numery dostępu i powiązane informacje, jeżeli są przedmiotem żądania wyłącznie w celu identyfikacji użytkownika, mogą być przydatne do uzyskania pierwszych poszlak w postępowaniu przygotowawczym umożliwiających ustalenie tożsamości podejrzanego, dane o ruchu – z wyjątkiem danych, których zażądano wyłącznie w celu identyfikacji użytkownika zdefiniowanych w niniejszym rozporządzeniu – i dane dotyczące treści są często bardziej istotne jako dowody. Zasadnicze znaczenie ma zatem objęcie niniejszym rozporządzeniem wszystkich tych kategorii danych. Z uwagi na różny stopień wpływu na prawa podstawowe w odniesieniu do pozyskiwania takich danych zastosowanie powinny mieć odpowiednie zabezpieczenia i warunki.
- (35) Sytuacje, w których istnieje bezpośrednie zagrożenie życia lub integralności cielesnej lub bezpieczeństwa osoby, powinny być traktowane jako sytuacje wyjątkowe i powinny pozwalać na stosowanie krótszych terminów dla usługodawcy i organu przymuszającego do wykonania nakazu. W przypadku gdy zakłócenie lub zniszczenie infrastruktury krytycznej zdefiniowanej w dyrektywie Rady 2008/114/WE<sup>(19)</sup> wiązałoby się z takim zagrożeniem, w tym poprzez poważne zakłócenie podstawowych dostaw dla ludności lub wykonywania podstawowych funkcji państwa, taką sytuację należy również traktować jako sytuację wyjątkową, zgodnie z prawem Unii.
- (36) 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 o ruchu – z wyjątkiem danych, których zażądano wyłącznie w celu identyfikacji użytkownika zdefiniowanych w niniejszym rozporządzeniu – i danych dotyczących treści, wydanie lub zatwierdzenie europejskiego nakazu wydania dowodów w celu pozyskania danych należących do tych kategorii wymaga rozpatrzenia przez sędziego. Ponieważ dane abonenta i dane, których zażądano wyłącznie

<sup>(19)</sup> 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 z 23.12.2008, s. 75).

w celu identyfikacji użytkownika zdefiniowanych w niniejszym rozporządzeniu są mniej wrażliwe, europejski nakaz wydania dowodów w celu pozyskania takich danych może być dodatkowo wydany lub zatwierdzony przez właściwego prokuratora. Zgodnie z prawem dostępu do bezstronnego sądu, chronionym na mocy Karty i europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, prokuratorzy wykonują swoje obowiązki w sposób obiektywny, podejmując decyzję w sprawie wydania lub zatwierdzenia europejskiego nakazu wydania dowodów lub europejskiego nakazu zabezpieczenia dowodów wyłącznie na podstawie okoliczności faktycznych zawartych w aktach sprawy i z uwzględnieniem wszystkich dowodów obciążających i uniewinniających.

- (37) Aby zapewnić pełną ochronę praw podstawowych, zatwierdzenie europejskich nakazów wydania dowodów lub europejskich nakazów zabezpieczenia dowodów przez organy sądowe należy z zasady uzyskać przed wydaniem danego nakazu. Wyjątki od tej reguły powinny być dopuszczane tylko w należycie ustalonych sytuacjach wyjątkowych, w przypadku żądania wydania danych abonenta lub danych, których zażądano wyłącznie w celu identyfikacji użytkownika zdefiniowanych w niniejszym rozporządzeniu, lub żądania zabezpieczenia danych, jeśli nie ma możliwości uzyskania na czas uprzedniego zatwierdzenia przez organ sądowy, w szczególności z powodu braku możliwości skontaktowania się z organem zatwierdzającym, a zagrożenie jest tak bezpośrednie, że konieczne są natychmiastowe działania. Wyjątki takie należy jednak stosować tylko wtedy, gdy organ wydający dany nakaz może wydać nakaz w podobnej sprawie krajowej na mocy prawa krajowego bez uprzedniego zatwierdzenia.
- (38) Europejski nakaz wydania dowodów powinno się wydawać wyłącznie wówczas, gdy jest on konieczny, proporcjonalny, odpowiedni i ma zastosowanie w danej sprawie. Organ wydający powinien brać pod uwagę prawa podejrzanego lub oskarżonego w postępowaniu dotyczącym przestępstwa i powinien wydawać europejski nakaz wydania dowodów tylko wtedy, gdy taki nakaz mógłby zostać wydany na takich samych warunkach w podobnej sprawie krajowej. Podczas oceny stosowności wydania europejskiego nakazu wydania dowodów należy wziąć pod uwagę, czy taki nakaz jest ograniczony do tego, co jest bezwzględnie konieczne do osiągnięcia zgodnego z prawem celu polegającego na pozyskaniu danych, które są odpowiednie i niezbędne jako dowód w indywidualnej sprawie.
- (39) W przypadku wydania europejskiego nakazu wydania dowodów w celu pozyskania różnych kategorii danych, organ wydający powinien zapewnić spełnienie wszystkich warunków i procedur, takich jak powiadomienie organu przymuszającego do wykonania nakazu, w odniesieniu do każdej ze stosownych kategorii danych.
- (40) Ze względu na bardziej wrażliwy charakter danych o ruchu – z wyjątkiem danych, których zażądano wyłącznie w celu identyfikacji użytkownika zdefiniowanych w niniejszym rozporządzeniu – i danych dotyczących treści, powinno się wprowadzić rozróżnienie dotyczące zakresu przedmiotowego niniejszego rozporządzenia. Powinna istnieć możliwość wydania europejskiego nakazu wydania dowodów służącego pozyskaniu danych abonenta lub pozyskaniu danych, których zażądano wyłącznie w celu identyfikacji użytkownika zdefiniowanych w niniejszym rozporządzeniu, w odniesieniu do jakiegokolwiek przestępstwa, podczas gdy europejski nakaz wydania dowodów mający na celu pozyskanie danych o ruchu – z wyjątkiem danych, których zażądano wyłącznie w celu identyfikacji użytkownika zdefiniowanych w niniejszym rozporządzeniu – lub pozyskanie danych dotyczących treści powinien podlegać bardziej rygorystycznym wymogom w celu odzwierciedlenia bardziej wrażliwego charakteru takich danych. W niniejszym rozporządzeniu należy przewidzieć próg w odniesieniu do jego zakresu, umożliwiający obranie proporcjonalnego podejścia, wraz z szeregiem innych warunków i zabezpieczeń *ex ante* i *ex post* mających na celu zapewnienie poszanowania zasady proporcjonalności i praw osób zainteresowanych. Jednocześnie próg taki nie powinien ograniczać skuteczności niniejszego rozporządzenia ani utrudniać jego stosowania przez praktyków. Umożliwienie wydawania europejskich nakazów wydania dowodów w postępowaniach karnych jedynie w sprawie przestępstw zagrożonych karą pozbawienia wolności o górnej granicy ustawowego zagrożenia w wysokości co najmniej trzech lat ograniczy zakres stosowania niniejszego rozporządzenia do poważniejszych przestępstw, nie oddziałując nadmiernie na możliwości jego stosowania przez praktyków. Ograniczenie to wyłączyłoby z zakresu stosowania niniejszego rozporządzenia znaczną liczbę przestępstw, które państwa członkowskie uważają za mniej poważne, co znajduje odzwierciedlenie w niższej maksymalnej karze. Zaletą tego ograniczenia będzie również łatwość jego stosowania w praktyce.
- (41) Istnieją szczególne przestępstwa, w przypadku których dowody będą w typowej sytuacji dostępne 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 mogłyby spowodować rozległe i znaczące szkody, w szczególności przestępstwa charakteryzujące się małym wpływem jednostkowym, ale znacznym wolumenem i wielkością ogólnych szkód. W większości przypadków, w których przestępstwo popełniono przy użyciu systemu informatycznego, zastosowanie tego samego progu co w odniesieniu do innych rodzajów przestępstw, prowadziłoby w znacznym zakresie do bezkarności. Uzasadnia to stosowanie niniejszego rozporządzenia w odniesieniu do takich przestępstw także w sytuacjach, w których górna granica ustawowego zagrożenia karą pozbawienia wolności jest niższa niż trzy lata. W przypadku pozostałych przestępstw związanych z terroryzmem w rozumieniu dyrektywy Parlamentu Europejskiego i Rady (UE) 2017/541<sup>(20)</sup>, a także

<sup>(20)</sup> 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).

przestępstw związanych z niegodziwym traktowaniem w celach seksualnych i wykorzystywaniem seksualnym dzieci w rozumieniu dyrektywy Parlamentu Europejskiego i Rady 2011/93/UE<sup>(21)</sup>, nie powinien mieć zastosowania próg górnej granicy ustawowego zagrożenia karą w wysokości co najmniej trzech lat pozbawienia wolności.

- (42) Co do zasady europejski nakaz wydania dowodów powinien być kierowany do usługodawcy działającego w charakterze administratora. W pewnych okolicznościach ustalenie, czy usługodawca pełni rolę administratora lub podmiotu przetwarzającego, może jednak okazać się szczególnie trudne, w szczególności gdy w przetwarzanie danych zaangażowanych jest kilku usługodawców lub gdy usługodawcy przetwarzają dane w imieniu osoby fizycznej. Rozróżnienie ról administratora i podmiotu przetwarzającego w odniesieniu do konkretnego zbioru danych wymaga nie tylko specjalistycznej wiedzy na temat kontekstu prawnego, ale również może wymagać interpretacji często bardzo złożonych struktur umownych przewidujących w konkretnym przypadku powierzenie różnym usługodawcom różnych zadań i ról w odniesieniu do określonego zbioru danych. W przypadku gdy usługodawcy przetwarzają dane w imieniu osoby fizycznej, w niektórych przypadkach ustalenie, kto jest administratorem, może być trudne, nawet jeżeli zaangażowany jest tylko jeden usługodawca. W przypadku gdy odnośne dane są przechowywane lub w inny sposób przetwarzane przez usługodawcę i pomimo rozsądnych starań ze strony organu wydającego nie ma jasności co do tego, kto jest administratorem, powinna istnieć możliwość skierowania europejskiego nakazu wydania dowodów bezpośrednio do tego usługodawcy. Ponadto w niektórych przypadkach zwrócenie się do administratora mogłoby zaszkodzić postępowaniu przygotowawczemu w danej sprawie, na przykład dlatego, że administrator jest podejrzanym, oskarżonym lub skazanym, lub istnieją przesłanki wskazujące na to, że administrator może działać w interesie osoby, której dotyczy postępowanie przygotowawcze. Również w takich przypadkach powinna istnieć możliwość skierowania europejskiego nakazu wydania dowodów bezpośrednio do usługodawcy przetwarzającego dane w imieniu administratora. Nie powinno to wpływać na prawo organu wydającego do nakazania usługodawcy zabezpieczenia danych.
- (43) Zgodnie z rozporządzeniem (UE) 2016/679 podmiot przetwarzający, który przechowuje lub w inny sposób przetwarza dane w imieniu administratora, powinien poinformować administratora o wydaniu danych, chyba że organ wydający zwrócił się do usługodawcy o powstrzymanie się od informowania administratora, tak długo, jak jest to konieczne i proporcjonalne, aby nie utrudniać odnośnego postępowania karnego. W takim przypadku organ wydający powinien wskazać w aktach sprawy przyczyny opóźnienia w poinformowaniu administratora, a w dołączanym zaświadczeniu przekazywanym adresatowi należy również dodać krótkie uzasadnienie.
- (44) Jeżeli dane są przechowywane lub przetwarzane w inny sposób w ramach infrastruktury zapewnianej przez usługodawcę organowi publicznemu, wydanie europejskiego nakazu wydania dowodów lub europejskiego nakazu zabezpieczenia dowodów powinno być możliwe tylko wtedy, gdy organ publiczny, dla którego dane są przechowywane lub przetwarzane w inny sposób, znajduje się w państwie wydającym.
- (45) W przypadku gdy dane chronione tajemnicą zawodową na podstawie prawa państwa wydającego są przechowywane lub przetwarzane w inny sposób przez usługodawcę w ramach infrastruktury zapewnianej przedstawicielom zawodów objętych tajemnicą zawodową w związku z ich działalnością zawodową, wydanie europejskiego nakazu wydania dowodów powinno być możliwe wyłącznie w celu pozyskania danych o ruchu – z wyjątkiem danych, których zażądano wyłącznie w celu identyfikacji użytkownika zdefiniowanych w niniejszym rozporządzeniu – lub w celu pozyskania danych dotyczących treści, jeżeli przedstawiciel zawodu objętego tajemnicą zawodową ma miejsce pobytu w państwie wydającym, w którym zwrócenie się do przedstawiciela zawodu objętego tajemnicą zawodową może zaszkodzić postępowaniu przygotowawczemu, lub jeżeli tajemnica zawodowa została uchylona zgodnie z obowiązującym prawem.
- (46) Zasada *ne bis in idem* jest jedną z podstawowych zasad prawa w Unii, uznaną w Karcie praw podstawowych i rozwiniętą w orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej. Jeżeli organ wydający ma podstawy, by sądzić, że w innym państwie członkowskim mogłoby toczyć się równoległe postępowanie karne, organ ten konsultuje się z organami tego państwa członkowskiego zgodnie z decyzją ramową Rady 2009/948/WSiSW<sup>(22)</sup>. W każdym wypadku nie wydaje się europejskiego nakazu wydania dowodów lub europejskiego nakazu zabezpieczenia dowodów, jeśli organ wydający ma podstawy, by sądzić, że byłoby to sprzeczne z zasadą *ne bis in idem*.
- (47) Immunitety i przywileje, które mogą dotyczyć pewnych kategorii osób, na przykład dyplomatów, lub relacje podlegające szczególnej ochronie, na przykład prawnicza tajemnica zawodowa lub prawo dziennikarzy do niewyjawiania swoich źródeł informacji, są wspomniane w innych instrumentach wzajemnego uznawania, takich jak dyrektywa 2014/41/UE ustanawiająca END. Zasięg i wpływ immunitetów i przywilejów jest różny w zależności od mającego zastosowanie prawa krajowego, które należy wziąć pod uwagę w momencie wydawania europejskiego nakazu wydania dowodów lub europejskiego nakazu zabezpieczenia dowodów, ponieważ organ wydający powinien mieć możliwość wydania nakazu jedynie wówczas, gdy można byłoby go wydać na takich

<sup>(21)</sup> 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).

<sup>(22)</sup> Decyzja ramowa Rady 2009/948/WSiSW z dnia 30 listopada 2009 r. w sprawie zapobiegania konfliktom jurysdykcji w postępowaniu karnym i w sprawie rozstrzygnięcia takich konfliktów (Dz.U. L 328 z 15.12.2009, s. 42).



samych warunkach w podobnej sprawie krajowej. W prawie Unii nie istnieje wspólna definicja immunitetu ani przywileju. Dokładna definicja tych terminów pozostawiona jest zatem prawu krajowemu, a definicja ta może obejmować środki ochrony, które mają zastosowanie na przykład do zawodów medycznych i prawniczych, w tym w przypadku korzystania przy wykonywaniu tych zawodów z wyspecjalizowanych platform. Dokładna definicja immunitetów i przywilejów może również obejmować zasady ustalania i granic odpowiedzialności karnej związane z wolnością prasy i wolnością wypowiedzi w innych mediach.

- (48) Jeżeli organ wydający stara się pozyskać dane o ruchu – z wyjątkiem danych, których zażądano wyłącznie w celu identyfikacji użytkownika zdefiniowanych w niniejszym rozporządzeniu – lub dane dotyczące treści poprzez europejski nakaz wydania dowodów i ma uzasadnione podstawy, by przypuszczać, że dane objęte nakazem chronione są immunitetami lub przywilejami przysługującymi na podstawie prawa państwa wykonującego lub, że dane te podlegają w tym państwie przepisom dotyczącym ustalania i granic odpowiedzialności karnej związanym z wolnością prasy i wolnością wypowiedzi w innych mediach, organ wydający powinien móc wystąpić o wyjaśnienia przed wydaniem europejskiego nakazu wydania dowodów, w tym w drodze konsultacji z właściwymi organami państwa wykonującego, bezpośrednio lub za pośrednictwem Eurojustu lub Europejskiej Sieci Sądowej.
- (49) Wydanie europejskiego nakazu zabezpieczenia powinno być możliwe w odniesieniu do dowolnego przestępstwa. Organ wydający powinien brać pod uwagę prawa podejrzanego lub oskarżonego w postępowaniu dotyczącym przestępstwa i powinien wydawać europejski nakaz zabezpieczenia dowodów tylko wtedy, gdy taki nakaz mógłby zostać wydany na takich samych warunkach w podobnej sprawie krajowej i gdy jest on konieczny, proporcjonalny, odpowiedni i ma zastosowanie w danej sprawie. Podczas oceny stosowności wydania europejskiego nakazu zabezpieczenia dowodów należy wziąć pod uwagę, czy taki nakaz jest ograniczony do tego, co jest bezwzględnie konieczne do osiągnięcia zgodnego z prawem celu polegającego na zapobieżeniu usunięciu, skasowaniu lub zmianie danych, które są istotne i konieczne jako dowód w indywidualnej sprawie, w sytuacjach, w których doprowadzenie do wydania tych danych mogłoby zająć więcej czasu.
- (50) Europejskie nakazy wydania dowodów i europejskie nakazy zabezpieczenia dowodów powinny być kierowane bezpośrednio do wyznaczonego zakładu wskazanego przez usługodawcę zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) 2023/1544<sup>(23)</sup> lub do przedstawiciela prawnego ustanowionego przez niego zgodnie z tą dyrektywą. Wyjątkowo, w sytuacjach wyjątkowych określonych w niniejszym rozporządzeniu, jeżeli wyznaczony zakład lub przedstawiciel prawny usługodawcy nie zareaguje na dołączone zaświadczenie europejskiego nakazu wydania dowodów (EPOC) lub zaświadczenie europejskiego nakazu zabezpieczenia dowodów (EPOC-PR) w określonych terminach lub nie został wskazany lub ustanowiony w terminach określonych w dyrektywie (UE) 2023/1544, powinna istnieć możliwość skierowania EPOC lub EPOC-PR do dowolnego innego zakładu lub przedstawiciela prawnego usługodawcy w Unii równoległe do postępowania przymuszającego do wykonania pierwotnego nakazu lub zamiast tego postępowania zgodnie z niniejszym rozporządzeniem. Z uwagi na te różne możliwe scenariusze, w przepisach niniejszego rozporządzenia stosuje się ogólny termin „adresat”.
- (51) Z uwagi na bardziej wrażliwy charakter europejskiego nakazu wydania dowodów mającego na celu pozyskanie danych o ruchu – z wyjątkiem danych, których zażądano wyłącznie w celu identyfikacji użytkownika zdefiniowanych w niniejszym rozporządzeniu – lub pozyskanie danych dotyczących treści, właściwe jest, by przewidzieć mechanizm powiadamiania mający zastosowanie do europejskich nakazów wydania dowodów mających na celu pozyskanie tych kategorii danych. Ten mechanizm powiadamiania powinien obejmować organ przymuszający do wykonania nakazu i polegać na przekazaniu EPOC temu organowi jednocześnie z przekazaniem EPOC adresatowi. Jeżeli jednak europejski nakaz wydania dowodów jest wydawany w celu pozyskania dowodów elektronicznych w postępowaniu karnym o istotnych i silnych powiązaniach z państwem wydającym, powiadomienie organu przymuszającego do wykonania nakazu nie powinno być wymagane. Należy założyć istnienie takich powiązań, jeżeli w chwili wydawania europejskiego nakazu wydania dowodów organ wydający ma uzasadnione podstawy, by sądzić, że przestępstwo zostało popełnione, jest popełniane lub istnieje prawdopodobieństwo jego popełnienia w państwie wydającym, a osoba, której dane są objęte nakazem, zamieszkuje w państwie wydającym.
- (52) Do celów niniejszego rozporządzenia uznaje się, że przestępstwo zostało popełnione, jest popełniane lub istnieje prawdopodobieństwo jego popełnienia w państwie wydającym, jeżeli uznaje się je za takie zgodnie z prawem krajowym państwa wydającego. W niektórych przypadkach, zwłaszcza w dziedzinie cyberprzestępczości, niektóre elementy faktyczne, takie jak miejsce pobytu osoby poszkodowanej, są zazwyczaj ważnymi przesłankami, które należy wziąć pod uwagę przy ustalaniu miejsca popełnienia przestępstwa. Na przykład przestępstwa z użyciem oprogramowania szantażującego można często uznać za popełnione tam, gdzie osoba poszkodowana przez takie przestępstwo ma miejsce pobytu, nawet jeżeli nie ma pewności co do dokładnego miejsca, z którego uruchomiono oprogramowanie szantażujące. Wszelkie ustalenia dotyczące miejsca popełnienia przestępstwa powinny pozostawać bez uszczerbku dla przepisów dotyczących jurysdykcji w odniesieniu do odnośnych przestępstw zgodnie z mającym zastosowanie prawem krajowym.

<sup>(23)</sup> Dyrektywa Parlamentu Europejskiego i Rady (UE) 2023/1544 z dnia 12 lipca 2023 r. w sprawie zharmonizowanych przepisów dotyczących wskazywania wyznaczonych zakładów i ustanawiania przedstawicieli prawnych w celu gromadzenia dowodów elektronicznych w postępowaniach karnych (zob. s. 181 niniejszego Dziennika Urzędowego).

- (53) Do organu wydającego należy ocena – w momencie wydawania europejskiego nakazu wydania dowodów w celu uzyskania danych o ruchu, z wyjątkiem danych, których zażądano wyłącznie w celu identyfikacji użytkownika zdefiniowanych w niniejszym rozporządzeniu, lub uzyskania danych dotyczących treści oraz na podstawie dostępnych wcześniej materiałów – czy istnieją uzasadnione podstawy, by sądzić, że osoba, której dane są objęte nakazem, ma miejsce pobytu w państwie wydającym. W tym względzie istotne mogą być różne obiektywne okoliczności, które mogą wskazywać na to, że dana osoba ustanowiła lub zamierza ustanowić zwykły ośrodek swoich interesów życiowych w danym państwie członkowskim. Z potrzeby jednolitego stosowania prawa Unii oraz z zasady równości wynika, że pojęcie „miejsca pobytu” w tym szczególnym kontekście powinno być interpretowane w całej Unii w sposób jednolity. Uzasadnione podstawy do przypuszczenia, że dana osoba ma miejsce pobytu w państwie wydającym, mogą istnieć w szczególności w przypadku gdy dana osoba jest zarejestrowana jako osoba zamieszkała w państwie wydającym, na co wskazuje posiadanie dokumentu tożsamości lub zezwolenia na pobyt lub rejestracja w oficjalnym rejestrze meldunkowym. W przypadku braku rejestracji w państwie wydającym miejsce pobytu w tym państwie członkowskim może wynikać z faktu, że dana osoba wyraziła zamiar osiedlenia się w nim lub zyskała, po stałym okresie pobytu w tym państwie członkowskim, pewne więzi z tym państwem, podobne do tych, które wynikają z ustanowienia formalnego miejsca pobytu w tym państwie członkowskim. W celu ustalenia, czy w konkretnej sytuacji istnieją wystarczające powiązania między daną osobą a państwem wydającym, dające uzasadnione podstawy, by sądzić, że dana osoba ma miejsce pobytu w tym państwie, można wziąć pod uwagę różne obiektywne czynniki charakteryzujące sytuację tej osoby, do których to czynników należą w szczególności długość, charakter i warunki obecności tej osoby w państwie wydającym lub więzi rodzinne lub gospodarcze, które łączą ją z tym państwem członkowskim. Zarejestrowany pojazd, rachunek bankowy, fakt nieprzerwanego pobytu danej osoby w państwie wydającym lub inne obiektywne czynniki mogą mieć znaczenie dla ustalenia, czy istnieją uzasadnione podstawy, by sądzić, że dana osoba ma miejsce pobytu w państwie wydającym. Krótka wizyta, spędzenie urlopu, w tym w domu wakacyjnym, lub podobnego rodzaju pobyt w państwie wydającym bez dalszych istotnych powiązań nie są wystarczające do stwierdzenia miejsca pobytu w tym państwie członkowskim. W przypadkach gdy w momencie wydawania europejskiego nakazu wydania dowodów w celu uzyskania danych o ruchu – z wyjątkiem danych, których zażądano wyłącznie w celu identyfikacji użytkownika zdefiniowanych w niniejszym rozporządzeniu – lub w celu uzyskania danych dotyczących treści, organ wydający nie ma uzasadnionych podstaw, by sądzić, że osoba, której dane są objęte nakazem, ma miejsce pobytu w państwie wydającym, organ wydający powinien powiadomić o tym organ przymuszający do wykonania nakazu.
- (54) Aby zapewnić sprawny przebieg postępowania, momentem, w którym należy zdecydować o istnieniu potrzeby powiadomienia organu przymuszającego do wykonania nakazu wydania dowodów w celu uzyskania danych o ruchu, z wyjątkiem danych, których zażądano wyłącznie w celu identyfikacji użytkownika zdefiniowanych w niniejszym rozporządzeniu, lub w celu uzyskania danych dotyczących treści, organ wydający powinien być moment wydania europejskiego nakazu wydania dowodów. Późniejsze zmiany miejsca pobytu nie powinny mieć wpływu na postępowanie. Zainteresowana osoba powinna mieć możliwość powoływania się na swoje prawa, a także na przepisy dotyczące ustalania i granic odpowiedzialności karnej związane z wolnością prasy i wolnością wypowiedzi w innych mediach, w trakcie całego postępowania karnego, a organ przymuszający do wykonania nakazu powinien mieć możliwość powołania się na podstawę odmowy, jeżeli, w wyjątkowych sytuacjach, istnieją istotne podstawy, by sądzić – na podstawie konkretnych i obiektywnych dowodów – że wykonanie nakazu w szczególnych okolicznościach danej sprawy wiązałoby się z oczywistym naruszeniem odpowiedniego prawa podstawowego określonego w art. 6 TUE i w Karcie. Ponadto powinna istnieć możliwość powoływania się na te podstawy również w toku postępowania przymuszającego do wykonania nakazu.
- (55) Europejski nakaz wydania dowodów należy przekazać w formie EPOC, a europejski nakaz zabezpieczenia dowodów należy przekazać w formie EPOC-PR. W razie potrzeby EPOC lub EPOC-PR powinien zostać przetłumaczony na język urzędowy Unii zaakceptowany przez adresata. Jeżeli usługodawca nie wskazał żadnego języka, EPOC lub EPOC-PR powinien zostać przetłumaczony na język urzędowy państwa członkowskiego, w którym znajduje się wyznaczony zakład lub przedstawiciel prawny usługodawcy lub na inny język urzędowy, który, zgodnie z deklaracją wyznaczonego zakładu lub przedstawiciela prawnego usługodawcy, zostanie przez niego zaakceptowany. Jeżeli powiadomienie organu przymuszającego do wykonania nakazu jest wymagane na podstawie niniejszego rozporządzenia, EPOC, które ma zostać przekazany temu organowi, należy przetłumaczyć na język urzędowy państwa wykonującego lub na inny język urzędowy Unii akceptowany przez to państwo. W tym względzie należy zachęcać każde państwo członkowskie do wskazania w każdym momencie w pisemnym oświadczeniu przedłożonym Komisji, czy i w jakim języku urzędowym lub językach urzędowych Unii – oprócz języka lub języków urzędowych tego państwa członkowskiego – akceptowałoby tłumaczenia EPOC oraz EPOC-PR. Komisja powinna udostępnić takie oświadczenia wszystkim państwom członkowskim oraz Europejskiej Sieci Sądowej.
- (56) Jeżeli wydano EPOC, a zgodnie z niniejszym rozporządzeniem powiadomienie organu przymuszającego do wykonania nakazu nie jest wymagane, adresat powinien zapewnić, aby po otrzymaniu EPOC objęte nakazem dane zostały przekazane bezpośrednio organowi wydającemu lub organom ścigania wskazanym w EPOC najpóźniej w ciągu 10 dni od otrzymania EPOC. W przypadku gdy zgodnie z niniejszym rozporządzeniem wymagane jest powiadomienie organu przymuszającego do wykonania nakazu, po otrzymaniu EPOC usługodawca powinien pilnie podjąć działania mające na celu zabezpieczenie danych. Jeżeli organ przymuszający do wykonania nakazu nie powołał się na żadne podstawy odmowy zgodnie z niniejszym rozporządzeniem w terminie 10 dni od otrzymania EPOC, adresat zapewnia przekazanie wymaganych danych bezpośrednio organowi wydającemu lub organom ścigania wskazanym w EPOC z końcem tego dziesięciodniowego terminu. Jeżeli organ przymuszający do wykonania nakazu już przed upływem tego terminu 10 dni potwierdzi organowi wydającemu i adresatowi, że

nie powoła się na żadne podstawy odmowy, adresat powinien podjąć działania jak najszybciej po takim potwierdzeniu, a najpóźniej z końcem tego terminu 10 dni. Adresat oraz, w stosownych przypadkach, organ przymuszający do wykonania nakazu powinni przestrzegać krótszych terminów mających zastosowanie w sytuacjach wyjątkowych zdefiniowanych w niniejszym rozporządzeniu. Adresat oraz, w stosownych przypadkach, organ przymuszający do wykonania nakazu powinni wykonać EPOC tak szybko, jak to możliwe, a najpóźniej w terminach określonych w niniejszym rozporządzeniu, uwzględniając w jak największym stopniu terminy proceduralne i inne terminy wskazane przez państwo wydające.

- (57) Jeżeli adresat uzna, wyłącznie na podstawie informacji zawartych w EPOC lub w EPOC-PR, że wykonanie EPOC lub EPOC-PR mogłoby kolidować z przewidzianymi w prawie państwa wykonującego immunitetami lub przywilejami, lub z przepisami dotyczącymi ustalania i granic odpowiedzialności karnej związanymi z wolnością prasy lub wolnością wypowiedzi w innych mediach, adresat powinien poinformować o tym organ wydający i organ przymuszający do wykonania nakazu. W odniesieniu do EPOC, jeżeli zgodnie z niniejszym rozporządzeniem organ przymuszający do wykonania nakazu nie został powiadomiony, organ wydający powinien uwzględnić informacje przekazane przez adresata i postanowić – z własnej inicjatywy lub na wniosek organu przymuszającego do wykonania nakazu – o wycofaniu, dostosowaniu albo utrzymaniu europejskiego nakazu wydania dowodów. Jeżeli zgodnie z niniejszym rozporządzeniem organ przymuszający do wykonania nakazu został powiadomiony, organ wydający powinien uwzględnić informacje przekazane przez adresata i postanowić o wycofaniu, dostosowaniu albo utrzymaniu europejskiego nakazu wydania dowodów. Organ przymuszający do wykonania nakazu powinien mieć również możliwość powołania się na podstawy odmowy określone w niniejszym rozporządzeniu.
- (58) W celu umożliwienia adresatowi zaradzenia formalnym problemom z EPOC lub EPOC-PR niezbędne jest ustanowienie procedury komunikacji pomiędzy adresatem a organem wydającym, a także – w sytuacji, w której zgodnie z niniejszym rozporządzeniem powiadomiono organ przymuszający do wykonania nakazu – między adresatem a organem przymuszającym do wykonania nakazu, w przypadkach, w których EPOC lub EPOC-PR są niekompletne, zawierają oczywiste błędy lub nie zawierają informacji wystarczających do wykonania danego nakazu. Ponadto, jeżeli adresat 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 lub europejski nakaz zabezpieczenia dowodów nie został wydany zgodnie z warunkami przewidzianymi w niniejszym rozporządzeniu, powinien on poinformować o tym organ wydający oraz – jeżeli został powiadomiony – organ przymuszający do wykonania nakazu i przedstawić uzasadnienie dla niewykonania w terminie EPOC lub EPOC-PR. Procedura komunikacji powinna umożliwiać skorygowanie lub ponowne rozpatrzenie europejskiego nakazu wydania dowodów lub europejskiego nakazu zabezpieczenia dowodów przez organ wydający na wczesnym etapie. W celu zagwarantowania dostępności danych objętych nakazem adresat powinien zabezpieczyć te dane, jeżeli jest w stanie je zidentyfikować.
- (59) Adresat nie powinien być zobowiązany do zastosowania się do europejskiego nakazu wydania dowodów lub europejskiego nakazu zabezpieczenia dowodów w przypadku faktycznej niemożliwości wynikającej z okoliczności, których nie można przypisać adresatowi ani – jeżeli są to różne podmioty – usługodawcy w momencie otrzymania europejskiego nakazu wydania dowodów lub europejskiego nakazu zabezpieczenia dowodów. Faktyczną niemożliwość domniemywa się w sytuacji, gdy osoba, której dane są objęte nakazem, nie jest klientem usługodawcy ani nie może być zidentyfikowana jako jego klient nawet po zwróceniu się o dalsze informacje do organu wydającego lub jeśli dane zostały zgodnie z prawem usunięte przed otrzymaniem nakazu.
- (60) Po otrzymaniu EPOC-PR adresat powinien zabezpieczyć dane objęte nakazem na okres maksymalnie 60 dni, chyba że organ wydający potwierdzi, że wydano następnie wniosek dotyczący wydania, w którym to przypadku zabezpieczenie powinno być kontynuowane. Organ wydający powinien mieć możliwość przedłużenia, przy użyciu formularza określonego w niniejszym rozporządzeniu, okresu zabezpieczenia o dodatkowe 30 dni, jeżeli jest to konieczne, aby umożliwić wydanie następnie wniosku dotyczącego wydania. Jeżeli organ wydający potwierdzi w czasie trwania zabezpieczenia, że wydano następnie wniosek dotyczący wydania, adresat powinien zabezpieczyć dane na tak długo, jak będzie to konieczne w celu wydania danych, gdy tylko doręczony zostanie wniosek dotyczący wydania. Potwierdzenie takie należy przesłać adresatowi w odpowiednim terminie, w języku urzędowym państwa wykonującego lub w innym języku akceptowanym przez adresata, przy użyciu formularza określonego w niniejszym rozporządzeniu. Aby zapobiec zakończeniu zabezpieczenia, wystarczające powinno być wydanie następnie w danej sprawie wniosku o wydanie oraz wysłanie potwierdzenia przez organ wydający; na tym etapie nie powinno być konieczne dopełnianie dalszych wymaganych formalności związanych z przekazaniem, takich jak tłumaczenie dokumentów. Jeżeli zabezpieczenie nie jest już konieczne, organ wydający powinien bez zbędnej zwłoki poinformować o tym adresata, a obowiązek zabezpieczenia danych na podstawie europejskiego nakazu zabezpieczenia dowodów powinien ustać.

- (61) Niezależnie od zasady wzajemnego zaufania organ przymuszający do wykonania nakazu powinien mieć możliwość powołania się na podstawy odmowy wykonania europejskiego nakazu wydania dowodów w oparciu o wykaz podstaw odmowy przewidziany w niniejszym rozporządzeniu, jeżeli powiadomienie organu przymuszającego do wykonania nakazu nastąpiło zgodnie z niniejszym rozporządzeniem. W przypadku gdy powiadomienie organu przymuszającego do wykonania nakazu lub wykonanie następuje zgodnie z niniejszym rozporządzeniem, państwo wykonujące może przewidzieć w swoim prawie krajowym, że wykonanie europejskiego nakazu wydania dowodów może wymagać, aby w procedurę zaangażowano sąd w państwie wykonującym.
- (62) W przypadku gdy organ przymuszający do wykonania nakazu zostaje powiadomiony o europejskim nakazie wydania dowodów wydanym w celu uzyskania danych o ruchu, z wyjątkiem danych, których zażądano wyłącznie w celu identyfikacji użytkownika zdefiniowanych w niniejszym rozporządzeniu, lub w celu uzyskania danych dotyczących treści, powinien mieć on prawo do oceny informacji określonych w nakazie i, w stosownych przypadkach, odmowy jego wykonania, jeżeli na podstawie obowiązkowej i należytej analizy informacji zawartych w tym nakazie oraz z poszanowaniem mających zastosowanie przepisów prawa pierwotnego Unii, w szczególności Karty, dojdzie do wniosku, że istnieje możliwość powołania się na co najmniej jedną z podstaw odmowy przewidzianych w niniejszym rozporządzeniu. Konieczność poszanowania niezależności organów sądowych wymaga przyznania im pewnego zakresu swobody uznania przy podejmowaniu decyzji dotyczącej podstaw odmowy.
- (63) Organ przymuszający do wykonania nakazu, w przypadku gdy został powiadomiony zgodnie z niniejszym rozporządzeniem, powinien mieć możliwość odmowy wykonania europejskiego nakazu wydania dowodów, jeżeli dane objęte nakazem są chronione immunitetami lub przywilejami przysługującymi na mocy prawa państwa wykonującego, które to immunitety lub przywileje uniemożliwiają wykonanie lub postępowanie przymuszające do wykonania europejskiego nakazu wydania dowodów, lub też do danych objętych nakazem stosuje się przepisy dotyczące ustalania i granic odpowiedzialności karnej związane z wolnością prasy lub wolnością wypowiedzi w innych mediach, uniemożliwiające wykonanie nakazu lub postępowanie przymuszające do wykonania nakazu.
- (64) Organ przymuszający do wykonania nakazu powinien mieć możliwość odmowy wykonania nakazu w sytuacjach wyjątkowych, gdy istnieją uzasadnione podstawy, by sądzić, na podstawie konkretnych i obiektywnych dowodów, że wykonanie europejskiego nakazu wydania dowodów w szczególnych okolicznościach danej sprawy wiązałoby się z oczywistym naruszeniem odpowiedniego prawa podstawowego określonego w art. 6 TUE i w Karcie. W szczególności przy ocenie tej podstawy odmowy, jeżeli organ przymuszający do wykonania nakazu dysponuje dowodami lub materiałami, takimi jak przedstawione w uzasadnionym wniosku jednej trzeciej państw członkowskich, Parlamentu Europejskiego lub Komisji Europejskiej, przyjętym na podstawie art. 7 ust. 1 TUE, wskazującym, że – w przypadku wykonania nakazu – istnieje wyraźne ryzyko poważnego naruszenia prawa podstawowego do skutecznego środka prawnego i dostępu do bezstronnego sądu na mocy art. 47 Karty, ze względu na systemowe lub ogólne braki w zakresie niezawisłości władzy sędziowskiej państwa wydającego, organ przymuszający do wykonania nakazu powinien w sposób konkretny i precyzyjny ustalić, czy – biorąc pod uwagę sytuację osobistą danej osoby, a także charakter przestępstwa, w związku z którym prowadzone jest postępowanie karne, oraz okoliczności faktyczne, na których opiera się nakaz, a także uwzględniając informacje przekazane przez organ wydający – istnieją istotne przesłanki, by sądzić, że istnieje ryzyko naruszenia prawa danej osoby dostępu do bezstronnego sądu.
- (65) Organ przymuszający do wykonania nakazu powinien mieć możliwość odmowy wykonania nakazu, jeżeli jego wykonanie byłoby sprzeczne z zasadą *ne bis in idem*.
- (66) Organ przymuszający do wykonania nakazu, jeżeli został powiadomiony zgodnie z niniejszym rozporządzeniem, powinien mieć możliwość odmowy wykonania europejskiego nakazu wydania dowodów w przypadku, gdy czyn, w związku z którym wydano nakaz, nie stanowi przestępstwa według prawa państwa wykonującego, chyba że dotyczy on przestępstwa wymienionego wśród kategorii przestępstw wyszczególnionych w załączniku do niniejszego rozporządzenia, jak wskazał organ wydający w EPOC, jeżeli w państwie wydającym to przestępstwo podlega karze pozbawienia wolności lub środkowi zabezpieczającemu polegającemu na pozbawieniu wolności o górnej granicy ustawowego zagrożenia w wysokości co najmniej trzech lat.
- (67) Ponieważ powiadomienie osoby, której dane są objęte nakazem, jest zasadniczym elementem prawa do ochrony danych i prawa do obrony, umożliwiającym skuteczną kontrolę i stosowanie środków odwoławczych, zgodnie z art. 6 TUE i Kartą, organ wydający powinien, bez zbędnej zwłoki, poinformować osobę, której dane są objęte nakazem, o wydaniu danych na podstawie europejskiego nakazu wydania dowodów. Organ wydający powinien jednak mieć możliwość, zgodnie z prawem krajowym, opóźnienia lub ograniczenia powiadomienia lub zaniechania powiadomienia osoby, której dane są objęte nakazem, w zakresie w jakim i tak długo, jak spełnione są warunki określone w dyrektywie (UE) 2016/680, w którym to przypadku organ wydający powinien wskazać w aktach sprawy przyczyny opóźnienia, ograniczenia lub zaniechania oraz zawrzeć w EPOC krótkie uzasadnienie. Adresaci oraz – jeżeli są to różne osoby – usługodawcy powinni stosować niezbędne najnowocześniejsze środki operacyjne i techniczne, aby zapewnić poufność, tajność i integralność EPOC lub EPOC-PR i danych wydawanych lub zabezpieczanych.

- (68) Usługodawca powinien mieć możliwość żądania od państwa wydającego zwrotu kosztów, które poniósł w celu udzielenia odpowiedzi na europejski nakaz wydania dowodów lub europejski nakaz zabezpieczenia dowodów, jeżeli prawo krajowe państwa wydającego przewiduje taką możliwość w podobnych sytuacjach, zgodnie z prawem krajowym tego państwa. Państwa członkowskie powinny informować Komisję o swoich zasadach zwrotu kosztów, a Komisja powinna podać te zasady do wiadomości publicznej. Niniejsze rozporządzenie przewiduje odrębne zasady mające zastosowanie do zwrotu kosztów związanych ze zdecentralizowanym systemem teleinformatycznym.
- (69) Bez uszczerbku dla przepisów krajowego prawa przewidujących nałożenie sankcji karnych państwa członkowskie powinny ustanowić przepisy dotyczące kar pieniężnych mających zastosowanie w przypadku naruszeń niniejszego rozporządzenia i powinny podjąć wszelkie niezbędne środki w celu zapewnienia wdrożenia tych kar. Państwa członkowskie powinny zapewnić, aby przewidziane ich prawem krajowym kary pieniężne były skuteczne, proporcjonalne i odstraszające. Państwa członkowskie powinny niezwłocznie powiadomić Komisję o tych przepisach i środkach, a także powinny niezwłocznie powiadamiać ją o wszelkich późniejszych zmianach, które ich dotyczą.
- (70) Oceniając indywidualnie dla każdego przypadku odpowiednią karę pieniężną, właściwe organy powinny uwzględnić wszystkie stosowne okoliczności, takie jak charakter, waga i czas trwania naruszenia, to, czy zostało ono popełnione umyślnie czy wskutek zaniedbania, czy dany usługodawca był odpowiedzialny za podobne naruszenia w przeszłości, a także kondycję finansową pociągniętego do odpowiedzialności usługodawcy. W wyjątkowych okolicznościach ocena ta mogłaby skłonić organ przymuszający do wykonania nakazu do podjęcia decyzji o powstrzymaniu się od nakładania kar pieniężnych. W tym względzie szczególną uwagę należy zwrócić na mikroprzedsiębiorstwa, które nie wykonują europejskiego nakazu wydania dowodów lub europejskiego nakazu zabezpieczenia dowodów w sytuacji wyjątkowej z powodu braku zasobów ludzkich dostępnych poza normalnymi godzinami działalności, jeżeli dane są przekazywane bez zbędnej zwłoki.
- (71) Bez uszczerbku dla obowiązków w zakresie ochrony danych usługodawcy nie powinni być pociągani do odpowiedzialności w państwach członkowskich za szkody spowodowane ich użytkownikom lub stronom trzecim wynikające wyłącznie z zastosowania się w dobrej wierze do EPOC lub EPOC-PR. Odpowiedzialność za zapewnienie zgodności danego nakazu z przepisami, w szczególności w zakresie konieczności jego wydania i proporcjonalności, powinna spoczywać na organie wydającym.
- (72) Jeżeli adresat nie zastosuje się do EPOC w terminie lub nie zastosuje się do EPOC-PR i nie poda powodów, które zostaną zaakceptowane przez organ wydający i, w stosownych wypadkach, jeżeli organ przymuszający do wykonania nakazu nie powołał się na jedną z podstaw odmowy uznania lub wykonania przewidzianych w niniejszym rozporządzeniu, organ wydający powinien mieć możliwość wnioskowania do organu przymuszającego do wykonania nakazu o wszczęcie postępowania przymuszającego do wykonania europejskiego nakazu wydania dowodów lub europejskiego nakazu zabezpieczenia dowodów. W tym celu organ wydający powinien przekazać organowi przymuszającemu do wykonania nakazu dany nakaz, uzupełniony przez adresata odpowiedni formularz przetłumaczony w niniejszym rozporządzeniu oraz wszelkie odpowiednie dokumenty. Organ wydający powinien przetłumaczyć dany nakaz i wszelkie dokumenty, które mają być przekazane, na jeden z języków akceptowanych przez państwo wykonujące i powinien poinformować adresata o przekazaniu. To państwo powinno przymusić do wykonania danego nakazu zgodnie ze swoim prawem krajowym.
- (73) W postępowaniu przymuszającym do wykonania nakazu adresat powinien mieć możliwość powoływania się na przesłanki, które stoją na przeszkodzie wykonaniu nakazu i są oparte na wykazie szczególnych przesłanek przewidzianych w niniejszym rozporządzeniu, w tym na to, że dany nakaz nie został wydany lub zatwierdzony przez właściwy organ, jak przewidziano w niniejszym rozporządzeniu, lub jeżeli nakaz nie dotyczy danych przechowywanych przez usługodawcę lub w jego imieniu w chwili otrzymania odpowiedniego zaświadczenia. Organ przymuszający do wykonania nakazu powinien mieć możliwość odmowy uznania i przymuszenia do wykonania europejskiego nakazu wydania dowodów lub europejskiego nakazu zabezpieczenia dowodów na podstawie tych samych przesłanek, a także, w sytuacjach wyjątkowych, z powodu oczywistego naruszenia odpowiedniego prawa podstawowego określonego w art. 6 TUE i w Karcie. Organ przymuszający do wykonania nakazu powinien skonsultować się z organem wydającym przed wydaniem decyzji o odmowie uznania nakazu lub wszczęcia postępowania przymuszającego do wykonania nakazu na podstawie tych przesłanek. Jeżeli adresat nie wywiązuje się z obowiązku przewidzianego w uznanym europejskim nakazie wydania dowodów lub europejskim nakazie zabezpieczenia dowodów, których wykonalność potwierdził organ przymuszający do wykonania nakazu, ten ostatni nakłada karę pieniężną. Kara ta powinna być proporcjonalna, w szczególności w kontekście szczególnych okoliczności takich jak powtarzające się lub systematyczne niewywiązywanie się z obowiązków.
- (74) Wykonanie europejskiego nakazu wydania dowodów może być sprzeczne z obowiązkami wynikającymi z mającego zastosowanie prawa państwa trzeciego. 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 rozporządzeniu przewidziano specjalny mechanizm kontroli sądowej na wypadek sytuacji, w których zastosowanie się do europejskiego nakazu wydania dowodów uniemożliwiłoby usługodawcy wywiązywanie się z obowiązków prawnych wynikających z prawa państwa trzeciego.

- (75) W każdym wypadku, gdy adresat uzna, że europejski nakaz wydania dowodów w konkretnej sprawie wiązałby się z pogwałceniem obowiązku prawnego wynikającego z prawa państwa trzeciego, powinien poinformować organ wydający i organ przymuszający do wykonania nakazu o przyczynach niewykonania nakazu w drodze uzasadnionego sprzeciwu, przy wykorzystaniu formularza przewidzianego w niniejszym rozporządzeniu. Organ wydający powinien skontrolować europejski nakaz wydania dowodów w oparciu o uzasadniony sprzeciw i wszelkie informacje przekazane przez państwo wykonujące, uwzględniając te same kryteria, których przestrzegać musiałby właściwy sąd państwa wydającego. Jeżeli organ wydający zamierza podjąć decyzję o utrzymaniu w mocy nakazu, powinien on wnieść o jego skontrolowanie przez właściwy sąd państwa wydającego powiadomiony przez odpowiednie państwo członkowskie; sąd ten powinien przeprowadzić kontrolę nakazu.
- (76) Ustalając, czy istnieją sprzeczne obowiązki w szczególnych okolicznościach rozpatrywanej sprawy, właściwy sąd mógłby skorzystać, w razie potrzeby, z odpowiedniej zewnętrznej wiedzy eksperckiej, na przykład co do wykładni prawa danego państwa trzeciego. W tym celu właściwy sąd mógłby na przykład skonsultować się z organem centralnym państwa trzeciego, z uwzględnieniem dyrektywy (UE) 2016/680. Państwo wydające powinno, w szczególności, zwrócić się do właściwego organu państwa trzeciego o udzielenie informacji, jeżeli konflikt dotyczy praw podstawowych lub innych podstawowych interesów państwa trzeciego związanych z bezpieczeństwem narodowym i obronnością.
- (77) Ekspercka wiedza dotycząca wykładni może być również w miarę możliwości zapewniona w drodze opinii biegłych. Informacje i orzecznictwo dotyczące wykładni prawa państwa trzeciego oraz procedur rozwiązywania kolizji przepisów w państwach członkowskich powinny być udostępnione na centralnej platformie takiej jak projekt SIRIUS lub Europejska Sieć Sądowa, aby umożliwić korzystanie z doświadczenia i eksperckiej wiedzy zgromadzonych w odniesieniu do tych samych lub podobnych zagadnień. Dostępność takich informacji na centralnej platformie nie powinna jednak w stosownych przypadkach uniemożliwiać ponownej konsultacji z państwem trzecim.
- (78) Oceniając, czy występują sprzeczne obowiązki, właściwy sąd powinien ustalić, czy zastosowanie ma prawo państwa trzeciego, a jeżeli tak, to czy prawo państwa trzeciego zabrania ujawniania odnośnych danych. Jeżeli właściwy sąd ustali, że prawo państwa trzeciego zabrania ujawnienia odnośnych danych, sąd powinien podjąć decyzję co do tego, czy utrzymać europejski nakaz wydania dowodów w mocy czy go uchylić, 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 adresata lub usługodawcy wynikających z wykonania nakazu. Podczas przeprowadzania oceny szczególne znaczenie i szczególną wagę należy przywiązywać do ochrony praw podstawowych przez odpowiednie przepisy państwa trzeciego i do innych podstawowych interesów, takich jak bezpieczeństwo narodowe państwa trzeciego, a także do stopnia powiązania sprawy karnej z obiema jurysdykcjami. Jeżeli sąd podejmie decyzję o uchyleniu nakazu, powinien poinformować o tym organ wydający i adresata. Jeżeli właściwy sąd stwierdzi, że nakaz ma być utrzymany w mocy, powinien poinformować organ wydający i adresata, który powinien przystąpić do wykonania tego nakazu. Organ wydający powinien poinformować organ przymuszający do wykonania nakazu o wyniku postępowania kontrolnego.
- (79) Warunki określone w niniejszym rozporządzeniu dotyczące wykonywania EPOC powinny mieć również zastosowanie w sytuacjach, w których konflikt obowiązków wynika z prawa państwa trzeciego. W związku z tym podczas kontroli sądowej sprawdzającej czy wykonanie europejskiego nakazu wydania dowodów uniemożliwiłoby usługodawcom wywiązanie się z obowiązku prawnego wynikającego z prawa państwa trzeciego, dane objęte nakazem powinny zostać zabezpieczone. Jeżeli po przeprowadzeniu kontroli sądowej właściwy sąd postanowi uchylić europejski nakaz wydania dowodów, powinna istnieć możliwość wydania europejskiego nakazu zabezpieczenia dowodów, aby umożliwić organowi wydającemu zażądanie wydania dowodów w inny sposób, na przykład w ramach wzajemnej pomocy prawnej.
- (80) Kluczowym jest, aby wszystkim osobom, których dane są objęte nakazem w ramach postępowania przygotowawczego lub procesu karnego, przysługiwał skuteczny środek prawny, zgodnie z art. 47 Karty. Zgodnie z tym wymogiem i bez uszczerbku dla dalszych środków prawnych dostępnych zgodnie z prawem krajowym, każda osoba, której dane były objęte europejskim nakazem wydania dowodów, powinna mieć prawo do skutecznych środków prawnych wobec tego nakazu. Jeżeli jest to podejrzany lub oskarżony, powinien on mieć prawo do skutecznych środków prawnych w toku postępowania karnego, w którym te dane wykorzystywane są jako dowód. Prawo do skutecznego środka prawnego powinno być wykonane przed sądem w państwie wydającym zgodnie z jego prawem krajowym i powinno obejmować możliwość podważenia legalności środka, w tym jego konieczności i proporcjonalności, bez uszczerbku dla gwarancji praw podstawowych w państwie wykonującym lub innych dodatkowych środków prawnych zgodnie z prawem krajowym. Niniejsze rozporządzenie nie powinno ograniczać możliwych przesłanek podważenia legalności nakazu. Prawo do skutecznych środków prawnych przewidziane w niniejszym rozporządzeniu powinno pozostawać bez uszczerbku dla prawa do korzystania ze środków prawnych na mocy rozporządzenia (UE) 2016/679 i dyrektywy (UE) 2016/680. Informacje na temat przewidzianych w prawie krajowym środków prawnych powinny być przekazywane w odpowiednim czasie, a także należy zapewnić możliwość skutecznego z nich korzystania.

- (81) Należy opracować odpowiednie kanały w celu zapewnienia, aby wszystkie strony mogły skutecznie współpracować za pomocą środków cyfrowych za pośrednictwem zdecentralizowanego systemu teleinformatycznego, który umożliwi szybką, bezpośrednią, interoperacyjną, zrównoważoną, niezawodną i bezpieczną transgraniczną elektroniczną wymianę formularzy, danych i informacji związanych ze sprawami.
- (82) Aby umożliwić skuteczną i bezpieczną komunikację pisemną między właściwymi organami i wyznaczonymi zakładami lub przedstawicielami prawnymi usługodawców na mocy niniejszego rozporządzenia, tym wyznaczonym zakładom lub przedstawicielom prawnym należy zapewnić elektroniczne środki dostępu do obsługiwanych przez państwa członkowskie krajowych systemów teleinformatycznych, stanowiących część zdecentralizowanego systemu teleinformatycznego.
- (83) Zdecentralizowany system teleinformatyczny powinien obejmować systemy teleinformatyczne państw członkowskich oraz agencji i organów Unii, a także interoperacyjne punkty dostępu zapewniające wzajemne połączenia tych systemów teleinformatycznych. Punkty dostępu zdecentralizowanego systemu teleinformatycznego powinny opierać się na systemie e-CODEX ustanowionym rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2022/850 <sup>(24)</sup>.
- (84) Usługodawcom korzystającym z dostosowanych do potrzeb rozwiązań informatycznych do celów wymiany informacji i danych związanych z wnioskami o wydanie dowodów elektronicznych należy zapewnić zautomatyzowane środki dostępu do zdecentralizowanych systemów teleinformatycznych za pomocą wspólnego standardu wymiany danych.
- (85) Co do zasady wszelka komunikacja pisemna między właściwymi organami lub między właściwymi organami a wyznaczonymi zakładami lub przedstawicielami prawnymi powinna być prowadzona za pośrednictwem zdecentralizowanego systemu teleinformatycznego. Stosowanie alternatywnych środków powinno być możliwe tylko wtedy, gdy korzystanie ze zdecentralizowanego systemu teleinformatycznego nie jest możliwe, na przykład ze względu na szczególne wymogi kryminalistyczne, ze względu na fakt, że ilość danych, które mają być przekazywane, przekracza możliwości techniczne systemu lub dlatego, że w sytuacji wyjątkowej istnieje potrzeba skontaktowania się z innym zakładem, pozbawionym dostępu do zdecentralizowanego systemu teleinformatycznego. W takich przypadkach przekazywanie informacji powinno odbywać się za pomocą najbardziej odpowiednich alternatywnych środków, z uwzględnieniem potrzeby zapewnienia szybkiej, bezpiecznej i niezawodnej wymiany informacji.
- (86) Aby zapewnić, że zdecentralizowany system teleinformatyczny zawiera pełny zapis pisemnej wymiany informacji na podstawie niniejszego rozporządzenia, każde przekazanie dokonane za pomocą alternatywnych środków powinno być bez zbędnej zwłoki rejestrowane w zdecentralizowanym systemie teleinformatycznym.
- (87) Należy zatem rozważyć zastosowanie mechanizmów zapewniających autentyczność przewidzianych rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 910/2014 <sup>(25)</sup>.
- (88) Usługodawcy, w szczególności małe i średnie przedsiębiorstwa, nie powinni być narażeni na nieproporcjonalne koszty związane z utworzeniem i funkcjonowaniem zdecentralizowanego systemu teleinformatycznego. W ramach tworzenia, utrzymywania i rozwoju oprogramowania wzorcowego Komisja ma zatem również udostępnić interfejs internetowy umożliwiający usługodawcom bezpieczną komunikację z organami bez konieczności tworzenia własnej specjalnej infrastruktury pozwalającej na dostęp do zdecentralizowanego systemu teleinformatycznego.
- (89) Państwa członkowskie powinny mieć możliwość korzystania z oprogramowania opracowanego przez Komisję, a mianowicie z oprogramowania wzorcowego, zamiast krajowego systemu teleinformatycznego. To oprogramowanie wzorcowe powinno mieć strukturę modułową, co oznacza, że powinno być oprogramowaniem pakietowym dostarczonym niezależnie od elementów systemu e-CODEX niezbędnych do podłączenia tego oprogramowania do zdecentralizowanego systemu teleinformatycznego. Dzięki tej strukturze państwa członkowskie powinny mieć możliwość ponownego wykorzystywania lub usprawnienia swoich odpowiednich istniejących krajowych infrastruktur komunikacji sądowej na potrzeby zastosowań transgranicznych.
- (90) Komisja powinna być odpowiedzialna za tworzenie, utrzymanie i rozwój oprogramowania wzorcowego. Komisja powinna zaprojektować, rozwijać i utrzymywać oprogramowanie wzorcowe zgodnie z wymogami i zasadami dotyczącymi ochrony danych określonymi w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2018/1725 <sup>(26)</sup>, rozporządzeniu (UE) 2016/679 i dyrektywie (UE) 2016/680, w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania i zasadą domyślnej ochrony danych oraz z zachowaniem wysokiego poziomu cyberbezpieczeństwa. Istotne jest, by oprogramowanie wzorcowe obejmowało również odpowiednie środki techniczne i umożliwiać podejmowanie środków organizacyjnych niezbędnych do zapewnienia odpowiedniego poziomu bezpieczeństwa i interoperacyjności.

<sup>(24)</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/850 z dnia 30 maja 2022 r. w sprawie informatycznego systemu transgranicznej elektronicznej wymiany danych w obszarze współpracy sądowej w sprawach cywilnych i współpracy wymiarów sprawiedliwości w sprawach karnych (system e-CODEX) oraz w sprawie zmiany rozporządzenia (UE) 2018/1726 (Dz.U. L 150 z 1.6.2022, s. 1).

<sup>(25)</sup> Rozporządzenie 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 uchylające dyrektywę 1999/93/WE (Dz.U. L 257 z 28.8.2014, s. 73).

<sup>(26)</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39).

- (91) W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia należy powierzyć Komisji uprawnienia wykonawcze. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011<sup>(27)</sup>.
- (92) W przypadku wymiany danych prowadzonej za pośrednictwem zdecentralizowanego systemu teleinformatycznego lub rejestrowanej w zdecentralizowanym systemie teleinformatycznym państwa członkowskie powinny mieć możliwość gromadzenia danych statystycznych, aby wypełnić swoje obowiązki w zakresie monitorowania i sprawozdawczości wynikające z niniejszego rozporządzenia za pośrednictwem swoich portali krajowych.
- (93) W celu monitorowania wyników, rezultatów i skutków niniejszego rozporządzenia Komisja powinna publikować roczne sprawozdanie za poprzedni rok kalendarzowy w oparciu o dane uzyskane od państw członkowskich. W tym celu państwa członkowskie powinny gromadzić i przekazywać Komisji kompleksowe dane statystyczne dotyczące różnych aspektów niniejszego rozporządzenia, według rodzaju danych objętych nakazem, adresatów oraz tego, czy była to sytuacja wyjątkowa.
- (94) Korzystanie z uprzednio przetłumaczonych i znormalizowanych formularzy ułatwiłoby współpracę i wymianę informacji na podstawie niniejszego rozporządzenia, umożliwiając szybszą i bardziej skuteczną komunikację w sposób przyjazny dla użytkownika. Takie formularze mogłyby także obniżyć koszty tłumaczenia i przyczynić się do zapewnienia komunikacji o wysokich standardach jakości. Formularze odpowiedzi również umożliwiłyby znormalizowaną wymianę informacji, w szczególności w sytuacjach, w których usługodawcy nie są w stanie wywiązać się z obowiązków, ponieważ konto użytkownika nie istnieje lub brak jest dostępnych danych. Formularze przewidziane w niniejszym rozporządzeniu ułatwiłyby również gromadzenie danych statystycznych.
- (95) W celu umożliwienia skutecznej reakcji na ewentualną potrzebę poprawienia treści formularzy EPOC i EPOC-PR oraz formularzy przeznaczonych do przekazania informacji na temat braku możliwości wykonania EPOC lub EPOC-PR, potwierdzenia wydania wniosku o wydanie w następstwie europejskiego nakazu zabezpieczenia dowodów oraz przedłużenia okresu zabezpieczenia dowodów elektronicznych, należy przekazać Komisji uprawnienia do przyjmowania aktów zgodnie z art. 290 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) w odniesieniu do modyfikacji treści formularzy przewidzianych w niniejszym rozporządzeniu. 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 z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa<sup>(28)</sup>. W szczególności, aby zapewnić Parlamentowi Europejskiemu i Radzie udział na równych zasadach 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.
- (96) Niniejsze rozporządzenie nie powinno wpływać na unijne ani inne międzynarodowe instrumenty, umowy i uzgodnienia w sprawie gromadzenia dowodów objętego zakresem stosowania niniejszego rozporządzenia. Organy państw członkowskich powinny wybrać narzędzie najlepiej dostosowane do rozpatrywanej sprawy. W niektórych przypadkach mogą one preferować korzystanie z unijnych i innych międzynarodowych instrumentów, umów i uzgodnień przy występowaniu do innego państwa członkowskiego o przeprowadzenie szeregu różnych czynności dochodzeniowo-śledczych, które nie ograniczają się do wydania dowodów elektronicznych. Najpóźniej trzy lata po wejściu w życie niniejszego rozporządzenia państwa członkowskie powinny powiadomić Komisję o istniejących instrumentach, umowach i uzgodnieniach, o których mowa w niniejszym rozporządzeniu, które nadal będą stosować. Państwa członkowskie powinny również powiadamiać Komisję o wszelkich nowych umowach lub uzgodnieniach, o których mowa w niniejszym rozporządzeniu, w terminie trzech miesięcy od dnia ich podpisania.
- (97) 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. Ważne jest zatem przeprowadzenie oceny jego stosowania.
- (98) Komisja powinna przeprowadzić ocenę niniejszego rozporządzenia, opartą na pięciu kryteriach: skuteczności, efektywności, zasadności, spójności i wartości dodanej dla UE, która to ocena zapewni podstawę do przeprowadzenia oceny skutków możliwych dalszych środków. Sprawozdanie z oceny powinno zawierać ocenę stosowania niniejszego rozporządzenia, wyników osiągniętych w odniesieniu do jego celów, a także ocenę wpływu niniejszego rozporządzenia na prawa podstawowe. Komisja powinna regularnie gromadzić informacje w celu zapewnienia materiału do przeprowadzenia oceny niniejszego rozporządzenia.

<sup>(27)</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.U. L 55 z 28.2.2011, s. 13).

<sup>(28)</sup> Dz.U. L 123 z 12.5.2016, s. 1.



- (99) Ponieważ cel niniejszego rozporządzenia, a mianowicie uzyskanie poprawy w dziedzinie transgranicznego zabezpieczenia i pozyskiwania dowodów elektronicznych, nie może zostać osiągnięty w sposób wystarczający przez państwa członkowskie ze względu na jego transgraniczny charakter, natomiast możliwe jest jego lepsze osiągnięcie na poziomie Unii, może ona podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 TUE. Zgodnie z zasadą proporcjonalności określoną w tym artykule, niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tego celu.
- (100) Zgodnie z art. 3 Protokołu nr 21 w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, załączonego do TUE i do TFUE, Irlandia powiadomiła o chęci uczestniczenia w przyjęciu i stosowaniu niniejszego rozporządzenia.
- (101) Zgodnie z art. 1 i 2 Protokołu nr 22 w sprawie stanowiska Danii, załączonego do TUE i do TFUE, Dania nie uczestniczy w przyjęciu niniejszego rozporządzenia i nie jest nim związana ani go nie stosuje.
- (102) Zgodnie z art. 42 ust. 1 rozporządzenia (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 6 listopada 2019 r. <sup>(29)</sup>,

PRZYMUJĄ NINIEJSZE ROZPORZĄDZENIE:

## ROZDZIAŁ I

### PRZEDMIOT, ZAKRES I DEFINICJE

#### Artykuł 1

##### Przedmiot

1. W niniejszym rozporządzeniu określa się zasady, zgodnie z którymi organ państwa członkowskiego może wydać w postępowaniu karnym europejski nakaz wydania dowodów lub europejski nakaz zabezpieczenia dowodów i tym samym nakazać usługodawcy oferującemu usługi w Unii i posiadającemu zakład w innym państwie członkowskim lub, jeżeli nie posiada zakładu, reprezentowanemu przez przedstawiciela prawnego w innym państwie członkowskim, wydanie lub zabezpieczenie dowodów elektronicznych, bez względu na lokalizację danych.

Niniejsze rozporządzenie pozostaje bez uszczerbku dla uprawnień organów krajowych do zwracania się do usługodawców posiadających zakład lub przedstawiciela na ich terytorium w celu zapewnienia, aby przestrzegali środków krajowych podobnych do środków, o których mowa w akapicie pierwszym.

2. O wydanie europejskiego nakazu wydania dowodów lub europejskiego nakazu zabezpieczenia dowodów może wnosić również podejrzany, oskarżony lub profesjonalny pełnomocnik działający w imieniu takiej osoby w ramach mającego zastosowanie prawa do obrony, zgodnie z przepisami krajowego prawa karnego procesowego.

3. Niniejsze rozporządzenie nie ma wpływu na obowiązek poszanowania praw podstawowych i podstawowych zasad prawnych zapisanych w Karcie oraz w art. 6 TUE i nie wpływa na obowiązki mające zastosowanie wobec organów ścigania lub organów sądowych w tym zakresie. Niniejsze rozporządzenie stosuje się bez uszczerbku dla podstawowych zasad, w szczególności wolności wypowiedzi i informacji, w tym wolności i pluralizmu mediów, poszanowania życia prywatnego i rodzinnego, ochrony danych osobowych, a także prawa do skutecznej ochrony sądowej.

#### Artykuł 2

##### 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 ramach i do celów postępowania karnego oraz w celu wykonania w ramach postępowania karnego wykonawczego kary pozbawienia wolności lub środka zabezpieczającego polegającego na pozbawieniu wolności w wymiarze co najmniej czterech miesięcy, o ile nie zostały one nałożone orzeczeniem wydanym zaocznie, w przypadkach gdy skazany ukrywa się przed wymiarem sprawiedliwości. Nakazy takie mogą być również wydawane w postępowaniach związanych z przestępstwami, w przypadku których osoba prawna mogłaby być pociągnięta do odpowiedzialności lub podlegać karze w państwie wydającym.

3. Europejskie nakazy wydania dowodów i europejskie nakazy zabezpieczenia dowodów mogą być wydawane wyłącznie w odniesieniu do danych dotyczących usług oferowanych w Unii, o których mowa w art. 3 pkt 3.

4. Niniejsze rozporządzenie nie ma zastosowania do postępowań prowadzonych w celu udzielenia wzajemnej pomocy prawnej innemu państwu członkowskiemu lub państwu trzeciemu.

<sup>(29)</sup> Dz.U. C 32 z 31.1.2020, s. 11.

## Artykuł 3

## Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

- 1) „europejski nakaz wydania dowodów” oznacza decyzję nakazującą wydanie dowodów elektronicznych, wydaną lub zatwierdzoną przez organ sądowy państwa członkowskiego zgodnie z art. 4 ust. 1, 2, 4 i 5 oraz skierowaną do wyznaczonego zakładu lub przedstawiciela prawnego usługodawcy oferującego usługi w Unii, w przypadku gdy ten wyznaczony zakład lub przedstawiciel prawny znajduje się w innym państwie członkowskim związanym niniejszym rozporządzeniem;
- 2) „europejski nakaz zabezpieczenia dowodów” oznacza decyzję nakazującą zabezpieczenie dowodów elektronicznych na potrzeby przyszłego wniosku o wydanie dowodów, wydaną lub zatwierdzoną przez organ sądowy państwa członkowskiego zgodnie z art. 4 ust. 3, 4 i 5 oraz skierowaną do wyznaczonego zakładu lub przedstawiciela prawnego usługodawcy oferującego usługi w Unii, w przypadku gdy ten wyznaczony zakład lub przedstawiciel prawny znajdują się w innym państwie członkowskim związanym niniejszym rozporządzeniem;
- 3) „usługodawca” oznacza osobę fizyczną lub prawną świadczącą usługi należące do co najmniej jednej z poniższych kategorii, z wyjątkiem usług finansowych, o których mowa w art. 2 ust. 2 lit. b) dyrektywy 2006/123/WE Parlamentu Europejskiego i Rady <sup>(30)</sup>:
  - a) usługi łączności elektronicznej zdefiniowane w art. 2 pkt 4 dyrektywy (UE) 2018/1972;
  - b) usługi dotyczące nazw domen internetowych i numeracji IP, takie jak przypisywanie adresów IP, usługi rejestru nazw domen, usługi rejestratora nazw domen, oraz powiązane z nazwami domen usługi ochrony prywatności i usługi proxy;
  - c) inne usługi społeczeństwa informacyjnego, o których mowa w art. 1 ust. 1 lit. b) dyrektywy (UE) 2015/1535, umożliwiające:
    - (i) ich użytkownikom komunikowanie się ze sobą; lub
    - (ii) przechowywanie lub przetwarzanie w inny sposób danych w imieniu użytkowników, na rzecz których świadczona jest usługa, o ile przechowywanie danych jest elementem definiującym usługę świadczoną na rzecz użytkownika;
- 4) „oferowanie usług w Unii” oznacza:
  - a) umożliwianie korzystania z usług, o których mowa w pkt 3, osobom fizycznym lub prawnym w państwie członkowskim; oraz
  - b) posiadanie istotnego związku – na podstawie określonych kryteriów faktycznych – z państwem członkowskim, o którym mowa w lit. a); uznaje się, że taki istotny związek istnieje, gdy usługodawca posiada zakład w państwie członkowskim lub, w przypadku braku takiego zakładu, gdy istnieje znaczna liczba użytkowników w co najmniej jednym państwie członkowskim lub gdy działalność jest ukierunkowana na co najmniej jedno państwo członkowskie;
- 5) „zakład” oznacza podmiot, który faktycznie prowadzi działalność gospodarczą przez nieokreślony czas przy wykorzystaniu stałej infrastruktury, za pomocą której świadczone są usługi lub za pomocą której zarządza się prowadzoną działalnością;
- 6) „wyznaczony zakład” oznacza zakład posiadający osobowość prawną wyznaczony na piśmie przez usługodawcę prowadzącego działalność w państwie członkowskim uczestniczącym w instrumencie prawnym, o którym mowa w art. 1 ust. 2 dyrektywy (UE) 2023/1544, do celów, o których mowa w art. 1 ust. 1 i art. 3 ust. 1 tej dyrektywy;
- 7) „przedstawiciel prawny” oznacza osobę fizyczną lub prawną wyznaczoną na piśmie przez usługodawcę nieposiadającego zakładu w państwie członkowskim uczestniczącym w instrumencie prawnym, o którym mowa w art. 1 ust. 2 dyrektywy (UE) 2023/1544, do celów, o których mowa w art. 1 ust. 1 i art. 3 ust. 1 tej dyrektywy;
- 8) „dowód elektroniczny” oznacza dane abonenta, dane o ruchu lub dane dotyczące treści przechowywane przez usługodawcę, lub w imieniu usługodawcy, w formie elektronicznej w momencie otrzymania zaświadczenia europejskiego nakazu wydania dowodów (EPOC) lub zaświadczenia europejskiego nakazu zabezpieczenia dowodów (EPOC-PR);

<sup>(30)</sup> Dyrektywa 2006/123/WE Parlamentu Europejskiego i Rady z dnia 12 grudnia 2006 r. dotycząca usług na rynku wewnętrznym (Dz.U. L 376 z 27.12.2006, s. 36).

- 9) „dane abonenta” oznaczają wszelkie dane przechowywane przez usługodawcę w związku z abonamentem na jego usługi, dotyczące:
- a) tożsamości abonenta lub klienta, takie jak podane imię i nazwisko, data urodzenia, adres pocztowy lub geograficzny, dane rozliczeniowe i dotyczące 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 w chwili pierwszej rejestracji lub aktywacji 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;
- 10) „dane, których zażądano wyłącznie w celu identyfikacji użytkownika” oznaczają adresy IP oraz, w razie potrzeby, odpowiednie porty źródłowe i znaczniki czasu, a mianowicie datę i czas lub techniczne odpowiedniki tych identyfikatorów i związanych z nimi informacji, jeżeli zażądały ich organy ścigania lub organy sądowe wyłącznie w celu identyfikacji użytkownika w konkretnym postępowaniu karnym;
- 11) „dane o ruchu” oznaczają dane związane ze świadczeniem usługi oferowanej przez usługodawcę, które są wykorzystywane do zapewnienia kontekstu lub dodatkowych informacji na temat tej usługi i są generowane lub przetwarzane przez system informatyczny usługodawcy, takie jak dane dotyczące źródła i miejsca przeznaczenia wiadomości lub interakcji innego rodzaju, dane na temat lokalizacji urządzenia, daty, czasu, czasu trwania, rozmiaru, trasy, formatu, wykorzystanego protokołu i typu kompresji, a także inne metadane i dane pochodzące z łączności elektronicznej, inne niż dane abonenta, dotyczące rozpoczęcia i zakończenia sesji dostępu użytkownika do usługi, takie jak data i czas korzystania z usługi, logowanie do i wylogowanie z usługi;
- 12) „dane dotyczące treści” oznaczają wszelkie dane w formacie cyfrowym takie jak tekst, głos, wideo, obrazy i dźwięk, inne niż dane abonenta lub dane o ruchu;
- 13) „system informatyczny” oznacza system informatyczny zdefiniowany w art. 2 lit. a) dyrektywy Parlamentu Europejskiego i Rady 2013/40/UE<sup>(31)</sup>;
- 14) „państwo wydające” oznacza państwo członkowskie, w którym wydany został europejski nakaz wydania dowodów lub europejski nakaz zabezpieczenia dowodów;
- 15) „organ wydający” oznacza właściwy organ w państwie wydającym, który jest uprawniony, zgodnie z art. 4, do wydania europejskiego nakazu wydania dowodów lub europejskiego nakazu zabezpieczenia dowodów;
- 16) „państwo wykonujące” oznacza państwo członkowskie, w którym znajduje się siedziba wyznaczonego zakładu lub w którym przedstawiciel prawny ma miejsce pobytu, i do którego organ wydający przekazuje europejski nakaz wydania dowodów oraz EPOC lub europejski nakaz zabezpieczenia dowodów i EPOC-PR, w celu powiadomienia o nakazie lub w celu wykonania nakazu zgodnie z niniejszym rozporządzeniem;
- 17) „organ przymuszający do wykonania nakazu” oznacza organ w państwie wykonującym, który, zgodnie z prawem krajowym tego państwa, jest właściwy do otrzymania europejskiego nakazu wydania dowodów i EPOC lub europejskiego nakazu zabezpieczenia dowodów i EPOC-PR przekazanych przez organ wydający, w celu powiadomienia o nakazie lub w celu wykonania nakazu zgodnie z niniejszym rozporządzeniem;
- 18) „sytuacja wyjątkowa” oznacza sytuację, w której istnieje bezpośrednie zagrożenie dla życia, integralności cielesnej lub bezpieczeństwa osoby lub dla infrastruktury krytycznej zdefiniowanej w art. 2 lit. a) dyrektywy 2008/114/WE, w przypadku gdy zakłócenie lub zniszczenie takiej infrastruktury krytycznej spowodowałoby bezpośrednie zagrożenie życia, integralności cielesnej lub bezpieczeństwa osoby, w tym przez poważne zakłócenie podstawowych dostaw dla ludności lub wykonywania podstawowych funkcji państwa;
- 19) „administrator” oznacza administratora zdefiniowanego w art. 4 pkt 7 rozporządzenia (UE) 2016/679;
- 20) „podmiot przetwarzający” oznacza podmiot przetwarzający zdefiniowany w art. 4 pkt 8 rozporządzenia (UE) 2016/679;

<sup>(31)</sup> 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).

- 21) „zdecentralizowany system teleinformatyczny” oznacza sieć systemów teleinformatycznych i interoperacyjnych punktów dostępu, za których działanie i za zarządzanie którymi odpowiadają indywidualnie poszczególne państwa członkowskie, agencje lub organy Unii, która to sieć umożliwi bezpieczną i niezawodną transgraniczną wymianę informacji.

## ROZDZIAŁ II

### EUROPEJSKI NAKAZ WYDANIA DOWODÓW, EUROPEJSKI NAKAZ ZABEZPIECZENIA DOWODÓW I ZAŚWIADCZENIA

#### Artykuł 4

#### Organ wydający

1. Europejski nakaz wydania dowodów służący uzyskaniu danych abonenta lub uzyskaniu danych, których zażądano wyłącznie w celu identyfikacji użytkownika zdefiniowanych w art. 3 pkt 10, może być wydany wyłącznie przez:

- a) sędziego, sąd, sędziego śledczego lub prokuratora właściwych w danej sprawie; lub
- b) inny właściwy organ określony przez państwo wydające, który w danej sprawie pełni funkcję organu dochodzeniowo-śledczego w postępowaniu karnym i jest organem właściwym, aby nakazać gromadzenie dowodów zgodnie z prawem krajowym; w takim przypadku 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 służący uzyskaniu danych o ruchu, z wyjątkiem danych, których zażądano wyłącznie w celu identyfikacji użytkownika zdefiniowanych w art. 3 pkt 10, lub służący uzyskaniu danych dotyczących treści może być wydany wyłącznie przez:

- a) sędziego, sąd, sędziego śledczego właściwych w danej sprawie; lub
- b) inny właściwy organ określony przez państwo wydające, który w danej sprawie pełni funkcję organu dochodzeniowo-śledczego w postępowaniu karnym i jest organem właściwym, aby nakazać gromadzenie dowodów zgodnie z prawem krajowym; w takim przypadku europejski nakaz wydania dowodów podlega zatwierdzeniu przez sędziego, sąd lub 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 dotyczący danych dowolnej kategorii może być wydany wyłącznie przez:

- a) sędziego, sąd, sędziego śledczego lub prokuratora właściwych w danej sprawie; lub
- b) inny właściwy organ określony przez państwo wydające, który w danej sprawie pełni funkcję organu dochodzeniowo-śledczego w postępowaniu karnym i jest organem właściwym, aby nakazać gromadzenie dowodów zgodnie z prawem krajowym; w takim przypadku europejski nakaz zabezpieczenia dowodów 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 europejski nakaz wydania dowodów lub europejski nakaz zabezpieczenia dowodów został zatwierdzony przez organ sądowy zgodnie z ust. 1 lit. b), ust. 2 lit. b) lub ust. 3 lit. b), organ ten może być również uważany za organ wydający na potrzeby przekazania EPOC i EPOC-PR.

5. W należycie ustalonych sytuacjach wyjątkowych zdefiniowanych w art. 3 pkt 18, właściwe organy, o których mowa w ust. 1 lit. b) i ust. 3 lit. b) niniejszego artykułu, mogą w drodze wyjątku wydać europejski nakaz wydania dowodów w odniesieniu do danych abonenta lub danych, których zażądano wyłącznie w celu identyfikacji użytkownika zdefiniowanych w art. 3 pkt 10, lub europejski nakaz zabezpieczenia dowodów bez uprzedniego zatwierdzenia danego nakazu, jeżeli nie można uzyskać zatwierdzenia w terminie i organy te mogłyby wydać nakaz w podobnej sprawie krajowej bez uprzedniego zatwierdzenia. Organ wydający bez zbędnej zwłoki zwraca się o uzyskanie następczego zatwierdzenia danego nakazu, w terminie nieprzekraczającym 48 godzin. Jeżeli taki nakaz nie zostanie następczo zatwierdzony, organ wydający natychmiast wycofuje nakaz i usuwa wszystkie uzyskane dane lub w inny sposób ogranicza ich wykorzystanie.

6. Każde państwo członkowskie może wyznaczyć jeden lub większą liczbę organów centralnych odpowiedzialnych za administracyjne przekazywanie EPOC, EPOC-PR, europejskich nakazów wydania dowodów, europejskich nakazów zabezpieczenia dowodów oraz powiadomień, a także za przekazywanie innej oficjalnej korespondencji związanej z takimi zaświadczeniami lub nakazami.

## Artykuł 5

**Warunki wydania europejskiego nakazu wydania dowodów**

1. Organ wydający może wydać europejski nakaz wydania dowodów tylko wtedy, gdy spełnione są warunki określone w niniejszym artykule.
2. Europejski nakaz wydania dowodów musi być konieczny dla osiągnięcia i proporcjonalny do celu postępowań, o których mowa w art. 2 ust. 3, z uwzględnieniem praw podejrzanego lub oskarżonego, i może być wydany tylko wtedy, gdy podobny nakaz mógłby zostać wydany na tych samych warunkach w podobnej sprawie krajowej.
3. Europejski nakaz wydania dowodów służący uzyskaniu danych abonenta lub uzyskaniu danych, których zażądano wyłącznie w celu identyfikacji użytkownika zdefiniowanych w art. 3 pkt 10, może być wydany w odniesieniu do każdego przestępstwa oraz w związku z wykonaniem w ramach postępowania karnego wykonawczego kary pozbawienia wolności lub środka zabezpieczającego polegającego na pozbawieniu wolności w wymiarze co najmniej czterech miesięcy, o ile nie zostały one wymierzone orzeczeniem wydanym zaocznie, w przypadkach gdy skazany ukrywa się przed wymiarem sprawiedliwości.
4. Europejski nakaz wydania dowodów służący uzyskaniu danych o ruchu – z wyjątkiem danych, których zażądano wyłącznie w celu identyfikacji użytkownika zdefiniowanych w art. 3 pkt 10 niniejszego rozporządzenia – lub uzyskaniu danych dotyczących treści jest wydawany 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 informatycznego:
    - (i) przestępstw określonych w art. 3–8 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/713 <sup>(32)</sup>;
    - (ii) przestępstw określonych w art. 3–7 dyrektywy 2011/93/UE;
    - (iii) przestępstw określonych w art. 3–8 dyrektywy 2013/40/UE;
  - c) przestępstw określonych w art. 3–12 i w art. 14 dyrektywy (UE) 2017/541;
  - d) w związku z wykonaniem w ramach postępowania karnego wykonawczego kary pozbawienia wolności lub środka zabezpieczającego polegającego na pozbawieniu wolności w wymiarze co najmniej czterech miesięcy, o ile nie zostały one wymierzone orzeczeniem wydanym zaocznie, w przypadkach gdy skazany ukrywa się przed wymiarem sprawiedliwości, w odniesieniu do przestępstw, o których mowa w lit. a), b) i c) niniejszego ustępu.
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) użytkownik, z wyjątkiem nakazu, którego jedynym celem jest identyfikacja użytkownika, lub wszelkie inne niepowtarzalne identyfikatory, takie jak nazwa użytkownika, login lub nazwa konta, w celu określenia danych objętych nakazem;
  - d) kategoria danych objętych nakazem według kategorii zdefiniowanych w art. 3 pkt 9–12;
  - e) w stosownych przypadkach przedział czasowy danych objętych nakazem wydania;
  - f) mające zastosowanie przepisy prawa karnego państwa wydającego;
  - g) w sytuacjach wyjątkowych zdefiniowanych w art. 3 pkt 18 – należyte uzasadnione powody, dla których sytuację uznano za wyjątkową;
  - h) w przypadku gdy europejski nakaz wydania dowodów jest skierowany bezpośrednio do usługodawcy, który przechowuje lub w inny sposób przetwarza dane w imieniu administratora – potwierdzenie, że spełnione są warunki określone w ust. 6 niniejszego artykułu;
  - i) podstawy uznania, że europejski nakaz wydania dowodów spełnia warunki konieczności i proporcjonalności, zgodnie z ust. 2 niniejszego artykułu;
  - j) zwięzły opis sprawy.

<sup>(32)</sup> Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/713 z dnia 17 kwietnia 2019 r. w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi, zastępująca decyzję ramową Rady 2001/413/WSiSW (Dz.U. L 123 z 10.5.2019, s. 18).

6. Europejski nakaz wydania dowodów jest skierowany do usługodawcy działającego w charakterze administratora, zgodnie z rozporządzeniem (UE) 2016/679.

W drodze wyjątku europejski nakaz wydania dowodów może być skierowany bezpośrednio do usługodawcy, który przechowuje lub w przetwarza w inny sposób dane w imieniu administratora, jeżeli:

- a) nie można zidentyfikować administratora pomimo racjonalnych wysiłków organu wydającego; lub
- b) zwrócenie się do administratora mogłoby zaszkodzić postępowaniu przygotowawczemu.

7. Zgodnie z rozporządzeniem (UE) 2016/679 podmiot przetwarzający, który przechowuje lub w inny sposób przetwarza dane w imieniu administratora, informuje administratora o wydaniu danych, chyba że organ wydający zwrócił się do usługodawcy o powstrzymanie się od informowania administratora, tak długo, jak jest to konieczne i proporcjonalne, aby nie utrudniać danego postępowania karnego. W takim przypadku organ wydający wskazuje w aktach sprawy przyczyny opóźnienia w poinformowaniu administratora. Krótkie uzasadnienie załącza się również do EPOC.

8. Jeżeli dane są przechowywane lub w inny sposób przetwarzane w infrastrukturze zapewnianej przez usługodawcę organowi publicznemu, europejski nakaz wydania dowodów może zostać wydany tylko wtedy, gdy organ publiczny, dla którego dane są przechowywane lub w inny sposób przetwarzane, znajduje się w państwie wydającym.

9. W przypadku gdy dane chronione tajemnicą zawodową na podstawie prawa państwa wydającego są przechowywane lub w inny sposób przetwarzane przez usługodawcę w infrastrukturze udostępnianej przedstawicielom zawodów objętych tajemnicą zawodową w związku z ich działalnością zawodową, europejski nakaz wydania dowodów w celu uzyskania danych o ruchu – z wyjątkiem danych, których zażądano wyłącznie w celu identyfikacji użytkownika zdefiniowanych w art. 3 pkt 10 – lub w celu uzyskania danych dotyczących treści może zostać wydany wyłącznie:

- a) jeżeli przedstawiciel zawodu objętego tajemnicą zawodową ma miejsce pobytu w państwie wydającym;
- b) jeżeli zwrócenie się do przedstawiciela zawodu objętego tajemnicą zawodową mogłoby zaszkodzić postępowaniu przygotowawczemu; lub
- c) jeżeli tajemnica zawodowa została uchylona zgodnie z mającym zastosowanie prawem.

10. Jeżeli organ wydający ma powody, by przypuszczać, że dane o ruchu – z wyjątkiem danych, których zażądano wyłącznie w celu identyfikacji użytkownika zdefiniowanych w art. 3 pkt 10 – lub dane dotyczące treści objęte europejskim nakazem wydania dowodów chronione są immunitetami lub przywilejami przysługującymi na podstawie prawa państwa wykonującego, lub że dane te podlegają w tym państwie przepisom dotyczącym ustalania i granic odpowiedzialności karnej związanym z wolnością prasy lub wolnością wypowiedzi w innych mediach, organ wydający może wystąpić o wyjaśnienia przed wydaniem europejskiego nakazu wydania dowodów, w tym w drodze konsultacji z właściwymi organami państwa wykonującego, bezpośrednio albo za pośrednictwem Eurojustu lub Europejskiej Sieci Sądowej.

Organ wydający nie może wydać europejskiego nakazu wydania dowodów, jeżeli uzna, że wymagane dane o ruchu – z wyjątkiem danych, których zażądano wyłącznie w celu identyfikacji użytkownika zdefiniowanych w art. 3 pkt 10 – lub dane dotyczące treści są chronione immunitetami lub przywilejami przysługującymi na podstawie prawa państwa wykonującego lub że dane te podlegają w tym państwie przepisom dotyczącym ustalania i granic odpowiedzialności karnej związanym z wolnością prasy i wolnością wypowiedzi w innych mediach.

#### Artykuł 6

#### Warunki wydania europejskiego nakazu zabezpieczenia dowodów

1. Organ wydający może wydać europejski nakaz zabezpieczenia dowodów tylko wtedy, gdy spełnione są warunki określone w niniejszym artykule. Art. 5 ust. 8 stosuje się odpowiednio.
2. Europejski nakaz zabezpieczenia dowodów musi być konieczny dla osiągnięcia i proporcjonalny do celu zapobieżenia usunięciu, skasowaniu lub modyfikacji danych, które mają być objęte następnie wnioskiem o wydanie tych danych w ramach wzajemnej pomocy prawnej, europejskiego nakazu dochodzeniowego (END) lub europejskiego nakazu wydania dowodów, z uwzględnieniem praw podejrzanego lub oskarżonego.
3. Europejski nakaz zabezpieczenia dowodów może być wydany w odniesieniu do każdego przestępstwa, jeżeli mógłby zostać wydany na tych samych warunkach w podobnej sprawie krajowej, oraz w związku z wykonaniem w ramach postępowania karnego wykonawczego kary pozbawienia wolności lub środka zabezpieczającego polegającego na pozbawieniu wolności w wymiarze co najmniej czterech miesięcy, o ile nie zostały one wymierzone orzeczeniem wydanym zaocznie, w przypadkach gdy skazany ukrywa się przed wymiarem sprawiedliwości.

4. Europejski nakaz zabezpieczenia dowodów zawiera następujące informacje:
- organ wydający oraz, w stosownych przypadkach, organ zatwierdzający;
  - adresat europejskiego nakazu zabezpieczenia dowodów, o którym mowa w art. 7;
  - użytkownik, z wyjątkiem nakazu, którego jedynym celem jest identyfikacja użytkownika, lub wszelkie inne niepowtarzalne identyfikatory, takie jak nazwa użytkownika, login lub nazwa konta, w celu określenia danych objętych nakazem zabezpieczenia;
  - kategoria danych objętych nakazem według kategorii zdefiniowanych w art. 3 pkt 9–12;
  - w stosownych przypadkach przedział czasowy danych objętych nakazem zabezpieczenia;
  - mające zastosowanie przepisy prawa karnego państwa wydającego;
  - podstawy uznania, że europejski nakaz zabezpieczenia dowodów spełnia warunki konieczności i proporcjonalności, zgodnie z ust. 2 niniejszego artykułu.

#### Artykuł 7

##### **Adresaci europejskich nakazów wydania dowodów i europejskich nakazów zabezpieczenia dowodów**

- Europejskie nakazy wydania dowodów i europejskie nakazy zabezpieczenia dowodów są kierowane bezpośrednio do wyznaczonego zakładu lub do przedstawiciela prawnego danego usługodawcy.
- Wyjątkowo, w sytuacjach wyjątkowych zdefiniowanych w art. 3 pkt 18, jeżeli wyznaczony zakład lub przedstawiciel prawny usługodawcy nie reaguje na EPOC lub EPOC-PR w terminie, wówczas ten EPOC lub EPOC-PR można skierować do innego zakładu lub przedstawiciela prawnego usługodawcy w Unii.

#### Artykuł 8

##### **Powiadomienie organu przymuszającego do wykonania nakazu**

- Jeżeli europejski nakaz wydania dowodów jest wydawany w celu uzyskania danych o ruchu – z wyjątkiem danych, których zażądano wyłącznie w celu identyfikacji użytkownika zdefiniowanych w art. 3 pkt 10 – lub w celu uzyskania danych dotyczących treści, organ wydający powiadamia organ przymuszający do wykonania nakazu, przekazując EPOC temu organowi równocześnie z przekazaniem EPOC adresatowi zgodnie z art. 9 ust. 1 i 2.
- Ust. 1 nie stosuje się, jeżeli w momencie wydawania nakazu organ wydający ma uzasadnione podstawy, by sądzić, że:
  - przestępstwo zostało popełnione, jest popełniane lub istnieje prawdopodobieństwo jego popełnienia w państwie wydającym; oraz
  - osoba, której dane są objęte nakazem, ma miejsce pobytu w państwie wydającym.
- Przekazując EPOC zgodnie z ust. 1 niniejszego artykułu, organowi przymuszającemu do wykonania nakazu, organ wydający zamieszcza, w stosownych przypadkach, wszelkie dodatkowe informacje, które mogą być potrzebne do oceny możliwości powołania się na podstawy odmowy zgodnie z art. 12.
- Powiadomienie organu przymuszającego do wykonania nakazu, o którym mowa w ust. 1 niniejszego artykułu, ma skutek zawieszający w odniesieniu do obowiązków adresata określonych w art. 10 ust. 2, z wyjątkiem sytuacjami wyjątkowych zdefiniowanych w art. 3 pkt 18.

#### Artykuł 9

##### **Zaświadczenie europejskiego nakazu wydania dowodów (EPOC) i zaświadczenie europejskiego nakazu zabezpieczenia dowodów (EPOC-PR)**

- Europejski nakaz wydania dowodów lub europejski nakaz zabezpieczenia dowodów przekazuje się adresatowi określonymu w art. 7, za pomocą EPOC lub EPOC-PR.

Organ wydający lub, w stosownych przypadkach, organ zatwierdzający wypełnia EPOC zawarte w załączniku I lub EPOC-PR zawarte w załączniku II, podpisuje je i zaświadcza, że jego treść jest prawdziwa i poprawna.

2. EPOC zawiera informacje wymienione w art. 5 ust. 5 lit. a)–h), w tym wystarczające informacje, które umożliwiają adresatowi identyfikację organu wydającego oraz organu przymuszającego do wykonania nakazu i kontakt z nimi, w razie potrzeby.

Jeżeli powiadomienie organu przymuszającego do wykonania nakazu jest wymagane na podstawie art. 8, EPOC przekazane temu organowi zawiera informacje wymienione w art. 5 ust. 5 lit. a)–j).

3. EPOC-PR zawiera informacje wymienione w art. 6 ust. 4 lit. a)–f), w tym wystarczające informacje umożliwiające adresatowi identyfikację organu wydającego i kontakt z nim.

4. W razie potrzeby EPOC lub EPOC-PR tłumaczy się na język urzędowy Unii akceptowany przez adresata zgodnie z art. 4 dyrektywy (UE) 2023/1544. Jeżeli usługodawca nie wskazał żadnego języka, EPOC lub EPOC-PR tłumaczy się na język urzędowy państwa członkowskiego, w którym znajduje się wyznaczony zakład lub przedstawiciel prawny usługodawcy.

Jeżeli powiadomienie organu przymuszającego do wykonania nakazu jest wymagane na podstawie art. 8, wówczas EPOC, które ma zostać przekazane temu organowi, tłumaczy się na język urzędowy państwa wykonującego lub na inny język urzędowy Unii akceptowany przez to państwo.

#### Artykuł 10

#### Wykonanie EPOC

1. Po otrzymaniu EPOC, adresat podejmuje pilnie działania, aby zabezpieczyć dane objęte nakazem.

2. Jeżeli powiadomienie organu przymuszającego do wykonania nakazu jest wymagane na podstawie art. 8, a organ ten nie podniósł żadnej podstawy odmowy zgodnie z art. 12 w terminie 10 dni od otrzymania EPOC, adresat zapewnia przekazanie danych objętych nakazem bezpośrednio organowi wydającemu lub organom ścigania, wskazanym w EPOC, z końcem tego 10-dniowego terminu. Jeżeli organ przymuszający do wykonania nakazu, jeszcze przed upływem tego 10-dniowego terminu, potwierdzi organowi wydającemu i adresatowi, że nie podniesie żadnej podstawy odmowy, adresat podejmuje działania jak najszybciej po takim potwierdzeniu, a najpóźniej z końcem tego 10-dniowego terminu.

3. Jeżeli powiadomienie organu przymuszającego do wykonania nakazu nie jest wymagane na podstawie art. 8, po otrzymaniu EPOC adresat zapewnia przekazanie wymaganych danych bezpośrednio organowi wydającemu lub organom ścigania, wskazanym w EPOC, najpóźniej w terminie 10 dni od otrzymania EPOC.

4. W sytuacjach wyjątkowych adresat przekazuje dane objęte nakazem bez zbędnej zwłoki, najpóźniej w ciągu ośmiu godzin po otrzymaniu EPOC. Jeżeli powiadomienie organu przymuszającego do wykonania nakazu jest wymagane na podstawie art. 8, organ przymuszający do wykonania nakazu może – jeżeli postanowi powołać się na podstawę odmowy zgodnie z art. 12 ust. 1 – niezwłocznie, a najpóźniej w ciągu 96 godzin od otrzymania powiadomienia, powiadomić organ wydający i adresata, że sprzeciwia się wykorzystaniu danych lub że dane mogą być wykorzystane wyłącznie na określonych przez niego warunkach. Jeżeli organ przymuszający do wykonania nakazu powoła się na podstawę odmowy, wówczas, jeżeli adresat przekazał już dane organowi wydającemu, organ wydający usuwa te dane lub w inny sposób ogranicza ich wykorzystanie lub, w przypadku gdy organ przymuszający do wykonania nakazu określił warunki wykorzystania danych, przestrzega takich warunków.

5. Jeżeli adresat uzna, wyłącznie na podstawie informacji zawartych w EPOC, że wykonanie EPOC mogłoby kolidować z przewidzianymi w prawie państwa wykonującego immunitetami lub przywilejami lub z przepisami dotyczącymi ustalania lub granic odpowiedzialności karnej związanymi z wolnością prasy lub wolnością wypowiedzi w innych mediach, adresat informuje o tym organ wydający i organ przymuszający do wykonania nakazu, korzystając z formularza zawartego w załączniku III.

Jeżeli organ przymuszający do wykonania nakazu nie został powiadomiony na podstawie art. 8, organ wydający uwzględni informacje, o których mowa w akapicie pierwszym niniejszego ustępu, i postanawia – z własnej inicjatywy lub na wniosek organu przymuszającego do wykonania nakazu – o wycofaniu, dostosowaniu albo utrzymaniu europejskiego nakazu wydania dowodów.

Jeżeli organ przymuszający do wykonania nakazu został powiadomiony na podstawie art. 8, organ wydający uwzględni informacje, o których mowa w akapicie pierwszym niniejszego ustępu, i postanawia o wycofaniu, dostosowaniu albo utrzymaniu europejskiego nakazu wydania dowodów. Organ przymuszający do wykonania nakazu może postanowić powołać się na podstawy odmowy określone w art. 12.



6. Jeżeli adresat nie jest w stanie wywiązać się z obowiązku wydania danych objętych nakazem, ponieważ EPOC jest niekompletny, zawiera oczywiste błędy lub nie zawiera informacji wystarczających do jego wykonania, adresat informuje bez zbędnej zwłoki organ wydający oraz – w przypadku gdy organ przymuszający do wykonania nakazu został powiadomiony na podstawie art. 8 – organ przymuszający do wykonania nakazu wskazany w EPOC i występuje o wyjaśnienia, korzystając z formularza zawartego w załączniku III. Jednocześnie adresat informuje organ wydający, czy identyfikacja i zabezpieczenie – zgodnie z ust. 9 niniejszego artykułu – danych objętych nakazem były możliwe.

Organ wydający odpowiada pilnie, a najpóźniej w terminie pięciu dni od otrzymania formularza. Adresat zapewnia, by miał możliwość otrzymania niezbędnych wyjaśnień lub sprostowania od organu wydającego, aby móc wypełniać swoje obowiązki określone w ust. 1–4. Obowiązki określone w ust. 1–4 nie mają zastosowania do czasu przedstawienia takich wyjaśnień lub takiego sprostowania przez organ wydający lub organ przymuszający do wykonania nakazu.

7. Jeżeli adresat nie jest w stanie wywiązać się z obowiązku wydania danych objętych nakazem ze względu na faktyczną niemożność wynikającą z okoliczności, których nie można przypisać adresatowi, informuje on bez zbędnej zwłoki organ wydający i – w przypadku gdy organ przymuszający do wykonania nakazu został powiadomiony na podstawie art. 8 – organ przymuszający do wykonania nakazu wskazany w EPOC i podaje powody tej faktycznej niemożności, korzystając z formularza zawartego w załączniku III. Jeżeli organ wydający stwierdzi taką faktyczną niemożność, informuje on adresata i – w przypadku gdy organ przymuszający do wykonania nakazu został powiadomiony na podstawie art. 8 – organ przymuszający do wykonania nakazu, że wykonanie EPOC nie jest już wymagane.

8. We wszystkich przypadkach, w których adresat nie przekazuje danych objętych nakazem lub nie przekazuje danych objętych nakazem w sposób wyczerpujący lub nie przekazuje danych objętych nakazem we wskazanym terminie z powodów innych niż te, o których mowa w art. 5, 6 i 7 niniejszego artykułu, adresat bez zbędnej zwłoki i nie później niż w terminach określonych w ust. 2, 3 i 4 niniejszego artykułu informuje organ wydający oraz – w przypadku gdy organ przymuszający do wykonania nakazu został powiadomiony na podstawie art. 8 – organ przymuszający do wykonania nakazu wskazany w EPOC, o tych powodach, korzystając z formularza zawartego w załączniku III. Organ wydający dokonuje kontroli europejskiego nakazu wydania dowodów w świetle informacji przekazanych przez adresata i w razie potrzeby wyznacza adresatowi nowy termin na wydanie danych.

9. Dane zabezpiecza się, na ile to możliwe, do momentu ich wydania – niezależnie od tego, czy wydanie jest ostatecznie przedmiotem żądania na podstawie opatrzonego wyjaśnieniami europejskiego nakazu wydania dowodów i dotyczącego go EPOC, czy też za pośrednictwem innych kanałów, takich jak wzajemna pomoc prawna – lub do momentu wycofania europejskiego nakazu wydania dowodów.

Jeżeli wydanie danych i ich zabezpieczenie nie są już konieczne, organ wydający oraz, w stosownych przypadkach przewidzianych w art. 16 ust. 8, organ przymuszający do wykonania nakazu informują o tym adresata bez zbędnej zwłoki.

#### Artykuł 11

#### Wykonanie EPOC-PR

1. Po otrzymaniu EPOC-PR adresat bez zbędnej zwłoki zabezpiecza dane objęte nakazem. Obowiązek zabezpieczenia danych ustaje po upływie 60 dni, chyba że organ wydający potwierdzi, korzystając z formularza zawartego w załączniku V, że wystąpiono następnie z wnioskiem o wydanie dowodów. W ciągu tego 60-dniowego okresu organ wydający może – korzystając z formularza zawartego w załączniku VI – przedłużyć trwanie obowiązku zabezpieczenia danych o dodatkowe 30 dni, jeżeli jest to konieczne do wydania następnie wniosku o wydanie dowodów.

2. Jeżeli w okresie zabezpieczenia określonym w ust. 1 organ wydający potwierdzi, że wydano następnie wniosek o wydanie dowodów, adresat zabezpiecza dane na tak długo, jak to konieczne w celu wydania dowodów, gdy tylko otrzyma ten wniosek o wydanie dowodów.

3. Jeżeli zabezpieczenie nie jest już konieczne, organ wydający informuje o tym adresata bez zbędnej zwłoki, a obowiązek zabezpieczenia danych na podstawie europejskiego nakazu zabezpieczenia dowodów ustaje.

4. Jeżeli adresat uzna, wyłącznie na podstawie informacji zawartych w EPOC-PR, że wykonanie EPOC-PR mogłoby kolidować z przewidzianymi w prawie państwa wykonującego immunitetami lub przywilejami lub z przepisami dotyczącymi ustalania lub granic odpowiedzialności karnej związanymi z wolnością prasy lub wolnością wypowiedzi w innych mediach, adresat informuje o tym organ wydający i organ przymuszający do wykonania nakazu, korzystając z formularza zawartego w załączniku III.

Organ wydający uwzględnia informacje, o których mowa w akapicie pierwszym niniejszego ustępu, i postanawia – z własnej inicjatywy lub na wniosek organu przymuszającego do wykonania nakazu – o wycofaniu, dostosowaniu albo utrzymaniu europejskiego nakazu zabezpieczenia dowodów.

5. Jeżeli adresat nie jest w stanie wywiązać się z obowiązku zabezpieczenia danych objętych nakazem, ponieważ EPOC-PR jest niekompletny, zawiera oczywiste błędy lub nie zawiera informacji wystarczających do jego wykonania, adresat informuje bez zbędnej zwłoki organ wydający wskazany w EPOC-PR i występuje o wyjaśnienia, korzystając z formularza zawartego w załączniku III.

Organ wydający odpowiada pilnie, a najpóźniej w terminie pięciu dni od otrzymania formularza. Adresat zapewnia możliwość otrzymania niezbędnych wyjaśnień lub sprostowania od organu wydającego, aby móc wypełniać swoje obowiązki określone w ust. 1, 2 i 3. W razie braku reakcji organu wydającego w terminie pięciu dni, usługodawca jest zwolniony z obowiązków określonych w ust. 1 i 2.

6. Jeżeli adresat nie jest w stanie wywiązać się z obowiązku zabezpieczenia danych objętych nakazem ze względu na faktyczną niemożność wynikającą z okoliczności, których nie można przypisać adresatowi, informuje on bez zbędnej zwłoki organ wydający wskazany w EPOC-PR i podaje powody tej faktycznej niemożności, korzystając z formularza zawartego w załączniku III. Jeżeli organ wydający stwierdzi, że zachodzi taka niemożność, informuje on adresata, że wykonanie EPOC-PR nie jest już wymagane.

7. We wszystkich przypadkach, w których adresat nie zabezpiecza danych objętych nakazem z powodów innych niż te, o których mowa w ust. 4, 5, i 6, adresat bez zbędnej zwłoki informuje organ wydający o tych powodach, korzystając z formularza zawartego w załączniku III. Organ wydający dokonuje kontroli europejskiego nakazu zabezpieczenia dowodów w świetle uzasadnienia przedstawionego przez adresata.

#### Artykuł 12

#### Podstawy odmowy wykonania europejskich nakazów wydania dowodów

1. Jeżeli organ wydający powiadomił organ przymuszający do wykonania nakazu na podstawie art. 8, bez uszczerbku dla art. 1 ust. 3, organ przymuszający do wykonania nakazu jak najszybciej, a najpóźniej w ciągu 10 dni po otrzymaniu powiadomienia lub, w sytuacjach wyjątkowych, najpóźniej w ciągu 96 godzin po jego otrzymaniu, ocenia informacje zawarte w nakazie i, w stosownych przypadkach, powołuje się na co najmniej jedną z następujących podstaw odmowy:

- a) dane objęte nakazem są chronione immunitetami lub przywilejami przysługującymi na mocy prawa państwa wykonującego, które uniemożliwiają wykonanie lub przymuszenie do wykonania nakazu, lub dane objęte nakazem są objęte przepisami dotyczącymi ustalania lub granic odpowiedzialności karnej związanymi z wolnością prasy lub wolnością wypowiedzi w innych mediach, uniemożliwiający wykonanie lub postępowanie przymuszające do wykonania nakazu;
- b) w sytuacjach wyjątkowych – istnieją istotne podstawy, by sądzić, na podstawie konkretnych i obiektywnych dowodów, że wykonanie nakazu w szczególnych okolicznościach danej sprawy wiązałoby się z oczywistym naruszeniem odpowiedniego prawa podstawowego określonego w art. 6 TUE i w Karcie;
- c) wykonanie nakazu byłoby sprzeczne z zasadą *ne bis in idem*;
- d) czyn, w związku z którym wydano nakaz, nie stanowi przestępstwa według prawa państwa wykonującego, chyba że dotyczy to przestępstwa wchodzącego w zakres kategorii przestępstw wyszczególnionych w załączniku IV, jak wskazał organ wydający w EPOC, jeżeli w państwie wydającym podlega ono karze pozbawienia wolności lub środkowi zabezpieczającemu polegającemu na pozbawieniu wolności o górnej granicy ustawowego zagrożenia w wysokości co najmniej trzech lat.

2. Jeżeli organ przymuszający do wykonania nakazu powołuje się na podstawę odmowy zgodnie z ust. 1, informuje o tym adresata i organ wydający. Adresat wstrzymuje wykonanie europejskiego nakazu wydania dowodów i nie przekazuje danych, a organ wydający wycofuje nakaz.

3. Przed podjęciem decyzji o powołaniu się na podstawę odmowy organ przymuszający do wykonania nakazu powiadomiony zgodnie z art. 8 kontaktuje się z organem wydającym w dowolny właściwy sposób, aby przeprowadzić konsultacje co do odpowiednich środków, które mają zostać podjęte. Na tej podstawie organ wydający może postanowić o dostosowaniu lub wycofaniu europejskiego nakazu wydania dowodów. Jeżeli takie konsultacje nie przyniosą rozwiązania, organ przymuszający do wykonania nakazu powiadomiony zgodnie z art. 8 może podjąć decyzję o powołaniu się na podstawy odmowy wydania europejskiego nakazu wydania dowodów oraz poinformować o tym organ wydający i adresata.

4. Jeżeli organ przymuszający do wykonania nakazu postanowi powołać się na podstawy odmowy zgodnie z ust. 1, może wskazać, czy sprzeciwia się przekazaniu wszystkich danych objętych europejskim nakazem wydania dowodów, czy też dane mogą zostać przekazane jedynie częściowo lub wykorzystane na warunkach określonych przez organ przymuszający do wykonania nakazu.

5. Jeżeli do uchylenia immunitetu lub przywileju określonego w ust. 1 lit. a) niniejszego artykułu uprawniony jest jeden z organów państwa wykonującego, organ wydający może zwrócić się do organu przymuszającego do wykonania nakazu powiadomionego na podstawie art. 8 o skontaktowanie się z tym organem państwa wykonującego i wystąpienie do niego, aby niezwłocznie skorzystał z tego uprawnienia. Jeżeli do uchylenia immunitetu lub przywileju uprawniony jest organ innego państwa członkowskiego lub państwa trzeciego lub organizacja międzynarodowa, organ wydający może zwrócić się do odpowiedniego organu, aby skorzystał z tego uprawnienia.

#### Artykuł 13

### Informowanie użytkowników i poufność

1. Organ wydający bez zbędnej zwłoki informuje osobę, której dane są objęte nakazem, o wydaniu danych na podstawie europejskiego nakazu wydania dowodów.
2. Organ wydający może, zgodnie z prawem krajowym państwa wydającego, opóźnić lub ograniczyć powiadomienie osoby, której dane są objęte nakazem, lub zaniechać jej powiadamiania, w zakresie, w jakim spełnione są warunki określone w art. 13 ust. 3 dyrektywy (UE) 2016/680, i tak długo, jak są one spełnione, i wskazuje wówczas w aktach sprawy przyczyny opóźnienia, ograniczenia lub zaniechania. Krótkie uzasadnienie załącza się również do EPOC.
3. Informując osobę, której dane są objęte nakazem zgodnie z ust. 1 niniejszego artykułu, organ wydający podaje informacje o dostępnych na podstawie art. 18 środkach prawnych.
4. Adresaci oraz – jeżeli adresaci nie są tożsami z usługodawcami – usługodawcy stosują niezbędne najnowocześniejsze środki operacyjne i techniczne w celu zapewnienia poufności, tajności i integralności EPOC lub EPOC-PR i wydawanych lub zabezpieczanych danych.

#### Artykuł 14

### Zwrot kosztów

1. Usługodawca może wystąpić o zwrot poniesionych przez siebie kosztów do państwa wydającego, jeżeli taką możliwość przewidziano w prawie krajowym państwa wydającego w odniesieniu do nakazów krajowych w podobnych sytuacjach zgodnie z prawem krajowym tego państwa. Państwa członkowskie informują Komisję o swoich zasadach zwrotu kosztów, a Komisja podaje te zasady do wiadomości publicznej.
2. Niniejszy artykuł nie ma zastosowania do zwrotu kosztów związanych ze zdecentralizowanym systemem teleinformatycznym, o którym mowa w art. 25.

## ROZDZIAŁ III

### KARY I POSTĘPOWANIE PRZYMUSZAJĄCE

#### Artykuł 15

### Kary

1. Bez uszczerbku dla prawa krajowego przewidującego nakładanie kar, państwa członkowskie ustanawiają – zgodnie z art. 16 ust. 10 – przepisy dotyczące kar pieniężnych mających zastosowanie w przypadku naruszeń art. 10 i 11 oraz art. 13 ust. 4 i podejmują wszelkie niezbędne środki w celu zapewnienia ich wykonywania. Przewidziane kary pieniężne muszą być skuteczne, proporcjonalne i odstrasżające. Państwa członkowskie zapewniają możliwość nałożenia kar pieniężnych o wysokości nieprzekraczającej 2 % całkowitego światowego rocznego obrotu usługodawcy w poprzednim roku obrotowym. Państwa członkowskie powiadamiają Komisję o tych przepisach i środkach niezwłocznie, a także powiadamiają ją niezwłocznie o wszelkich późniejszych zmianach, które ich dotyczą.
2. Bez uszczerbku dla obowiązków w zakresie ochrony danych, usługodawców nie pociąga się do odpowiedzialności w państwach członkowskich za szkody wyrządzone ich użytkownikom lub stronom trzecim wyłącznie w wyniku zastosowania się w dobrej wierze do EPOC lub EPOC-PR.

#### Artykuł 16

### Postępowanie przymuszające

1. Jeżeli adresat nie zastosuje się do EPOC w terminie lub nie zastosuje się do EPOC-PR i nie poda powodów, które zostaną zaakceptowane przez organ wydający i, w stosownych przypadkach, jeżeli organ przymuszający do wykonania nakazu nie powołał się na jedną z podstaw odmowy przewidzianych w art. 12, organ wydający może wystąpić do organu przymuszającego do wykonania nakazu o wszczęcie postępowania przymuszającego do wykonania europejskiego nakazu wydania dowodów lub europejskiego nakazu zabezpieczenia dowodów.

Do celów postępowania przymuszającego, o którym mowa w akapicie pierwszym, organ wydający przekazuje dany nakaz, formularz zawarty w załączniku III wypełniony przez adresata oraz wszelkie odpowiednie dokumenty zgodnie z art. 19. Organ wydający tłumaczy dany nakaz i wszelkie dokumenty, które mają być przekazane, na jeden z języków akceptowanych przez państwo wykonujące i informuje adresata o przekazaniu.

2. Po otrzymaniu europejskiego nakazu wydania dowodów lub europejskiego nakazu zabezpieczenia dowodów organ przymuszający do wykonania nakazu bez dodatkowych formalności uznaje dany nakaz i podejmuje niezbędne środki mające na celu przymuszenie do wykonania:

- a) europejskiego nakazu wydania dowodów, chyba że organ przymuszający do wykonania nakazu uzna, że zastosowanie ma jedna z podstaw przewidzianych w ust. 4; lub
- b) europejskiego nakazu zabezpieczenia dowodów, chyba że organ przymuszający do wykonania nakazu uzna, że zastosowanie ma jedna z podstaw przewidzianych w ust. 5.

Organ przymuszający do wykonania nakazu podejmuje decyzję o uznaniu danego nakazu bez zbędnej zwłoki i nie później niż w terminie pięciu dni roboczych od otrzymania tego nakazu.

3. Organ przymuszający do wykonania nakazu występuje do adresata z formalnym wnioskiem o zastosowanie się do odpowiednich obowiązków i informuje adresata o:

- a) możliwości wniesienia sprzeciwu wobec wykonania danego nakazu przez powołanie się na co najmniej jedną z podstaw wymienionych w ust. 4 lit. a)–f) lub w ust. 5 lit. a)–e);
- b) karach mających zastosowanie w razie niewywiązania się z obowiązku; oraz
- c) terminie na wywiązanie się z obowiązku lub wniesienie sprzeciwu.

4. Wszczęcia postępowania przymuszającego do wykonania europejskiego nakazu wydania dowodów można odmówić wyłącznie na podstawie co najmniej jednej z następujących podstaw:

- a) europejski nakaz wydania dowodów nie został wydany lub zatwierdzony przez organ wydający na zasadach określonych w art. 4;
- b) europejski nakaz wydania dowodów nie został wydany w związku z przestępstwem określonym w art. 5 ust. 4;
- c) adresat nie mógł zastosować się do EPOC ze względu na faktyczną niemożność spowodowaną okolicznościami, których nie można mu przypisać, lub ze względu na oczywiste błędy zawarte w EPOC;
- d) europejski nakaz wydania dowodów nie dotyczy danych przechowywanych przez usługodawcę lub w jego imieniu w momencie otrzymania EPOC;
- e) usługa nie jest objęta niniejszym rozporządzeniem;
- f) dane objęte nakazem są chronione immunitetami lub przywilejami przysługującymi na mocy prawa państwa wykonującego lub dane objęte nakazem są objęte przepisami dotyczącymi ustalania lub granic odpowiedzialności karnej związanymi z wolnością prasy lub wolnością wypowiedzi w innych mediach, uniemożliwiającymi wykonanie lub przymuszenie do wykonania europejskiego nakazu wydania dowodów;
- g) w sytuacjach wyjątkowych, gdy same informacje zawarte w EPOC wskazują na to, że istnieją istotne przesłanki, by sądzić, na podstawie konkretnych i obiektywnych dowodów, że wykonanie europejskiego nakazu wydania dowodów w szczególnych okolicznościach danej sprawy wiązałoby się z oczywistym naruszeniem odpowiedniego prawa podstawowego określonego w art. 6 TUE i w Karcie.

5. Wszczęcia postępowania przymuszającego do wykonania europejskiego nakazu zabezpieczenia dowodów można odmówić wyłącznie na podstawie co najmniej jednej z następujących podstaw:

- a) europejski nakaz zabezpieczenia dowodów nie został wydany lub zatwierdzony przez organ wydający na zasadach przewidzianych w art. 4;
- b) adresat nie mógł zastosować się do EPOC-PR ze względu na faktyczną niemożność spowodowaną okolicznościami, których nie można mu przypisać, lub ze względu na oczywiste błędy zawarte w EPOC-PR;
- c) europejski nakaz zabezpieczenia dowodów nie dotyczy danych przechowywanych przez usługodawcę lub w jego imieniu w momencie otrzymania EPOC-PR;
- d) usługa nie jest objęta zakresem stosowania niniejszego rozporządzenia;

- e) dane objęte nakazem są chronione immunitetami lub przywilejami przysługującymi na mocy prawa państwa wykonującego lub dane objęte nakazem są objęte przepisami dotyczącymi ustalania lub granic odpowiedzialności karnej związanymi z wolnością prasy lub wolnością wypowiedzi w innych mediach, uniemożliwiający wykonanie lub przymuszenie do wykonania europejskiego nakazu zabezpieczenia dowodów;
- f) w sytuacjach wyjątkowych, gdy same informacje zawarte w EPOC-PR wskazują na to, że istnieją uzasadnione przesłanki, by sądzić, na podstawie konkretnych i obiektywnych dowodów, że wykonanie europejskiego nakazu zabezpieczenia dowodów w szczególnych okolicznościach danej sprawy wiązałoby się z oczywistym naruszeniem odpowiedniego prawa podstawowego określonego w art. 6 TUE i w Karcie.
6. W razie wniesienia przez adresata sprzeciwu, o którym mowa w ust. 3 lit. a), organ przymuszający do wykonania nakazu podejmuje decyzję, czy wszcząć postępowanie przymuszające do wykonania europejskiego nakazu wydania dowodów lub europejskiego nakazu zabezpieczenia dowodów 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 europejskiego nakazu wydania dowodów lub europejskiego nakazu zabezpieczenia dowodów zgodnie z – odpowiednio – ust. 2 lub ust. 6 organ przymuszający do wykonania nakazu konsultuje się z organem wydającym wszelkimi właściwymi sposobami. W stosownych przypadkach organ przymuszający do wykonania nakazu występuje o dalsze informacje do organu wydającego. Organ wydający udziela odpowiedzi na takie wnioski w terminie pięciu dni roboczych.
8. Organ przymuszający do wykonania nakazu natychmiast powiadamia organ wydający oraz adresata o wszystkich swoich decyzjach.
9. Jeżeli organ przymuszający do wykonania nakazu uzyska dane objęte europejskim nakazem wydania dowodów od adresata, przekazuje te dane organowi wydającemu bez zbędnej zwłoki.
10. Jeżeli adresat nie wywiązuje się z obowiązku przewidzianego w uznanym europejskim nakazie wydania dowodów lub europejskim nakazie zabezpieczenia dowodów, których wykonalność została potwierdzona przez organ przymuszający do wykonania nakazu, organ przymuszający nakłada karę pieniężną zgodnie z art. 15. Wobec decyzji o nałożeniu kary pieniężnej przysługuje skuteczny środek prawny.

#### ROZDZIAŁ IV

#### NORMY KOLIZYJNE I ŚRODKI PRAWNE

##### Artykuł 17

#### **Postępowanie kontrolne w razie konfliktu obowiązków**

1. Jeżeli adresat uzna, że zastosowanie się do europejskiego nakazu wydania dowodów pozostawałoby w konflikcie z obowiązkiem wynikającym z mającego zastosowanie prawa państwa trzeciego, informuje organ wydający i organ przymuszający do wykonania nakazu o powodach niewykonania europejskiego nakazu wydania dowodów zgodnie z procedurą określoną w art. 10 ust. 8 i 9, korzystając z formularza zawartego w załączniku III (dalej jako „uzasadniony sprzeciw”).
2. Uzasadniony sprzeciw musi zawierać wszelkie odpowiednie informacje na temat przepisów państwa trzeciego, ich stosowności do danej sprawy oraz charakteru sprzecznych obowiązków. Uzasadniony sprzeciw nie może opierać się na:
- a) fakcie, że podobne przepisy dotyczące warunków, formalności i procedur związanych z wydaniem nakazu wydania dowodów nie istnieją w mającym zastosowanie prawie tego państwa trzeciego; lub
- b) samym tylko fakcie, że dane są przechowywane w państwie trzecim.

Uzasadniony sprzeciw wnosi się w terminie 10 dni od dnia, w którym adresat otrzymał EPOC.

3. Organ wydający dokonuje kontroli europejskiego nakazu wydania dowodów na podstawie uzasadnionego sprzeciwu i wszelkich uwag przekazanych przez państwo wykonujące. Jeżeli organ wydający zamierza utrzymać europejski nakaz wydania dowodów w mocy, wnioskuje o dokonanie kontroli przez właściwy sąd państwa wydającego. Wykonanie europejskiego nakazu wydania dowodów zawieszają się do ukończenia postępowania kontrolnego.
4. Właściwy sąd ocenia w pierwszej kolejności, czy konflikt obowiązków istnieje, w oparciu o analizę, czy:
- a) prawo państwa trzeciego ma zastosowanie do szczególnych okoliczności rozpatrywanej sprawy; oraz
- b) prawo państwa trzeciego, jeżeli ma zastosowanie, o czym mowa w lit. a), zabrania ujawniania odnośnych danych w szczególnych okolicznościach rozpatrywanej sprawy.

5. Jeżeli właściwy sąd uzna, że nie występuje konflikt obowiązków w rozumieniu ust. 1 i ust. 4, utrzymuje europejski nakaz wydania dowodów w mocy.

6. Jeżeli właściwy sąd stwierdzi, na podstawie analizy przewidzianej w art. 4 lit. b), że prawo państwa trzeciego zabrania ujawnienia odnośnych danych, właściwy sąd ustala, czy utrzymać w mocy, czy też uchylić europejski nakaz wydania dowodów. Ocena ta opiera się w szczególności na następujących elementach, ze szczególnym uwzględnieniem elementów, o których mowa w lit. a) i b):

- a) interesy chronione odnośnym prawem państwa trzeciego, w tym prawa podstawowe, a także inne podstawowe interesy uniemożliwiające ujawnienie danych, w szczególności interesy bezpieczeństwa narodowego państwa trzeciego;
- b) stopień powiązania sprawy karnej, w której wydano europejski nakaz wydania dowodów, z każdą z dwóch jurysdykcji, między innymi na podstawie:
  - (i) lokalizacji, obywatelstwa i miejsca pobytu osoby, której dane objęte są nakazem, lub osoby poszkodowanej lub osób poszkodowanych danym przestępstwem;
  - (ii) miejsca popełnienia danego przestępstwa;
- c) stopień powiązania między usługodawcą a państwem trzecim, którego sprawa dotyczy; w tym kontekście sama lokalizacja przechowywania danych nie stanowi wystarczającej podstawy do stwierdzenia istotnego stopnia powiązania;
- d) interesy państwa prowadzącego postępowanie przygotowawcze związane z uzyskaniem odnośnych dowodów w oparciu o wagę przestępstwa i znaczenie pilnego uzyskania dowodów;
- e) możliwe konsekwencje dla adresata lub usługodawcy związane z wykonaniem europejskiego nakazu wydania dowodów, w tym ewentualne kary.

7. Właściwy sąd może zwrócić się z wnioskiem o udzielenie informacji do właściwego organu państwa trzeciego, uwzględniając dyrektywę (UE) 2016/680, w szczególności jej rozdział V, w zakresie, w jakim wniosek ten nie utrudni odnośnego postępowania karnego. Państwo wydające, w szczególności, zwraca się do właściwego organu państwa trzeciego z wnioskiem o udzielenie informacji, jeżeli konflikt obowiązków dotyczy praw podstawowych lub innych podstawowych interesów państwa trzeciego związanych z bezpieczeństwem narodowym i obronnością.

8. Jeżeli właściwy sąd postanowi o uchyleniu europejskiego nakazu wydania dowodów, informuje organ wydający i adresata. Jeżeli właściwy sąd stwierdzi, że europejski nakaz wydania dowodów ma być utrzymany w mocy, informuje organ wydający i adresata, a adresat przystępuje do wykonania europejskiego nakazu wydania dowodów.

9. Do celów procedur przewidzianych w niniejszym artykule terminy oblicza się zgodnie z prawem krajowym organu wydającego.

10. Organ wydający informuje organ przymuszający do wykonania nakazu o wyniku postępowania kontrolnego.

#### Artykuł 18

#### Skuteczne środki prawne

1. Bez uszczerbku dla dodatkowych środków prawnych dostępnych zgodnie z prawem krajowym każda osoba, której dane są objęte europejskim nakazem wydania dowodów, ma prawo do skutecznych środków prawnych wobec tego nakazu. Jeżeli osoba ta jest podejrzanym lub oskarżonym, ma ona prawo do skutecznych środków prawnych w toku postępowania karnego, w którym wykorzystano te dane. Prawo do skutecznych środków prawnych, o którym mowa w niniejszym paragrafie, pozostaje bez uszczerbku dla prawa do środków prawnych na podstawie rozporządzenia (UE) 2016/679 i dyrektywy (UE) 2016/680.

2. Prawo do skutecznych środków prawnych jest wykonywane przed sądem w państwie wydającym zgodnie z jego prawem krajowym i obejmuje możliwość podważenia legalności środka, w tym jego konieczności i proporcjonalności, bez uszczerbku dla gwarancji praw podstawowych w państwie wykonującym.

3. Do celów art. 13 ust. 1 informacje na temat środków prawnych przewidzianych w prawie krajowym przekazuje się w odpowiednim czasie i zapewnia się możliwość skutecznego korzystania z tych środków.

4. Takie same terminy lub inne warunki korzystania ze środków prawnych, jakie obowiązują w podobnych sprawach krajowych, stosuje się do celów niniejszego rozporządzenia, w sposób gwarantujący zainteresowanym osobom skuteczne korzystanie z tych środków prawnych.

5. Bez uszczerbku dla krajowego prawa procesowego państwo wydające i każde inne państwo członkowskie, któremu przekazano dowody elektroniczne na podstawie niniejszego rozporządzenia, zapewnia przestrzeganie prawa do obrony i do rzetelnego postępowania przy ocenie dowodów uzyskanych za pomocą europejskiego nakazu wydania dowodów.

## ROZDZIAŁ V

### ZDECENTRALIZOWANY SYSTEM TELEINFORMATYCZNY

#### Artykuł 19

#### **Bezpieczna komunikacja cyfrowa i wymiana danych między właściwymi organami a usługodawcami oraz między właściwymi organami**

1. Komunikacja pisemna między właściwymi organami a wyznaczonymi zakładami lub przedstawicielami prawnymi na podstawie niniejszego rozporządzenia, w tym wymiana formularzy przewidzianych w niniejszym rozporządzeniu i danych objętych europejskim nakazem wydania dowodów lub europejskim nakazem zabezpieczenia dowodów, odbywa się za pośrednictwem bezpiecznego i niezawodnego zdecentralizowanego systemu teleinformatycznego (zwanego dalej „zdecentralizowanym systemem teleinformatycznym”).

2. Każde państwo członkowskie zapewnia wyznaczonym zakładom lub przedstawicielom prawnym usługodawców znajdującym się w tym państwie członkowskim dostęp do zdecentralizowanego systemu teleinformatycznego za pośrednictwem swojego krajowego systemu teleinformatycznego.

3. Usługodawcy zapewniają wyznaczonym zakładom lub przedstawicielom prawnym możliwość korzystania ze zdecentralizowanego systemu teleinformatycznego za pośrednictwem odpowiedniego krajowego systemu teleinformatycznego, tak by mogli oni otrzymywać EPOC i EPOC-PR, wysyłać dane objęte nakazem organowi wydającemu i kontaktować się w inny sposób z organem wydającym i organem przymuszającym do wykonania nakazu zgodnie z niniejszym rozporządzeniem.

4. Komunikacja pisemna między właściwymi organami na podstawie niniejszego rozporządzenia, w tym wymiana formularzy przewidzianych w niniejszym rozporządzeniu oraz danych, które są objęte postępowaniem przymuszającym do wykonania nakazu przewidzianym w art. 16, a także komunikacja pisemna z właściwymi agencjami lub organami Unii, odbywa się za pośrednictwem zdecentralizowanego systemu teleinformatycznego.

5. Jeżeli komunikacja za pośrednictwem zdecentralizowanego systemu teleinformatycznego zgodnie z ust. 1 lub 4 nie jest możliwa, na przykład ze względu na zakłócenie funkcjonowania zdecentralizowanego systemu teleinformatycznego, charakter przekazywanych materiałów, ograniczenia techniczne, takie jak rozmiar danych, ograniczenia prawne związane z dopuszczalnością wymaganych danych jako dowodów lub z wymogami kryminalistycznymi dotyczącymi wymaganych danych, lub ze względu na sytuacje wyjątkowe, przekazanie odbywa się najwłaściwszymi sposobami alternatywnymi, z uwzględnieniem potrzeby zapewnienia szybkiej, bezpiecznej i niezawodnej wymiany informacji, przy zapewnieniu odbiorcy możliwości stwierdzenia autentyczności.

6. Jeżeli przekazanie odbywa się sposobami alternatywnymi przewidzianymi w ust. 5, inicjator bez zbędnej zwłoki rejestruje w zdecentralizowanym systemie teleinformatycznym to przekazanie, w tym, stosownie do przypadku, datę i czas przekazania, nadawcę i odbiorcę oraz nazwę i wielkość pliku.

#### Artykuł 20

#### **Skutki prawne dokumentów elektronicznych**

Dokumentów przekazywanych w ramach komunikacji elektronicznej nie pozbawia się skutku prawnego ani nie uznaje się ich za niedopuszczalne w kontekście transgranicznych postępowania sądowych objętych niniejszym rozporządzeniem wyłącznie z tego powodu, że dokumenty te mają postać elektroniczną.

#### Artykuł 21

#### **Podpisy i pieczęcie elektroniczne**

1. Do komunikacji elektronicznej na podstawie niniejszego rozporządzenia zastosowanie mają ogólne ramy prawne dotyczące korzystania z usług zaufania określone w rozporządzeniu (UE) nr 910/2014.

2. Jeżeli dokument przekazywany w ramach komunikacji elektronicznej na podstawie art. 19 ust. 1 lub 4 niniejszego rozporządzenia wymaga użycia pieczęci lub podpisu zgodnie z niniejszym rozporządzeniem, dokument ten opatruje się kwalifikowaną pieczęcią elektroniczną lub kwalifikowanym podpisem elektronicznym zdefiniowanymi w rozporządzeniu (UE) nr 910/2014.

#### Artykuł 22

### Oprogramowanie wzorcowe

1. Komisja jest odpowiedzialna za utworzenie, utrzymywanie i rozwój oprogramowania wzorcowego, które państwa członkowskie mogą wykorzystywać jako system zaplecza zamiast krajowego systemu teleinformatycznego. Utworzenie, utrzymywanie i rozwój oprogramowania wzorcowego finansowane są z budżetu ogólnego Unii.
2. Komisja bezpłatnie udostępnia, utrzymuje i wspiera oprogramowanie wzorcowe.

#### Artykuł 23

### Koszty związane ze zdecentralizowanym systemem teleinformatycznym

1. Każde państwo członkowskie ponosi koszty instalacji, obsługi i utrzymania punktów dostępu zdecentralizowanego systemu teleinformatycznego, za które odpowiada.
2. Każde państwo członkowskie ponosi koszty utworzenia i dostosowania swoich krajowych systemów teleinformatycznych w celu zapewnienia ich interoperacyjności z punktami dostępu, a także ponosi koszty związane z zarządzaniem tymi systemami, ich obsługą i utrzymaniem.
3. Agencje i organy Unii ponoszą koszty instalacji, obsługi i utrzymania komponentów składających się na zdecentralizowany system teleinformatyczny, za który odpowiadają.
4. Agencje i organy Unii ponoszą koszty utworzenia i dostosowania swoich systemów zarządzania sprawami w celu zapewnienia ich interoperacyjności z punktami dostępu, a także ponoszą koszty związane z zarządzaniem tymi systemami, ich obsługą i utrzymaniem.
5. Usługodawcy ponoszą wszelkie koszty niezbędne do skutecznej integracji lub innej interakcji ze zdecentralizowanym systemem teleinformatycznym.

#### Artykuł 24

### Okres przejściowy

Do dnia rozpoczęcia stosowania obowiązku prowadzenia komunikacji pisemnej za pośrednictwem zdecentralizowanego systemu teleinformatycznego, o którym mowa w art. 19 (dalej jako „okres przejściowy”), komunikacja pisemna między właściwymi organami a wyznaczonymi zakładami lub przedstawicielami prawnymi na podstawie niniejszego rozporządzenia odbywa się najwłaściwszymi sposobami alternatywnymi, z uwzględnieniem potrzeby zapewnienia szybkiej, bezpiecznej i niezawodnej wymiany informacji. Jeżeli usługodawcy, państwa członkowskie lub agencje bądź organy Unii utworzą specjalne platformy lub inne bezpieczne kanały obsługi wniosków o udostępnienie danych kierowanych przez organy ścigania i organy sądowe, organy wydające mogą również zdecydować, że w okresie przejściowym będą przekazywać EPOC lub EPOC-PR wyznaczonym zakładom lub przedstawicielom prawnym za pośrednictwem tych kanałów.

#### Artykuł 25

### Akty wykonawcze

1. Komisja przyjmuje akty wykonawcze niezbędne do utworzenia i użytkowania zdecentralizowanego systemu teleinformatycznego do celów niniejszego rozporządzenia, określające:
  - a) specyfikacje techniczne określające metody komunikacji elektronicznej na potrzeby zdecentralizowanego systemu teleinformatycznego;
  - b) specyfikacje techniczne protokołów komunikacyjnych;
  - c) cele w zakresie bezpieczeństwa informacji oraz odpowiednie środki techniczne zapewniające minimalne normy bezpieczeństwa informacji i wysoki poziom bezpieczeństwa cyberprzestrzeni w odniesieniu do przetwarzania i przesyłania informacji w ramach zdecentralizowanego systemu teleinformatycznego;
  - d) minimalne cele związane z dostępnością i ewentualne związane z tym wymogi techniczne dotyczące usług zapewnianych przez zdecentralizowany system informatyczny.



2. Akty wykonawcze, o których mowa w ust. 1 niniejszego artykułu, przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 26.
3. Akty wykonawcze, o których mowa w ust. 1, przyjmuje się do dnia 18 sierpnia 2025 r.

#### Artykuł 26

#### **Procedura komitetowa**

1. Komisję wspomaga komitet. Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.
2. W przypadku odesłania do niniejszego ustępu, stosuje się art. 5 rozporządzenia (UE) nr 182/2011.

#### ROZDZIAŁ VI

#### **PRZEPISY KOŃCOWE**

#### Artykuł 27

#### **Języki**

Każde państwo członkowskie może w każdej chwili postanowić, że będzie akceptować tłumaczenia EPOC i EPOC-PR na jeden lub większą ilość języków urzędowych Unii innych niż jego język urzędowy lub języki urzędowe, i informuje o tej decyzji w pisemnym oświadczeniu przedkładanym Komisji. Komisja udostępnia te oświadczenia wszystkim państwom członkowskim oraz Europejskiej Sieci Sądowej.

#### Artykuł 28

#### **Monitorowanie i sprawozdawczość**

1. Do dnia 18 sierpnia 2026 r. Komisja ustanowi szczegółowy program monitorowania wyników, rezultatów i skutków niniejszego rozporządzenia. Program monitorowania określa środki służące do gromadzenia danych, a także przedziały czasowe, w jakich będą one gromadzone. Wskazuje się w nim również działania podejmowane przez Komisję i przez państwa członkowskie w celu gromadzenia i analizowania danych.
2. W każdym przypadku od dnia 18 sierpnia 2026 r. państwa członkowskie gromadzą kompleksowe dane statystyczne uzyskiwane od odpowiednich organów i zachowują takie dane statystyczne. Zgromadzone dane za poprzedni rok kalendarzowy przesyła się Komisji każdego roku do dnia 31 marca i obejmują one:
  - a) liczbę wydanych EPOC i EPOC-PR w podziale na rodzaje danych objętych nakazem, na adresatów i na charakter sytuacji (sytuacja wyjątkowa czy nie);
  - b) liczbę EPOC wydanych w ramach odstępstw związanych z sytuacją wyjątkową;
  - c) liczbę wykonanych i niewykonanych EPOC i EPOC-PR w podziale na rodzaje danych objętych nakazem, adresatów i charakter sytuacji (sytuacja wyjątkowa czy nie);
  - d) liczbę powiadomień kierowanych na podstawie art. 8 do organów przymuszających do wykonania nakazu i liczbę EPOC rozpatrzonych odmownie w podziale na rodzaje danych objętych nakazem, adresatów, charakter sytuacji (sytuacja wyjątkowa czy nie) i wskazane podstawy odmowy;
  - e) w przypadku wykonanych EPOC – średni czas od momentu wydania EPOC do momentu uzyskania danych objętych nakazem w podziale na rodzaje danych objętych nakazem, adresatów i charakter sytuacji (sytuacja wyjątkowa czy nie);
  - f) w przypadku wykonanych EPOC-PR – średni czas od momentu wydania EPOC-PR do momentu wydania następnie wniosku o wydanie dowodów w danej sprawie w podziale na rodzaje danych objętych nakazem i adresatów;
  - g) liczbę europejskich nakazów wydania dowodów lub europejskich nakazów zabezpieczenia dowodów przekazanych państwu wykonującemu i przez nie otrzymanych do celów postępowania przymuszającego do wykonania nakazu w podziale na rodzaje danych objętych nakazem, adresatów i charakter sytuacji (sytuacja wyjątkowa czy nie) oraz liczbę wykonanych nakazów;
  - h) liczbę środków prawnych wniesionych wobec europejskich nakazów wydania dowodów w państwie wydającym i państwie wykonującym w podziale na rodzaje danych objętych nakazem;

- i) liczbę przypadków, w których odmówiono następczego zatwierdzenia przewidzianego w art. 4 ust. 5;
  - j) przegląd kosztów zgłoszonych przez usługodawców w związku z wykonaniem EPOC lub EPOC-PR oraz kosztów zwróconych przez organy wydające.
3. Od dnia 18 sierpnia 2026 r. w przypadku wymiany danych prowadzonej za pośrednictwem zdecentralizowanego systemu teleinformatycznego na podstawie art. 19 ust. 1 dane statystyczne, o których mowa w ust. 2 niniejszego artykułu, mogą być programowo gromadzone przez portale krajowe. Oprogramowanie wzorcowe, o którym mowa w art. 22, musi być dostosowane technicznie do zapewnienia takiej funkcjonalności.
4. Usługodawcy mogą gromadzić, przechowywać i publikować dane statystyczne zgodnie z istniejącymi zasadami ochrony danych. Jeżeli gromadzone są dane statystyczne za poprzedni rok kalendarzowy, można przesłać je Komisji do dnia 31 marca i mogą one, w miarę możliwości, obejmować:
- a) liczbę otrzymanych EPOC i EPOC-PR w podziale na rodzaje danych objętych nakazem, państwa wydające i charakter sytuacji (sytuacja wyjątkowa czy nie);
  - b) liczbę wykonanych i niewykonanych EPOC i EPOC-PR w podziale na rodzaje danych objętych nakazem, państwo wydające i charakter sytuacji (sytuacja wyjątkowa czy nie);
  - c) w przypadku wykonanych EPOC – średni czas potrzebny do uzyskania danych objętych wnioskiem od momentu otrzymania EPOC do momentu przekazania danych w podziale na rodzaje danych objętych nakazem, państwa wydające i charakter sytuacji (sytuacja wyjątkowa czy nie);
  - d) w przypadku wykonanych EPOC-PR – średni czas od momentu wydania EPOC-PR do momentu wydania następnie wniosku o wydanie dowodów w danej sprawie w podziale na rodzaje danych objętych nakazem i państwa wydające.
5. Od dnia 18 sierpnia 2027 r. Komisja do dnia 30 czerwca każdego roku publikuje sprawozdanie zawierające dane, o których mowa w ust. 2 i 3, w formie opracowanej i w podziale na państwa członkowskie i rodzaje usługodawców.

#### Artykuł 29

### Zmiany zaświadczeń i formularzy

Komisja przyjmuje akty delegowane zgodnie z art. 30 dotyczące zmian w załącznikach I, II, III, V i VI w celu poprawienia, o ile zajdzie taka potrzeba, treści formularzy EPOC i EPOC-PR oraz formularzy wykorzystywanych do przekazywania informacji na temat niemożliwości wykonania EPOC lub EPOC-PR, potwierdzania wystąpienia z wnioskiem o wydanie dowodów w następstwie europejskiego nakazu zabezpieczenia dowodów oraz przedłużania zabezpieczenia dowodów elektronicznych.

#### Artykuł 30

### Wykonywanie przekazanych uprawnień

1. Powierzenie Komisji uprawnień do przyjmowania aktów delegowanych podlega warunkom określonym w niniejszym artykule.
2. Uprawnienia do przyjmowania aktów delegowanych, o których mowa w art. 29, powierza się Komisji na czas nieokreślony od dnia 18 sierpnia 2026 r.
3. Przekazanie uprawnień, o którym mowa w art. 29, 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 następnego dnia po jej opublikowaniu w Dzienniku Urzędowym Unii Europejskiej lub w późniejszym terminie określonym w tej decyzji. Nie wpływa ona na ważność 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 z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa.
5. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie.

6. Akt delegowany przyjęty na podstawie art. 29 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 31

##### **Powiadomienia Komisji**

1. Do dnia 18 sierpnia 2025 r. każde państwo członkowskie informuje Komisję o:
  - a) organie lub organach, które zgodnie z jego prawem krajowym są organami właściwymi zgodnie z art. 4 do celów wydawania, zatwierdzania lub przekazywania europejskich nakazów wydania dowodów i europejskich nakazów zabezpieczenia dowodów lub powiadomień o nich;
  - b) organie lub organach właściwych do otrzymywania powiadomień zgodnie z art. 8 oraz do przymuszania do wykonania europejskich nakazów wydania dowodów i europejskich nakazów zabezpieczenia dowodów w imieniu innego państwa członkowskiego, zgodnie z art. 16;
  - c) organie lub organach właściwych do rozpatrywania uzasadnionych sprzeciwów adresatów na podstawie art. 17;
  - d) językach akceptowanych do celów powiadamiania i przekazywania EPOC, EPOC-PR, europejskiego nakazu wydania dowodów lub europejskiego nakazu zabezpieczenia dowodów, w przypadku wykonania, zgodnie z art. 27.
2. Komisja publicznie udostępnia informacje otrzymane na podstawie niniejszego artykułu na specjalnej stronie internetowej albo na stronie internetowej Europejskiej Sieci Sądowej w sprawach karnych, o której mowa w art. 9 decyzji Rady 2008/976/WSiSW<sup>(33)</sup>.

#### Artykuł 32

##### **Związek z innymi instrumentami, umowami i uzgodnieniami**

1. Niniejsze rozporządzenie nie wpływa na unijne lub inne międzynarodowe instrumenty, umowy i uzgodnienia w sprawie gromadzenia dowodów objętego zakresem stosowania niniejszego rozporządzenia.
2. Państwa członkowskie powiadamiają Komisję do dnia 18 sierpnia 2026 r. o istniejących instrumentach, umowach i uzgodnieniach, o których mowa w ust. 1, które będą nadal stosować. Państwa członkowskie powiadamiają również Komisję o wszelkich nowych umowach lub uzgodnieniach, o których mowa w ust. 1, w terminie trzech miesięcy od ich podpisania.

#### Artykuł 33

##### **Ocena**

Do dnia 18 sierpnia 2029 r. Komisja przeprowadza ocenę niniejszego rozporządzenia. Komisja przekazuje sprawozdanie z oceny Parlamentowi Europejskiemu, Radzie, Europejskiemu Inspektorowi Ochrony Danych i Agencji Praw Podstawowych Unii Europejskiej. Sprawozdanie z oceny zawiera ocenę stosowania niniejszego rozporządzenia i wyników osiągniętych w odniesieniu do jego celów, a także ocenę wpływu niniejszego rozporządzenia na prawa podstawowe. Ocena ta jest przeprowadzana zgodnie z wytycznymi Komisji dotyczącymi lepszego stanowienia prawa. Państwa członkowskie przekazują Komisji informacje niezbędne do przygotowania sprawozdania z oceny.

#### Artykuł 34

##### **Wejście w życie i rozpoczęcie stosowania**

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

<sup>(33)</sup> 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).

2. Niniejsze rozporządzenie stosuje się od dnia 18 sierpnia 2026 r.

Spoczywający na właściwych organach i usługodawcach obowiązek korzystania ze zdecentralizowanego systemu teleinformatycznego ustanowionego w art. 19 na potrzeby komunikacji pisemnej na mocy niniejszego rozporządzenia stosuje się po upływie roku od dnia przyjęcia aktów wykonawczych, o których mowa w art. 25.

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

Sporządzono w Strasburgu dnia 12 lipca 2023 r.

*W imieniu Parlamentu Europejskiego*  
*Przewodnicząca*  
R. METSOLA

*W imieniu Rady*  
*Przewodniczący*  
P. NAVARRO RÍOS

—

## ZAŁĄCZNIK I

## ZAŚWIADCZENIE EUROPEJSKIEGO NAKAZU WYDANIA DOWODÓW (EPOC) DOTYCZĄCE WYDANIA DOWODÓW ELEKTRONICZNYCH

Zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2023/1543<sup>(1)</sup> adresat niniejszego zaświadczenia europejskiego nakazu wydania dowodów (EPOC) ma obowiązek wykonać niniejszy EPOC i przekazać dane objęte nakazem w terminach określonych w sekcji C niniejszego EPOC właściwemu organowi wskazanemu w sekcji L lit. a) niniejszego EPOC.

W każdym przypadku, po otrzymaniu EPOC, adresat ma obowiązek pilnie zabezpieczyć dane objęte nakazem chyba że informacje zawarte w EPOC nie pozwalają mu na identyfikację tych danych. Zabezpieczenie danych należy utrzymać do momentu wydania danych lub do momentu, w którym organ wydający lub, w stosownych przypadkach, organ przymuszający do wykonania nakazu wskażą, że zabezpieczenie i wydanie danych nie są już konieczne.

Adresat ma obowiązek podjąć środki konieczne do zapewnienia poufności, tajności i integralności EPOC oraz wydanych lub zabezpieczonych danych.

## SEKCJA A: Organ wydający/zatwierdzający

Państwo wydające: .....

Organ wydający: .....

Organ zatwierdzający (w stosownym przypadku): .....

Uwaga: dane organu wydającego i zatwierdzającego należy podać na końcu (sekcje I i J) .....

Numer sprawy nadany przez organ wydający: .....

Numer sprawy nadany przez organ zatwierdzający: .....

## SEKCJA B: Adresat

Adresat: .....

Wyznaczony zakład

Przedstawiciel prawny

Niniejszy nakaz wydaje się określone mu adresatowi w sytuacji wyjątkowej, ponieważ wyznaczony zakład lub przedstawiciel prawny usługodawcy nie odpowiedział na EPOC w terminach określonych w art. 10 rozporządzenia (UE) 2023/1543 lub nie został wskazany lub ustanowiony w terminach określonych w dyrektywie Parlamentu Europejskiego i Rady (UE) 2023/1544<sup>(2)</sup>.

Adres: .....

Numer telefonu/faksu/adres e-mail (jeśli są znane): .....

Osoba kontaktowa (jeśli jest znana): .....

Numer sprawy nadany przez adresata (jeśli jest znany): .....

Odnośny usługodawca (jeśli jest inny niż adresat): .....

Wszelkie inne odpowiednie informacje: .....

<sup>(1)</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1543 z dnia 12 lipca 2023 r. w sprawie europejskich nakazów wydania i europejskich nakazów zabezpieczenia dowodów elektronicznych w postępowaniu karnym oraz w postępowaniu karnym wykonawczym w związku z wykonaniem kar pozbawienia wolności (Dz.U. L 191 z 28.7.2023, s. 118).

<sup>(2)</sup> Dyrektywa Parlamentu Europejskiego i Rady (UE) 2023/1544 z dnia 12 lipca 2023 r. w sprawie zharmonizowanych przepisów dotyczących wskazywania wyznaczonych zakładów i ustanawiania przedstawicieli prawnych w celu gromadzenia dowodów elektronicznych w postępowaniach karnych (Dz.U. L 191 z 28.7.2023, s. 181).

SEKCJA C: Terminy (proszę zaznaczyć właściwe pole i w razie konieczności uzupełnić):

Po otrzymaniu EPOC dane objęte nakazem należy wydać:

- jak najszybciej, a najpóźniej w ciągu 10 dni (bez powiadamiania organu przymuszającego do wykonania nakazu)
- w przypadku powiadomienia organu przymuszającego do wykonania nakazu: po upływie 10 dni, jeżeli organ wykonujący nie powołał się na podstawy odmowy w tym terminie, lub po potwierdzeniu przez organ przymuszający do wykonania nakazu przed upływem 10 dni, że nie powoła się na podstawy odmowy – tak szybko, jak to możliwe, a najpóźniej z końcem terminu 10 dni;
- bez zbędnej zwłoki i nie później niż w ciągu ośmiu godzin w sytuacji wyjątkowej, która obejmuje:
- bezpośrednie zagrożenie życia, integralności cielesnej lub bezpieczeństwa osoby;
  - bezpośrednie zagrożenie dla infrastruktury krytycznej zdefiniowanej w art. 2 lit. a) dyrektywy Rady 2008/114/WE<sup>(3)</sup>, w przypadku gdy zakłócenie lub zniszczenie takiej infrastruktury krytycznej spowodowałoby bezpośrednie zagrożenie życia, integralności cielesnej lub bezpieczeństwa osoby, w tym przez poważne zakłócenie podstawowych dostaw dla ludności lub wykonywania podstawowych funkcji państwa.

Proszę wskazać, czy istnieją terminy proceduralne lub inne, które należy uwzględnić przy wykonywaniu niniejszego EPOC: .....

W stosownych przypadkach, proszę podać dodatkowe informacje: .....

SEKCJA D: Związek z wcześniejszym wnioskiem o wydanie/zabezpieczenie (proszę zaznaczyć i uzupełnić w stosownym przypadku i w razie dostępności)

- Dane, których dotyczy wniosek, zostały całkowicie/częściowo zabezpieczone zgodnie z wcześniejszym wnioskiem o zabezpieczenie

wydanym przez ..... (proszę wskazać organ i numer sprawy)

w dniu ..... (proszę wstawić datę wydania wniosku)

i przekazany dnia ..... (proszę wstawić datę przekazania wniosku)

do ..... (proszę wskazać usługodawcę/przedstawiciela prawnego/wyznaczony zakład/organ właściwy, któremu przekazano wniosek, oraz numer sprawy nadany przez adresata, o ile numer ten jest dostępny).

- Dane, których dotyczy wniosek, odnoszą się do wcześniejszego wniosku o wydanie

wydanego przez ..... (proszę wskazać organ i numer sprawy)

w dniu ..... (proszę wstawić datę wydania wniosku)

i przekazany dnia ..... (proszę wstawić datę przekazania wniosku)

do ..... (proszę wskazać usługodawcę/przedstawiciela prawnego/wyznaczony zakład/organ właściwy, któremu przekazano wniosek, oraz numer sprawy nadany przez adresata, o ile numer ten jest dostępny).

Wszelkie inne odpowiednie informacje: .....

<sup>(3)</sup> 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 z 23.12.2008, s. 75).

SEKCJA E: Informacje pomocne do identyfikacji danych objętych nakazem (proszę uzupełnić, podając dostępne informacje w zakresie niezbędnym do identyfikacji danych)

Adres lub adresy IP i znaczniki czasu (w tym data i strefa czasowa): .....

Numer telefonu: .....

Adres lub adresy e-mail: .....

Numer lub numery IMEI: .....

Adres lub adresy MAC: .....

Użytkownik lub użytkownicy lub inny unikalny identyfikator lub identyfikatory, takie jak imię i nazwisko lub nazwa użytkownika, login lub nazwa konta: .....

Nazwa lub nazwy odnośnej usługi (odnośnych usług): .....

Inne: .....

W stosownych przypadkach, przedział czasowy danych objętych nakazem wydania:

.....

Dodatkowe informacje (jeśli są konieczne): .....

SEKCJA F: Dowody elektroniczne, które należy przedstawić

Niniejszy EPOC dotyczy (proszę zaznaczyć właściwe pole lub pola):

a)  danych abonenta:

imienia i nazwiska lub nazwy, daty urodzenia, adresu pocztowego lub geograficznego, informacji kontaktowych (adres e-mail, numer telefonu) i innych odpowiednich informacji dotyczących tożsamości użytkownika/abonenta;

daty i czasu pierwotnej rejestracji, rodzaju rejestracji, kopii umowy, środków pozwalających zweryfikować tożsamość w momencie rejestracji, kopii dokumentów dostarczonych przez abonenta;

rodzaju usługi i czasu jej trwania, w tym identyfikatora lub identyfikatorów użytych przez abonenta lub dostarczonych mu w momencie pierwotnej rejestracji lub aktywacji (np. numer telefonu, numer karty SIM, adres MAC) i powiązanego urządzenia lub urządzeń;

informacji profilowych (imię i nazwisko użytkownika, nazwa użytkownika, zdjęcie profilowe);

danych dotyczących potwierdzenia użytkownika usługi, takich jak alternatywny adres e-mail podawany przez użytkownika/abonenta;

informacji dotyczących karty debetowej lub kredytowej (podawanych przez użytkownika do celów naliczania opłat), w tym informacji dotyczących innych sposobów płatności;

kodów PUK;

innych: .....

- b)  danych, których zażądano wyłącznie w celu identyfikacji użytkownika zdefiniowanych w art. 3 pkt 10 rozporządzenia (UE) 2023/1543:
- danych dotyczących połączeń, takich jak adresy IP/dzienniki/numery dostępowe, wraz z innymi identyfikatorami technicznymi, takimi jak porty źródłowe, znaczniki czasu lub ich odpowiedniki, identyfikator użytkownika i interfejs używany w kontekście korzystania z usługi (proszę określić, jeśli jest to konieczne): .....
  - przedziału czasowego danych objętych nakazem wydania (jeżeli jest inny niż w sekcji E): .....
  - innych: .....
- c)  danych o ruchu:
- (i) w przypadku telefonii (komórkowej):
    - identyfikatorów wychodzących (A) i przychodzących (B) (numer telefonu, numer IMSI, numer IMEI);
    - czasu nawiązania i trwania połączenia lub połączeń;
    - próby lub prób połączenia;
    - identyfikatora stacji bazowej, w tym informacji geograficznych (współrzędne X/Y), w momencie rozpoczęcia i zakończenia połączenia;
    - wykorzystywanej usługi przenoszenia/teleusługi (np. UMTS, GPRS);
    - innych: .....
  - (ii) w przypadku internetu:
    - informacji dotyczących routingu (źródłowy adres IP, docelowy adres lub adresy IP, numer lub numery portów, przeglądarka internetowa, informacje z nagłówka wiadomości e-mail, identyfikator wiadomości);
    - identyfikatora stacji bazowej, w tym informacji geograficznych (współrzędne X/Y), w momencie rozpoczęcia i zakończenia połączenia lub połączeń;
    - wolumenu danych;
    - daty i czasu połączenia lub połączeń;
    - czasu trwania połączenia lub sesji dostępu;
    - innych: .....
  - (iii) w przypadku usług hostingowych:
    - plików dziennika;
    - plików typu ticket;
    - innych: .....
  - (iv) pozostałych:
    - historii zakupów;



historii naliczania opłat na koncie przedpłaconym;

innych: .....

d)  danych dotyczących treści:

zrzutu (sieciowej) skrzynki pocztowej;

zrzutu pamięci online (dane wygenerowane przez użytkownika);

zrzutu strony;

dziennika wiadomości/kopii zapasowej;

zrzutu poczty głosowej;

treści serwera;

kopii zapasowej urządzenia;

spisu kontaktów;

innych: .....

Dodatkowe informacje, jeśli są konieczne do (dalszego) określenia lub ograniczenia zakresu danych objętych nakazem: .....

#### SEKCJA G: Informacje o okolicznościach wydania nakazu

a) Niniejszy EPOC dotyczy (proszę zaznaczyć właściwe pole lub pola):

postępowania karnego w sprawie przestępstwa lub przestępstw;

wykonania w ramach postępowania karnego wykonawczego wyroku skazującego na karę pozbawienia wolności lub orzeczenia o zastosowaniu środka zabezpieczającego polegającego na pozbawieniu wolności w wymiarze co najmniej czterech miesięcy, niewydanego zaocznie, w przypadkach gdy skazany ukrywa się przed wymiarem sprawiedliwości.

b) Charakter i kwalifikacja prawna przestępstwa lub przestępstw, w związku z którymi wydano EPOC, oraz odnośny przepis ustawy <sup>(4)</sup>:

.....

c) Niniejszy EPOC wydaje się w odniesieniu do danych o ruchu, których nie zażądano wyłącznie w celu identyfikacji użytkownika, lub w odniesieniu do danych dotyczących treści i dotyczy on (proszę zaznaczyć odpowiednie pole lub pola, w stosownych przypadkach):

przestępstwa lub przestępstw zagrożonych w państwie wydającym karę pozbawienia wolności o górnej granicy ustawowego zagrożenia w wysokości co najmniej trzech lat;

<sup>(4)</sup> W przypadku wykonania wyroku skazującego na karę pozbawienia wolności lub orzeczenia o zastosowaniu środka zabezpieczającego w odniesieniu do danych o ruchu, których nie zażądano wyłącznie w celu identyfikacji użytkownika, lub w odniesieniu do danych dotyczących treści, proszę wskazać w lit. b) i c) przestępstwo, w związku z którym wydano wyrok.

- co najmniej jednego z następujących przestępstw, o ile popełniono je w całości lub częściowo z wykorzystaniem systemu informatycznego:
- przestępstwa lub przestępstw określonych w art. 3–8 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/713 <sup>(5)</sup>;
  - przestępstwa lub przestępstw określonych w art. 3–7 dyrektywy Parlamentu Europejskiego i Rady 2011/93/UE <sup>(6)</sup>;
  - przestępstwa lub przestępstw określonych w art. 3–8 dyrektywy Parlamentu Europejskiego i Rady 2013/40/UE <sup>(7)</sup>;
  - przestępstw określonych w art. 3–12 i w art. 14 dyrektywy Parlamentu Europejskiego i Rady (UE) 2017/541 <sup>(8)</sup>.

d) Administrator/podmiot przetwarzający:

Europejskie nakazy wydania dowodów należy kierować do usługodawców działających w charakterze administratora. W drodze wyjątku europejski nakaz wydania dowodów można skierować bezpośrednio do usługodawcy przetwarzającego dane w imieniu administratora.

Proszę zaznaczyć w stosownym przypadku:

- Niniejszy EPOC jest skierowany do usługodawcy działającego w charakterze administratora.
- Niniejszy EPOC jest skierowany do usługodawcy, który przetwarza dane w imieniu administratora lub który prawdopodobnie je przetwarza, w przypadku gdy nie można zidentyfikować administratora, ponieważ:
  - nie można zidentyfikować administratora pomimo racjonalnych wysiłków organu wydającego;
  - zwrócenie się do administratora mogłoby zaszkodzić postępowaniu przygotowawczemu.

Jeżeli niniejszy EPOC jest skierowany do usługodawcy, który przetwarza dane w imieniu administratora:

- podmiot przetwarzający informuje administratora o wydaniu danych;
- podmiot przetwarzający nie informuje administratora o wydaniu danych do czasu podjęcia dalszej decyzji, ponieważ mogłoby to zaszkodzić postępowaniu przygotowawczemu. Proszę przedstawić zwięzłe uzasadnienie <sup>(9)</sup>: .....

e) wszelkie inne odpowiednie informacje: .....

#### SEKCJA H: Informacje dla użytkownika

Adresat w każdym przypadku powstrzymuje się od informowania osoby, której dane są objęte nakazem. Organ wydający ma obowiązek poinformować daną osobę, bez zbędnej zwłoki, o wydaniu danych.

<sup>(5)</sup> Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/713 z dnia 17 kwietnia 2019 r. w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi, zastępująca decyzję ramową Rady 2001/413/WSiSW (Dz.U. L 123 z 10.5.2019, s. 18).

<sup>(6)</sup> 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).

<sup>(7)</sup> 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).

<sup>(8)</sup> 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).

<sup>(9)</sup> Organ wydający musi wskazać w aktach sprawy przyczynę opóźnienia, a do EPOC należy dołączyć jedynie zwięzłe uzasadnienie;

Uwaga (proszę zaznaczyć właściwe pole):

- organ wydający opóźni poinformowanie osoby, której dane są objęte nakazem, o ile spełniony jest co najmniej jeden z następujących warunków:
- jest to niezbędne, aby zapobiec utrudnianiu urzędowych lub sądowych postępowań wyjaśniających, postępowań przygotowawczych lub innych postępowań;
  - jest to niezbędne, aby zapobiec negatywnemu wpływowi na zapobieganie przestępstwom, ich wykrywanie, prowadzenie postępowań przygotowawczych w ich sprawie, ich ściganie lub wykonywanie sankcji karnych;
  - jest to niezbędne do ochrony bezpieczeństwa publicznego;
  - jest to niezbędne do ochrony bezpieczeństwa narodowego;
  - jest to niezbędne do ochrony praw i wolności innych osób.

SEKCJA I: Dane organu wydającego

Rodzaj organu wydającego (proszę zaznaczyć właściwe pole lub pola):

- sędzia, sąd lub sędzia śledczy;
- prokurator;
- inny właściwy organ określony przez prawo państwa wydającego.

Jeśli konieczne jest zatwierdzenie nakazu, proszę uzupełnić także sekcję J.

Uwaga (w stosownych przypadkach proszę zaznaczyć):

- Niniejszy EPOC został wydany w odniesieniu do danych abonenta lub danych, których zażądano wyłącznie w celu identyfikacji użytkownika, w należycie ustalonej sytuacji wyjątkowej bez wcześniejszego zatwierdzenia lub ponieważ uzyskanie zatwierdzenia na czas było niemożliwe. Organ wydający potwierdza możliwość wydania w podobnej sytuacji krajowej nakazu bez zatwierdzenia oraz zamiar zwrócenia się bez zbędnej zwłoki o następcze zatwierdzenie w terminie nieprzekraczającym 48 godzin (uwaga: adresat nie zostanie o tym poinformowany).

Dane organu wydającego lub jego przedstawiciela, potwierdzających prawdziwość i poprawność informacji zawartych w niniejszym EPOC:

Nazwa organu: .....

Imię i nazwisko jego przedstawiciela: .....

Zajmowane stanowisko (tytuł/stopień): .....

Numer sprawy: .....

Adres: .....

Numer telefonu: (numer kierunkowy państwa) (numer kierunkowy regionu/miejscowości) .....

Numer faksu: (numer kierunkowy państwa) (numer kierunkowy regionu/miejscowości) .....

Adres e-mail: .....

Używany język lub języki: .....

Organ/punkt kontaktowy (np. organ centralny), do którego można się zwrócić w razie pytań związanych z wykonaniem niniejszego EPOC (jeśli jest inny niż powyżej):

Nazwa organu/imię i nazwisko: .....

Adres: .....

Numer telefonu: (numer kierunkowy państwa) (numer kierunkowy regionu/miejscowości) .....

Numer faksu: (numer kierunkowy państwa) (numer kierunkowy regionu/miejscowości) .....

Adres e-mail: .....

Podpis organu wydającego lub jego przedstawiciela, potwierdzających prawdziwość i poprawność informacji zawartych w niniejszym EPOC:

Data: .....

Podpis <sup>(10)</sup>: .....

SEKCJA J: Dane organu zatwierdzającego (proszę uzupełnić w stosownym przypadku)

Rodzaj organu zatwierdzającego

sędzia, sąd lub sędzia śledczy;

prokurator.

Dane organu zatwierdzającego lub jego przedstawiciela, potwierdzających prawdziwość i poprawność informacji zawartych w niniejszym EPOC:

Nazwa organu: .....

Imię i nazwisko jego przedstawiciela: .....

Zajmowane stanowisko (tytuł/stopień): .....

Numer sprawy: .....

Adres: .....

Numer telefonu: (numer kierunkowy państwa) (numer kierunkowy regionu/miejscowości) .....

Numer faksu: (numer kierunkowy państwa) (numer kierunkowy regionu/miejscowości) .....

Adres e-mail: .....

Używany język lub języki: .....

<sup>(10)</sup> Jeżeli zdecentralizowany system teleinformatyczny nie jest stosowany, proszę również dodać pieczęć urzędową, pieczęć elektroniczną lub inne równoważne uwierzytelnienie.

Data: .....

Podpis <sup>(1)</sup>: .....

SEKCJA K: Powiadomienie i dane powiadamianego organu przymuszającego do wykonania nakazu (w stosownym przypadku)

o niniejszym EPOC powiadamia się następujący organ przymuszający do wykonania nakazu:

.....

Proszę podać dane kontaktowe powiadamianego organu przymuszającego do wykonania nakazu (jeżeli są dostępne):

Nazwa organu przymuszającego do wykonania nakazu: .....

Adres: .....

Numer telefonu: (numer kierunkowy państwa) (numer kierunkowy regionu/miejscowości) .....

Numer faksu: (numer kierunkowy państwa) (numer kierunkowy regionu/miejscowości) .....

Adres e-mail: .....

SEKCJA L: Przekazanie danych

a) Organ, któremu należy przekazać dane

organ wydający

organ zatwierdzający

inny właściwy organ (np. organ centralny)

Nazwa i dane kontaktowe: .....

b) Preferowany format, w którym dane mają być przekazane, lub środki, za pomocą których dane mają być przekazane (w stosownych przypadkach): .....

SEKCJA M: Dalsze informacje, które należy zamieścić (ale nie można przysyłać ich adresatowi – należy je przekazać organowi przymuszającemu do wykonania nakazu, w przypadku gdy jest to wymagane)

Podstawy uznania, że europejski nakaz zabezpieczenia dowodów spełnia warunki konieczności i proporcjonalności:

.....

Zwięzły opis sprawy:

.....

<sup>(1)</sup> Jeżeli zdecentralizowany system teleinformatyczny nie jest stosowany, proszę również dodać pieczęć urzędową, pieczęć elektroniczną lub inne równoważne uwierzytelnienie.

Czy czyn, w związku z którym zostaje wydany europejski nakaz wydania dowodów, podlega w państwie wydającym karze pozbawienia wolności lub środkowi zabezpieczającemu polegającemu na pozbawieniu wolności o górnej granicy ustawowego zagrożenia w wysokości co najmniej trzech lat i figuruje w poniższym wykazie przestępstw (proszę zaznaczyć właściwe pole lub pola)?

- udział w organizacji przestępczej;
- terroryzm;
- handel ludźmi;
- wykorzystywanie seksualne dzieci i pornografia dziecięca;
- nielegalny handel środkami odurzającymi i substancjami psychotropowymi;
- nielegalny handel bronią, amunicją i materiałami wybuchowymi;
- korupcja;
- nadużycia finansowe, w tym nadużycia i inne przestępstwa naruszające interesy finansowe Unii zdefiniowane w dyrektywie Parlamentu Europejskiego i Rady (UE) 2017/1371 <sup>(12)</sup>;
- pranie korzyści pochodzących z przestępstwa;
- fałszowanie walut, w tym euro;
- przestępstwo komputerowe;
- przestępstwo przeciwko środowisku, w tym nielegalny handel zagrożonymi gatunkami zwierząt oraz zagrożonymi gatunkami i odmianami roślin;
- ułatwianie bezprawnego wjazdu i pobytu;
- zabójstwo lub spowodowanie ciężkiego uszczerbku na zdrowiu;
- nielegalny handel organami i tkankami ludzkimi;
- uprowadzenie, bezprawne przetrzymywanie lub wzięcie zakładników;
- rasizm i ksenofobia;
- rozbój w formie zorganizowanej lub przy użyciu broni;
- nielegalny handel dobrami kultury, w tym antykami i dziełami sztuki;
- oszustwo;
- wymuszenie rozbójnicze;
- podrabianie produktów i piractwo;
- fałszowanie dokumentów urzędowych i obrót takimi dokumentami;
- fałszowanie pieniędzy i środków płatniczych;
- nielegalny handel substancjami hormonalnymi i innymi środkami pobudzającymi wzrost;

<sup>(12)</sup> Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/1371 z dnia 5 lipca 2017 r. w sprawie zwalczania za pośrednictwem prawa karnego nadużyć na szkodę interesów finansowych Unii (Dz.U. L 198 z 28.7.2017, s. 29).

- nielegalny handel materiałami jądrowymi lub radioaktywnymi;
- handel skradzionymi pojazdami;
- zgwałcenie;
- podpalenie;
- przestępstwa podlegające jurysdykcji Międzynarodowego Trybunału Karnego;
- bezprawne zawładnięcie statkiem powietrznym lub statkiem;
- sabotaż.

W stosownym przypadku proszę dodać wszelkie dodatkowe informacje, których organ przymuszający do wykonania nakazu może potrzebować, aby ocenić możliwość podniesienia podstaw odmowy:

.....

## ZAŁĄCZNIK II

ZAŚWIADCZENIE EUROPEJSKIEGO NAKAZU ZABEZPIECZENIA DOWODÓW (EPOC-PR) DOTYCZĄCEGO  
ZABEZPIECZENIA DOWODÓW ELEKTRONICZNYCH

Zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2023/1543 <sup>(1)</sup>, po otrzymaniu niniejszego zaświadczenia europejskiego nakazu zabezpieczenia dowodów (EPOC-PR), adresat ma obowiązek zabezpieczyć bez zbędnej zwłoki dane, których dotyczy ten EPOC-PR. Zabezpieczenie ustaje po upływie 60 dni, chyba że organ wydający przedłuży ten okres o dodatkowe 30 dni lub potwierdzi, że wydano następnie wniosek o wydanie dowodów. Jeżeli organ wydający potwierdzi w tym terminie, że wydano w następnie wniosek o wydanie dowodów, adresat musi zabezpieczyć dane na tak długo, jak będzie to konieczne do ich wydania po otrzymaniu tego następczego wniosku o wydanie dowodów.

Adresat ma obowiązek podjąć środki konieczne do zapewnienia poufności, tajności i integralności EPOC-PR oraz zabezpieczonych danych.

SEKCJA A: Organ wydający/zatwierdzający:

Państwo wydające:.....

Organ wydający:.....

Organ zatwierdzający (w stosownym przypadku):.....

Uwaga: dane organu wydającego i zatwierdzającego należy podać na końcu (sekcje F i G)

Numer sprawy nadany przez organ wydający:.....

Numer sprawy nadany przez organ zatwierdzający:.....

SEKCJA B: Adresat

Adresat:.....

Wyznaczony zakład

Przedstawiciel prawny

Niniejszy nakaz wydaje się określone mu adresatowi w sytuacji wyjątkowej, ponieważ wyznaczony zakład lub przedstawiciel prawny usługodawcy nie odpowiedział na EPOC-PR w przewidzianych terminach lub nie został wskazany lub ustanowiony w terminach określonych w dyrektywie Parlamentu Europejskiego i Rady (UE) 2023/1544 <sup>(2)</sup>.

<sup>(1)</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1543 z dnia 12 lipca 2023 r. w sprawie europejskich nakazów wydania i europejskich nakazów zabezpieczenia dowodów elektronicznych w postępowaniu karnym oraz w postępowaniu karnym wykonawczym w związku z wykonaniem kar pozbawienia wolności (Dz.U. L 191 z 28.7.2023, s. 118).

<sup>(2)</sup> Dyrektywa Parlamentu Europejskiego i Rady (UE) 2023/1544 z dnia 12 lipca 2023 r. w sprawie zharmonizowanych przepisów dotyczących wskazywania wyznaczonych zakładów i ustanawiania przedstawicieli prawnych w celu gromadzenia dowodów elektronicznych w postępowaniach karnych (Dz.U. L 191 z 28.7.2023, s. 181)



Adres:.....

Numer telefonu/faksu/adres e-mail (jeśli są znane):.....

Osoba kontaktowa (jeśli jest znana):.....

Numer sprawy nadany przez adresata (jeśli jest znany):.....

Odnosny usługodawca (jeśli inny niż adresat):.....

Wszelkie inne odpowiednie informacje: .....

SEKCJA C: Informacje pomocne do identyfikacji danych objętych nakazem zabezpieczenia (proszę uzupełnić, podając dostępne informacje w zakresie niezbędnym do identyfikacji danych)

- Adres lub adresy IP i znaczniki czasu (w tym data i strefa czasowa):.....
- Numer telefonu:.....
- Adres lub adresy e-mail:.....
- Numer lub numery IMEI:.....
- Adres lub adresy MAC:.....
- Użytkownik lub użytkownicy usługi lub inny unikalny identyfikator lub identyfikatory, takie jak imię i nazwisko lub użytkownika, login lub nazwa konta.....
- Nazwa lub nazwy odnośnej usługi lub usług:.....
- Inne: .....
- W stosownym przypadku przedział czasowy danych objętych nakazem zabezpieczenia: .....
- Dodatkowe informacje (jeśli są konieczne): .....

SEKCJA D: Dowody elektroniczne, które należy zabezpieczyć

Niniejszy EPOC-PR dotyczy (proszę zaznaczyć właściwe pole lub pola):

- a)  danych abonenta:
- imienia i nazwiska lub nazwy, daty urodzenia, adresu pocztowego lub geograficznego, informacji kontaktowych (adres e-mail, numer telefonu) i innych odpowiednich informacji dotyczących tożsamości użytkownika/abonenta;
- daty i czasu pierwotnej rejestracji, rodzaju rejestracji, kopii umowy, środków pozwalających zweryfikować tożsamość w momencie rejestracji, kopii dokumentów dostarczonych przez abonenta;

- rodzaju usługi i czasu jej trwania, w tym identyfikatora lub identyfikatorów użytych przez abonenta lub dostarczonych mu w momencie pierwotnej rejestracji lub aktywacji (np. numer telefonu, numer karty SIM, adres MAC) i powiązanego urządzenia lub urządzeń;
  - informacji profilowych (imię i nazwisko użytkownika, nazwa użytkownika, zdjęcie profilowe);
  - danych dotyczących potwierdzenia użytkownika usługi, takich jak alternatywny adres e-mail podawany przez użytkownika/abonenta;
  - informacji dotyczących karty debetowej lub kredytowej (podawanych przez użytkownika do celów naliczania opłat), w tym informacji dotyczących innych sposobów płatności;
  - kodów PUK;
  - innych: ..... ;
- b)  danych, których zażądano wyłącznie w celu identyfikacji użytkownika zdefiniowanych w art. 3 pkt 10 rozporządzenia (UE) 2023/1543:
- danych dotyczących połączeń, takich jak adresy IP/dzienniki/numery dostępowe, wraz z innymi identyfikatorami, takimi jak porty źródłowe, znaczniki czasu lub ich odpowiedniki, identyfikator użytkownika i interfejs używany w kontekście korzystania z usługi, które są bezwzględnie konieczne do celów identyfikacji; proszę określić, jeśli to konieczne: ..... ;
  - przedziału czasowego danych objętych nakazem zabezpieczenia (jeżeli jest inny niż w sekcji C):..... ;
  - innych: ..... ;
- c)  danych o ruchu:
- (i) w przypadku telefonii (komórkowej):
- identyfikatorów wychodzących (A) i przychodzących (B) (numer telefonu, numer IMSI, numer IMEI);
  - czasu nawiązania i trwania połączenia lub połączeń;
  - próby lub prób połączenia;
  - identyfikatora stacji bazowej, w tym informacji geograficznych (współrzędne X/Y), w momencie rozpoczęcia i zakończenia połączenia;
  - wykorzystywanej usługi przesyłania/teleusługi (np. UMTS, GPRS);
  - innych: ..... ;
- (ii) w przypadku internetu:
- informacji dotyczących routingu (źródłowy adres IP, docelowy adres lub adresy IP, numer lub numery portów, przeglądarka internetowa, informacje z nagłówka wiadomości e-mail, identyfikator wiadomości);
  - identyfikatora stacji bazowej, w tym informacji geograficznych (współrzędne X/Y), w momencie rozpoczęcia i zakończenia połączenia lub połączeń;

- wolumenu danych;
- daty i czasu połączenia lub połączeń;
- czasu trwania połączenia lub sesji dostępu;
- innych: ..... ;

(iii) w przypadku usług hostingowych:

- plików dziennika;
- plików typu ticket;
- innych: ..... ;

(iv) pozostałych:

- historii zakupów;
- historii naliczania opłat na koncie przedpłaconym;
- innych: ..... ;

d)  danych dotyczących treści:

- zrzutu (sieciowej) skrzynki pocztowej;
- zrzutu pamięci online (dane wygenerowane przez użytkownika);
- zrzutu strony;
- dziennika wiadomości/kopii zapasowej;
- zrzutu poczty głosowej;
- treści serwera;
- kopii zapasowej urzędnika;
- spisu kontaktów;
- innych: ..... ;

Dodatkowe informacje, jeśli są konieczne do (dalszego) określenia lub ograniczenia zakresu danych objętych nakazem: .....

## SEKCJA E: Informacje o okolicznościach wydania nakazu

a) Niniejszy EPOC-PR dotyczy (proszę zaznaczyć właściwe pole lub pola):

- postępowania karnego w sprawie przestępstwa;
- wykonania w ramach postępowania karnego wykonawczego wyroku skazującego na karę pozbawienia wolności lub orzeczenia o zastosowaniu środka zabezpieczającego polegającego na pozbawieniu wolności w wymiarze co najmniej czterech miesięcy, niewydanego zaocznie, w przypadkach gdy skazany ukrywa się przed wymiarem sprawiedliwości.

b) Charakter i kwalifikacja prawna przestępstwa lub przestępstw, w związku z którymi wydano EPOC-PR, oraz odnośny przepis ustawy <sup>(3)</sup>: .....

## SEKCJA F: Dane organu wydającego

Rodzaj organu wydającego (proszę zaznaczyć właściwe pole lub pola):

- sędzia, sąd lub sędzia śledczy;
- prokurator;
- inny właściwy organ określony przez prawo państwa wydającego.

Jeśli konieczne jest zatwierdzenie nakazu, proszę uzupełnić także sekcję G.

Uwaga (w stosownych przypadkach proszę zaznaczyć):

- Niniejszy EPOC-PR został wydany w odniesieniu do danych abonenta lub danych, których zażądano wyłącznie w celu identyfikacji użytkownika, w należycie ustalonej sytuacji wyjątkowej bez wcześniejszego zatwierdzenia lub ponieważ uzyskanie zatwierdzenia na czas było niemożliwe. Organ wydający potwierdza możliwość wydania w podobnej sytuacji krajowej nakazu bez zatwierdzenia oraz zamiar zwrócenia się bez zbędnej zwłoki o następcze zatwierdzenie w terminie nieprzekraczającym 48 godzin (uwaga: adresat nie zostanie o tym poinformowany).

Ta sytuacja wyjątkowa odnosi się do bezpośredniego zagrożenia dla życia, integralności cielesnej lub bezpieczeństwa osoby lub do bezpośredniego zagrożenia dla infrastruktury krytycznej zdefiniowanej w art. 2 lit. a) dyrektywy Rady 2008/114/WE <sup>(4)</sup>, w przypadku gdy zakłócenie lub zniszczenie takiej infrastruktury krytycznej spowodowałoby bezpośrednie zagrożenie życia, integralności cielesnej lub bezpieczeństwa osoby, w tym przez poważne zakłócenie podstawowych dostaw dla ludności lub wykonywania podstawowych funkcji państwa.

Dane organu wydającego lub jego przedstawiciela, potwierdzających prawdziwość i poprawność informacji zawartych w niniejszym EPOC-PR:

Nazwa organu:.....

Imię i nazwisko jego przedstawiciela:.....

Zajmowane stanowisko (tytuł/stopień):.....

<sup>(3)</sup> W przypadku wykonania wyroku skazującego na karę pozbawienia wolności lub orzeczenia o zastosowaniu środka zabezpieczającego polegającego na pozbawieniu wolności, proszę wskazać przestępstwo, w związku z którym wydano wyrok.

<sup>(4)</sup> Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej (Dz.U. L 345 z 23.12.2008, s. 75).

Numer sprawy: .....

Adres: .....

Numer telefonu: (numer kierunkowy państwa) (numer kierunkowy regionu/miejscowości) .....

Numer faksu: (numer kierunkowy państwa) (numer kierunkowy regionu/miejscowości).....

Adres e-mail: .....

Używany język lub języki: .....

Organ/punkt kontaktowy (np. organ centralny), do którego można się zwrócić w razie pytań związanych z wykonaniem niniejszego EPOC-PR (jeśli jest inny niż powyżej):

Nazwa organu/imię i nazwisko: .....

Adres: .....

Numer telefonu: (numer kierunkowy państwa) (numer kierunkowy regionu/miejscowości) .....

Numer faksu: (numer kierunkowy państwa) (numer kierunkowy regionu/miejscowości).....

Adres e-mail: .....

Podpis organu wydającego lub jego przedstawiciela, potwierdzających prawdziwość i poprawność informacji zawartych w niniejszym EPOC-PR:

Data: .....

Podpis <sup>(5)</sup>: .....

SEKCJA G: Dane organu zatwierdzającego (proszę uzupełnić w stosownym przypadku)

Rodzaj organu zatwierdzającego:

sędzia, sąd lub sędzia śledczy;

prokurator.

Dane organu zatwierdzającego lub jego przedstawiciela, potwierdzających prawdziwość i poprawność informacji zawartych w niniejszym EPOC-PR:

Nazwa organu:.....

Imię i nazwisko jego przedstawiciela: .....

Zajmowane stanowisko (tytuł/stopień):.....

<sup>(5)</sup> Jeżeli zdecentralizowany system teleinformatyczny nie jest stosowany, proszę również dodać pieczęć urzędową, pieczęć elektroniczną lub inne równoważne uwierzytelnienie.

Numer sprawy: .....
Adres: .....
Numer telefonu: (numer kierunkowy państwa) (numer kierunkowy regionu/miejscowości) .....
Numer faksu: (numer kierunkowy państwa) (numer kierunkowy regionu/miejscowości).....
Adres e-mail: .....
Używany język lub języki: .....
Data: .....
Podpis <sup>(6)</sup> : .....

<sup>(6)</sup> Jeżeli zdecentralizowany system teleinformatyczny nie jest stosowany, proszę również dodać pieczęć urzędową, pieczęć elektroniczną lub inne równoważne uwierzytelnienie.

## ZAŁĄCZNIK III

## INFORMACJE DOTYCZĄCE BRAKU MOŻLIWOŚCI WYKONANIA EPOC/EPOC-PR

Zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2023/1543<sup>(1)</sup>, jeżeli adresat nie może wywiązać się z obowiązku zabezpieczenia danych, których dotyczy EPOC-PR, lub z obowiązku wydania danych określonych w EPOC, nie jest w stanie dotrzymać określonego terminu lub nie przekazuje wyczerpujących danych, powinien on bez zbędnej zwłoki wypełnić niniejszy formularz i odesłać go organowi wydającemu, jak również – w przypadku gdy miało miejsce powiadomienie oraz w innych stosownych przypadkach – wymienionemu w EPOC organowi przymuszającemu do wykonania nakazu.

W miarę możliwości adresat zabezpiecza dane objęte nakazem nawet wówczas, gdy do dokładnej identyfikacji danych konieczne są dodatkowe informacje, chyba że informacje zawarte w EPOC/EPOC-PR są do tego niewystarczające. Jeśli potrzebne są wyjaśnienia ze strony organu wydającego, adresat zwraca się o nie, bez zbędnej zwłoki, korzystając z niniejszego formularza.

## SEKCJA A: Zaświadczenie, którego dotyczą informacje

Poniższe informacje dotyczą:

- zaświadczenia europejskiego nakazu wydania dowodów (EPOC);
- zaświadczenia europejskiego nakazu zabezpieczenia dowodów (EPOC-PR).

## SEKCJA B: Odnośny organ lub odnośne organy

Organ wydający:.....

Numer sprawy nadany przez organ wydający:.....

W stosownym przypadku, organ zatwierdzający: .....

W stosownym przypadku, numer sprawy nadany przez organ zatwierdzający: .....

Data wydania EPOC/EPOC-PR: .....

Data otrzymania EPOC/EPOC-PR: .....

W stosownym przypadku, organ przymuszający do wykonania nakazu: .....

Numer sprawy nadany przez organ przymuszający do wykonania nakazu (jeżeli numer jest dostępny):.....

## SEKCJA C: Adresat EPOC/EPOC-PR

Adresat EPOC/EPOC-PR: .....

Numer sprawy nadany przez adresata: .....

<sup>(1)</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1543 z dnia 12 lipca 2023 r. w sprawie europejskich nakazów wydania i europejskich nakazów zabezpieczenia dowodów elektronicznych w postępowaniu karnym oraz w postępowaniu karnym wykonawczym w związku z wykonaniem kar pozbawienia wolności (Dz.U. L 191 z 28.7.2023, s. 118).

SEKCJA D: Podstawy odmowy wykonania

a) EPOC/EPOC-PR nie można wykonać lub nie można go wykonać w określonym terminie z następującego powodu lub powodów:

- jest niekompletny;
- zawiera oczywiste błędy;
- nie zawiera wystarczających informacji;
- nie dotyczy danych przechowywanych przez usługodawcę lub w jego imieniu w momencie otrzymania EPOC/EPOC-PR;
- w momencie otrzymania EPOC/EPOC-PR wystąpiły inne powody faktycznej niemożliwości wykonania wynikające z okoliczności, których nie można przypisać adresatowi ani usługodawcy;
- europejski nakaz wydania dowodów/europejski nakaz zabezpieczenia dowodów nie został wydany lub zatwierdzony przez organ wydający na zasadach określonych w art. 4 rozporządzenia (UE) 2023/1543;
- europejski nakaz wydania dowodów służący uzyskaniu danych o ruchu innych niż dane, których zażądano wyłącznie w celu identyfikacji użytkownika zdefiniowanych w art. 3 pkt 10 rozporządzenia (UE) 2023/1543, lub uzyskaniu danych dotyczących treści, wydano w odniesieniu do przestępstwa, które nie jest objęte art. 5 ust. 4 rozporządzenia (UE) 2023/1543;
- usługa nie jest objęta rozporządzeniem (UE) 2023/1543;
- dane objęte nakazem są chronione immunitetami lub przywilejami przysługującymi na mocy prawa państwa wykonującego lub też dane objęte nakazem są objęte przepisami dotyczącymi ustalania lub ograniczania odpowiedzialności karnej związanymi z wolnością prasy lub wolnością wypowiedzi w innych mediach, uniemożliwiającymi wykonanie europejskiego nakazu wydania dowodów/europejskiego nakazu zabezpieczenia dowodów;
- wykonanie europejskiego nakazu wydania dowodów byłoby sprzeczne z mającym zastosowanie prawem państwa trzeciego. Proszę uzupełnić także sekcję E.

b) Proszę szerzej wyjaśnić powody odmowy wykonania, o których mowa w lit. a), oraz, w razie konieczności, wskazać i wyjaśnić wszelkie inne powody, których nie wymieniono w lit. a):

.....

SEKCJA E: Konflikt obowiązków wynikający z prawa państwa trzeciego

W przypadku konfliktu obowiązków wynikającego z prawa państwa trzeciego, proszę podać następujące informacje:

— tytuł aktu prawnego lub aktów prawnych państwa trzeciego:

.....

— mające zastosowanie przepisy ustawy i treść odnośnych przepisów:

.....

— charakter konfliktu obowiązków, w tym interes podlegający ochronie na podstawie prawa państwa trzeciego:

prawa podstawowe osób fizycznych (proszę określić):

.....

podstawowe interesy państwa trzeciego związane z bezpieczeństwem narodowym i obronnością (proszę określić):

.....



inne interesy (proszę określić):

- .....
- proszę wyjaśnić, dlaczego dany akt prawny ma zastosowanie w przedmiotowym przypadku:
- .....
- proszę wyjaśnić, dlaczego uważają Państwo, że w przedmiotowym przypadku zachodzi konflikt:
- .....
- proszę wyjaśnić powiązanie pomiędzy usługodawcą a przedmiotowym państwem trzecim:
- .....
- możliwe konsekwencje dla adresata związane z wykonaniem europejskiego nakazu wydania dowodów, w tym kary, które mogą zostać nałożone:
- .....
- Proszę dodać wszelkie odpowiednie informacje dodatkowe:.....

SEKCJA F: Wniosek o dodatkowe informacje/wyjaśnienie (proszę wypełnić w stosownym przypadku)

W celu wykonania EPOC/EPOC-PR potrzebne są dalsze informacje od organu wydającego:

.....

SEKCJA G: Zabezpieczenie danych

Dane objęte nakazem (proszę zaznaczyć właściwe pole i uzupełnić):

- są zabezpieczone do momentu wydania danych lub do momentu, w którym organ wydający lub, w stosownym przypadku, organ przymuszający do wykonania nakazu wskaże, że zabezpieczenie i wydanie danych nie są już konieczne, lub do momentu, w którym organ wydający przekaze konieczne informacje umożliwiające zawężenie zakresu danych, które mają zostać zabezpieczone/wydane;
- nie są zabezpieczone (powinno to mieć miejsce tylko w drodze wyjątku, np. gdy usługodawca nie posiada danych w momencie otrzymania wniosku lub nie jest w stanie w wystarczający sposób zidentyfikować danych objętych nakazem).

SEKCJA H: Dane kontaktowe wyznaczonego zakładu/przedstawiciela prawnego usługodawcy

Nazwa wyznaczonego zakładu/imię i nazwisko lub nazwa przedstawiciela prawnego usługodawcy:

.....

Imię i nazwisko osoby wyznaczonej do kontaktów:.....

Zajmowane stanowisko:.....

Adres:.....

Numer telefonu: (numer kierunkowy państwa) (numer kierunkowy regionu/miejscowości).....

Numer faksu: (numer kierunkowy państwa) (numer kierunkowy regionu/miejscowości).....

Adres e-mail:.....

Imię i nazwisko osoby upoważnionej:.....

Data:.....

Podpis (?):.....

(?) Jeżeli zdecentralizowany system teleinformatyczny nie jest stosowany, proszę również dodać pieczęć urzędową, pieczęć elektroniczną lub inne równoważne uwierzytelnienie.

## ZAŁĄCZNIK IV

## KATEGORIE PRZESTĘPSTW, O KTÓRYCH MOWA W ART. 12 UST. 1 LIT. D)

- 1) udział w organizacji przestępczej;
- 2) terroryzm;
- 3) handel ludźmi;
- 4) wykorzystywanie seksualne dzieci i pornografia dziecięca;
- 5) nielegalny handel środkami odurzającymi i substancjami psychotropowymi;
- 6) nielegalny handel bronią, amunicją i materiałami wybuchowymi;
- 7) korupcja;
- 8) nadużycia finansowe, w tym nadużycia i inne przestępstwa naruszające interesy finansowe Unii zdefiniowane w dyrektywie Parlamentu Europejskiego i Rady (UE) 2017/1371 <sup>(1)</sup>;
- 9) pranie korzyści pochodzących z przestępstwa;
- 10) fałszowanie walut, w tym euro;
- 11) przestępstwo komputerowe;
- 12) przestępstwo przeciwko środowisku, w tym nielegalny handel zagrożonymi gatunkami zwierząt oraz zagrożonymi gatunkami i odmianami roślin;
- 13) ułatwianie bezprawnego wjazdu i pobytu;
- 14) zabójstwo lub spowodowanie ciężkiego uszczerbku na zdrowiu;
- 15) nielegalny handel organami i tkankami ludzkimi;
- 16) uprowadzenie, bezprawne przetrzymywanie lub wzięcie zakładników;
- 17) rasizm i ksenofobia;
- 18) rozbój w formie zorganizowanej lub przy użyciu broni;
- 19) nielegalny handel dobrami kultury, w tym antykami i dziełami sztuki;
- 20) oszustwo;
- 21) wymuszenie rozbójnicze;
- 22) podrabianie produktów i piractwo;

<sup>(1)</sup> Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/1371 z dnia 5 lipca 2017 r. w sprawie zwalczania za pośrednictwem prawa karnego nadużyć na szkodę interesów finansowych Unii (Dz.U. L 198 z 28.7.2017, s. 29).

- 23) fałszowanie dokumentów urzędowych i handel nimi;
  - 24) fałszowanie pieniędzy i środków płatniczych;
  - 25) nielegalny handel substancjami hormonalnymi i innymi środkami pobudzającymi wzrost;
  - 26) nielegalny handel materiałami jądrowymi lub radioaktywnymi;
  - 27) handel skradzionymi pojazdami;
  - 28) zgwałcenie;
  - 29) podpalenie;
  - 30) przestępstwa podlegające jurysdykcji Międzynarodowego Trybunału Karnego;
  - 31) bezprawne zawładnięcie statkiem powietrznym lub statkiem;
  - 32) sabotaż.
-

## ZAŁĄCZNIK V

POTWIERDZENIE WYDANIA WNIOSKU O WYDANIE DOWODÓW W NASTĘPSTWIE EUROPEJSKIEGO NAKAZU  
ZABEZPIECZENIA

Zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2023/1543 <sup>(1)</sup>, po otrzymaniu zaświadczenia europejskiego nakazu zabezpieczenia dowodów (EPOC-PR), adresat ma obowiązek zabezpieczyć bez zbędnej zwłoki dane, których dotyczy ten EPOC-PR. Zabezpieczenie ustaje po upływie 60 dni, chyba że organ wydający przedłuży ten okres o dodatkowe 30 dni lub potwierdzi, że wydano następnie wniosek o wydanie dowodów, za pomocą formularza przewidzianego w niniejszym załączniku.

Po otrzymaniu tego potwierdzenia adresat musi zabezpieczyć dane na tak długo, jak to konieczne, do czasu otrzymania tego następczego wniosku o wydanie dowodów.

## SEKCJA A: Organ wydający EPOC-PR

Państwo wydające:.....

Organ wydający:.....

Jeżeli jest on inny niż punkt kontaktowy wskazany w EPOC-PR, organ/punkt kontaktowy (np. organ centralny), do którego można się zwrócić w razie pytań związanych z wykonaniem niniejszego EPOC-PR:

Nazwa i dane kontaktowe: .....

## SEKCJA B: Adresat EPOC-PR

Adresat:.....

Adres:.....

Numer telefonu/faksu/adres e-mail (jeśli są znane):.....

Osoba kontaktowa (jeśli jest znana):.....

Numer sprawy nadany przez adresata (jeśli jest znany):.....

Oдноśny usługodawca (jeśli inny niż adresat):.....

Wszelkie inne odpowiednie informacje: .....

<sup>(1)</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1543 z dnia 12 lipca 2023 r. w sprawie europejskich nakazów wydania i europejskich nakazów zabezpieczenia dowodów elektronicznych w postępowaniu karnym oraz w postępowaniu karnym wykonawczym w związku z wykonaniem kar pozbawienia wolności (Dz.U. L 191 z 28.7.2023, s. 118).

## SEKCJA C: Informacje o EPOC-PR:

Dane zabezpieczono zgodnie z EPOC-PR wydanym..... (proszę wskazać datę wydania wniosku) i przekazano... (proszę wskazać datę przekazania wniosku) pod numerem sprawy ..... (proszę wskazać numer sprawy).

- Organ wydający ... przedłużył okres zabezpieczenia danych o 30 dni w sprawie numer ... w dniu ... (proszę zaznaczyć właściwe pole i wskazać, w stosownym przypadku).

## SEKCJA D: Potwierdzenie

Niniejszym potwierdza się, że wystawiono wskazany poniżej wniosek o wydanie (proszę zaznaczyć właściwe pole i uzupełnić w razie potrzeby):

- zaświadczenie europejskiego nakazu wydania dowodów wydane przez..... (proszę wskazać organ) w dniu..... (proszę wskazać datę wydania wniosku) i przekazane w dniu..... (proszę wstawić datę przekazania wniosku) pod numerem sprawy..... (proszę wskazać numer sprawy) do..... (proszę wskazać usługodawcę/wyznaczony zakład/ przedstawiciela prawnego/właściwy organ, któremu przekazano wniosek, oraz numer sprawy nadany przez adresata, o ile numer ten jest dostępny);

- europejski nakazu dochodzeniowy wydany przez ..... (proszę wskazać organ) w dniu..... (proszę wskazać datę wydania wniosku) i przekazany w dniu..... (proszę wstawić datę przekazania wniosku) pod numerem sprawy ..... (proszę wskazać numer sprawy) do ..... (proszę wskazać państwo i właściwy organ, którym przekazano wniosek, oraz numer sprawy nadany przez organy współpracujące, o ile numer ten jest dostępny);

- wniosek o wzajemną pomoc prawną wydany przez ..... (proszę wskazać organ) w dniu..... (proszę wskazać datę wydania wniosku) i przekazany w dniu..... (proszę wstawić datę przekazania wniosku) pod numerem sprawy ..... (proszę wskazać numer sprawy) do..... (proszę wskazać państwo i właściwy organ, którym przekazano wniosek, oraz numer sprawy nadany przez organy współpracujące, o ile numer ten jest dostępny).

Podpis organu wydającego lub jego przedstawiciela:

Imię i nazwisko: .....

Data: .....

Podpis (?): .....

(<sup>2</sup>) Jeżeli zdecentralizowany system teleinformatyczny nie jest stosowany, proszę również dodać pieczęć urzędową, pieczęć elektroniczną lub inne równoważne uwierzytelnienie.

## ZAŁĄCZNIK VI

## PRZEDŁUŻENIE ZABEZPIECZENIA DOWODÓW ELEKTRONICZNYCH

Zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2023/1543 <sup>(1)</sup>, po otrzymaniu zaświadczenia europejskiego nakazu zabezpieczenia dowodów (EPOC-PR), adresat ma obowiązek zabezpieczyć bez zbędnej zwłoki dane, których dotyczy ten EPOC-PR. Zabezpieczenie ustaje po upływie 60 dni, chyba że organ wydający potwierdzi, że wydano następnie wniosek o wydanie dowodów. W terminie tych 60 dni organ wydający może przedłużyć okres zabezpieczenia o dodatkowe 30 dni, jeżeli jest to konieczne, aby umożliwić wydanie następnie wniosku o wydanie dowodów, przy użyciu formularza określonego w niniejszym załączniku.

## SEKCJA A: Organ wydający EPOC-PR

Państwo wydające: .....

Organ wydający: ... ..

Numer sprawy nadany przez organ wydający: ... ..

Jeżeli jest on inny niż punkt kontaktowy wskazany w EPOC-PR, organ/punkt kontaktowy (np. organ centralny), do którego można się zwrócić w razie pytań związanych z wykonaniem niniejszego EPOC-PR:

Nazwa i dane kontaktowe: ... ..

## SEKCJA B: Adresat EPOC-PR

Adresat: ... ..

Adres: .....

Numer telefonu/faksu/adres e-mail (jeśli są znane): ... ..

Osoba kontaktowa (jeśli jest znana): .....

Numer sprawy nadany przez adresata (jeśli jest znany): .....

Odnosny usługodawca (jeśli inny niż adresat): .....

Wszelkie inne odpowiednie informacje: .....

## SEKCJA C: Informacje o poprzednim EPOC-PR:

Dane zabezpieczono zgodnie z EPOC-PR wydanym ..... (proszę wskazać datę wydania wniosku) i przekazany w dniu ..... (proszę wskazać datę przekazania wniosku) pod numerem sprawy ..... (proszę wskazać numer sprawy) do .....

<sup>(1)</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1543 z dnia 12 lipca 2023 r. w sprawie europejskich nakazów wydania i europejskich nakazów zabezpieczenia dowodów elektronicznych w postępowaniu karnym oraz w postępowaniu karnym wykonawczym w związku z wykonaniem kar pozbawienia wolności (Dz.U. L 191 z 28.7.2023, s. 118).

SEKCJA D: Przedłużenie poprzedniego nakazu zabezpieczenia

Obowiązek zabezpieczenia danych na podstawie EPOC-PR, o którym mowa w sekcji C, zostaje niniejszym przedłużony o dodatkowe 30 dni.

Podpis organu wydającego lub jego przedstawiciela:

Imię i nazwisko: ... ..

Data: ... ..

Podpis <sup>(?)</sup>: ... ..

<sup>(?)</sup> Jeżeli zdecentralizowany system teleinformatyczny nie jest stosowany, proszę również dodać pieczęć urzędową, pieczęć elektroniczną lub inne równoważne uwierzytelnienie.