

Brusel 18. května 2018
(OR. en)

8110/18

Interinstitucionální spis:
2018/0108 (COD)

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

NÁVRH

Odesílatel:	Jordi AYET PUIGARNAU, ředitel, za generálního tajemníka Evropské komise
Datum přijetí:	18. května 2018
Příjemce:	Jeppe TRANHOLM-MIKKELSEN, generální tajemník Rady Evropské unie
Č. dok. Komise:	COM(2018) 225 final
Předmět:	Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech

Delegace naleznou v příloze dokument COM(2018) 225 final.

Příloha: COM(2018) 225 final



EVROPSKÁ
KOMISE

Ve Štrasburku dne 17.4.2018
COM(2018) 225 final

2018/0108 (COD)

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY

o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech

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

DŮVODOVÁ ZPRÁVA

1. SOUVISLOSTI NÁVRHU

• Odůvodnění a cíle návrhu

Používání sociálních médií, webového e-mailu, služeb pro rychlou výměnu zpráv a mobilních aplikací ke komunikaci, práci, společenskému styku a získávání informací je dnes v mnoha částech světa již samozřejmostí. Tyto služby propojují stovky milionů uživatelů. Významně zlepšují ekonomické a sociální podmínky uživatelů v Unii i za jejími hranicemi. Mohou však též být zneužity k páčání nebo umožňování trestných činů, včetně závažných trestných činů, jako jsou teroristické útoky. Pokud se tak stane, jsou tyto služby a aplikace často jediným místem, kde vyšetřovatelé mohou najít vodítka k určení toho, kdo trestný čin spáchal, a k získání důkazů, které lze použít u soudu.

Vzhledem k tomu, že internet je bez hranic, lze takové služby poskytovat z jakéhokoli místa ve světě a není k tomu nutně zapotřebí fyzická infrastruktura, přítomnost podniku nebo zaměstnanců v členských státech, kde jsou služby nabízeny, nebo na vnitřním trhu jako celku. Nevyžadují ani konkrétní místo k uchovávání údajů, které si poskytovatel služeb často vybírá na základě legitimních ohledů, jako je bezpečnost údajů, úspory z objemu a rychlost přístupu. Výsledkem je to, že orgány členských států ve stále větším počtu trestních případů zahrnujících všechny druhy trestné činnosti¹ vyžadují přístup k údajům, které by mohly posloužit jako důkazy a které jsou uloženy mimo území jejich země a/nebo které poskytovatelé služeb uchovávají v jiných členských státech či třetích zemích.

Pro situace, kde se buď důkazy, nebo poskytovatel služeb nacházejí někde jinde, byly před několika desetiletími vytvořeny mechanismy pro spolupráci mezi zeměmi². Navzdory pravidelným reformám jsou tyto mechanismy spolupráce vystaveny stále většímu tlaku z důvodu rostoucí potřeby včasného přeshraničního přístupu k elektronickým důkazům. V reakci na to se řada členských států a třetích zemí uchýlila k rozšíření svých vnitrostátních nástrojů. Výsledné roztržštění je příčinou právní nejistoty a rozporných povinností a vyvolává otázky ohledně ochrany základních práv a procesních záruk osob dotčených takovými žádostmi.

V roce 2016 vyzvala Rada k přijetí konkrétních opatření na základě společného přístupu EU ke zefektivnění vzájemné právní pomoci, ke zlepšení spolupráce mezi orgány členských států a poskytovateli služeb se sídlem v zemích mimo EU a k navržení řešení problému souvisejícího s určením a vymáháním příslušných právních předpisů³ v kyberprostoru⁴. Podobně pak také Evropský parlament vyzdvihl problémy, které současný roztržštěný právní rámec může způsobovat poskytovatelům služeb, kteří se snaží vyhovět žádostem donucovacích orgánů, a vyslovil se pro evropský právní rámec obsahující záruky práv a svobod pro všechny zúčastněné⁵.

¹ Viz oddíly 2.1.1 a 2.3 posouzení dopadů.

² V Unii to jsou mechanismy vzájemného uznávání, které se nyní opírají o směrnici o evropském vyšetřovacím příkazu; pro spolupráci s třetími zeměmi to jsou mechanismy vzájemné právní pomoci.

³ V tomto dokumentu odkazuje výraz „pravomoc vymáhat právo“ na kompetenci příslušných orgánů provádět vyšetřovací opatření.

⁴ [Závěry Rady o zlepšení trestního soudnictví v kyberprostoru, ST9579/16.](#)

⁵ [P8_TA\(2017\)0366.](#)

Tento návrh se zaměřuje na konkrétní problém, který je způsoben nestálou povahou elektronických důkazů a jejich mezinárodním rozměrem. Mechanismy spolupráce se pokouší přizpůsobit digitálnímu věku, přičemž soudnictví a donucovacím orgánům dává nástroje k přístupu ke způsobu, jakým zločinci dnes komunikují, a k boji proti moderním formám trestné činnosti. Takové nástroje musí přitom podléhat silným mechanismům ochrany základních práv. Cílem tohoto návrhu je zvýšit právní jistotu orgánů, poskytovatelů služeb a dotčených osob a zachovat vysoký standard žádostí donucovacích orgánů, čímž se zajistí ochrana základních práv, transparentnost a odpovědnost. Tento návrh též urychluje proces zajištění a získání elektronických důkazů, které mají uloženy a/nebo vlastní poskytovatelé služeb usazení v jiné jurisdikci. Tento nástroj bude existovat vedle současných nástrojů soudní spolupráce, které jsou nadále významné a které mohou příslušné orgány ve vhodných případech využít. Komise souběžně pracuje na posílení stávajících mechanismů soudní spolupráce prostřednictvím takových opatření, jako je vytvoření bezpečné platformy pro rychlou výměnu žádostí mezi soudními orgány v EU a investice ve výši 1 milionu EUR na školení odborníků z praxe ze všech členských států EU o problematice vzájemné právní pomoci a spolupráce, přičemž je pozornost věnována Spojeným státům americkým jako třetí zemi, kam z EU směřuje nejvíce žádostí⁶.

Pokud jde o doručování a výkon příkazů podle tohoto nástroje, měly by se orgány spoléhat na právní zástupce ustanovené poskytovateli služeb. Komise dnes předkládá návrh, který má zajistit účinné ustanovování takových právních zástupců. Poskytuje společné, celounijní řešení pro adresování příkazů poskytovatelům služeb prostřednictvím právního zástupce.

- **Soulad s existujícím právním rámcem EU v oblasti politiky a Budapešťskou úmluvou Rady Evropy**

Současný právní rámec EU tvoří unijní nástroje spolupráce v trestních věcech, např. směrnice 2014/41/EU o evropském vyšetřovacím příkazu v trestních věcech⁷ (dále jen „směrnice o evropském vyšetřovacím příkazu“), Úmluva o vzájemné pomoci ve věcech trestních mezi členskými státy Evropské unie⁸, rozhodnutí Rady 2002/187/SVV o zřízení Evropské jednotky pro soudní spolupráci (Eurojust)⁹, nařízení (EU) 2016/794 o Europolu¹⁰, rámcové rozhodnutí Rady 2002/465/SVV o společných vyšetřovacích týmech¹¹, jakož i dvoustranné smlouvy

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

⁷ [Směrnice Evropského parlamentu a Rady 2014/41/EU](#) ze dne 3. dubna 2014 o evropském vyšetřovacím příkazu v trestních věcech (Úř. věst. L 130, 1.5.2014, s. 1).

⁸ [Akt Rady ze dne 29. května 2000](#), kterým se v souladu s článkem 34 Smlouvy o Evropské unii vypracovává Úmluva o vzájemné pomoci ve věcech trestních mezi členskými státy Evropské unie.

⁹ [Rozhodnutí Rady 2002/187/SVV](#) ze dne 28. února 2002 o zřízení Evropské jednotky pro soudní spolupráci (Eurojust) za účelem posílení boje proti závažné trestné činnosti. V roce 2013 přijala Komise [návrh nařízení](#) o reformě Eurojustu (návrh nařízení Evropského parlamentu a Rady o Agentuře Evropské unie pro justiční spolupráci v trestních věcech (Eurojust), COM/2013/0535 final).

¹⁰ [Nařízení Evropského parlamentu a Rady \(EU\) č. 2016/794](#) ze dne 11. května 2016 o Agentuře Evropské unie pro spolupráci v oblasti prosazování práva (Europol) a o zrušení a nahrazení rozhodnutí 2009/371/SVV, 2009/934/SVV, 2009/935/SVV, 2009/936/SVV a 2009/968/SVV.

¹¹ [Rámcové rozhodnutí Rady 2002/465/SVV](#) ze dne 13. června 2002 o společných vyšetřovacích týmech.

mezi Uníí a zeměmi mimo EU, např. dohoda o vzájemné právní pomoci mezi EU a USA¹² a dohoda o vzájemné právní pomoci mezi EU a Japonskem¹³.

Zavedením evropských předávacích příkazů a evropských uchovávacích příkazů návrh usnadňuje zajištění a shromažďování elektronických důkazů pro trestní řízení uchovávaných nebo držaných poskytovateli služeb v jiné jurisdikci. Směrnice o evropském vyšetřovacím příkazu, která z velké části nahradila Úmluvu o vzájemné pomoci ve věcech trestních, se vztahuje na všechny vyšetřovací opatření¹⁴. Mezi ně patří i přístup k elektronickým důkazům, avšak uvedená směrnice neobsahuje žádná konkrétní ustanovení o tomto druhu důkazů¹⁵. Nový nástroj směrnici o evropském vyšetřovacím příkazu, pokud jde o získávání elektronických důkazů, nenahradí, ale poskytne orgánům další prostředek. Mohou nastat situace, například když je ve vykonávajícím členském státě nutné provést několik vyšetřovacích opatření, kdy veřejné orgány upřednostní evropský vyšetřovací příkaz. Vytvoření nového nástroje pro elektronické důkazy je lepší alternativou než změna směrnice o evropském vyšetřovacím příkazu, a to kvůli specifickým problémům spojeným se získáváním elektronických důkazů, které nemají dopad na ostatní vyšetřovací opatření, na něž se vztahuje směrnice o evropském vyšetřovacím příkazu.

Aby se usnadnil přeshraniční sběr elektronických důkazů, bude nový nástroj vycházet ze zásad vzájemného uznávání. Orgán v zemi, kde se nachází adresát příkazu, se nebude muset podílet na doručování a výkonu příkazu přímo, ledaže dojde k neplnění, kdy pak bude nutné vymáhání a zasáhne příslušný orgán v zemi, kde se nachází zástupce. Nástroj tudíž vyžaduje soubor spolehlivých záruk a ustanovení, jako je v každém případě potvrzení justičním orgánem. Například evropské předávací příkazy k předání údajů o transakcích nebo obsahu (na rozdíl od údajů o účastníkovi a přístupu) lze vydávat pouze v případě trestných činů postihnutelných ve vydávajícím státu trestem odnětím svobody s horní hranicí sazby v délce nejméně tři let nebo v případě konkrétních trestných činů závislých na kybernetické činnosti, umožněných kybernetickou činností nebo souvisejících s terorismem tak, jak je uvedeno v návrhu.

Osobní údaje, na něž se vztahuje tento návrh, jsou chráněny a mohou být zpracovávány pouze v souladu s obecným nařízením o ochraně osobních údajů (tzv. GDPR)¹⁶ a směrnicí o ochraně údajů pro policii a orgány činné v trestním řízení (dále jen „směrnice o ochraně údajů při vymáhání práva“)¹⁷. Obecné nařízení o ochraně osobních údajů vstoupí v platnost dne 25. května 2018, zatímco směrnice o ochraně údajů při vymáhání práva musí být členskými státy provedena ve vnitrostátním právu do 6. května 2018.

¹² [Rozhodnutí Rady 2009/820/SZBP](#) ze dne 23. října 2009 o uzavření Dohody o vydávání mezi Evropskou unií a Spojenými státy americkými a Dohody o vzájemné právní pomoci mezi Evropskou unií a Spojenými státy americkými jménem Evropské unie.

¹³ [Rozhodnutí Rady 2010/616/EU](#) ze dne 7. října 2010 o uzavření Dohody mezi Evropskou unií a Japonskem o vzájemné právní pomoci v trestních věcech.

¹⁴ Kromě společných vyšetřovacích týmů (viz článek 3 směrnice o evropském vyšetřovacím příkazu); směrnice o evropském vyšetřovacím příkazu se neúčastní všechny členské státy (Irsko, Dánsko).

¹⁵ Kromě odkazu na identifikaci osoby zaregistrované pod IP adresou uvedeného v čl. 10 odst. 2 písm. e), kdy nelze uplatnit oboustrannou trestnost jako důvod pro neuznání žádosti a odmítnutí jejího vyřízení.

¹⁶ [Nařízení Evropského parlamentu a Rady \(EU\) 2016/679](#) ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES.

¹⁷ [Směrnice Evropského parlamentu a Rady \(EU\) 2016/680](#) ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.

Budapešťská úmluva Rady Evropy o kyberkriminalitě (CETS č. 185), kterou ratifikovala většina členských států EU, zavádí mezinárodní mechanismy pro spolupráci proti kyberkriminalitě¹⁸. Úmluva se zabývá trestnými činy, které byly spáchány přes internet a jiné počítačové sítě. Požaduje též, aby smluvní strany stanovily pravomoci a postupy k získávání elektronických důkazů a poskytování vzájemné právní pomoci, a sice nejen v souvislosti s kyberkriminalitou. Úmluva zejména požaduje, aby smluvní strany zavedly předávací příkazy za účelem získání počítačových dat od poskytovatelů služeb na jejich území a údajů o účastníkovi od poskytovatelů služeb nabízejících služby na jejich území. Kromě toho stanoví úmluva uchovávací příkazy, pokud lze předpokládat, že počítačové údaje jsou zvláště náchylné ke ztrátě nebo pozměnění. Další otázky vyvolávají doručování a vynutitelnost vnitrostátních předávacích příkazů vůči poskytovatelům usazeným mimo území smluvní strany úmluvy. V tomto ohledu jsou v současnosti zvažována další opatření ke zlepšení přeshraničního přístupu k elektronickým důkazům¹⁹.

• **Shrnutí navrhovaného nařízení**

Navrhované nařízení zavádí závazné evropské předávací a uchovávací příkazy. Oba příkazy musí vydat nebo potvrdit justiční orgán členského státu. Příkaz lze vydat za účelem uchování nebo předání údajů, které jsou uloženy u poskytovatele služeb v jiné jurisdikci a které jsou potřebné jako důkazy v trestním vyšetřování nebo trestním řízení. Tyto příkazy lze vydat pouze za předpokladu, že ve vydávajícím státě je ve srovnatelné vnitrostátní situaci k dispozici obdobné opatření za stejný trestný čin. Oba příkazy mohou být doručeny poskytovatelům služeb elektronické komunikace, sociálním sítím, online tržištím, jiným poskytovatelům hostingových služeb a poskytovatelům internetové infrastruktury, jako jsou registry IP adres a názvů domén, nebo jejich právním zástupcům, existují-li. Evropský uchovávací příkaz, podobně jako evropský předávací příkaz, je adresován právnímu zástupci mimo jurisdikci vydávajícího členského státu za účelem uchování údajů s ohledem na následnou žádost o předání těchto údajů, například prostřednictvím kanálů vzájemné právní pomoci v případě třetích zemí nebo prostřednictvím evropského vyšetřovacího příkazu mezi zúčastněnými členskými státy. Na rozdíl od opatření dohledu nebo povinností uchovávat údaje stanovených zákonem, které toto nařízení nestanoví, je evropský uchovávací příkaz příkazem, který vydal nebo potvrdil justiční orgán v konkrétním trestním řízení po individuálním vyhodnocení přiměřenosti a nezbytnosti v každém jednotlivém případě. Podobně jako evropský předávací příkaz se odvolává na konkrétní známé nebo neznámé pachatele trestného činu, který již byl spáchán. Evropský uchovávací příkaz dovoluje pouze uchování údajů, které jsou v době obdržení příkazu již uloženy, a nikoli přístup k údajům v budoucnosti po obdržení evropského uchovávacího příkazu.

Oba příkazy lze použít pouze v trestním řízení, od úvodní přípravné vyšetřovací fáze až do uzavření řízení rozsudkem nebo jiným rozhodnutím. Příkazy k předání údajů o účastníkovi a přístupu lze vydat u jakéhokoli trestného činu, zatímco příkaz k předání údajů o transakcích nebo obsahu lze vydat pouze u trestných činů postihnutelných ve vydávajícím státě trestem odnětí svobody s horní hranicí sazby nejméně tří let nebo u specifických trestných činů, které

¹⁸ Ve Strategii kybernetické bezpečnosti Evropské unie z roku 2013 byla Budapešťská úmluva uznána jako hlavní mnohostranný rámec pro boj proti kyberkriminalitě – společné sdělení Komise a vysoké představitelky Unie pro zahraniční věci a bezpečnostní politiku Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor, JOIN(2013) 1 final.

¹⁹ Na svém 17. plenárním zasedání (červen 2017) přijal Výbor pro Úmluvu o kyberkriminalitě (T-CY) mandát k přípravě druhého dodatkového protokolu k úmluvě (dále jen „druhý dodatkový protokol“), který má výbor T-CY připravit a dokončit do prosince 2019. Cílem je ustoupit od kritéria místa uložení coby rozhodujícího faktoru.

jsou uvedeny v návrhu a kde je konkrétní vazba na elektronické nástroje a trestné činy zahrnuté do směrnice 2017/541/EU o terorismu.

Vzhledem k různým úrovním narušující povahy opatření ukládaných v souvislosti se sledovanými údaji stanovuje návrh řadu podmínek a záruk. K nim patří povinnost získat předchozí potvrzení příkazů justičním orgánem. Návrh se týká pouze uložených údajů. Nevztahuje se na odposlech telekomunikačního provozu v reálném čase. Opatření se omezuje na to, co je nezbytné a přiměřené účelu příslušných trestních řízení. Umožňuje též poskytovatelům služeb požádat vydávající orgány v případě potřeby o objasnění. Nelze-li tyto problémy vyřešit a vydávající orgán se rozhodne, že přistoupí k vymáhání, mohou poskytovatelé služeb použít stejné důvody k odporu proti vymáhání ze strany svých vlastních orgánů. Kromě toho je stanoven konkrétní postup pro situace, v nichž je povinnost poskytnout údaje v rozporu s konkurenční povinností vyplývající z práva třetí země.

Právní předpisy EU chrání práva podezřelých a obviněných osob v trestních řízeních a pravidla na ochranu osobních údajů již existují. Avšak v případě osob, o jejichž údaje se žádá, poskytují tyto další záruky uvedené v návrhu procesní práva těmto osobám v trestních řízeních nebo mimo ně. To zahrnuje možnost napadnout zákonnost, nezbytnost nebo přiměřenost příkazu, aniž jsou omezeny důvody pro napadení v souladu s vnitrostátním právem. Práva podle právních předpisů vymáhajícího státu jsou plně dodržována tím, že vydávající stát bere v potaz imunity a výsady, které chrání žádané údaje v členském státě poskytovatele služeb. To platí zejména v případech, kdy poskytují vyšší míru ochrany než právní předpisy vydávajícího státu.

Příkazy podle navrhovaného nařízení jsou vymahatelné stejně jako srovnatelné vnitrostátní příkazy v jurisdikci, v níž poskytovatel služeb příkaz obdrží. Nařízení stanoví, že členské státy by měly uplatňovat účinné a přiměřené sankce.

2. PRÁVNÍ ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

• Právní základ

Právním základem na podporu opatření v této oblasti je čl. 82 odst. 1 Smlouvy o fungování Evropské unie. V čl. 82 odst. 1 se stanoví, že opatření mohou být přijímána řádným legislativním postupem s cílem stanovit pravidla a postupy pro zajištění uznávání všech forem rozsudků a soudních rozhodnutí v celé Unii. Opatření mohou být též přijímána s cílem usnadňovat spolupráci mezi justičními nebo rovnocennými orgány členských států v rámci trestního řízení a vymáhání rozhodnutí.

Tento právní základ se uplatňuje na mechanismy zahrnuté do tohoto nařízení. Ustanovením čl. 82 odst. 1 je zajištěno vzájemné uznávání soudních rozhodnutí, která justiční orgán ve vydávajícím státě adresuje právnické osobě v jiném členském státě a jimiž jí dokonce ukládá povinnosti bez předchozího zásahu justičního orgánu v tomto jiném členském státě. Evropský předávací nebo uchovávací příkaz může v případě potřeby vést k zásahu justičního orgánu vykonávajícího státu za účelem výkonu rozhodnutí.

• Volba nástroje

Ustanovení čl. 82 odst. 1 SFEU dává normotvůrci Unie možnost přijímat nařízení a směrnice.

Jelikož se návrh týká přeshraničních postupů, v nichž jsou vyžadována jednotná pravidla, není nutné nechávat členským státům prostor k provedení takových pravidel. Nařízení je přímo použitelné, poskytuje jasnost a větší právní jistotu a předchází odchylnému výkladu v

členských státech a dalším problémům při provádění, ke kterým dochází v případě rámcových rozhodnutí o vzájemném uznávání rozsudků a soudních rozhodnutí. Nařízení navíc umožňuje, aby stejná povinnost byla v celé Unii uložena jednotným způsobem. Z těchto důvodů se má za to, že nejvhodnější formou pro tento nástroj vzájemného uznávání je nařízení.

- **Subsidiarita**

Vzhledem k přeshraničnímu rozměru řešených problémů musí být opatření zahrnutá do návrhu přijata na úrovni Unie, aby mohlo být dosaženo cílů. Trestné činy, pro které existují elektronické důkazy, často zahrnují situace, kdy infrastruktura, v níž jsou elektronické důkazy uloženy, a poskytovatel služeb provozující infrastrukturu spadají pod jiný vnitrostátní právní rámec, ať už v Unii nebo mimo ni, než vnitrostátní právní rámec oběti a pachatele trestného činu. V důsledku toho může být pro příslušnou zemi velmi časově nákladné a náročné získat bez společných minimálních pravidel účinný přeshraniční přístup k elektronickým důkazům. Zejména pro členské státy, které jednájí samy, by bylo obtížné řešit následující otázky:

- rozříštěnost právních rámců v členských státech, kterou poskytovatelé služeb snaží se vyhovět žádostem na základě různých vnitrostátních právních předpisů, považují za velký problém,
- větší prospěšnost justiční spolupráce na základě stávajících právních předpisů Unie, zejména prostřednictvím evropského vyšetřovacího příkazu.

Vzhledem k rozmanitosti právních přístupů, počtu dotčených oblastí politiky (bezpečnost, základní práva včetně procesních práv a ochrany osobních údajů, hospodářské otázky) a velkému množství zúčastněných stran jsou nejvhodnějšími prostředky k řešení zjištěných problémů právní předpisy na úrovni Unie.

- **Proporcionalita**

Návrh stanoví pravidla, za nichž příslušný orgán v Unii může nařídít poskytovateli služeb, který nabízí služby v Unii a není usazen v témže členském státě, aby předal nebo uchoval elektronické důkazy. Klíčové prvky návrhu, např. věcná působnost evropského předávacího příkazu, podmínky zaručující mezinárodní zdvořilost, sankční mechanismus a systém záruk a právních prostředků, se soustřeďují na to, co je nezbytné pro dosažení hlavních cílů návrhu. Návrh se zejména omezuje na žádosti o uložení údajů (údaje z odposlechnutí telekomunikačního provozu v reálném čase do něho nejsou zahrnuty) a na příkazy vydané v trestních řízeních ve věci vyšetřování konkrétního trestného činu. Nezahrnuje tudíž prevenci trestné činnosti ani jiné druhy řízení či porušení (např. správní řízení ohledně porušení právních pravidel) a nevyžaduje, aby poskytovatelé služeb systematicky shromažďovali nebo uchovávali více údajů, než jaké již shromažďují nebo uchovávají z obchodních důvodů nebo za účelem plnění jiných právních požadavků. Navíc zatímco příkazy k předání údajů o účastníkovi a přístupu lze vydat u jakéhokoli trestného činu, příkaz k předání údajů o transakcích nebo obsahu lze vydat pouze u trestných činů postihnutelných ve vydávajícím státě trestem odnětí svobody s horní hranicí sazby nejméně tří let nebo u konkrétních trestných činů závislých na kybernetické činnosti a umožněných kybernetickou činností definovaných v návrhu a u trestných činů souvisejících s terorismem. A konečně návrh objasňuje procesní pravidla a záruky použitelné na přeshraniční přístup k elektronickým důkazům, avšak nezachází až k harmonizaci vnitrostátních opatření. Je omezen na to, co je nezbytné a přiměřené k řešení potřeb donucovacích orgánů a justičních orgánů v digitálním věku.

3. VÝSLEDKY HODNOCENÍ *EX POST*, KONZULTACÍ SE ZÚČASTNĚNÝMI STRANAMI A POSOUZENÍ DOPADŮ

• Konzultace se zúčastněnými stranami

Komise déle než rok a půl konzultovala všechny příslušné zúčastněné strany, aby zjistila problémy a jejich možná řešení. Dělo se tak prostřednictvím řady průzkumů, počínaje otevřenou veřejnou konzultací a konče cílenými průzkumy s příslušnými veřejnými orgány. Byla zorganizována i skupinová odborná setkání a dvoustranná jednání, na nichž byly projednávány potenciální dopady právních předpisů EU. Zpětná vazba o iniciativě byla získávána i na konferencích o přeshraničním přístupu k elektronickým důkazům.

Respondenti průzkumů vesměs vnímali rostoucí využívání informačních služeb jako výzvu pro vymáhání práva, jelikož příslušné orgány jsou často nedostatečně vybaveny k práci s důkazy on-line. Za jednu z hlavních překážek je označován též zdoluhavý postup získávání důkazů. K dalším klíčovým problémům, na které veřejné orgány upozornily, patří nedostatečně spolehlivá spolupráce s poskytovateli služeb, nedostatečná transparentnost a právní nejistota týkající se pravomoci k vyšetřovacím opatřením. Přímá přeshraniční spolupráce mezi donucovacími orgány a poskytovateli digitálních služeb byla vnímána jako přidaná hodnota v trestním vyšetřování. Poskytovatelé služeb a některé organizace občanské společnosti uváděli nutnost zajistit právní jistotu při spolupráci s veřejnými orgány a předcházet kolizím norem. U obav z toho, jak by nový právní předpis EU mohl ovlivnit práva, měly zúčastněné strany pocit, že nezbytnou podmínkou pro jakýkoli přeshraniční nástroj by měla být garance konkrétních záruk.

Zpětná vazba shromážděná z počátečního posouzení dopadů ukázala, že zúčastněné strany věří, že vyřešení nedostatků současného systému vzájemné právní pomoci by jej zefektivnilo a zlepšilo by právní jistotu. Některé organizace občanské společnosti byly proti právním předpisům na úrovni EU v oblasti přímé spolupráce. Upřednostňovaly omezení opatření EU na zlepšení postupů vzájemné právní pomoci. Tato myšlenka bude uplatněna jako součást praktických opatření schválených Radou v červnu 2016.

Prostřednictvím cíleného průzkumu mezi veřejnými orgány v členských státech bylo též odhaleno, že neexistuje žádný společný přístup k získání přeshraničního přístupu k elektronickým důkazům, jelikož každý členský stát má svou vlastní vnitrostátní praxi. Poskytovatelé služeb též reagují na žádosti zahraničních donucovacích orgánů odlišně a doby reakce se různí v závislosti na žádajícím členském státě. Toto vyvolává právní nejistotu pro všechny zainteresované zúčastněné strany.

Konzultace se zúčastněnými stranami obecně naznačila, že současný právní rámec je roztržštěný a složitý. To může vést ke zpožděním během fáze výkonu a k nedostatečně účinnému vyšetřování a stíhání trestných činů, jejichž součástí je přeshraniční přístup k elektronickým důkazům.

• Posouzení dopadů

Výbor pro kontrolu regulace vydal pozitivní stanovisko k posouzení dopadů na podporu tohoto návrhu²⁰ a přednesl různé návrhy na zlepšení²¹. V návaznosti na toto stanovisko bylo

²⁰ Pracovní dokument útvarů Komise – Posouzení dopadů provázející návrh nařízení o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech a návrh směrnice, kterou se stanoví harmonizovaná pravidla pro jmenování právních zástupců za účelem shromažďování důkazů v trestním řízení, SWD(2018) 118.

posouzení dopadů změněno, aby se ještě hlouběji zaměřilo na otázky základních práv spojené s přeshraničním sdílením údajů, a zejména na vazby mezi různými opatřeními, která jsou součástí upřednostňované možnosti. Posouzení bylo upraveno též proto, aby lépe odráželo názory zúčastněných subjektů a členských států a to, jak byly vzaty v úvahu. Dále byly revidovány politické souvislosti a zahrnuty do nich byly další odkazy na různé aspekty, jako jsou diskuse v odborných skupinách, které pomáhaly při tvorbě iniciativy. Objasněna z hlediska oblasti působnosti, načasování a hloubky byla doplňkovost různých opatření (zejména směrnice o evropském vyšetřovacím příkazu, jednání o dodatkovém protokolu k Budapešťské úmluvě a společný přezkum dohody o vzájemné právní pomoci mezi EU a USA) a proběhla revize základního scénáře, aby lépe odrážel vývoj, který pravděpodobně nastane nezávisle na přijetí navrhovaných opatření. A konečně byly přidány vývojové diagramy pro lepší popis pracovních toků pro sdílení údajů.

Vedle základního scénáře (možnost O) byly zvažovány čtyři hlavní politické možnosti: několik praktických opatření ke zlepšení postupů justiční spolupráce a přímé spolupráce mezi veřejnými orgány a poskytovateli služeb (možnost A: nelegislativní), možnost kombinující praktická opatření možnosti A s mezinárodními řešeními na dvoustranné nebo mnohostranné úrovni (možnost B: legislativní), možnost kombinující předchozí opatření obsažená v možnosti B s evropským předávacím příkazem a opatřením ke zlepšení přístupu k databázím, které poskytují informace o účastnících na základě dotazů, např. databáze názvů domén Whois (možnost C: legislativní), a možnost kombinující všechna předchozí opatření obsažená v možnosti C s právními předpisy o přímém přístupu ke vzdáleně uloženým údajům (možnost D: legislativní)²².

Nebude-li přijato žádné opatření (možnost O), zhorší rostoucí počet žádostí situaci. Všechny ostatní možnosti pomáhají dosáhnout cílů iniciativy, ale v různé míře. Možnost A by zlepšila účinnost současných procesů, např. tím, že by zvýšila kvalitu žádostí, ale prostor pro zlepšení by byl omezen strukturálními nedostatky současného systému.

Možnost B by vedla k větším zlepšením tím, že by poskytla mezinárodně uznávaná řešení, jejich výsledek by však ve velké míře závisel na třetích státech. Řešení jsou tudíž nejistá a není pravděpodobné, že by byla účinná a že by nabízela tolik záruk jako unijní řešení.

Možnost C by jasně přidala hodnotu v porovnání s předchozími možnostmi tím, že by poskytla nástroj uvnitř EU pro přímou spolupráci s poskytovateli služeb, který by řešil většinu zjištěných otázek v případech, že by existoval poskytovatel služeb, který má dotčené údaje.

Možnost D je nejkomplexnějším souborem řešení. Navíc k předchozím opatřením je jeho součástí i legislativní opatření o přímém přístupu pro situace, v nichž zapojení poskytovatele služeb není nutné.

Tato legislativní iniciativa, kterou Komise navrhuje, se opírá o zjištění posouzení dopadů. Tento právní předpis bude doplněn o praktická opatření popsaná v posouzení dopadů a o

²¹ Výbor Evropské komise pro kontrolu regulace – Stanovisko k posouzení dopadů – Návrh nařízení o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech a návrh směrnice, kterou se stanoví harmonizovaná pravidla pro jmenování právních zástupců za účelem shromažďování důkazů v trestním řízení, SEC(2018) 199.

²² Ohledně podrobností srov. pracovní dokument útvarů Komise – Posouzení dopadů provádějící návrh nařízení o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech a návrh směrnice, kterou se stanoví harmonizovaná pravidla pro jmenování právních zástupců za účelem shromažďování důkazů v trestním řízení, SWD(2018) 118.

pokračující práce na dodatkovém protokolu Budapešťské úmluvy. Na základě svého legislativního návrhu projedná Komise s USA a dalšími třetími zeměmi i možnost budoucích dvoustranných nebo mnohostranných dohod o přeshraničním přístupu k elektronickým důkazům s průvodními zárukami. Pokud jde o opatření přímého přístupu a přístupu do databází, která tvoří součást možnosti D, nepředkládá Komise v tuto chvíli žádný právní předpis, ale i dále bude uvažovat o nejlepším způsobu, jak postupovat v těchto dvou otázkách.

Očekává se, že iniciativa umožní účinnější a efektivnější vyšetřování a stíhání a že současně zvýší transparentnost a odpovědnost a zajistí dodržování základních práv. Očekává se též, že podpoří důvěru v jednotný digitální trh tím, že zlepší bezpečnost a sníží vnímání beztrestnosti za trestné činy spáchané na zařízeních připojených k síti nebo jejich prostřednictvím.

Z pohledu veřejných orgánů lze očekávat, že jim iniciativa přinese počáteční náklady na její zavedení, které by byly v dlouhodobém horizontu vyrovnány úsporami u opakujících se nákladů. Vnitrostátní orgány by se musely přizpůsobit novým postupům a investovat do odborné přípravy. Avšak poté by těžily ze zefektivnění a centralizace a jasného právního rámce upravujícího žádosti o přístup k údajům, které by měly vést k vyšší efektivnosti. Jelikož by upřednostňovaná možnost snížila tlak na kanály justiční spolupráce, došlo by podobně v zemích, které jsou příjemci žádostí, ke snížení počtu žádostí, které musí zpracovat.

Poskytovatelé služeb by se museli přizpůsobit novému legislativnímu rámci zavedením (nových) postupů a vyškolením zaměstnanců. Harmonizovaný rámec by na druhou stranu mohl snížit zátěž těch poskytovatelů, kteří v současnosti odpovídají na žádosti o neobsahové údaje, které musí posuzovat podle různých zákonů jednotlivých členských států. Právní jistota a normalizace postupů by měly mít kladný dopad i na malé a střední podniky, jelikož by zmírnily administrativní zátěž a měly příznivý vliv na konkurenceschopnost. Obecně se též očekává, že iniciativa by pro ně představovala úspory.

• **Základní práva**

Návrh by potenciálně mohl mít dopad na řadu základních práv:

- práva fyzických osob, k jejichž údajům se přistupuje: právo na ochranu osobních údajů, právo na respektování soukromého a rodinného života, právo na svobodu projevu, právo na obhajobu, právo na účinnou právní ochranu a spravedlivý proces,
- práva poskytovatelů služeb: právo na svobodu podnikání, právo na účinnou právní ochranu,
- práva všech občanů: právo na svobodu a bezpečnost.

S ohledem na relevantní *acquis* o ochraně údajů jsou do navrhovaného nařízení zahrnuty dostatečné a důležité záruky s cílem zajistit ochranu práv těchto osob.

Jelikož příkazy lze vydávat pouze v trestních řízeních a ve srovnatelných vnitrostátních situacích během přípravné i soudní fáze, jsou použitelné všechny trestněprávní procesní záruky. Mezi ty patří zejména právo na spravedlivý proces zakotvené v článku 6 Evropské úmluvy o lidských právech a v člancích 47 a 48 Listiny základních práv. Patří sem i příslušné právní předpisy na úrovni EU týkající se procesních práv v trestním řízení: směrnice 2010/64/EU o právu na tlumočení a překlad v trestním řízení, směrnice 2012/13/EU o právu na informace o právech a poplatcích a o přístupu ke spisu, směrnice 2013/48/EU o právu na přístup k obhájci a právu na komunikaci s příbuznými v případě zatčení a zajištění, směrnice 2016/343, kterou se posilují některé aspekty presumpce neviny a právo být přítomen při

trestním řízení před soudem, směrnice 2016/800 o procesních zárukách pro děti a směrnice 2016/1919 o právní pomoci pro podezřelé nebo obviněné osoby v trestním řízení a pro osoby vyžádané v rámci řízení týkajícího se evropského zatýkacího rozkazu.

Konkrétněji vzato předchozí zásah justičního orgánu při vydání příkazu zajišťuje ověření zákonnosti opatření a jeho nezbytnost a přiměřenost konkrétnímu případu. Zajišťuje rovněž, aby příkaz nepřiměřeně nezasahoval do základních práv, včetně účinků právních zásad, jako je povinnost mlčenlivosti. Vydávající orgán musí v každém jednotlivém případě zajistit, aby opatření bylo nezbytné a přiměřené, a to i s ohledem na závažnost vyšetřovaného trestného činu. Součástí návrhu jsou i prahové hodnoty pro údaje o transakcích a obsahu, které zajišťují, aby byl evropský předávací příkaz používán pouze u závažnějších forem trestných činů v souvislosti s takovými údaji.

Výslovně je řešeno i právo na účinnou právní ochranu pro osoby, jejichž údaje jsou požadovány. Během soudního řízení ve vydávajícím státě musí být brány v úvahu též uznané imunity a výsady některých profesí, jako jsou právníci, jakož i základní zájmy národní bezpečnosti nebo obrany ve státě adresáta. Přezkum justičním orgánem zde slouží jako další záruka.

Jelikož příkaz je závazné opatření, má dopad i na práva poskytovatelů služeb, zejména na svobodu podnikání. Návrh obsahuje právo poskytovatele služeb vznášet ve vydávajícím členském státě určité nároky, např. pokud příkaz nevydal nebo nepotvrdil justiční orgán. Je-li příkaz předán k vymáhání vymáhajícímu státu, může vymáhající orgán rozhodnout, že příkaz neuzná nebo nebude vymáhat, pokud jsou při obdržení zjevné některé z omezených důvodů pro odpor, a po konzultaci s vydávajícím orgánem. Navíc pokud by byl zahájen vymáhací postup, bude před vymáhajícím orgánem na základě některého z takových omezených důvodů moci podat odpor proti příkazu sám adresát. To zahrnuje například případy, kdy je zjevné, že příkaz nevydal nebo nepotvrdil příslušný orgán, nebo kdy by plnění očividně porušilo Listinu základních práv nebo by bylo očividně nepatřičné. To však nevylučuje právo adresáta na účinný opravný prostředek proti rozhodnutí ukládajícímu sankci.

Možným problémem v souvislosti s opatřeními EU v této oblasti je možnost, že by to mohlo vést k tomu, že by třetí země zavedly reciproční povinnosti pro poskytovatele služeb v EU, které by nebyly v souladu s podmínkami základních práv EU, včetně vysoké úrovně ochrany údajů zajišťované *acquis* EU. Návrh řeší tuto situaci dvěma způsoby: zaprvé tím, že poskytuje opatření, které obsahuje silné záruky a výslovné odkazy na podmínky a záruky, jež jsou již nedílnou součástí *acquis* EU, a slouží tak jako model pro zahraniční právní předpisy, a zadruhé tím, že obsahuje zvláštní ustanovení o „rozporných povinnostech“, které poskytovatelům služeb umožní upozornit na rozporné povinnosti, jimž čelí, a iniciovat tak soudní přezkum. Toto ustanovení má zajistit dodržování jak obecných předpisů o blokování, například zákon USA o důvěrnosti elektronické komunikace (U.S. Electronic Communications Privacy Act, dále jen „zákon ECPA“), který s výjimkou několika málo okolností zakazuje sdělování údajů o obsahu v jeho geografické oblasti působnosti, tak zákonů, které zveřejnění obecně nezakazují, ale mohou tak učinit v jednotlivých případech. U případů souvisejících se zákonem ECPA může být v některých situacích zamezeno přístupu k údajům o obsahu, a hlavním nástrojem k přístupu k údajům by proto měla zůstat vzájemná právní pomoc. Avšak vzhledem ke změnám, které přineslo přijetí zákona CLOUD²³, by

²³ Dne 23. března 2018 byl ve Spojených státech amerických přijat zákon objasňující zákonné používání údajů v zahraničí (Clarifying Lawful Overseas Use of Data (CLOUD) Act). Zákon CLOUD je k dispozici [zde](#).

předpis o blokování mohl být zrušen, pokud by EU uzavřela s USA dohodu. Kolize norem mohou ještě více omezit další mezinárodní dohody s jinými klíčovými partnery.

Vzhledem k výše uvedenému jsou opatření v tomto návrhu slučitelná se základními právy.

4. ROZPOČTOVÉ DŮSLEDKY

Legislativní návrh nařízení nemá dopad na rozpočet Unie.

5. OSTATNÍ PRVKY

- Plány provádění a způsob monitorování, hodnocení a podávání zpráv**

Nařízení je přímo použitelné v Unii. Budou ho přímo uplatňovat osoby z praxe bez nutnosti upravovat vnitřní právní systémy.

Nařízení bude vyhodnoceno a zprávu Evropskému parlamentu a Radě předloží Komise nejpozději pět let po jeho vstupu v platnost. Na základě zjištění zprávy, zejména na základě toho, zda v nařízení zůstaly nějaké nedostatky, které jsou relevantní v praxi, a s ohledem na technický vývoj posoudí Komise nutnost rozšířit oblast působnosti nařízení. V případě potřeby předloží Komise návrhy úprav tohoto nařízení. Členské státy poskytnou Komisi informace nezbytné pro přípravu této zprávy. Členské státy shromáždí údaje nezbytné pro každoroční monitorování nařízení.

V případě potřeby vydá Komise pro poskytovatele služeb pokyny, jak mají plnit povinnosti podle nařízení.

- Podrobné vysvětlení konkrétních ustanovení návrhu**

	<i>NAŘÍZENÍ</i>	
	Článek	Bod odůvodnění
I. Předmět, definice a oblast působnosti	1. Předmět	1–15
	2. Definice	16–23
	3. Oblast působnosti	24–27
II. Evropský předávací příkaz, evropský uchovávací příkaz a certifikáty, právní zástupce	4. Vydávající orgán	30
	5. Podmínky pro vydání evropského předávacího příkazu	28–29, 31–35
	6. Podmínky pro vydání evropského uchovávacího příkazu	36
	7. Adresát evropského předávacího příkazu a evropského uchovávacího příkazu	37

	8. Certifikát evropského předávacího příkazu a certifikát evropského uchovávacího příkazu	38–39
	9. Provedení EPOC	40–41
	10. Provedení EPOC-PR	42
	11. Důvěrnost a informace o uživateli	43
	12. Náhrada nákladů	žádný
III. Sankce a vymáhání	13. Sankce	žádný
	14. Vymáhací postup	44–45, 55
IV. Opravné prostředky	15. a 16. Přezkumné řízení v případě rozporných povinností vyplývajících z právních předpisů třetí země	47–53
	17. Účinná právní ochrana	54
	18. Zajištění výsad a imunit podle práva vymáhajícího státu	35
V. Závěrečná ustanovení	19. Monitorování a podávání zpráv	58
	20. Změny certifikátů a formulářů	59–60
	21. Výkon přenesené pravomoci	60
	22. Oznámení	žádný
	23. Vztah k evropským vyšetřovacím příkazům	61
	24. Hodnocení	62
	25. Vstup v platnost	žádný

Kapitola 1: Předmět, definice a oblast působnosti

Článek 1: Předmět

Tento článek stanoví obecnou oblast působnosti a účel návrhu, jímž je stanovit pravidla, podle kterých smí příslušný justiční orgán v Evropské unii nařídit prostřednictvím evropského předávacího nebo uchovávacího příkazu poskytovateli služeb nabízejícímu služby v Unii, aby předal nebo uchoval elektronické důkazy. Tyto nástroje lze používat pouze v přeshraničních situacích, tzn. v situacích, kdy je poskytovatel služeb usazen nebo zastoupen v jiném členském státě.

Toto nařízení dává vyšetřovacím orgánům další nástroje k získání elektronických důkazů, aniž omezuje vnitrostátním právem již dané pravomoci donutit poskytovatele služeb usazené

nebo zastoupené na jejich území, aby plnili své povinnosti. Je-li poskytovatel služeb usazen nebo zastoupen v témže členském státě, uplatňují orgány tohoto členského státu k tomu, aby poskytovatele donutily k plnění jeho povinností, vnitrostátní opatření.

Údaje nařízené prostřednictvím evropského předávacího příkazu by měly být poskytnuty přímo daným orgánům bez zapojení orgánů v členském státě, kde je poskytovatel služeb usazen nebo zastoupen. Nařízení se též odklání od umístění údajů coby určujícího spojovacího faktoru, jelikož uchovávání údajů nemá zpravidla za následek žádnou kontrolu ze strany státu, na jehož území jsou údaje uchovávány. Takové uchovávání určuje ve většině případů sám poskytovatel na základě obchodních hledisek²⁴.

Kromě toho je nařízení též použitelné za předpokladu, že poskytovatelé služeb nejsou usazeni nebo zastoupeni v Unii, ale nabízejí v Unii služby. To odráží čl. 3 odst. 1.

Pokud návrh odkazuje na poskytovatele služeb usazeného nebo zastoupeného v členském státě prostřednictvím právního zástupce, samotné ustanovení právního zástupce nezakládá provozovnu poskytovatele služeb pro účely tohoto nařízení.

V čl. 1 odst. 2 se připomíná, že tímto nařízením není změněna povinnost dodržovat základní práva a právní zásady zakotvené v článku 6 Smlouvy o EU.

Článek 2: Definice

Tento článek stanoví definice, které jsou použity v celém nástroji.

Do oblasti působnosti nařízení spadají následující typy poskytovatelů služeb: poskytovatelé služeb elektronické komunikace, poskytovatelé služeb informační společnosti, u kterých je určující složkou služby poskytované uživateli uchovávání údajů, včetně sociálních sítí, nakolik je nelze kvalifikovat jako služby elektronické komunikace, internetová tržiště umožňující transakce mezi jejich uživateli (např. spotřebiteli nebo podniky) a jiní poskytovatelé hostingových služeb a poskytovatelé služeb v oblasti číslování a názvů internetových domén.

Do oblasti působnosti nařízení spadají poskytovatelé služeb elektronické komunikace definovaných [ve směrnici, kterou se zřizuje evropský kodex pro elektronické komunikace]. Tradiční telekomunikační služby, spotřebitelé a podniky stále více spoléhají namísto tradičních komunikačních služeb na nové internetové služby umožňující interpersonální komunikaci, jako například VoIP, výměna rychlých zpráv (instant messaging) a e-mailové služby. Tyto služby by společně se sociálními sítěmi, jako je Twitter a Facebook, které uživatelům umožňují sdílet obsah, měly být do tohoto návrhu též zahrnuty.

V mnoha případech se údaje již neuchovávají v zařízení uživatele, ale jsou zpřístupněny v cloudové infrastruktuře umožňující v zásadě přístup odkudkoli. Poskytovatelé služeb nemusí být usazeni nebo mít servery v každé jurisdikci a místo toho k uchovávání údajů a poskytování svých služeb využívají centralizovanou administrativu a decentralizované systémy. Činí tak proto, aby dosáhli optimálního vyrovnaní zátěže a zkrátili prodlení při reagování na žádosti uživatelů o údaje. Ke zrychlení dodávání obsahu jeho zkopírováním na několika serverech rozmístěných po světě se obvykle používají sítě pro doručování obsahu (CDN). Díky tomu mohou společnosti poskytovat obsah ze serveru, který má uživatel nejbližší

²⁴ Další vysvětlení obsahuje posouzení dopadů.

nebo ze kterého probíhá komunikace méně přetíženou sítí. Aby byl zohledněn tento vývoj, zahrnují definice cloudové a jiné hostingové služby, které poskytují širokou škálu výpočetních prostředků, jako jsou síť, servery nebo jiná infrastruktura, úložiště, aplikace a služby, které umožňují uchovávat data pro různé účely. Nástroj se vztahuje i na digitální tržiště, díky nimž mohou spotřebitelé a/nebo podniky uskutečňovat transakce prostřednictvím on-line prodeje nebo smluv o službách. Takové transakce probíhají buď na webové stránce internetového tržiště, nebo na webové stránce obchodníka, který využívá počítačové služby poskytované internetovým tržištěm. Je to tudíž toto tržiště, které vlastní elektronické důkazy, jež mohou být potřebné v průběhu trestních řízení.

Služby, u kterých uchovávání údajů není určující složkou, do návrhu zahrnuty nejsou. Ačkoli většina služeb dodávaných poskytovateli obsahuje nějakou formu uchovávání údajů, zejména tam, kde jsou dodávány on-line na dálku, lze odlišit služby, u kterých uchovávání údajů není jejich hlavním znakem, nýbrž jen doplňkovou vlastností, např. právní, architektonické, inženýrské a účetní služby poskytované on-line na dálku.

Pro trestní řízení mohou mít význam údaje, kterými disponují poskytovatelé služeb internetové infrastruktury, jako jsou registrátoři a registry názvů domén a poskytovatelé služeb zajištění soukromí a proxy serverů nebo regionální internetové registry adres internetových protokolů, jelikož takové údaje mohou poskytovat stopy umožňující identifikaci fyzické či právnické osoby zapojené do trestné činnosti.

Kategorie údajů, které příslušné orgány mohou získat díky evropskému předávacímu příkazu, zahrnují údaje o účastníkovi, údaje o přístupu, údaje o transakcích (tyto tři kategorie jsou obecně označovány společně jako „neobsahové údaje“) a údaje o uloženém obsahu. Toto rozdělení, kromě údajů o přístupu, existuje v právních rámcích mnoha členských států a též v právních rámcích zemí mimo EU.

Všechny kategorie obsahují osobní údaje, a vztahují se tak na ně záruky podle *acquis* EU o ochraně údajů. Intenzita dopadu na základní práva se mezi nimi různí, zejména mezi údaji o účastníkovi na jedné straně a údaji o transakcích a obsahu na straně druhé. Je zásadní, aby nástroj obsáhl všechny tyto kategorie: údaje o účastníkovi a přístupu jsou často výchozím bodem pro získání vodítek k totožnosti podezřelé osoby při vyšetřování. Údaje o transakcích a obsahu mohou být zase nejrelevantnější jako důkazní materiál. Z důvodu různé míry zásahu do základních práv je důvodné spojit různé podmínky s údaji o účastníkovi na jedné straně a s údaji o transakcích a obsahu na straně druhé, jak je provedeno v několika ustanoveních nařízení.

Je vhodné vyčlenit údaje o přístupu jako zvláštní kategorii údajů použitou v tomto nařízení. Údaje o přístupu tak, jak jsou zde definovány, jsou využívány pro též cíl jako údaje o účastníkovi, tj. identifikovat uživatele, a míra zásahu do základních práv je podobná. Měly by tudíž podléhat stejným podmínkám jako údaje o účastníkovi. Tento návrh tak zavádí novou kategorii údajů, s níž je třeba zacházet jako s údaji o účastníkovi, pokud je sledován stejný cíl.

Článek 2 definuje členské státy a orgány, které by mohly být do postupu zapojeny. Definice vydávajícího orgánu je zahrnuta do článku 4.

Naléhavé případy jsou výjimečné situace, které pravidelně vyžadují včasnou reakci poskytovatelů služeb a pro které budou platit zvláštní podmínky. Jsou proto v tomto článku definovány samostatně.

Článek 3: Oblast působnosti

Tento článek stanoví oblast působnosti návrhu. Nařízení se vztahuje na všechny poskytovatele služeb, kteří nabízejí služby v Unii, včetně poskytovatelů služeb, kteří v Unii nejsou usazeni. Aktivní nabízení služeb v Unii se všemi výhodami z toho vyplývajících odůvodňuje to, že se nařízení vztahuje i na tyto poskytovatele služeb, a vytváří rovné podmínky pro účastníky na těchto trzích. Navíc nezahrnutím těchto poskytovatelů služeb by vznikla mezera, které by pachatelé trestné činnosti využili k obcházení oblasti působnosti nařízení.

Aby orgány zjistily, zda jsou služby nabízeny, musí posoudit, zda poskytovatel služeb umožňuje právníkům nebo fyzickým osobám v jednom či více členských státech využívat jeho služby. Avšak pouhá dostupnost služby (která by mohla vyplynout i z dostupnosti webové stránky, e-mailové adresy a jiných kontaktních údajů poskytovatele služeb či zprostředkovatele) by neměla být dostatečnou podmínkou pro použití tohoto nařízení. Pro zjištění dostatečné vazby mezi poskytovatelem a územím, kde nabízí své služby, je vyžadováno podstatné spojení mezi těmito členskými státy. Takové podstatné spojení existuje v případě, že má poskytovatel služeb provozovnu v jednom nebo více členských státech. Pokud v Unii provozovnu nemá, mělo by být kritérium podstatného spojení s Uníí posuzováno na základě existence významného počtu uživatelů v jednom nebo více členských státech nebo zacílení činností na jeden nebo více členských států. Zacílení činností na jeden nebo více členských států lze určit na základě všech relevantních okolností, včetně takových faktorů, jako je používání jazyka či měny obecně používaných v daném členském státě. Zacílení činností na některý členský stát by mohlo být též odvozeno od dostupnosti aplikace v příslušném národním obchodě s aplikacemi, od poskytování místních reklam nebo reklam v jazyce používaném v daném členském státě, od využívání jakýchkoli informací pocházejících od osob v členských státech v průběhu jeho činností nebo od řešení vztahů se zákazníky, např. poskytováním zákaznického servisu v jazyce obecně používaném v daném členském státě. Podstatné spojení je třeba předpokládat i v případě, že poskytovatel služeb zaměřuje své činnosti na jeden nebo více členských států, jak stanoví čl. 17 odst. 1 písm. c) nařízení 1215/2012 o příslušnosti a uznávání a výkonu soudních rozhodnutí v občanských a obchodních věcech.

Evropský předávací příkaz a evropský uchovávací příkaz jsou vyšetřovací opatření, která lze vydávat pouze při trestních vyšetřováních nebo trestních řízeních u konkrétních trestných činů. Vazba na konkrétní vyšetřování je odlišuje od preventivních opatření nebo povinností uchovávat údaje stanovených zákonem a zajišťuje uplatňování procesních práv použitelných na trestní řízení. Předpokladem pro použití nařízení je tudíž příslušnost zahájit vyšetřování konkrétního trestného činu.

Doplňujícím požadavkem je, že žádané údaje musí souviset se službami, které poskytovatel služeb nabízí v Unii.

Kapitola 2: Evropský předávací příkaz, evropský uchovávací příkaz a certifikáty

Článek 4: Vydávající orgán

Při vydávání evropského předávacího nebo uchovávacího příkazu musí být justiční orgán vždy zapojen jako vydávající nebo potvrzující orgán. U příkazů k předání údajů o transakcích a obsahu je vyžadován soudce nebo soud. U údajů o účastníkovi nebo přístupu to může učinit i státní zástupce.

Článek 5: Podmínky pro vydání evropského předávacího příkazu

Článek 5 stanoví podmínky pro vydání evropského předávacího příkazu. Musí je posoudit vydávající justiční orgán.

Evropský předávací příkaz může být vydán pouze za předpokladu, že je to v individuálním případě nezbytné a přiměřené. Měl by být navíc vydán pouze za předpokladu, že by ve srovnatelné vnitrostátní situaci ve vydávajícím státě bylo k dispozici obdobné opatření.

Příkazy k předání údajů o účastníkovi a údajů o přístupu lze vydat v souvislosti s jakýmkoli trestným činem. Na údaje o transakcích a obsahu by se měly vztahovat přísnější požadavky, aby odrážely citlivější povahu takových údajů a odpovídající vyšší míru invazivnosti příkazů u takových údajů v porovnání s údaji o účastníkovi a přístupu. Příkazy lze tudíž vydávat u trestných činů, pro které je stanoven maximální trest odnětí svobody v délce nejméně tři roky. Stanovení prahové hodnoty na základě maximálního trestu odnětí svobody umožňuje přiměřenější přístup společně s několika dalšími podmínkami a zárukami *ex ante* a *ex post*, aby bylo zajištěno dodržování přiměřenosti a práv dotčených osob.

Prahová hodnota by současně neměla snižovat účinnost nástroje a jeho používání v praxi. Členské státy uplatňují různá maxima pro tresty, která souvisejí s jejich vnitrostátním systémem. Vnitrostátní trestní zákoníky se různí a nejsou harmonizovány. Je tomu tak v případě trestných činů a sankcí na ně použitelných. Vnitrostátní procesní zákoníky se liší i z hlediska prahových hodnot pro získání údajů o transakcích nebo obsahu: některé členské státy neurčují žádné konkrétní prahové hodnoty, jiné stanovují seznam trestných činů. Tříletá prahová hodnota omezuje oblast působnosti nástroje na závažnější trestné činy, aniž nadměrně omezuje možnosti jeho využití v praxi. Tato prahová hodnota vylučuje z oblasti působnosti širokou škálu trestných činů v závislosti na trestním zákoníku členského státu (například v některých členských státech podíl na činnosti zločinného spolčení a únosu, ale též takové trestné činy, jako je drobná krádež, podvod a napadení, u nichž může být použití přeshraničního předávacího příkazu žádajícího o citlivější údaje považováno za nepřiměřené). Na druhou stranu zahrnuje tříletá prahová hodnota trestné činy, které vyžadují účinnější přístup, jako je členství ve zločinném spolčení, financování teroristických skupin, podpora nebo propagace zločinného spolčení, teroristický výcvik, některé trestné činy spáchané s teroristickým záměrem a příprava trestného činu s teroristickým záměrem nebo příprava k braní rukojmí, které by jinak byly vyloučeny, pokud by se v závislosti na členském státě uplatňovala vyšší prahová hodnota. Tato prahová hodnota byla zvolena proto, aby u všech členských států byla zajištěna rovnováha mezi efektivností trestních vyšetřování a ochranou práv a přiměřeností. Prahová hodnota má i výhodu v tom, že je snadno použitelná v praxi.

Kromě toho příkazy k předání údajů o transakcích nebo obsahu lze vydat i u specifických harmonizovaných trestných činů vyjmenovaných v ustanovení, pro které budou důkazy zpravidla k dispozici většinou pouze v elektronické formě. To odůvodňuje uplatňování nařízení též v případech, kdy je maximální trest odnětí svobody nižší než výše uvedená prahová hodnota, jinak by tyto trestné činy nemohly být řádně vyšetřeny, což by mohlo vést k beztrestnosti. Trestné činy jsou specifickými ustanoveními: i) rámcového rozhodnutí Rady 2001/413/SVV o potírání podvodů a padělání bezhotovostních platebních prostředků, ii) směrnice 2011/93/EU o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV, a iii) směrnice 2013/40/EU o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV. Příkazy lze vydávat i u trestných činů vyjmenovaných ve směrnici 2017/541/EU o boji proti terorismu, kterou se nahrazuje rámcové rozhodnutí Rady

2002/475/SVV a mění rozhodnutí Rady 2005/671/SVV. Některé z těchto trestných činů mají minimální maximální prahové hodnoty alespoň jeden rok, jiné dva roky, ale žádný nemá maximální prahovou hodnotu nižší než jeden rok.

Článek též stanoví povinné informace, které musí evropský předávací příkaz obsahovat, aby poskytovatel služeb mohl požadované údaje identifikovat a předat. Součástí evropského předávacího příkazu je i odůvodnění s vysvětlením nezbytnosti a přiměřenosti tohoto opatření.

Evropský předávací příkaz se provádí vydáním certifikátu evropského předávacího příkazu (EPOC) (viz článek 8), který je přeložen a zaslán poskytovateli služeb. EPOC obsahuje stejné povinné informace jako příkaz, kromě důvodů pro nezbytnost a přiměřenost opatření nebo dalších podrobností o případu.

V situacích, kdy jsou žádané údaje uloženy nebo zpracovány jako součást infrastruktury poskytované společnosti poskytovatelem služeb, zpravidla v případě hostingových nebo softwarových služeb, by měla být prvotním adresátem žádosti vyšetřovacích orgánů sama společnost. To může vyžadovat evropský vyšetřovací příkaz nebo postup vzájemné právní pomoci, pokud by společnost nebyla poskytovatelem služeb zahrnutým do oblasti působnosti tohoto nařízení. Poskytovateli služeb může být evropský předávací příkaz adresován pouze v případě, kdy by nebylo vhodné adresovat žádost společnosti, zejména pokud by to ohrozilo vyšetřování, například v případech, kdy je vyšetřována sama společnost.

Před vydáním evropského předávacího příkazu musí vydávající orgán též zohlednit potenciální imunity a výsady podle práva členského státu poskytovatele služeb nebo jakýkoli dopad na základní zájmy tohoto členského státu, jako je národní bezpečnost a obrana. Cílem tohoto ustanovení je zajistit, aby ve vydávajícím státě byly brány v úvahu imunity a výsady, které chrání žádané údaje v členském státě poskytovatele služeb, zejména pokud poskytují vyšší ochranu než právo vydávajícího státu.

Článek 6: Podmínky pro vydání evropského uchovávacího příkazu

Na evropský uchovávací příkaz se vztahují obdobné podmínky jako na evropský předávací příkaz. Lze ho vydat u jakéhokoli trestného činu v souladu s ostatními podmínkami podle článku 6. Jeho cílem je zabránit odstranění, smazání nebo změně příslušných údajů v situacích, kdy může dosažení předání těchto údajů trvat déle, například proto, že budou použity kanály justiční spolupráce. Například vzhledem k tomu, že evropský vyšetřovací příkaz může být obecně vydán u jakéhokoli trestného činu bez jeho omezení na jakékoli prahové hodnoty, není omezen ani evropský uchovávací příkaz. Jinak by tento nástroj nebyl účinný. Aby vyšetřovací orgány mohly jednat rychle, a vzhledem k tomu, že následující žádostí bude příslušná žádost o předání údajů, v níž budou opět ověřeny všechny podmínky, může evropské uchovávací příkazy vydávat nebo potvrzovat i státní zástupce.

Článek 7: Adresát evropského předávacího příkazu nebo evropského uchovávacího příkazu

Evropské předávací příkazy a evropské uchovávací příkazy by měly být adresovány právnímu zástupci ustanovenému poskytovatelem služeb za účelem shromažďování důkazů v trestním řízení v souladu se směrnicí, kterou se stanoví harmonizovaná pravidla pro jmenování právních zástupců za účelem shromažďování důkazů v trestním řízení. Jejich předání bude v podobě certifikátu evropského předávacího příkazu (dále jen „EPOC“) nebo certifikátu evropského uchovávacího příkazu (dále jen „EPOC-PR“) podle článku 8. Tento právní

zástupce bude odpovědný za jejich přijetí a včasné a úplné provedení. Poskytovatelé služeb si tak mohou vybrat, jak se zorganizují, aby údaje nařízené orgány členského státu předaly.

Nebyl-li jmenován žádný právní zástupce, mohou být příkazy adresovány jakékoli provozovně poskytovatele služeb v Unii. Tato záložní možnost má zajistit účinnost systému v případě, že poskytovatel služeb (dosud) nejmenoval zvláštního zástupce, například pokud v souladu se směrnicí není povinen jmenovat právního zástupce, protože poskytovatelé služeb jsou usazeni a působí pouze v jednom členském státě, nebo v případech, kdy povinnost jmenovat právního zástupce ještě není v platnosti, před lhůtou k provedení směrnice.

V případě neplnění ze strany právního zástupce, nastávají dvě situace, kdy se vydávající orgán může obrátit na kteroukoli provozovnu poskytovatele služeb v Unii: v naléhavých případech uvedených v čl. 9 odst. 2 a v případech, kdy právní zástupce neplní své povinnosti podle článků 9 a 10 a kdy se vydávající orgán domnívá, že existují zjevná rizika ztráty údajů.

Článek 8: Certifikát evropského předávacího a uchovávacího příkazu

Certifikáty EPOC a EPOC-PR slouží k předávání příkazů adresátovi definovanému v článku 7. Vzory obou certifikátů jsou stanoveny v příloze I a II nařízení; musí být přeloženy do jednoho z úředních jazyků členského státu, kde se nachází adresát. Poskytovatel služeb může prohlásit, že příkazy budou akceptovány též v jiných úředních jazycích Unie. Cílem certifikátů je poskytnout adresátovi všechny nezbytné informace ve standardizovaném formátu, který minimalizuje příčiny chyb, umožňuje snadnou identifikaci údajů a co nejvíce vyhýbá se volnému textu, což snižuje náklady na překlad. Úplné odůvodnění s důvody pro nezbytnost a přiměřenost nebo další podrobnosti o případu se do certifikátu neuvádějí, aby nedošlo k ohrožení vyšetřování. Bude je třeba uvést až na samotném příkazu, aby bylo později podezřelé osobě umožněno napadnout je během trestního řízení.

Někteří poskytovatelé služeb již zavedly platformy k podávání žádostí ze strany orgánů činných v trestním řízení. Nařízení používání těchto platform nebrání, jelikož nabízí mnoho výhod, včetně možnosti snadné autentizace a bezpečného přenosu údajů. Tyto platformy však musí umožňovat podávání certifikátů EPOC a EPOC-PR ve formátu stanoveném v přílohách I a II, bez nutnosti žádat o dodatečné údaje ohledně příkazu.

Také platformy zavedené členskými státy nebo institucemi Unie mohou představovat bezpečný prostředek přenosu a usnadňovat autentizaci příkazů a sběr statistik. Zváženo by mělo být i případné rozšíření platform eCodex a SIRIUS o bezpečné připojení s poskytovateli služeb pro účely přenosu certifikátů EPOC a EPOC-PR a případně odpovědi poskytovatelů služeb.

Článek 9: Provedení certifikátu EPOC

Článek 9 stanoví povinnost adresátů odpovídat na certifikáty EPOC a zavádí povinné lhůty. Obvyklá lhůta činí deset dnů, přičemž orgány mohou v odůvodněných případech stanovit kratší lhůtu. V naléhavých případech, definovaných jako situace, kdy je bezprostředně ohrožen život nebo tělesná integrita osoby nebo je bezprostředně ohrožena kritická infrastruktura, činí lhůta šest hodin.

Ustanovení zajišťuje též možnost dialogu mezi adresátem a vydávajícím orgánem. Pokud je certifikát EPOC neúplný, očividně nesprávný nebo neobsahuje dostatečné informace, aby poskytovatel služeb mohl EPOC provést, kontaktuje adresát vydávající orgán a požádá o objasnění, přičemž použije formulář uvedený v příloze III. Adresát vydávající orgán

informuje též v případech, kdy údaje nemůže poskytnout z důvodu vyšší moci nebo faktické nemožnosti. To se stává například tehdy, kdy osoba, jejíž údaje jsou požadovány, nebyla zákazníkem této služby, nebo kdy – například v rámci jiných povinností zachovávat soukromí – poskytovatel služeb údaje ze zákona smazal předtím, než on nebo jeho právní zástupce obdrželi příkaz. Vydávající orgán by si musel být těchto okolností vědom, aby reagoval rychle, aby například získal elektronické důkazy od jiného poskytovatele služeb a aby ne zahájil vymáhací postup, pokud by to nemělo žádný smysl.

Pokud adresát neposkytne žádné informace nebo je neposkytne vyčerpávajícím způsobem či včas z jiných důvodů, než jsou důvody uvedené výše, musí vydávající orgán informovat o důvodech ve formuláři uvedeném v příloze III. Adresáti tedy mohou před vydávajícím orgánem vznést jakoukoli otázku související s prováděním certifikátu EPOC. Vydávající orgán tak může opravit nebo znovu zvážit EPOC v rané fázi před fází vymáhání.

Pokud nejsou údaje předány okamžitě, zejména v případech, kdy je zahájen dialog mezi adresátem a vydávajícím orgánem, což znamená, že lhůty podle čl. 9 odst. 1 nebudou dodrženy, má poskytovatel služeb po obdržení certifikátu EPOC povinnost údaje, pokud je lze identifikovat, uchovat, aby předešel jejich ztrátě. Uchování se může týkat objasněného certifikátu EPOC nebo následné žádosti v rámci vzájemné právní pomoci nebo evropského vyšetřovacího příkazu, která bude zaslána místo původního certifikátu EPOC.

Článek 10: Provedení certifikátu EPOC-PR

Provedení certifikátu EPOC-PR požaduje uchování údajů dostupných v době obdržení příkazu. Poskytovatelé služeb by měli uchovat údaje tak dlouho, jak to bude nezbytné k předání požadovaných údajů, pokud vydávající orgán do 60 dnů po vydání příkazu potvrdí, že vydal následnou žádost o předání. To vyžaduje, aby byly podniknuty alespoň některé formální kroky, například zaslání žádosti o překlad v rámci vzájemné právní pomoci.

Na druhou stranu by žádosti o uchování měly být podávány nebo udržovány tak dlouho, jak to bude nezbytné k umožnění následné žádosti o předání těchto údajů. Aby se předešlo zbytečnému nebo nadměrně dlouhému uložení, informuje orgán, který vydal evropský uchovávací příkaz, adresáta, jakmile se rozhodne o nevydání předávacího příkazu nebo žádosti o justiční spolupráci nebo o jejich stažení.

Toto ustanovení zajišťuje též možnost dialogu mezi adresátem a vydávajícím orgánem, podobnou ustanovením článku 9. Pokud je certifikát EPOC-PR neúplný, očividně nesprávný nebo neobsahuje dostatečné informace, aby poskytovatel služeb mohl EPOC-PR provést, kontaktuje adresát vydávající orgán a požádá o objasnění, přičemž použije formulář uvedený v příloze III. Adresát vydávající orgán informuje též v případech, kdy údaje nemůže poskytnout z důvodu okolností, které jsou pokládány za vyšší moc nebo faktickou nemožnost, nebo z jiných důvodů.

Článek 11: Důvěrnost a informace o uživateli

Důvěrnost probíhajícího vyšetřování, včetně skutečnosti, že byl vydán příkaz k získání příslušných údajů, musí být chráněna. Tento článek je inspirován článkem 19 směrnice o evropském vyšetřovacím příkazu. Stanoví povinnost adresáta, a nejsou-li totožní, poskytovatele služeb zachovat důvěrnost certifikátu EPOC nebo EPOC-PR, zejména tím, že v souladu s článkem 23 nařízení obecného nařízení o ochraně osobních údajů neinformuje osobu, jejíž údaje vydávající orgán žádá, aby bylo chráněno vyšetřování trestných činů.

Na druhé straně je důležité, i pro uplatnění právních prostředků, aby osoba, jejíž údaje byly žádány, byla informována. Pokud tak neučiní poskytovatel služeb na žádost vydávajícího orgánu, informuje vydávající orgán danou osobu v souladu s článkem 13 směrnice o ochraně údajů při vymáhání práva, jakmile pomine riziko ohrožení vyšetřování, a zahrne informace o dostupných právních prostředcích. Z důvodu menšího zásahu do dotčených práv nejsou takové informace poskytovány v případě evropského uchovávacího příkazu, nýbrž pouze v případě evropských předávacích příkazů.

Článek 12: Náhrada nákladů

Pokud tak vnitrostátní právo vydávajícího státu stanoví pro vnitrostátní příkazy v obdobných vnitrostátních případech, mohou poskytovatelé služeb požádat o náhradu svých nákladů vydávajícím státem v souladu s vnitrostátním právem vydávajícího státu. To zajišťuje rovné zacházení s poskytovateli služeb, jimž je adresován vnitrostátní příkaz, a s poskytovateli služeb, jimž je adresován certifikát EPOC stejným členským státem, pokud se tento členský stát rozhodl nahradit náklady některým poskytovatelům služeb. Na druhou stranu navrhované nařízení neharmonizuje náhradu nákladů, jelikož členské státy mají v tomto ohledu různé preference.

O náhradu nákladů může požádat buď přímo poskytovatel služeb, nebo jeho právní zástupce. Náklady mohou být nahrazeny pouze jednou.

Kapitola 3: Sankce a vymáhání

Článek 13: Sankce

Členské státy zajistí, aby byly dostupné účinné, přiměřené a odrazující peněžité pokuty pro případ, že poskytovatelé služeb nesplní své závazky podle článků 9, 10 nebo 11. Tím nejsou dotčeny vnitrostátní právní předpisy pro ukládání trestních sankcí pro takové situace.

Článek 14: Vymáhací postup

Článek 14 stanoví postup pro vymáhání příkazů v případě neplnění s pomocí členského státu, v němž se nachází adresát předávaného certifikátu. Podle toho, kdo je počátečním adresátem, je to buď členský stát poskytovatele služeb, nebo členský stát právního zástupce. Vydávající orgán předává celý příkaz včetně odůvodnění nezbytnosti a přiměřenosti, provázený certifikátem, příslušnému orgánu ve vymáhajícím státě, který ho vymáhá v souladu se svým vnitrostátním právem a v případě potřeby pomocí sankcí uvedených v článku 13. Je-li příkaz předán k vymáhání vymáhajícímu státu, může vymáhající orgán rozhodnout, že příkaz neuzná a nebude vymáhat, pokud se při obdržení domnívá, že je použitelný jeden z omezených důvodů pro odpor, a po konzultaci s vydávajícím orgánem. Navíc pokud by byl zahájen vymáhací postup, bude před vymáhajícím orgánem moci podat odpor proti příkazu sám adresát. Adresát tak může učinit na základě jakéhokoli z takových důvodů, vyjma imunit a výsad, ale včetně případů, kdy je zjevné, že příkaz nevydal nebo nepotvrdil příslušný orgán nebo že by splnění očividně porušilo Listinu základních práv Evropské unie nebo by bylo očividně nepatřičné. Například příkaz požadující předání údajů o obsahu týkajících se nedefinované třídy osob v zeměpisné oblasti nebo bez vazby na konkrétní trestní řízení by očividně ignoroval podmínky pro vydání evropského předávacího příkazu stanovené v tomto nařízení a byl by zjevný již z obsahu samotného certifikátu. Další důvody může uplatnit pouze osoba, jejíž údaje jsou žádány, v rámci právních prostředků ve vydávajícím státě (viz článek 17 níže). Poskytovatelé služeb mají navíc k dispozici právní prostředek proti rozhodnutí vymáhajícího orgánu o uložení pokuty.

Vymáhací postup obsahuje několik lhůt pro vymáhající a vydávající orgán, aby se předešlo dalšímu prodloužení během tohoto postupu.

Kapitola 4: Opravné prostředky

Články 15 a 16: Přezkumné řízení v případě rozporných povinností vyplývajících z práva třetí země

Články 15 a 16 stanoví přezkumné řízení v případě, že poskytovatelé služeb, kteří mají ústředí v třetích zemích, čelí rozporným povinnostem. Tato ustanovení mají též velký význam, pokud jde o ochranu individuálních práv a mezinárodní zdvořilost. Svým vysokým standardem se snaží vést třetí země k tomu, aby podobnou úroveň ochrany zajistily i ony. V opačné situaci, kdy se orgány třetí země snaží získat údaje o občanovi EU od poskytovatele služeb v EU, mohou takovému sdělení podobně zabránit právní předpisy Unie nebo členských států chránící základní práva, např. *acquis* o ochraně údajů. Evropská unie očekává, že třetí země budou takové zákazy respektovat stejně jako tento návrh.

Postup v článku 15 může adresát iniciovat, pokud by plnění evropského předávacího příkazu způsobilo porušení právního předpisu či předpisů třetí země, která zakazuje sdělování údajů z těchto důvodů, že je to nezbytné buď pro ochranu základních práv dotčených fyzických osob, nebo pro ochranu základních zájmů třetí země v souvislosti s národní bezpečností nebo obranou. Adresát musí vydávající orgán odůvodněnou námitkou informovat o důvodech svého závěru, že existují rozporné povinnosti. Taková odůvodněná námitka se nemůže opírat o pouhou skutečnost, že obdobná ustanovení v právu třetí země neexistují, ani o samotnou okolnost, že údaje jsou uloženy v třetí zemi. Odůvodněná námitka musí být podána postupem podle čl. 9 odst. 5 pro oznámení záměru nesplnit příkaz a prostřednictvím formuláře uvedeného v příloze III.

Na základě této odůvodněné námitky provede vydávající orgán přezkum svého vlastního příkazu. Pokud se vydávající orgán rozhodne, že příkaz stáhne, postup skončí. Pokud chce vydávající orgán potvrdit oprávněnost příkazu, je případ předán příslušnému soudu jeho členského státu. Soud poté na základě odůvodněné námitky a s přihlédnutím ke všem relevantním skutečnostem případu posoudí, zda se na daný konkrétní případ uplatňuje právo třetí země a – pokud se uplatňuje – zda v daném konkrétním případě dochází ke kolizi. Při provádění tohoto posouzení by měl soud vzít v úvahu, zda právo třetí země místo toho, aby chránilo základní práva nebo základní zájmy třetí země související s národní bezpečností nebo obranou, se očividně snaží chránit jiné zájmy nebo je zaměřeno na ochranu nezákonných činností před žádostmi donucovacích orgánů v kontextu trestního vyšetřování.

Rozhodne-li soud, že opravdu existuje rozpor s povinnostmi vyplývajících z právních předpisů chránících základní práva fyzických osob nebo základní zájmy třetí země související s národní bezpečností nebo obranou, musí prostřednictvím vnitrostátních ústředních orgánů příslušné třetí země požádat o stanovisko této země. Pokud konzultovaná třetí země potvrdí existenci rozporu a protestuje proti výkonu příkazu, musí soud příkaz stáhnout.

Vznikne-li rozpor na základě jiných právních předpisů třetí země, které neslouží k ochraně základních práv fyzických osob nebo základních zájmů třetí země souvisejících s národní bezpečností nebo obranou, rozhodne se soud na základě vyvážení zájmů, zda oprávněnost příkazu potvrdí.

Podmínky stanovené v článku 9, zejména povinnosti uchovat popsané v čl. 9 odst. 6, jsou též použitelné v situacích, kdy se vyskytují rozporné povinnosti vyplývající z práva třetí země. Určí-li soud, že příkaz je oprávněný, jsou vydávající orgán a poskytovatel služeb informováni ohledně přistoupení k jeho výkonu. Je-li příkaz zrušen, může být vydán samostatný evropský

uchovávací příkaz, aby byla zajištěna dostupnost údajů tam, kde by mohly být získány prostřednictvím žádosti o vzájemnou právní pomoc.

Vzhledem k tomu, že výsledkem samotného evropského uchovávacího příkazu není sdělení údajů, a tudíž podobné obavy nevyvolává, je přezkumné řízení omezeno na evropský předávací příkaz.

Článek 17: Účinná právní ochrana

Toto ustanovení zajišťuje, aby osoby dotčené evropským předávacím příkazem měly k dispozici účinnou právní ochranu. Tyto opravné prostředky jsou uplatňovány ve vydávajícím státě v souladu s vnitrostátním právem. V případě podezřelých a obviněných osob jsou opravné prostředky zpravidla uplatňovány během trestního řízení. Pro evropský uchovávací příkaz, který sám o sobě nepovoluje sdělování údajů, nejsou k dispozici žádné konkrétní opravné prostředky mimo případů, kdy po něm následují evropský předávací příkaz nebo jiný nástroj vedoucí ke sdělení údajů, které pak vedou ke konkrétním opravným prostředkům.

Na právní prostředek ve vydávajícím státě mají též právo osoby, jejichž údaje byly žádány a které nejsou podezřelé nebo obviněné v trestním řízení. Žádným z těchto práv nejsou dotčeny opravné prostředky podle směrnice o ochraně údajů při vymáhání práva a obecného nařízení o ochraně osobních údajů.

Na rozdíl od toho, co je stanoveno pro poskytovatele služeb, neomezuje nařízení možné důvody pro všechny tyto osoby k napadení zákonnosti příkazu. K těmto důvodům patří nezbytnost a přiměřenost příkazu.

Uplatnění opravných prostředků ve vydávajícím státě nezatěžuje dotčené osoby nepřiměřeným způsobem. Stejně jako v případě příkazů, které jsou vymáhány prostřednictvím jiných forem justiční spolupráce, mají soudy ve vydávajícím státě nejlepší podmínky k přezkumu zákonnosti evropských předávacích příkazů, které vydaly jejich vlastní orgány, a k posouzení slučitelnosti s jejich vlastním vnitrostátním právem. Během fáze vymáhání mohou navíc adresáti samostatně podat odpor proti vymáhání certifikátů EPOC nebo EPOC-PR v jejich hostitelském členském státě na základě seznamu důvodů vyjmenovaných v nařízení (viz článek 14 výše).

Článek 18: Zajištění výsad a imunit podle práva přijímajícího státu

Toto ustanovení má stejný cíl jako čl. 5 odst. 7, a to zajistit, aby ve vydávajícím státě byly brány v potaz imunity a výsady, které chrání žádané údaje v členském státě poskytovatele služeb, zejména pokud jsou mezi těmito členskými státy rozdíly, jakož i základní zájmy tohoto členského státu, jako je národní bezpečnost a obrana. Článek 18 stanoví, že soud ve vydávajícím státě je musí vzít v úvahu, jako kdyby byly stanoveny podle jeho vnitrostátního práva. Z důvodu rozdílů mezi členskými státy při posuzování relevantnosti a přípustnosti důkazů dává ustanovení soudům určitou flexibilitu, pokud jde o způsob, jak je brát v úvahu.

Kapitola 5: Závěrečná ustanovení

Článek 19: Monitorování a podávání zpráv

Tento článek po členských státech požaduje, aby hlásily konkrétní informace týkající se uplatňování nařízení s cílem pomoci Komisi při plnění jejích povinností podle článku 24.

Komise zavede podrobný program pro monitorování výstupů, výsledků a dopadů tohoto nařízení.

Článek 20: Změny certifikátů a formulářů

Certifikáty a formuláře obsažené v přílohách I, II a III tohoto návrhu usnadní provádění certifikátu EPOC a EPOC-PR. Z tohoto důvodu je nutné, aby v budoucnosti bylo možné řešit případnou potřebu zlepšit obsah certifikátu a formuláře co nejrychleji. Změna těchto tří příloh řádným legislativním postupem neodpovídá tomuto požadavku a přílohy tvoří zásadní prvky legislativních aktů, přičemž hlavní prvky jsou definovány v článku 8. Rychlejší a flexibilnější postup pro změny prostřednictvím aktů v přenesené pravomoci je tudíž stanoven v článku 20.

Článek 21: Výkon přenesené pravomoci

Tento článek stanovuje podmínky, za kterých má Komise pravomoc přijmout akty v přenesené pravomoci, aby stanovila nezbytné změny certifikátu a formulářů v přílohách návrhu. Stanovuje standardní postup pro přijetí takových aktů v přenesené pravomoci.

Článek 22: Oznámení

Členské státy jsou povinny oznámit Komisi, kdo jsou příslušné vydávající a vymáhající orgány a které soudy jsou příslušné, pokud jde o vyřizování odůvodněných námitek poskytovatelů služeb v případě kolize norem.

Článek 23: Vztah k evropským vyšetřovacím příkazům

Toto ustanovení objasňuje, že nařízení nebrání orgánům členských států vydávat evropské vyšetřovací příkazy v souladu se směrnicí 2014/41/EU za účelem získání elektronických důkazů.

Článek 24: Hodnocení

Toto ustanovení stanoví, že Komise provádí hodnocení tohoto nařízení v souladu s pokyny Komise ke zlepšování právní úpravy a podle bodu 22 interinstitucionální dohody ze dne 13. dubna 2016²⁵. Komise pět let po vstupu navrhovaného nařízení v platnost předloží Evropskému parlamentu a Radě zprávu o zjištěních hodnocení, včetně posouzení potřeby rozšířit oblast působnosti nařízení na služby, které do něj ještě nejsou zahrnuty, které se však mohou stát relevantnějšími pro vyšetřování.

Článek 25: Vstup v platnost

Navrhované nařízení vstoupí v platnost dvacátým dnem po vyhlášení v *Úředním věstníku*. Nařízení se použije po uplynutí šesti měsíců od jeho vstupu v platnost.

²⁵ Interinstitucionální dohoda mezi Evropským parlamentem, Radou Evropské unie a Evropskou komisí o zdokonalení tvorby právních předpisů ze dne 13. dubna 2016; Úř. věst. L 123, 12.5.2016, s. 1.

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY**o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech**

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na čl. 82 odst. 1 této smlouvy,

s ohledem na návrh Evropské komise,

po postoupení návrhu legislativního aktu vnitrostátním parlamentům,

s ohledem na stanovisko Evropského hospodářského a sociálního výboru²⁶,

v souladu s řádným legislativním postupem,

vzhledem k těmto důvodům:

- (1) Unie si stanovila za cíl udržovat a rozvíjet prostor svobody, bezpečnosti a práva. Pro postupné vytváření takového prostoru má Unie přijmout opatření týkající se justiční spolupráce v trestních věcech na základě zásady vzájemného uznávání rozsudků a soudních rozhodnutí, které je od zasedání Evropské rady v Tampere ve dnech 15. a 16. října 1999 obvykle označováno za základní kámen justiční spolupráce v trestních věcech v Unii.
- (2) Opatření k získání a uchování elektronických důkazů jsou stále důležitější proto, aby umožnila trestní vyšetřování a stíhání napříč Uníí. Pro boj proti trestné činnosti jsou zásadní účinné mechanismy k získávání elektronických důkazů, s výhradou podmínek, které mají zajistit plný soulad se základními právy a zásadami uznanými v Listině základních práv Evropské unie tak, jak jsou zakotveny ve Smlouvách, zejména pak zásadami nezbytnosti a přiměřenosti, spravedlivého procesu, ochrany údajů, listovního tajemství a soukromí.
- (3) Dne 22. března 2016 zdůraznilo společné prohlášení ministrů spravedlnosti a vnitra a zástupců orgánů Unie o teroristických útocích v Bruselu, že je třeba prioritně nalézt způsoby k rychlejšímu a efektivnějšímu zajištění a získávání elektronických důkazů a vymezit konkrétní opatření pro řešení této otázky.
- (4) Závěry Rady ze dne 9. června 2016 podtrhly rostoucí důležitost elektronických důkazů v trestních řízeních a ochrany kyberprostoru před zneužíváním a trestnou činností ve prospěch ekonomik a společností, a tudíž potřebu, aby justiční orgány a donucovací orgány měly účinné nástroje k vyšetřování a stíhání trestných činů týkajících se kyberprostoru.
- (5) Ve společném sdělení Odolnost, odrazování a obrana ze dne 13. září 2017²⁷ Komise zdůraznila, že klíčovým odrazujícím prvkem, pokud jde o kybernetické útoky, je

²⁶ Úř. věst. C , , s. .

²⁷ JOIN(2017) 450 final.

účinné vyšetřování a stíhání trestné činnosti související s kyberprostorem a že současný procedurální rámec se musí lépe přizpůsobit internetovému věku. Současné postupy se mnohdy nedokázaly vyrovnat rychlosti kybernetických útoků, které zejména vytvářejí potřebu rychle spolupracovat přes hranice.

- (6) Evropský parlament zopakoval tyto obavy ve svém usnesení o boji proti kyberkriminalitě ze dne 3. října 2017²⁸, přičemž zdůraznil problémy, které současný roztržštěný právní rámec může způsobovat poskytovatelům služeb, kteří se snaží vyhovět žádostem donucovacích orgánů, a vyzval Komisi k zavedení unijního právního rámce pro elektronické důkazy s dostatečnými zárukami práv a svobod pro všechny zúčastněné.
- (7) Síťové služby mohou být poskytovány odkudkoli a nevyžadují fyzickou infrastrukturu, prostory ani zaměstnance v příslušné zemi. V důsledku toho se příslušné důkazy často uchovávají mimo území vyšetřujícího státu nebo jsou uchovávány poskytovatelem služeb sídlícím mimo tento stát. Často neexistuje žádné jiné spojení mezi vyšetřovaným případem v dotčeném státě a státem, kde se nachází místo uložení nebo kde má hlavní provozovnu poskytovatel služeb.
- (8) Z důvodu absence tohoto spojení jsou žádosti o justiční spolupráci často adresovány státům, které jsou hostiteli velkého počtu poskytovatelů služeb, které však nemají k danému případu žádný jiný vztah. Počet žádostí se též znásobil vzhledem ke stále více využívaným síťovým službám, které jsou svou povahou bez hranic. V důsledku toho trvá získání elektronických důkazů pomocí kanálů justiční spolupráce často dlouho – déle, než jak dlouho mohou být k dispozici následná vodítka. Kromě toho neexistuje žádný jasný rámec pro spolupráci s poskytovateli služeb, ačkoli někteří poskytovatelé z třetích zemí přijímají přímé žádosti o neobsahové údaje tak, jak povoluje jejich příslušné vnitrostátní právo. V důsledku toho se všechny členské státy spoléhají na spolupráci s poskytovateli služeb, je-li k dispozici, s využitím různých vnitrostátních nástrojů, podmínek a postupů. Navíc pokud jde o údaje o obsahu, podnikají některé členské státy jednostranné kroky, zatímco jiné se i nadále spoléhají na justiční spolupráci.
- (9) Roztržštěný právní rámec způsobuje problémy poskytovatelům služeb, kteří se snaží vyhovět žádostem donucovacích orgánů. Je tudíž zapotřebí zřídit evropský právní rámec pro elektronické důkazy, který poskytovatelům služeb v působnosti tohoto nástroje uloží povinnost odpovídat přímo orgánům bez účasti justičního orgánu v členském státě poskytovatele služeb.
- (10) Příkazy podle tohoto nařízení by měly být adresovány právním zástupcům poskytovatelů služeb ustanoveným pro tento účel. Neustanovil-li poskytovatel služeb usazený v Unii právního zástupce, mohou být příkazy adresovány jakékoli provozovně tohoto poskytovatele služeb v Unii. Tato záložní možnost má zajistit účinnost systému v případě, že poskytovatel služeb (dosud) nejmenoval zvláštního zástupce.
- (11) Mechanismus evropského předávacího příkazu a evropského uchovávacího příkazu pro elektronické důkazy v trestních věcech může fungovat pouze na základě vysoké míry vzájemné důvěry mezi členskými státy, což je zásadní předpoklad řádného fungování tohoto nástroje.
- (12) Toto nařízení respektuje základní práva a dodržuje zásady uznané zejména Listinou základních práv Evropské unie. Patří k nim právo na svobodu a bezpečnost,

28

2017/2068(INI).

respektování soukromého a rodinného života, ochranu osobních údajů, svobodu podnikání, právo na majetek, právo na účinnou právní ochranu a spravedlivý proces, presumpce nevinny a právo na obhajobu, zásady zákonnosti a přiměřenosti, jakož i právo nebýt souzen nebo potrestán dvakrát v trestních řízeních ze stejný trestný čin. Má-li vydávající členský stát náznaky toho, že by v jiném členském státě mohlo probíhat souběžné trestní řízení, konzultuje orgány tohoto členského státu v souladu s rámcovým rozhodnutím Rady 2009/948/SVV²⁹.

- (13) Aby bylo zaručeno plné dodržování základních práv, odkazuje toto nařízení výslovně na nezbytné normy týkající se získávání jakýchkoli osobních údajů, zpracování takových údajů, soudního přezkumu použití vyšetřovacího opatření stanoveného tímto nástrojem a dostupné opravné prostředky.
- (14) Použitím tohoto nařízení by neměla být dotčena procesní práva v trestním řízení stanovená ve směrnici Evropského parlamentu a Rady 2010/64/EU³⁰, 2012/13/EU³¹, 2013/48/EU³², 2016/343³³, 2016/800³⁴ a 2016/1919³⁵.
- (15) Tento nástroj stanoví pravidla, podle kterých smí příslušný justiční orgán v Evropské unii nařídit prostřednictvím evropského předávacího nebo uchovávacího příkazu poskytovateli služeb nabízejícímu služby v Unii, aby předal nebo uchoval elektronické důkazy. Toto nařízení je použitelné ve všech případech, kdy je poskytovatel služeb usazen nebo zastoupen v jiném členském státě. Pro případ vnitrostátních situací, kdy nástroje stanovené tímto nařízením nemohou být použity, by nařízení nemělo omezovat pravomoci vnitrostátních příslušných orgánů již stanovené vnitrostátním právem, které nutí poskytovatele služeb usazené nebo zastoupené na jejich území k plnění jejich povinností.
- (16) Poskytovateli služeb, kteří jsou nejrelevantnější pro trestní řízení, jsou poskytovatelé služeb elektronické komunikace a konkrétní poskytovatelé služeb informační společnosti, které usnadňují interakci mezi uživateli. Toto nařízení by se tudíž mělo vztahovat na obě skupiny. Poskytovatelé služeb elektronické komunikace jsou definováni v návrhu směrnice, kterou se zřizuje evropský kodex pro elektronické komunikace. Patří mezi ně i interpersonální komunikace, jako např. funkce voice-over-IP, výměna rychlých zpráv (instant messaging) a e-mailové služby. Kategorie

²⁹ [Rámcové rozhodnutí Rady 2009/948/SVV](#) ze dne 30. listopadu 2009 o předcházení kompetenčním sporům při výkonu pravomoci v trestním řízení a jejich řešení (Úř. věst. L 328, 15.12.2009, s. 42).

³⁰ [Směrnice Evropského parlamentu a Rady 2010/64/EU](#) ze dne 20. října 2010 o právu na tlumočení a překlad v trestním řízení (Úř. věst. L 280, 26.10.2010, s. 1).

³¹ [Směrnice Evropského parlamentu a Rady 2012/13/EU](#) ze dne 22. května 2012 o právu na informace v trestním řízení (Úř. věst. L 142, 1.6.2012, s. 1).

³² [Směrnice Evropského parlamentu a Rady 2013/48/EU](#) ze dne 22. října 2013 o právu na přístup k obhájci v trestním řízení a řízení týkajícím se evropského zatýkacího rozkazu a o právu na informování třetí strany a právu na komunikaci s třetími osobami a konzulárními úřady v případě zbavení osobní svobody (Úř. věst. L 294, 6.11.2013, s. 1).

³³ [Směrnice Evropského parlamentu a Rady \(EU\) 2016/343](#) ze dne 9. března 2016, kterou se posilují některé aspekty presumpce nevinny a právo být přítomen při trestním řízení před soudem (Úř. věst. L 65, 11.3.2016, s. 1).

³⁴ [Směrnice Evropského parlamentu a Rady \(EU\) 2016/800](#) ze dne 11. května 2016 o procesních zárukách pro děti, které jsou podezřelými nebo obviněnými osobami v trestním řízení (Úř. věst. L 132, 21.5.2016, s. 1).

³⁵ [Směrnice Evropského parlamentu a Rady \(EU\) 2016/1919](#) ze dne 26. října 2016 o právní pomoci pro podezřelé nebo obviněné osoby v trestním řízení a pro osoby vyžádané v rámci řízení týkajícího se evropského zatýkacího rozkazu (Úř. věst. L 297, 4.11.2016, s. 1).

služeb informační společnosti zde zahrnuté jsou ty, pro které je určující složkou služby poskytované uživateli uchovávání údajů, a odkazují zejména na sociální sítě, nakolik je nelze kvalifikovat jako služby elektronické komunikace, internetová tržiště umožňující transakce mezi jejich uživateli (např. spotřebiteli nebo podniky) a jiné poskytovatele hostingových služeb včetně případů, kdy je služba poskytována přes cloud. Služby informační společnosti, pro které uchovávání údajů není určující složkou služby poskytované uživateli a pro které má pouze doplňkový charakter, jako jsou právní, architektonické, inženýrské a účetní služby poskytované on-line na dálku, by měly být z oblasti působnosti tohoto nařízení vyloučeny, i když mohou spadat do definice služeb informační společnosti podle směrnice (EU) 2015/1535.

- (17) V mnoha případech se údaje již neuchovávají nebo nezpracovávají v zařízení uživatele, ale jsou zpřístupněny v cloudové infrastruktuře pro přístup odkudkoli. Aby poskytovatelé služeb mohli tyto služby provozovat, nemusí být usazeni nebo mít servery v konkrétní jurisdikci. Uplatňování tohoto nařízení by tudíž nemělo záviset na skutečném umístění provozovny poskytovatele nebo zařízení ke zpracování či uchovávání údajů.
- (18) Pokud jde o identifikaci aktérů ukrytých za zákeřnými nebo zkompromitovanými webovými stránkami, mají zvláštní význam poskytovatelé služeb internetové infrastruktury související s přidělováním názvů a čísel, jako jsou registrátoři a registry názvů domén a poskytovatelé služeb zajištění soukromí a proxy serverů nebo regionální internetové registry adres internetových protokolů (dále jen „IP“). Ti mají údaje, které mají obzvláštní význam pro trestní řízení, jelikož mohou umožnit identifikaci fyzické či právnické osoby ukryté za webovou stránkou používanou při trestné činnosti nebo identifikaci oběti trestné činnosti v případě zkompromitované webové stránky, která byla napadena pachateli trestné činnosti.
- (19) Toto nařízení upravuje pouze shromažďování uložených údajů, to znamená údaje, které drží poskytovatel služeb v době obdržení evropského předávacího nebo uchovávacího certifikátu. Nestanovuje obecnou povinnost uchovávat údaje, ani neopravňuje k odposlouchávání údajů či k získávání údajů uložených až po obdržení certifikátu předávacího nebo uchovávacího příkazu. Údaje by měly být poskytnuty bez ohledu na to, zda jsou zašifrované či nikoli.
- (20) Mezi kategorie údajů, které toto nařízení zahrnuje, patří údaje o účastníkovi, údaje o přístupu, údaje o transakcích (tyto tři kategorie jsou označovány jako „neobsahové údaje“) a údaje o obsahu. Toto rozdělení, kromě údajů o přístupu, existuje v právních předpisech mnoha členských států a též v současném právním rámci USA, který umožňuje poskytovatelům služeb dobrovolné sdílení neobsahových údajů se zahraničními donucovacími orgány.
- (21) Je vhodné vyčlenit údaje o přístupu jako zvláštní kategorii údajů použitou v tomto nařízení. Údaje o přístupu jsou využívány pro též cíl jako údaje o účastníkovi, jinými slovy k identifikaci konkrétního uživatele, a míra narušování základních práv je obdobná jako u údajů o účastníkovi. Údaje o přístupu jsou zpravidla zaznamenávány jako součást záznamu událostí (jinými slovy serverový žurnál či log) a uvádějí začátek a ukončení relace přístupu uživatele ke službě. Často je to individuální IP adresa (statická nebo dynamická) nebo jiný identifikátor, který identifikuje síťové rozhraní použité během přístupové relace. Pokud je uživatel neznámý, je obvykle nutné ji získat předtím, než lze od poskytovatele služeb vyžádat údaje o účastníkovi související s tímto identifikátorem.

- (22) Údaje o transakcích jsou na druhou stranu obecně vyžadovány k získání informací o kontaktech a umístění uživatele a mohou posloužit k vytvoření profilu dotčené fyzické osoby. To znamená, že údaje o přístupu nemohou samy o osobě sloužit k podobnému účelu, například nesdělují žádné informace o tom, s kým uživatel komunikoval. Tento návrh tudíž zavádí novou kategorii údajů, s níž je třeba zacházet jako s údaji o účastníkovi, pokud je cíl získat tyto údaje podobný.
- (23) Všechny kategorie údajů obsahují osobní údaje, a vztahují se na ně tudíž záruky podle *acquis* Unie o ochraně údajů, ale intenzita dopadu na základní práva se různí, a to zejména mezi údaji o účastníkovi a přístupu na jedné straně a údaji o transakcích a obsahu na straně druhé. Zatímco údaje o účastníkovi a přístupu jsou užitečné k získání prvních vodítek ve vyšetřování ohledně totožnosti podezřelé osoby, jako důkazní materiál jsou nejrelevantnější údaje o transakcích a obsahu. Je tudíž zásadní, aby nástroj obsáhl všechny tyto kategorie údajů. Z důvodu různého stupně zásahu do základních práv jsou stanoveny různé podmínky pro získání údajů o účastníkovi a přístupu na jedné straně a údajů o transakcích a obsahu na straně druhé.
- (24) Evropský předávací příkaz a evropský uchovávací příkaz jsou vyšetřovací opatření, která by se měla vydávat pouze v rámci konkrétních trestních řízení proti konkrétním známým nebo dosud neznámým pachatelům konkrétního trestného činu, který byl již spáchán, po individuálním vyhodnocení přiměřenosti a nezbytnosti v každém jednotlivém případě.
- (25) Tímto nařízením nejsou dotčeny vyšetřovací pravomoci orgánů v občanskoprávním nebo správním řízení, a to i v případech, kdy taková řízení mohou vést k sankcím.
- (26) Toto nařízení by se mělo uplatňovat na poskytovatele služeb nabízející služby v Unii a příkazy stanovené tímto nařízením mohou být vydávány pouze v souvislosti s údaji týkajícími se služeb nabízených v Unii. Služby nabízené výhradně mimo Unii do oblasti působnosti tohoto nařízení nespadají, ani pokud je poskytovatel služeb usazen v Unii.
- (27) K určení, zda poskytovatel služeb nabízí služby v Unii, je nutné posoudit, zda poskytovatel služeb umožňuje právníkům nebo fyzickým osobám v jednom či více členských státech využívat jeho služby. Avšak pouhá dostupnost on-line rozhraní, jako například dostupnost webové stránky, e-mailové adresy a jiných kontaktních údajů poskytovatele služeb či zprostředkovatele v jednom nebo více členských státech bráněných izolovaně, by neměla být dostatečnou podmínkou pro použití tohoto nařízení.
- (28) Pro stanovení rozsahu použití tohoto nařízení by mělo být relevantní i podstatné spojení s Unií. Existence takového podstatného spojení s Unií by měla být předpokládána, pokud má poskytovatel služeb provozovnu v Unii. Pokud takovou provozovnu nemá, mělo by být kritérium podstatného spojení posuzováno na základě existence významného počtu uživatelů v jednom nebo více členských státech nebo zacílení činností na jeden nebo více členských států. Zacílení činností na jeden nebo více členských států lze určit na základě všech relevantních okolností, včetně takových faktorů, jako je používání jazyka či měny obecně používaných v daném členském státě nebo možnost objednání zboží či služeb. Zacílení činností na některý členský stát by mohlo být též odvozeno od dostupnosti aplikace v příslušném národním obchodě s aplikacemi, od poskytování místních reklam nebo reklam v jazyce používaném v daném členském státě nebo od řešení vztahů se zákazníky, např. poskytováním zákaznického servisu v jazyce obecně používaném v tomto členském státě. Podstatné spojení je třeba předpokládat i v případě, že poskytovatel služeb zaměřuje své činnosti na jeden nebo více členských států, jak stanoví čl. 17 odst. 1 písm. c) nařízení

1215/2012 o příslušnosti a uznávání a výkonu soudních rozhodnutí v občanských a obchodních věcech³⁶. Na druhou stranu poskytování služby s ohledem na pouhý soulad se zákazem diskriminace stanovený v nařízení (EU) 2018/302³⁷ nelze jen z tohoto důvodu pokládat za zaměření nebo zacílení činností na dané území v Unii.

- (29) Evropský předávací příkaz by měl být vydán pouze za předpokladu, že je to nezbytné a přiměřené. Při posouzení by se mělo vzít v úvahu, zda je příkaz omezen na to, co je pouze v jednotlivém případě nutné k dosažení oprávněného cíle získat relevantní a nezbytné údaje, které poslouží jako důkazy.
- (30) Je-li evropský předávací nebo uchovávací příkaz vydán, měl by být do procesu jeho vydání nebo potvrzení vždy zapojen justiční orgán. S ohledem na citlivější charakter údajů o transakcích a obsahu vyžaduje vydání nebo potvrzení evropských předávacích příkazů k předání těchto kategorií údajů přezkum soudcem. Jelikož údaje o účastníkovi a přístupu jsou méně citlivé, mohou evropské předávací příkazy pro jejich sdělení vydávat nebo potvrzovat také příslušní státní zástupci.
- (31) Z téhož důvodu je nutné činit rozdíl i z hlediska věcné působnosti tohoto nařízení: příkazy k předání údajů o účastníkovi a údajů o přístupu lze vydat v souvislosti s jakýmkoli trestným činem, zatímco na přístup k údajům o transakcích a obsahu by se měly vztahovat přísnější požadavky, které odrážejí citlivější povahu takových údajů. Přiměřenější přístup umožňuje prahová hodnota společně s několika dalšími podmínkami a zárukami ex ante a ex post, které návrh stanoví, aby bylo zajištěno dodržování přiměřenosti a práv dotčených osob. Prahová hodnota by přitom neměla omezovat účinnost nástroje a jeho používání v praxi. Možnost vydávat příkazy u vyšetřování trestných činů, které jsou spojeny s nejméně tříletým maximálním trestem, omezuje působnost nástroje na závažnější trestné činy, aniž příliš ovlivňuje možnosti jeho používání v praxi. Vylučuje z oblasti působnosti významný počet trestných činů, které jsou členskými státy pokládány za méně závažné, jak je vyjádřeno nižším maximálním trestem. Výhoda je i v tom, že je snadno použitelný v praxi.
- (32) U některých specifických trestných činů bývají důkazy obvykle k dispozici pouze v elektronické formě, která je svou podstatou mimořádně pomíjivá. To je případ trestných činů souvisejících s kybernetickou činností, a to i těch, které by samy o sobě nemusely být pokládány za závažné, které by však mohly způsobit rozsáhlé nebo značné škody, především včetně případů s malým individuálním dopadem, ale velkým objemem a celkovou škodou. U většiny případů, kdy byl trestný čin spáchán prostřednictvím informačního systému, by uplatnění stejné prahové hodnoty jako u jiných typů trestných činů převážně vedlo k beztrestnosti. To odůvodňuje použití nařízení též u těch trestných činů, kde je trestní sazba nižší než tři roky odnětí svobody. U dalších trestných činů souvisejících s terorismem popsaných ve směrnici 2017/541/EU se nevyžaduje minimální maximální prahová hodnota tří let.
- (33) Dále je nezbytné stanovit, že evropský předávací příkaz lze vydat pouze za předpokladu, že by byl ve srovnatelné vnitrostátní situaci ve vydávajícím státě k dispozici obdobný příkaz.

³⁶ [Nařízení Evropského parlamentu a Rady \(EU\) č. 1215/2012](#) ze dne 12. prosince 2012 o příslušnosti a uznávání a výkonu soudních rozhodnutí v občanských a obchodních věcech (Úř. věst. L 351, 20.12.2012, s. 1).

³⁷ [Nařízení Evropského parlamentu a Rady \(EU\) 2018/302](#) ze dne 28. února 2018 o řešení neoprávněného zeměpisného blokování a dalších forem diskriminace založených na státní příslušnosti, místě bydliště či místě usazení zákazníků v rámci vnitřního trhu a o změně nařízení (ES) č. 2006/2004 a (EU) 2017/2394 a směrnice 2009/22/ES (Úř. věst. L 601, 2.3.2018, s. 1).

- (34) V případech, kdy jsou žádané údaje uchovávány nebo zpracovávány jako součást infrastruktury poskytované poskytovatelem služeb společnosti nebo jinému subjektu mimo fyzických osob, zpravidla v případě hostingových služeb, by se evropský předávací příkaz měl používat pouze tehdy, když jiná vyšetřovací opatření adresovaná společnosti nebo subjektu nejsou vhodná, zejména pokud by tím vzniklo riziko, že to ohrozí vyšetřování. To je významné zejména u větších subjektů, jako jsou obchodní společnosti nebo vládní subjekty, které využívají služby poskytovatelů služeb k zajišťování své podnikové IT infrastruktury či služeb nebo obojího. Prvním adresátem evropského předávacího příkazu by v takových situacích měla být tato společnost nebo jiný subjekt. Tato společnost nebo jiný subjekt nemusí být poskytovatelem služeb spadajícím do oblasti působnosti tohoto nařízení. Avšak v případech, kdy adresování tohoto subjektu není vhodné, například proto, že je podezřelý ze zapojení do dotčeného případu nebo že jsou známky koluze s cílem vyšetřování, měly by mít příslušné orgány možnost adresovat žádost o údaje poskytovateli služeb poskytujícího dotčnou infrastrukturu. Toto ustanovení nemá vliv na právo přikázat poskytovateli služeb údaje uchovat.
- (35) Na imunity a výsady, které se mohou vztahovat na kategorie osob (např. diplomaty) nebo zvláště chráněné vztahy (např. povinnost mlčenlivosti ve vztahu mezi právním zástupcem a jeho klientem), odkazují jiné nástroje vzájemného uznávání, např. evropský vyšetřovací příkaz. Jejich rozsah a vliv se liší podle použitelného vnitrostátního práva, které by mělo být bráno v úvahu v době vydání příkazu, jelikož vydávající orgán smí příkaz vydat jen tehdy, pokud je ve srovnatelné vnitrostátní situaci k dispozici obdobný příkaz. Vedle této základní zásady by měly být ve vydávajícím státě co nejvíce brány v potaz imunity a výsady, které chrání údaje o přístupu, transakcích nebo obsahu v členském státě poskytovatele služeb, a to stejně, jakoby byly stanoveny podle vnitrostátního práva vydávajícího státu. To je relevantní zejména tehdy, když právo členského státu, kde je poskytovatel služeb nebo jeho právní zástupce osloven, stanoví vyšší ochranu než právo vydávajícího státu. Ustanovení též zajišťuje respektování případů, kdy sdělení údajů může mít vliv na základní zájmy tohoto členského státu, např. národní bezpečnost a obranu. Jako doplňková záruka by tyto aspekty měly být brány v potaz nejen při vydávání příkazu, ale i později při posuzování relevantnosti a přípustnosti dotčených údajů v příslušné fázi trestního řízení, a pokud probíhá vymáhací postup ze strany vymáhajícího orgánu.
- (36) Evropský uchovávací příkaz může být vydán v souvislosti s jakýmkoli trestným činem. Jeho cílem je zabránit odstranění, smazání nebo změně relevantních údajů v situacích, kdy může dosažení předání těchto údajů trvat déle, například proto, že budou použity kanály justiční spolupráce.
- (37) Evropský předávací a uchovávací příkaz by měl být adresován právnímu zástupci, kterého ustanoví poskytovatel služeb. Nebyl-li ustanoven žádný právní zástupce, mohou být příkazy adresovány provozovně poskytovatele služeb v Unii. To může platit v případech, kdy poskytovatel služeb nemá zákonnou povinnost jmenovat právního zástupce. V případě neplnění ze strany právního zástupce může být v naléhavých situacích evropský předávací nebo uchovávací příkaz adresován též poskytovateli služeb, a to souběžně s vymáháním původního příkazu podle článku 14 nebo místo něj. V případě neplnění ze strany právního zástupce v nenaléhavých situacích, kdy však zjevně hrozí ztráta údajů, může být evropský předávací nebo uchovávací příkaz adresován i jakékoli provozovně poskytovatele služeb v Unii. Z důvodu těchto různých možných scénářů se v ustanoveních používá obecný výraz „adresát“. Uplatňuje-li se povinnost, například zachování důvěrnosti, nejen na

adresáta, ale též na poskytovatele služeb, pokud není adresátem, je to upřesněno v příslušném ustanovení.

- (38) Evropský předávací a evropský uchovávací příkaz by měl být poskytovateli služeb předáván prostřednictvím certifikátu evropského předávacího příkazu (dále jen „EPOC“) nebo certifikátu evropského uchovávacího příkazu (dále jen „EPOC-PR“), který by měl být přeložen. Certifikáty by měly obsahovat stejné povinné informace jako příkazy, kromě důvodů pro nezbytnost a přiměřenost opatření nebo dalších podrobností o případu, aby nedošlo k ohrožení vyšetřování. Protože však jsou součástí samotného příkazu, umožňují podezřelému napadnout je později během trestního řízení. V případě potřeby je třeba certifikát přeložit do úředního jazyka či (jednoho z) úředních jazyků členského státu adresáta nebo do jiného úředního jazyka, který poskytovatel služeb dle svého prohlášení akceptuje.
- (39) Příslušný vydávající orgán by měl certifikát EPOC nebo EPOC-PR předat přímo adresátovi jakýmkoli způsobem umožňujícím vyhotovení písemného záznamu za podmínek, jež poskytovateli služeb umožňují ověřit pravost, např. doporučenou poštou, zajištěným e-mailem a prostřednictvím platformy nebo jiných zajištěných kanálů, včetně těch, které dá k dispozici poskytovatel služeb, a to v souladu s pravidly pro ochranu osobních údajů.
- (40) Požadované údaje by měly být předány orgánům nejpozději deset dnů po obdržení certifikátu EPOC. V naléhavých případech, a uvede-li vydávající orgán jiné důvody pro odchylku od desetidenní lhůty, by měl poskytovatel dodržet kratší lhůty. Kromě bezprostředního nebezpečí smazání požadovaných údajů by k takovým důvodům mohly patřit okolnosti, které souvisejí s probíhajícím vyšetřováním, například pokud jsou požadované údaje spojeny s jinými naléhavými vyšetřovacími opatřeními, která nemohou být provedena bez chybějících údajů nebo která na nich jinak závisejí.
- (41) Aby poskytovatelé služeb mohli řešit formální problémy, je nezbytné stanovit postup pro komunikaci mezi poskytovatelem služeb a vydávajícím justičním orgánem v případech, kdy by certifikát EPOC mohl být neúplný nebo kdy obsahuje zjevné chyby nebo neobsahuje dostatek informací k provedení příkazu. Pokud by navíc poskytovatel služeb z jakéhokoli jiného důvodu neposkytl informace vyčerpávajícím způsobem nebo včas, například protože si myslí, že došlo k rozporu s povinností podle práva třetí země, nebo protože se domnívá, že evropský předávací příkaz nebyl vydán v souladu s podmínkami tohoto nařízení, měl by se obrátit na vydávající orgány a podat vhodné odůvodnění. Tento komunikační postup by tedy měl v podstatě vydávajícímu orgánu umožnit, aby certifikát EPOC opravil nebo znovu zvážil ještě v rané fázi. Aby byla zaručena dostupnost údajů, měl by poskytovatel služeb uchovat údaje, pokud mohou identifikovat žádané údaje.
- (42) Po obdržení certifikátu evropského uchovávacího příkazu (dále jen „EPOC-PR“) by měl poskytovatel služeb uchovat požadované údaje nejvýše šedesát dnů, ledaže ho vydávající orgán informuje, že zahájil řízení o vydání následné žádosti o předání, v kterémžto případě by mělo uchování pokračovat. Toto šedesátidenní období je vypočteno tak, aby bylo umožněno zahájení oficiální žádosti. K tomu je zapotřebí, aby byly podniknuty alespoň některé formální kroky, například zasláním například zaslání žádosti o překlad v rámci vzájemné právní pomoci. Po obdržení těchto informací by měly být údaje uchovávány tak dlouho, jak to bude nezbytné, dokud nebudou předány v rámci následné žádosti o předání.
- (43) Poskytovatelé služeb a jejich právní zástupci by měli zajistit důvěrnost, a požaduje-li to vydávající orgán, neměli by informovat osobu, jejíž údaje jsou žádány, aby bylo

chráněno vyšetřování trestných činů, v souladu s článkem 23 nařízení (EU) 2016/679³⁸. Informace o uživateli jsou však zásadním prvkem umožňujícím přezkum a soudní nápravu a měl by je poskytnout orgán, pokud byl poskytovatel služeb požádán, aby uživatele neinformoval, jestliže neexistuje žádné riziko, že budou probíhající vyšetřování ohrožena, v souladu s vnitrostátním opatřením provádějícím článek 13 směrnice (EU) 2016/680³⁹.

- (44) V případě neplnění ze strany adresáta může vydávající orgán předat celý příkaz včetně odůvodnění nezbytnosti a přiměřenosti, provázený certifikátem, příslušnému orgánu v členském státě, v němž adresát certifikátu pobývá nebo je usazen. Tento členský stát by ho měl vymáhat v souladu se svým vnitrostátním právem. Členský stát by měl stanovit účinné, přiměřené a odrazující peněžité sankce pro případ porušení povinností podle tohoto nařízení.
- (45) Vymáhací postup je postup, v němž adresát může proti vymáhání podat odpor na základě určitých vymezených důvodů. Vymáhající orgán může odmítnout uznat a vymáhat příkaz ze stejných důvodů, nebo pokud se uplatňují imunity a výsady podle vnitrostátního práva nebo pokud sdělení údajů může mít dopad na jeho základní zájmy, jako je národní bezpečnost a obrana. Před odmítnutím uznat nebo vymáhat příkaz z těchto důvodů by měl vymáhající orgán konzultovat vydávající orgán. V případě neplnění mohou orgány uložit sankce. Tyto sankce by měly být přiměřené též z hlediska konkrétních okolností, jako je opakované nebo systémové neplnění.
- (46) Bez ohledu na své povinnosti chránit údaje by poskytovatelé služeb neměli ručit v členských státech za újmu způsobenou svým uživatelům či třetím stranám výhradně v důsledku splnění certifikátů EPOC nebo EPOC-PR v dobré víře.
- (47) Vedle fyzických osob, o jejichž údaje je žádáno, mohou být vyšetřovacím opatřením dotčeni poskytovatelé služeb a třetí země. V zájmu zajištění mezinárodní zdvořilosti v souvislosti se svrchovanými zájmy třetích zemí, ochrany dotčené fyzické osoby a řešení rozporných povinností poskytovatelů služeb poskytuje tento nástroj specifický mechanismus soudního přezkumu pro případ, kdy by dodržení evropského předávacího příkazu bránilo poskytovatelům služeb splnit právní povinnost vyplývající z práva třetího státu.
- (48) Za tímto účelem, kdykoli se adresát domnívá, že by evropský předávací příkaz v konkrétním případě vedl k porušení právní povinnosti vyplývající z práva třetí země, měl by cestou odůvodněné námitky a pomocí poskytnutých formulářů informovat vydávající orgán. Vydávající orgán by poté měl provést s ohledem na odůvodněnou námitku přezkum evropského předávacího příkazu a při něm by měl vzít v úvahu stejná kritéria, jimiž by se musel řídit příslušný soud. Rozhodne-li se orgán, že oprávněnost příkazu potvrdí, mělo by být řízení postoupeno příslušnému soudu oznámenému příslušným členským státem, který poté příkaz přezkoumá.
- (49) Při určování existence rozporných povinností ve specifických okolnostech zkoumaného případu by se příslušný soud měl v případě potřeby opřít o příslušné

³⁸ [Nařízení Evropského parlamentu a Rady \(EU\) 2016/679](#) ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

³⁹ [Směrnice Evropského parlamentu a Rady \(EU\) 2016/680](#) ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV (Úř. věst. L 119, 4.5.2016, s. 89).

externí odborné poznatky, například pokud přezkum vyvolává otázky ohledně výkladu práva dotčené třetí země. To by mohlo zahrnovat konzultace ústředních orgánů této země.

- (50) Odborné poznatky ohledně výkladu by mohly být případně poskytovány ve znaleckých posudcích. Informace a judikatura týkající se výkladu právních předpisů třetích zemí a rozporných postupů v členských státech by měly být k dispozici na ústřední platformě, jako je projekt SIRIUS a/nebo Evropská soudní síť. Díky tomu by soudy mohly využívat zkušenosti a odborné poznatky shromážděné jinými soudy ohledně stejných nebo podobných otázek. To by nemělo bránit v případné obnovené konzultaci třetího státu.
- (51) Existují-li rozporné povinnosti, měl by soud určit, zda rozporná ustanovení třetí země zakazují sdělit dotčené údaje z důvodu, že je to nezbytné buď pro ochranu základních práv dotčených fyzických osob, nebo pro ochranu základních zájmů třetí země v souvislosti s národní bezpečností nebo obranou. Při provádění tohoto posouzení by měl soud vzít v úvahu, zda právo třetí země místo toho, aby chránilo základní práva nebo základní zájmy třetí země související s národní bezpečností nebo obranou, se očividně snaží chránit jiné zájmy nebo je zaměřeno na ochranu nezákonných činností před žádostmi donucovacích orgánů v kontextu trestního vyšetřování. Dojde-li soud k závěru, že rozporná ustanovení třetí země zakazují sdělit dotčené údaje z důvodu, že je to nezbytné buď pro ochranu základních práv dotčených fyzických osob, nebo pro ochranu základních zájmů třetí země v souvislosti s národní bezpečností nebo obranou, měl by konzultovat třetí zemi prostřednictvím svých ústředních orgánů, které jsou již zřízeny pro účely vzájemné právní pomoci ve většině částí světa. Měl by stanovit lhůtu, v níž třetí země může vznést námitky proti výkonu evropského předávacího příkazu; v případě, že orgány třetí země neodpoví v (prodloužené) lhůtě i navzdory připomínce, v níž jim jsou sděleny důsledky neposkytnutí odpovědi, soud oprávněnost příkazu potvrdí. Vznese-li orgány třetí země proti sdělení odpor, měl by soud příkaz zrušit.
- (52) Ve všech ostatních případech rozporných povinností, které se netýkají základních práv fyzických osob nebo základních zájmů třetí země souvisejících s národní bezpečností nebo obranou, by soud měl rozhodnout o tom, zda oprávněnost evropského předávacího příkazu potvrdí, zvážením řady prvků, které mají zjistit sílu spojení s některou z obou zapojených jurisdikcí, příslušné zájmy na získání údajů nebo naopak na zabránění jejich sdělení a možné důsledky pro poskytovatele služeb z toho, že musí příkaz splnit. U trestných činů souvisejících s kybernetickou činností je důležité, že místo, kde byl trestný čin spáchán, zahrnuje místo či místa, kde byl čin proveden, a místo či místa, kde se účinky trestného činu projeví.
- (53) Podmínky stanovené v článku 9 jsou též použitelné v situacích, kdy se vyskytují rozporné povinnosti vyplývající z práva třetí země. Během tohoto postupu by údaje měly být uchovávané. Je-li příkaz zrušen, může být vydán nový uchovávací příkaz, aby vydávající orgán mohl usilovat o předání údajů jinými kanály, například prostřednictvím vzájemné právní pomoci.
- (54) Je zásadní, aby všechny osoby, jejichž údaje jsou v trestním vyšetřování nebo řízení požadovány, měly v souladu s článkem 47 Listiny základních práv Evropské unie přístup k účinné právní ochraně. V případě podezřelých a obviněných osob by mělo být během trestních řízení uplatňováno právo na účinnou právní ochranu. To může ovlivnit přípustnost nebo případně váhu důkazů, které byly získány takovými prostředky, v řízeních. Navíc tyto osoby požívají všech procesních záruk, které na ně

lze uplatnit, např. právo na informace. Právo na účinnou právní ochranu by měly mít i jiné osoby, které nejsou podezřelé nebo obviněné. Měla by být minimálně stanovena možnost napadnout zákonnost evropského předávacího příkazu, včetně jeho nezbytnosti a přiměřenosti. Toto nařízení by nemělo omezovat případné důvody pro napadení zákonnosti příkazu. Tyto opravné prostředky by měly být uplatňovány ve vydávajícím státě v souladu s vnitrostátním právem. Pravidla pro předběžné opatření by se měla řídit vnitrostátním právem.

- (55) Navíc během vymáhacího postupu a následného právního prostředku může adresát podat odpor proti vymáhání evropského předávacího nebo uchovávacího příkazu z řady omezených důvodů, včetně toho, že ho nevydal nebo nepotvrdil příslušný orgán nebo že je zjevné, že očividně porušuje Listinu základních práv Evropské unie nebo že je očividně nepatřičný. Například příkaz žádající o předání údajů o obsahu týkajících se nedefinované třídy osob v zeměpisné oblasti nebo bez vazby na konkrétní trestní řízení by zjevně ignoroval podmínky pro vydání evropského předávacího příkazu.
- (56) Ochrana fyzických osob pro účely zpracování osobních údajů je základním právem. Podle čl. 8 odst. 1 Listiny základních práv Evropské unie a čl. 16 odst. 1 SFEU má každý právo na ochranu osobních údajů, které se ho týkají. Při provádění tohoto nařízení by členské státy měly zajistit, aby byly osobní údaje chráněny a mohly být zpracovávány pouze v souladu s nařízením (EU) 2016/679 a směrnicí (EU) 2016/680.
- (57) Osobní údaje získané podle tohoto nařízení by měly být zpracovávány pouze v případech, kdy je to nezbytné a přiměřené účelům předcházení trestným činům a jejich vyšetřování, odhalování a stíhání nebo uplatňování trestních sankcí a práva na obhajobu. Členské státy by měly zejména zajistit, aby se na přenos osobních údajů od příslušných orgánů k poskytovatelům služeb pro účely tohoto nařízení vztahovaly vhodné strategie a opatření ochrany údajů včetně opatření k zajištění bezpečnosti údajů. Poskytovatelé služeb by měli totéž zajistit pro přenos osobních údajů příslušným orgánům. Přístup k informacím obsahujícím osobní údaje, jehož může být dosaženo prostřednictvím autentizačních postupů, by měly mít pouze oprávněné osoby. Mělo by být zvaženo používání mechanismů k zajištění pravosti, jako jsou oznámené vnitrostátní systémy elektronické identifikace nebo služby vytvářející důvěru stanovené nařízením Evropského parlamentu a Rady (EU) 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.
- (58) Komise by měla provést hodnocení tohoto nařízení, které by se mělo opírat o pět kritérií efektivnosti, účelnosti, relevantnosti, soudržnosti a přidané hodnoty EU a měla by poskytnout základ pro posouzení dopadů možných dalších opatření. Informace by měly být shromažďovány pravidelně a s cílem získat podklady pro hodnocení tohoto nařízení.
- (59) Používání předem přeložených a standardizovaných formulářů usnadňuje spolupráci a výměnu informací mezi justičními orgány a poskytovateli služeb, čímž jim umožňuje zajistit a předávat elektronické důkazy rychleji a účelněji a současně též plnit nezbytné bezpečnostní požadavky uživatelsky přívětivým způsobem. Tyto formuláře snižují náklady na překlad a přispívají k vysoké kvalitě. Formuláře pro odpovědi by obdobným způsobem měly umožnit standardizovanou výměnu informací, zejména v případech, kdy poskytovatelé služeb nejsou schopni plnit své závazky, jelikož účet neexistuje nebo nejsou k dispozici žádné údaje. Formuláře by měly též usnadnit sběr statistik.

- (60) Pro účinné řešení případné potřeby zlepšení obsahu certifikátů EPOC a EPOC-PR a formuláře, který má být použit k poskytnutí informací o nemožnosti provést EPOC nebo EPOC-PR, by měla být na Komisi přenesena pravomoc přijímat akty v souladu s článkem 290 Smlouvy o fungování Evropské unie, aby mohla změnit přílohy I, II a III tohoto nařízení. Je obzvláště důležité, aby Komise v rámci přípravné činnosti vedla odpovídající konzultace, a to i na odborné úrovni, a aby tyto konzultace probíhaly v souladu se zásadami stanovenými v interinstitucionální dohodě o zdokonalení tvorby právních předpisů ze dne 13. dubna 2016⁴⁰. Pro zajištění rovné účasti na vypracovávání aktů v přenesené pravomoci obdrží Evropský parlament a Rada veškeré dokumenty současně s odborníky z členských států, přičemž jejich odborníci mají systematicky přístup na jednání skupin odborníků Komise, jež se věnují přípravě aktů v přenesené pravomoci.
- (61) Opatření na základě tohoto nařízení by neměla nahrazovat evropské vyšetřovací příkazy v souladu se směrnicí Evropského parlamentu a Rady 2014/41/EU⁴¹ pro účely získávání elektronických důkazů. Orgány členských států by si měly vybrat nástroj, který je pro jejich situaci nevhodnější; mohou upřednostnit použití evropského vyšetřovacího příkazu, když žádají o soubor různých typů vyšetřovacích opatření, včetně mimo jiné předání elektronických důkazů z jiného členského státu.
- (62) Z důvodu technologického vývoje mohou za několik let převládat nové formy komunikačních nástrojů nebo se mohou při uplatňování tohoto nařízení objevit mezery. Je tudíž důležité stanovit přezkum jeho uplatňování.
- (63) Jelikož cíle tohoto nařízení, totiž zvýšení zabezpečení a získávání elektronických důkazů přes hranice, nemůže být vzhledem k jeho přeshraniční povaze dosaženo uspokojivě členskými státy, ale spíše jej může být lépe dosaženo na úrovni Unie, může Unie přijmout opatření v souladu se zásadou subsidiarity stanovenou v článku 5 Smlouvy o Evropské unii. V souladu se zásadou proporcionality stanovenou v uvedeném článku nepřekračuje toto nařízení rámec toho, co je nezbytné k dosažení těchto cílů.
- (64) V souladu s článkem 3 Protokolu o postavení Spojeného království a Irska s ohledem na prostor svobody, bezpečnosti a práva, připojeného ke Smlouvě o Evropské unii a ke Smlouvě o fungování Evropské unie, *[Spojené království / Irsko oznámilo své přání podílet se na přijímání a používání tohoto nařízení] / [a aniž by byl dotčen článek 4 uvedeného protokolu se Spojené království / Irsko neúčastní přijímání tohoto nařízení a toto nařízení pro ně není závazné ani použitelné]*.
- (65) V souladu s články 1 a 2 Protokolu č. 22 o postavení Dánska, připojeného ke Smlouvě o Evropské unii, a Smlouvě o fungování Evropské unie, se Dánsko neúčastní přijímání tohoto nařízení, a proto pro ně není závazné ani použitelné.
- (66) Evropský inspektor ochrany údajů byl konzultován v souladu s čl. 28 odst. 2 nařízení Evropského parlamentu a Rady (ES) č. 45/2001⁴² a vydal stanovisko dne (...) ⁴³,

⁴⁰ Úř. věst. L 123, 12.5.2016, s. 1.

⁴¹ [Směrnice 2014/41/EU](#) ze dne 3. dubna 2014 o evropském vyšetřovacím příkazu v trestních věcech (Úř. věst. L 130, 1.5.2014, s. 1).

⁴² Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů (Úř. věst. L 8, 12.1.2001, s. 1).

⁴³ Úř. věst. C , , s. .

Kapitola 1: Předmět, definice a oblast působnosti

Článek 1

Předmět

1. Toto nařízení stanoví pravidla, podle kterých smí orgán členského státu nařídít poskytovateli služeb nabízejícímu služby v Unii, aby předal nebo uchovával elektronické důkazy bez ohledu na umístění údajů. Tímto nařízením nejsou dotčeny pravomoci vnitrostátních orgánů nutit poskytovatele služeb usazené nebo zastoupené na jejich území dodržovat obdobná vnitrostátní opatření.
2. Tímto nařízením není dotčena povinnost ctít základní práva a právní zásady zakotvené v článku 6 Smlouvy o EU, včetně práva osob, proti nimž je vedeno trestní řízení, na obhajobu, a nejsou jím dotčeny související povinnosti donucovacích nebo justičních orgánů.

Článek 2

Definice

Pro účely tohoto nařízení se rozumí:

- (1) „evropským předávacím příkazem“ závazné rozhodnutí vydávajícího orgánu členského státu nutící poskytovatele služeb nabízejícího služby v Unii a usazeného nebo zastoupeného v jiném členském státě předat elektronické důkazy;
- (2) „evropským uchovávacím příkazem“ závazné rozhodnutí vydávajícího orgánu členského státu nutící poskytovatele služeb nabízejícího služby v Unii a usazeného nebo zastoupeného v jiném členském státě uchovávat elektronické důkazy vzhledem k následné žádosti o předání údajů;
- (3) „poskytovatelem služeb“ jakákoli fyzická nebo právnická osoba, která poskytuje jednu či více z následujících kategorií služeb:
 - (a) služby elektronické komunikace definované v čl. 2 bodě 4 [směrnice, kterou se zřizuje evropský kodex pro elektronické komunikace];
 - (b) služby informační společnosti definované v čl. 1 odst. 1 písm. b) směrnice Evropského parlamentu a Rady (EU) 2015/1535⁴⁴, pro které je uchovávání údajů určující složkou služby poskytované uživateli, včetně sociálních sítí, internetových tržišť umožňujících transakce mezi jejich uživateli a jiných poskytovatelů hostingových služeb;
 - (c) služby číslování IP adres a názvů internetových domén, např. poskytovatelé IP adres, registry názvů domén, registrátoři názvů domén a související služby zajištění soukromí a proxy serverů;
- (4) „nabízením služeb v Unii“:

⁴⁴ [Směrnice Evropského parlamentu a Rady \(EU\) 2015/1535](#) ze dne 9. září 2015 o postupu při poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti (Úř. věst. L 241, 17.9.2015, s. 1).

- (a) umožnění právníkům nebo fyzickým osobám v jednom nebo více členských státech využívat služby vyjmenované v bodě 3 výše a
 - (b) existence podstatného spojení s členským státem či státy uvedenými v písmeni a);
- (5) „provozovnou“ buď vlastní výkon hospodářské činnosti po dobu neurčitou prostřednictvím stálé infrastruktury, odkud je prováděna podnikatelská činnost poskytování služeb, nebo stálá infrastruktura, odkud je podnikatelská činnost řízena;
- (6) „elektronickými důkazy“ důkazy uložené v elektronické podobě poskytovatelem služeb nebo jeho jménem v době obdržení certifikátu předávacího nebo uchovávacího příkazu, sestávající z uložených údajů o účastníkovi, údajů o přístupu, údajů o transakcích a údajů o obsahu;
- (7) „údaji o účastníkovi“ jakékoli údaje týkající se:
- (a) totožnosti účastníka nebo zákazníka, např. poskytnuté jméno, datum narození, poštovní nebo zeměpisná adresa, fakturační a platební údaje, telefon nebo e-mail;
 - (b) druhu služby a jejího trvání včetně technických údajů a údajů identifikujících související technická opatření nebo rozhraní použitá účastníkem nebo zákazníkem nebo mu poskytnutá a údajů týkajících se potvrzení použití služby, vyjma hesel nebo jiných autentizačních prostředků použitých místo hesla a poskytnutých uživatelem nebo vytvořených na žádost uživatele;
- (8) „údaji o přístupu“ údaje, které se týkají začátku nebo ukončení relace přístupu uživatele ke službě a které jsou naprosto nezbytné pro jediný účel identifikace uživatele služby, např. datum a čas použití nebo přihlášení ke službě a odhlášení od ní, společně s IP adresou přidělenou uživateli služby poskytovatelem služby přístupu na internet, údaje identifikující použité rozhraní a identifikační údaj uživatele. Patří sem metadata elektronické komunikace definované v čl. 4 odst. 3 písm. g) [nařízení o respektování soukromého života a ochraně osobních údajů při elektronické komunikaci];
- (9) „údaji o transakcích“ údaje, které se týkají poskytování služby nabízené poskytovatelem služeb a které poskytují kontext nebo doplňující informace o takové službě a jsou vytvářeny nebo zpracovávány informačním systémem poskytovatele služeb, např. zdroj a cíl zprávy nebo jiného typu interakce, údaje o umístění zařízení, datum, čas, trvání, velikost, trasa, formát, použitý protokol a typ komprese, pokud takové údaje nepředstavují údaje o přístupu. Patří sem metadata elektronické komunikace definovaná v čl. 4 odst. 3 písm. g) [nařízení o respektování soukromého života a ochraně osobních údajů při elektronické komunikaci];
- (10) „údaji o obsahu“ jakékoli uložené údaje v digitálním formátu, jako je text, hlas, videa, obrázky a zvuk, a to jiné než údaje o účastníkovi, přístupu či transakcích;
- (11) „informačním systémem“ informační systém podle definice čl. 2 písm. a) směrnice Evropského parlamentu a Rady (EU) 2013/40/EU⁴⁵;
- (12) „vydávajícím státem“ členský stát, v němž se vydává evropský předávací příkaz nebo evropský uchovávací příkaz;

⁴⁵ [Směrnice Evropského parlamentu a Rady 2013/40/EU](#) ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV (Úř. věst. L 218, 14.8.2013, s. 8).

- (13) „vymáhajícím státem“ členský stát, v němž pobývá nebo je usazen adresát evropského předávacího příkazu nebo evropského uchovávacího příkazu a jemuž je pro účely vymáhání zaslán evropský předávací příkaz a certifikát evropského předávacího příkazu nebo evropský uchovávací příkaz a certifikát evropského uchovávacího příkazu;
- (14) „vymáhajícím orgánem“ příslušný orgán ve vymáhajícím státě, jemuž je vydávajícím orgánem pro účely vymáhání zaslán evropský předávací příkaz a certifikát evropského předávacího příkazu nebo evropský uchovávací příkaz a certifikát evropského uchovávacího příkazu;
- (15) „naléhavými případy“ situace, v nichž je bezprostředně ohrožen život nebo tělesná integrita osoby nebo je bezprostředně ohrožena kritická infrastruktura podle definice čl. 2 písm. a) směrnice Rady 2008/114/ES⁴⁶.

Článek 3 *Oblast působnosti*

1. Toto nařízení se vztahuje na poskytovatele služeb, kteří nabízejí služby v Unii.
2. Evropský předávací příkaz a evropský uchovávací příkaz mohou být vydány pouze pro trestní řízení během jak přípravné, tak soudní fáze. Příkazy mohou být vydány též v řízeních týkajících se trestného činu, za který může ve vydávajícím státě nést odpovědnost nebo být potrestána právnická osoba.
3. Příkazy stanovené tímto nařízením mohou být vydávány pouze v souvislosti s údaji týkajícími se služeb definovaných v čl. 2 bodě 3 nabízených v Unii.

Kapitola 2: Evropský předávací příkaz, evropský uchovávací příkaz a certifikáty

Článek 4 *Vydávající orgán*

1. Evropský předávací příkaz pro údaje o účastníkovi a údaje o přístupu může vydat:
 - (a) soudce, soud, vyšetřující soudce nebo státní zástupce příslušný v daném případě nebo
 - (b) jakýkoli jiný příslušný orgán, který vydávající stát určí a který v konkrétním případě jedná jako vyšetřující orgán v trestním řízení a má v souladu s vnitrostátním právem pravomoc nařídit shromažďování důkazů. Takový evropský předávací příkaz potvrdí po přezkoumání jeho souladu s podmínkami pro vydání evropského předávacího příkazu podle tohoto nařízení soudce, soud, vyšetřující soudce nebo státní zástupce ve vydávajícím státě.
2. Evropský předávací příkaz pro údaje o transakcích a údaje o obsahu může vydat pouze:
 - (a) soudce, soud nebo vyšetřující soudce příslušný v daném případě nebo

⁴⁶ [Směrnice Rady 2008/114/ES](#) ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu (Úř. věst. L 345, 23.2.2008, s. 75).

- (b) jakýkoli jiný příslušný orgán, který vydávající stát určí a který v konkrétním případě jedná jako vyšetřující orgán v trestním řízení a má v souladu s vnitrostátním právem pravomoc nařídít shromažďování důkazů. Takový evropský předávací příkaz potvrdí soudce, soud nebo vyšetřující soudce ve vydávajícím státě po přezkoumání jeho souladu s podmínkami pro vydání evropského předávacího příkazu podle tohoto nařízení.
3. Evropský uchovávací příkaz může vydat:
- (a) soudce, soud, vyšetřující soudce nebo státní zástupce příslušný v daném případě nebo
- (b) jakýkoli jiný příslušný orgán, který vydávající stát určí a který v konkrétním případě jedná jako vyšetřující orgán v trestním řízení a má v souladu s vnitrostátním právem pravomoc nařídít shromažďování důkazů. Takový evropský uchovávací příkaz potvrdí soudce, soud, vyšetřující soudce nebo státní zástupce ve vydávajícím státě po přezkoumání jeho souladu s podmínkami pro vydání evropského uchovávacího příkazu podle tohoto nařízení.
4. Pokud příkaz potvrdil justiční orgán podle odst. 1 písm. b), odst. 2 písm. b) a odst. 3 písm. b), lze tento orgán pokládat též za vydávající orgán pro účely předání certifikátu evropského předávacího příkazu a certifikátu evropského uchovávacího příkazu.

Článek 5

Podmínky pro vydání evropského předávacího příkazu

1. Vydávající orgán může evropský předávací příkaz vydat pouze za předpokladu, že jsou splněny podmínky uvedené v tomto článku.
2. Evropský předávací příkaz musí být nezbytný a přiměřený účelu řízení podle čl. 3 odst. 2 a může být vydán pouze za předpokladu, že by pro stejný trestný čin bylo ve srovnatelné vnitrostátní situaci ve vydávajícím státě k dispozici obdobné opatření.
3. Evropské předávací příkazy k předání údajů o účastníkovi nebo údajů o přístupu lze vydat u všech trestných činů.
4. Evropské předávací příkazy k předání údajů o transakcích nebo údajů o obsahu lze vydat pouze
 - (a) u trestných činů postihnutelných ve vydávajícím státě trestem odnětí svobody s horní hranicí sazby nejméně tří let nebo
 - (b) u následujících trestných činů, pokud jsou zcela nebo zčásti páchány pomocí informačního systému:
 - trestné činy definované v člancích 3, 4 a 5 rámcového rozhodnutí Rady 2001/413/SVV⁴⁷,
 - trestné činy definované v člancích 3 až 7 směrnice Evropského parlamentu a Rady 2011/93/EU⁴⁸,

⁴⁷ [Rámcové rozhodnutí Rady 2001/413/SVV](#) ze dne 28. května 2001 o potírání podvodů a padělání bezhotovostních platebních prostředků (Úř. věst. L 149, 2.6.2001, s. 1).

- trestné činy definované v člancích 3 až 8 směrnice Evropského parlamentu a Rady 2013/40/EU;
 - (c) u trestných činů definovaných v člancích 3 až 12 a článku 14 směrnice Evropského parlamentu a Rady 2017/541/EU⁴⁹.
5. Evropský předávací příkaz obsahuje tyto informace:
- (a) vydávající orgán a případně potvrzující orgán;
 - (b) adresáta evropského předávacího příkazu ve smyslu článku 7;
 - (c) osoby, jejichž údaje jsou požadovány, kromě případu, kdy je jediným účelem příkazu identifikace osoby;
 - (d) kategorii požadovaných údajů (údaje o účastníkovi, údaje o přístupu, údaje o transakcích nebo údaje o obsahu);
 - (e) případně požadované časové rozpětí, které má být předáno;
 - (f) použitelná ustanovení trestního práva vydávajícího státu;
 - (g) v případě naléhavé situace nebo žádosti o dřívější sdělení důvody pro dřívější sdělení;
 - (h) v případech, kdy jsou žádané údaje uchovávány nebo zpracovávány jako součást infrastruktury poskytované poskytovatelem služeb společnosti nebo jinému subjektu mimo fyzických osob, potvrzení, že příkaz je vydáván v souladu s odstavcem 6;
 - (i) důvody pro nezbytnost a přiměřenost opatření.
6. V případech, kdy jsou žádané údaje uchovávány nebo zpracovávány jako součást infrastruktury poskytované poskytovatelem služeb společnosti nebo jinému subjektu mimo fyzických osob, může být evropský předávací příkaz adresován pouze poskytovateli služeb, pokud vyšetřovací opatření adresovaná společnosti nebo subjektu nejsou vhodná, zejména pokud by mohla ohrozit vyšetřování.
7. Má-li vydávající orgán důvod domnívat se, že jsou požadované údaje o transakcích nebo obsahu chráněny imunitami a výsadami udělenými podle práva členského státu, kde je poskytovateli služeb adresován příkaz, nebo že jejich sdělení může mít dopad na základní zájmy tohoto členského státu, jako je národní bezpečnost a obrana, musí vydávající orgán před vydáním evropského předávacího příkazu požádat o objasnění, mimo jiné konzultováním příslušných orgánů dotčeného členského státu, a sice přímo nebo prostřednictvím Eurojustu nebo Evropské soudní sítě. Shledá-li vydávající orgán, že požadované údaje o přístupu, transakcích nebo obsahu takovými imunitami a výsadami chráněny jsou nebo že jejich sdělení by mělo dopad na základní zájmy druhého členského státu, evropský předávací příkaz nevydává.

⁴⁸ [Směrnice Evropského parlamentu a Rady 2011/93/EU](#) ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV (Úř. věst. L 335, 17.12.2011, s. 1).

⁴⁹ [Směrnice Evropského parlamentu a Rady \(EU\) 2017/541](#) ze dne 15. března 2017 o boji proti terorismu, kterou se nahrazuje rámcové rozhodnutí Rady 2002/475/SVV a mění rozhodnutí Rady 2005/671/SVV (Úř. věst. L 88, 31.3.2017, s. 6).

Článek 6

Podmínky pro vydání evropského uchovávacího příkazu

1. Vydávající orgán může evropský uchovávací příkaz vydat pouze za předpokladu, že jsou splněny podmínky uvedené v tomto článku.
2. Může být vydán, je-li to nezbytné a přiměřené k tomu, aby se zabránilo odstranění, smazání nebo změně údajů vzhledem k následné žádosti o předání těchto údajů prostřednictvím vzájemné právní pomoci, evropského vyšetřovacího příkazu nebo evropského předávacího příkazu. Evropské uchovávací příkazy k uchování údajů lze vydat u všech trestných činů.
3. Evropský uchovávací příkaz obsahuje tyto informace:
 - (a) vydávající orgán a případně potvrzující orgán;
 - (b) adresáta evropského uchovávacího příkazu ve smyslu článku 7;
 - (c) osoby, jejichž údaje mají být uchovány, kromě případů, kdy je jediným účelem příkazu identifikace osoby;
 - (d) kategorii údajů, které mají být uchovány (údaje o účastníkovi, údaje o přístupu, údaje o transakcích nebo údaje o obsahu);
 - (e) případně požadované časové rozpětí, které má být uchováno;
 - (f) použitelná ustanovení trestního práva vydávajícího státu;
 - (g) důvody pro nezbytnost a přiměřenost opatření.

Článek 7

Adresát evropského předávacího příkazu a evropského uchovávacího příkazu

1. Evropský předávací příkaz a evropský uchovávací příkaz jsou adresovány přímo právnímu zástupci ustanovenému poskytovatelem služeb pro účely shromáždění důkazů v trestním řízení.
2. Nebyl-li jmenován žádný zvláštní právní zástupce, mohou být evropský předávací příkaz a evropský uchovávací příkaz adresovány jakékoli provozovně poskytovatele služeb v Unii.
3. Nevyhoví-li právní zástupce certifikátu EPOC v naléhavém případě podle čl. 9 odst. 2, může být certifikát EPOC adresován jakékoli provozovně poskytovatele služeb v Unii.
4. Nesplní-li právní zástupce své povinnosti podle článku 9 nebo 10 a vydávající orgán se domnívá, že existuje závažné riziko ztráty údajů, mohou být evropský předávací příkaz nebo evropský uchovávací příkaz adresovány jakékoli provozovně poskytovatele služeb v Unii.

Článek 8

Certifikát evropského předávacího a uchovávacího příkazu

1. Evropský předávací nebo uchovávací příkaz musí být předán adresátovi ve smyslu článku 7 prostřednictvím certifikátu evropského předávacího příkazu (dále jen „EPOC“) nebo certifikátu evropského uchovávacího příkazu (dále jen „EPOC-PR“).

Vydávající nebo potvrzující orgán vyplní certifikát EPOC stanovený v příloze I nebo certifikát EPOC-PR stanovený v příloze II, podepíše ho a potvrdí přesnost a správnost jeho obsahu.

2. Certifikát EPOC nebo EPOC-PR je předán přímo jakýmkoli způsobem umožňujícím vyhotovení písemného záznamu za podmínek, jež adresátovi umožňují ověřit jeho pravost.

Pokud poskytovatelé služeb, členské státy nebo instituce Unie zavedly zvláštní platformy nebo jiné bezpečné kanály pro vyřizování žádostí o údaje podávaných ze strany donucovacích a justičních orgánů, může se vydávající orgán též rozhodnout, že certifikát odešle prostřednictvím těchto kanálů.

3. Certifikát EPOC obsahuje informace vyjmenované v čl. 5 odst. 5 písm. a) až h), včetně dostatečných informací, které adresátovi umožňují identifikovat a kontaktovat vydávající orgán. Důvody pro nezbytnost a přiměřenost opatření nebo další podrobnosti o vyšetřování se neuvádějí.
4. Certifikát EPOC-PR obsahuje informace vyjmenované v čl. 6 odst. 3 písm. a) až f), včetně dostatečných informací, které adresátovi umožňují identifikovat a kontaktovat vydávající orgán. Důvody pro nezbytnost a přiměřenost opatření nebo další podrobnosti o vyšetřování se neuvádějí.
5. Je-li to nutné, přeloží se certifikát EPOC nebo EPOC-PR do úředního jazyka Unie akceptovaného adresátem. Pokud nebyl upřesněn žádný jazyk, přeloží se certifikát EPOC nebo EPOC-PR do jednoho z úředních jazyků členského státu, v němž pobývá nebo je usazen právní zástupce.

Článek 9

Provedení certifikátu EPOC

1. Po obdržení certifikátu EPOC adresát zajistí, aby požadované údaje byly předány přímo vydávajícímu orgánu nebo donucovacím orgánům, jak je uvedeno v certifikátu EPOC, nejpozději do deseti dnů po obdržení tohoto certifikátu, ledaže vydávající orgán uvede důvody pro dřívější sdělení.
2. V naléhavých případech předá adresát požadované údaje bez zbytečného odkladu, nejpozději do šesti hodin od obdržení certifikátu EPOC.
3. Pokud adresát nemůže svou povinnost splnit, jelikož certifikát EPOC není úplný, obsahuje zjevné chyby nebo neobsahuje dostatečné informace k jeho provedení, bez zbytečného odkladu informuje vydávající orgán uvedený v certifikátu a požádá ho o objasnění prostřednictvím formuláře uvedeného v příloze III. Informuje vydávající orgán o tom, zda identifikace a uchování byly možné v souladu s odstavcem 6. Vydávající orgán odpoví obratem a nejpozději do pěti dnů. Lhůty uvedené v odstavcích 1 a 2 se neuplatňují, dokud není poskytnuto objasnění.
4. Pokud adresát nemůže svou povinnost splnit z důvodu vyšší moci nebo faktické nemožnosti nezaviněné adresátem či, nejsou-li totožní, poskytovatelem služeb zejména proto, že osoba, o jejíž údaje je žádáno, není jeho zákazníkem nebo údaje byly smazány před přijetím certifikátu EPOC, adresát bez zbytečného odkladu informuje vydávající orgán uvedený v certifikátu společně s vysvětlením důvodů prostřednictvím formuláře uvedeného v příloze III. Jsou-li splněny relevantní podmínky, vydávající orgán certifikát EPOC stáhne.

5. Ve všech případech, kdy adresát neposkytne požadované informace, neposkytne je vyčerpávajícím způsobem nebo je neposkytne ve lhůtě z jiných důvodů, informuje o důvodech těchto případů vydávající orgán bez zbytečného odkladu a nejpozději ve lhůtách stanovených v odstavcích 1 a 2 prostřednictvím formuláře uvedeného v příloze III. Vydávající orgán přezkoumá příkaz s ohledem na informace sdělené poskytovatelem služeb a v případě potřeby stanoví poskytovateli služeb novou lhůtu k předání údajů.

Domnívá-li se adresát, že certifikát EPOC nelze provést, jelikož je na základě informací v něm obsažených samotných zjevné, že očividně porušuje Listinu základních práv Evropské unie nebo je očividně nepatřičný, zašle adresát formulář v příloze III i příslušnému donucovacímu orgánu v členském státě adresáta. V takových případech může příslušný donucovací orgán požádat vydávající orgán o objasnění evropského předávacího příkazu, a to buď přímo, nebo prostřednictvím Eurojustu nebo Evropské soudní sítě.

6. Adresát požadované údaje uchová, pokud je okamžitě nepředá, ledaže mu informace v certifikátu EPOC neumožňují identifikovat požadované údaje, v kterémžto případě požádá v souladu s odstavcem 3 o objasnění. Uchovávání trvá, dokud údaje nejsou předány, ať už k tomu dojde na základě objasněného evropského předávacího příkazu a jeho certifikátu nebo prostřednictvím jiných kanálů, např. vzájemné právní pomoci. Pokud předání údajů a jejich uchování již není nutné, informuje vydávající orgán a případně v souladu s čl. 14 odst. 8 vymáhající orgán bez zbytečného odkladu adresáta.

Článek 10

Provedení certifikátu EPOC-PR

1. Po obdržení certifikátu EPOC-PR adresát uchová bez zbytečného odkladu požadované údaje. Uchování skončí po šedesáti dnech, pokud vydávající orgán nepotvrdí, že byla podána následná žádost o předání.
2. Potvrdí-li vydávající orgán ve lhůtě stanovené v odstavci 1, že následná žádost o předání byla podána, uchová adresát údaje tak dlouho, jak to bude nutné k předání údajů, jakmile je následná žádost o předání doručena.
3. Pokud uchování již není nutné, vydávající orgán bez zbytečného odkladu informuje adresáta.
4. Pokud adresát nemůže svou povinnost splnit, jelikož certifikát EPOC-PR není úplný, obsahuje zjevné chyby nebo neobsahuje dostatečné informace k jeho provedení, bez zbytečného odkladu informuje vydávající orgán uvedený v certifikátu EPOC-PR a požádá ho o objasnění prostřednictvím formuláře uvedeného v příloze III. Vydávající orgán odpoví obratem a nejpozději do pěti dnů. Adresát na své straně zajistí, aby mohl obdržet potřebné objasnění, a mohl tak splnit svou povinnost podle odstavce 1.
5. Pokud adresát nemůže svou povinnost splnit z důvodu vyšší moci nebo faktické nemožnosti nezaviněné adresátem či, nejsou-li totožní, poskytovatelem služeb zejména proto, že osoba, o jejíž údaje je žádáno, není jeho zákazníkem nebo údaje byly smazány před přijetím příkazu, adresát bez zbytečného odkladu kontaktuje vydávající orgán uvedený v certifikátu EPOC-PR společně s vysvětlením důvodů prostřednictvím formuláře obsaženého v příloze III. Jsou-li tyto podmínky splněny, vydávající orgán certifikát EPOC-PR stáhne.

6. Ve všech případech, kdy adresát neuchová požadované informace z dalších důvodů vyjmenovaných ve formuláři v příloze III, informuje adresát vydávající orgán bez zbytečného odkladu o důvodech neuchování požadovaných informací prostřednictvím formuláře obsaženého v příloze III. Vydávající orgán přezkoumá příkaz s ohledem na odůvodnění, které uvedl poskytovatel služeb.

Článek 11

Důvěrnost a informace o uživateli

1. Adresáti, a nejsou-li totožní, poskytovatelé služeb přijmou nezbytná opatření, aby zajistili důvěrnost certifikátu EPOC nebo EPOC-PR a údajů předaných nebo uchovaných, a požaduje-li to vydávající orgán, neinformují osobu, o jejíž údaje je žádáno, aby nebylo narušeno příslušné trestní řízení.
2. Pokud vydávající orgán požádal adresáta, aby neinformoval osobu, o jejíž údaje je žádáno, informuje vydávající orgán osobu, o jejíž údaje je žádáno certifikátem EPOC, bez zbytečného odkladu o předání údajů. Tyto informace mohou být pozdrženy tak dlouho, jak to bude nezbytné a přiměřené k tomu, aby nedošlo k narušení příslušného trestního řízení.
3. Při informování této osoby uvede vydávající orgán jakékoli opravné prostředky uvedené v článku 17.

Článek 12

Náhrada nákladů

Poskytovatel služeb může požádat o náhradu svých nákladů vydávajícím státem, stanoví-li to vnitrostátní právo vydávajícího státu pro vnitrostátní příkazy v obdobných situacích, v souladu s těmito vnitrostátními ustanoveními.

Kapitola 3: Sankce a vymáhání

Článek 13

Sankce

Aniž jsou dotčeny vnitrostátní právní předpisy, které stanoví ukládání trestních sankcí, stanoví členské státy pravidla pro peněžité sankce použitelné na porušení povinností podle článků 9, 10 a 11 tohoto nařízení a přijmou veškerá nezbytná opatření k zajištění jejich provedení. Stanovené peněžité sankce musí být účinné, přiměřené a odrazující. Členské státy neprodleně uvědomí o takových pravidlech a takových opatřeních Komisi a neprodleně ji informují o jakýchkoli pozdějších změnách těchto pravidel nebo opatření.

Článek 14

Vymáhací postup

1. Pokud adresát nevyhoví certifikátu EPOC ve lhůtě nebo certifikátu EPOC-PR, aniž uvede důvody akceptované vydávajícím orgánem, může vydávající orgán příslušnému orgánu ve vymáhajícím státě předat evropský předávací příkaz s certifikátem EPOC nebo evropský uchovávací příkaz s certifikátem EPOC-PR, jakož

i formulář obsažený v příloze III vyplněný adresátem a jakýkoli jiný relevantní dokument pro účely jeho vymáhání jakýmkoli způsobem umožňujícím vyhotovení písemného záznamu za podmínek, jež vymáhajícímu orgánu umožní ověřit pravost. Za tímto účelem vydávající orgán přeloží příkaz, formulář a jakékoli jiné průvodní dokumenty do jednoho z úředních jazyků tohoto členského státu a informuje o předání adresáta.

2. Po obdržení vymáhající orgán bez dalších formalit uzná evropský předávací příkaz nebo evropský uchovávací příkaz předaný v souladu s odstavcem 1 a učiní nezbytná opatření pro jeho vymáhání, ledaže se domnívá, že se uplatňuje jeden z důvodů stanovených v odstavcích 4 nebo 5 nebo že jsou dotčené údaje chráněny imunitou nebo výsadou podle jeho vnitrostátního práva nebo že jejich sdělení může mít dopad na jeho základní zájmy, jako je národní bezpečnost a obrana. Vymáhající orgán přijme rozhodnutí o uznání příkazu bez zbytečného odkladu a nejpozději pět pracovních dnů po obdržení příkazu.
3. Pokud vymáhající orgán příkaz uzná, formálně požádá adresáta, aby splnil příslušnou povinnost, přičemž ho informuje o možnosti podat odpor proti vymáhání tím, že uplatní důvody uvedené v odstavcích 4 nebo 5, a rovněž respektovat použitelné sankce pro případ nesplnění povinnosti, a stanoví lhůtu pro splnění nebo odpor.
4. Adresát může podat odpor proti vymáhání evropského předávacího příkazu na základě následujících důvodů:
 - (a) evropský předávací příkaz nebyl vydán nebo potvrzen vydávajícím orgánem, jak stanoví článek 4;
 - (b) evropský předávací příkaz nebyl vydán pro trestný čin stanovený v čl. 5 odst. 4;
 - (c) adresát nemohl vyhovět certifikátu EPOC z důvodu faktické nemožnosti nebo vyšší moci nebo proto, že certifikát EPOC obsahuje zjevné chyby;
 - (d) evropský předávací příkaz se netýká údajů uložených poskytovatelem služeb nebo jeho jménem v době obdržení certifikátu EPOC;
 - (e) toto nařízení se na službu nevztahuje;
 - (f) na základě samotných informací obsažených v certifikátu EPOC je zjevné, že tento certifikát očividně porušuje Listinu základních práv Evropské unie nebo je očividně nepatřičný.
5. Adresát může podat odpor proti výkonu evropského uchovávacího příkazu na základě následujících důvodů:
 - (a) evropský uchovávací příkaz nebyl vydán nebo potvrzen vydávajícím orgánem, jak stanoví článek 4;
 - (b) poskytovatel služeb nemohl vyhovět certifikátu EPOC-PR z důvodu faktické nemožnosti nebo vyšší moci nebo proto, že certifikát EPOC-PR obsahuje zjevné chyby;
 - (c) evropský uchovávací příkaz se netýká údajů uložených poskytovatelem služeb nebo jeho jménem v době obdržení certifikátu EPOC-PR;
 - (d) služba nespadá do oblasti působnosti tohoto nařízení;

- (e) na základě samotných informací obsažených v certifikátu EPOC-PR zjevné, že tento certifikát očividně porušuje Listinu základních práv Evropské unie nebo je očividně nepatřičný.
6. V případě námítky adresáta rozhodne vymáhající orgán, zda bude vymáhat příkaz na základě informací poskytnutých adresátem a v případě potřeby na základě doplňujících informací získaných od vydávajícího orgánu v souladu s odstavcem 7.
 7. Před rozhodnutím o neuznání nebo nevymáhání příkazu v souladu s odstavci 2 a 6 konzultuje vymáhající orgán jakýmkoli vhodným způsobem vydávající orgán. Je-li to vhodné, požádá vydávající orgán o další informace. Vydávající orgán odpoví na jakoukoli takovou žádost do pěti pracovních dnů.
 8. Všechna rozhodnutí musí být neprodleně oznámena vydávajícímu orgánu a adresátovi jakýmkoli způsobem umožňujícím vyhotovení písemného záznamu.
 9. Získá-li vymáhající orgán údaje od adresáta, zašle je do dvou pracovních dnů vydávajícímu orgánu, ledaže jsou dotčené údaje chráněny imunitou nebo výsadou podle jeho vnitrostátního práva nebo mají dopad na jeho základní zájmy, jako je národní bezpečnost a obrana. V takovém případě informuje vydávající orgán o důvodech pro nezaslání údajů.
 10. V případě, že adresát nesplní své povinnosti podle uznaného příkazu, jehož vymahatelnost potvrdil vymáhající orgán, uloží tento orgán v souladu s vnitrostátním právem peněžitou sankci. Proti rozhodnutí ukládajícímu sankci je k dispozici účinný opravný prostředek.

Kapitola 4: Opravné prostředky

Článek 15

Přezkumné řízení v případě rozporných povinností v souvislosti se základními právy nebo základními zájmy třetí země

1. Domnívá-li se adresát, že by v případě splnění evropského předávacího příkazu došlo k rozporu s příslušnými právními předpisy třetí země zakazujícími sdělení dotčených údajů z toho důvodu, že je to nezbytné buď pro ochranu základních práv dotčených fyzických osob, nebo pro ochranu základních zájmů třetí země v souvislosti s národní bezpečností nebo obranou, informuje vydávající orgán o svých důvodech pro neprovedení evropského předávacího příkazu v souladu s postupem podle čl. 9 odst. 5.
2. Odůvodněná námitka zahrnuje všechny relevantní podrobnosti o právu třetí země, jeho použitelnosti v daném případě a povaze rozporné povinnosti. Nemůže se opírat o skutečnost, že obdobná ustanovení týkající se podmínek, formalit a postupů vydání předávacího příkazu neexistují v použitelném právu třetí země, ani o samotnou okolnost, že údaje jsou uloženy v třetí zemi.
3. Vydávající orgán přezkoumá evropský předávací příkaz na základě odůvodněné námítky. Má-li vydávající orgán v úmyslu potvrdit oprávněnost evropského předávacího příkazu, požádá příslušný soud ve svém členském státě o přezkum. Provádění příkazu se až do ukončení přezkumného procesu pozastaví.
Příslušný soud nejprve posoudí, zda existuje rozpor, na základě zkoumání toho, zda

- (a) se právo třetí země uplatňuje na základě konkrétních okolností dotčeného případu, a pokud ano,
 - (b) právo třetí země, uplatňuje-li se na konkrétní okolnosti dotčeného případu, zakazuje sdělení dotčených údajů.
- 4. Při provádění tohoto posouzení by měl soud vzít v úvahu, zda právo třetí země místo toho, aby chránilo základní práva nebo základní zájmy třetí země související s národní bezpečností nebo obranou, se očividně snaží chránit jiné zájmy nebo je zaměřeno na ochranu nezákonných činností před žádostmi donucovacích orgánů v kontextu trestního vyšetřování.
 - 5. Shledá-li příslušný soud, že neexistuje žádný relevantní rozpor ve smyslu odstavců 1 a 4, oprávněnost příkazu potvrdí. Shledá-li příslušný soud, že příslušný rozpor ve smyslu odstavců 1 a 4 existuje, předá příslušný soud všechny relevantní faktické a právní informace týkající se případu včetně jeho posouzení ústředním orgánům v dotčené třetí zemi prostřednictvím jejího vnitrostátního ústředního orgánu s patnáctidenní lhůtou na odpověď. Na základě odůvodněné žádosti ústředního orgánu třetí země může být lhůta prodloužena o třicet dnů.
 - 6. Pokud ústřední orgán třetí země informuje ve lhůtě příslušný soud o tom, že vznáší odpor proti výkonu evropského předávacího příkazu v tomto případě, zruší příslušný soud příkaz a informuje vydávající orgán a adresáta. Není-li v (prodloužené) lhůtě vznesena žádná námitka, zašle příslušný soud připomínku, na jejímž základě dostane ústřední orgán třetí země pět dalších dnů na odpověď, a informaci o důsledcích neposkytnutí odpovědi. Není-li v této doplňující lhůtě vznesena žádná námitka, příslušný soud oprávněnost příkazu potvrdí.
 - 7. Určí-li příslušný soud, že příkaz je oprávněný, informuje vydávající orgán a adresáta, který přistoupí k provedení příkazu.

Článek 16

Přezkumné řízení v případě rozporných povinností na základě jiných důvodů

- 1. Domnívá-li se adresát, že v případě splnění evropského předávacího příkazu by došlo k rozporu s příslušnými právními předpisy třetí země zakazujícími sdělení dotčených údajů z jiných důvodů, než jsou důvody uvedené v článku 15, informuje vydávající orgán o svých důvodech pro neprovedení evropského předávacího příkazu v souladu s postupem podle čl. 9 odst. 5.
- 2. Odůvodněná námitka musí zahrnovat všechny relevantní podrobnosti o právu třetí země, jeho použitelnosti v daném případě a povaze rozporné povinnosti. Nemůže se opírat o skutečnost, že obdobná ustanovení týkající se podmínek, formalit a postupů vydání předávacího příkazu neexistují v použitelném právu třetí země, ani o samotnou okolnost, že údaje jsou uloženy v třetí zemi.
- 3. Vydávající orgán přezkoumá evropský předávací příkaz na základě odůvodněné námitky. Má-li vydávající orgán v úmyslu potvrdit oprávněnost evropského předávacího příkazu, požádá příslušný soud ve svém členském státě o přezkum. Provádění příkazu se až do ukončení přezkumného procesu pozastaví.
- 4. Příslušný soud nejprve posoudí, zda existuje rozpor, na základě zkoumání toho, zda

- (a) se právo třetí země uplatňuje na základě konkrétních okolností dotčeného případu, a pokud ano,
 - (b) právo třetí země, uplatňuje-li se na konkrétní okolnosti dotčeného případu, zakazuje sdělení dotčených údajů.
5. Shledá-li příslušný soud, že neexistuje žádný relevantní rozpor ve smyslu odstavců 1 a 4, oprávněnost příkazu potvrdí. Zjistí-li příslušný soud, že právo třetí země uplatněné na specifické okolnosti zkoumaného případu zakazuje sdělení dotčených údajů, rozhodne, zda oprávněnost příkazu potvrdí nebo příkaz zruší, především na základě následujících faktorů:
- (a) zájem chráněný příslušným právem třetí země, včetně zájmu třetí země na tom, aby se zabránilo sdělení údajů;
 - (b) míra spojení trestní věci, pro kterou byl příkaz vydán, s některou z těchto dvou jurisdikcí, jak poukazuje mimo jiné:

místo, státní příslušnost a bydliště osoby, jejíž údaje jsou žádány, a/nebo místo, státní příslušnost a bydliště oběti či obětí;

místo, kde byl daný trestný čin spáchán;
 - (c) míra spojení mezi poskytovatelem služeb a dotčenou třetí zemí; v této souvislosti nestačí k určení podstatné míry spojení místo uchovávání údajů;
 - (d) zájmy vyšetřujícího státu na získání dotčených důkazů na základě závažnosti trestného činu a důležitosti rychlého získání důkazů;
 - (e) možné důsledky nesplnění evropského předávacího příkazu pro adresáta nebo poskytovatele služeb, včetně sankcí, které mohou vzniknout.
6. Rozhodne-li příslušný soud, že příkaz zruší, informuje vydávající orgán a adresáta. . Určí-li příslušný soud, že příkaz je oprávněný, informuje vydávající orgán a adresáta, který přistoupí k provedení příkazu.

Článek 17 *Účinná právní ochrana*

1. Podezřelé a obviněné osoby, jejichž údaje byly získány prostřednictvím evropského předávacího příkazu, mají právo na účinnou právní ochranu proti evropskému předávacímu příkazu během trestního řízení, pro které byl příkaz vydán, aniž jsou dotčeny prostředky právní ochrany dostupné podle směrnice (EU) 2016/680 a nařízení (EU) 2016/679.
2. Pokud osoba, jejíž údaje byly získány, není podezřelou ani obviněnou osobou v trestním řízení, pro které byl příkaz vydán, má tato osoba právo na účinnou právní ochranu proti evropskému předávacímu příkazu ve vydávajícím státě, aniž jsou dotčeny prostředky právní ochrany dostupné podle směrnice (EU) 2016/680 a nařízení (EU) 2016/679.
3. Toto právo na účinnou právní ochranu se uplatňuje u soudu ve vydávajícím státě v souladu s jeho vnitrostátním právem a zahrnuje možnost napadnout zákonost opatření, včetně jeho nezbytnosti a přiměřenosti.

4. Aniž je dotčen článek 11, přijme vydávající orgán vhodná opatření k tomu, aby zajistil poskytnutí informací o možnostech právní ochrany podle vnitrostátního práva a její účinné uplatnění.
5. Uplatňují se zde stejné lhůty nebo jiné podmínky pro uplatnění právní ochrany v obdobných vnitrostátních případech, a to způsobem, který zaručuje dotčeným osobám účinné využití této ochrany.
6. Aniž jsou dotčena vnitrostátní procesní pravidla, členské státy zajistí, aby při trestním řízení ve vydávajícím státě byla při posuzování důkazů získaných prostřednictvím evropského předávacího příkazu dodržována práva na obhajobu a na spravedlivý proces.

Článek 18

Zajištění výsad a imunit podle práva vymáhajícího státu

Pokud jsou údaje o transakcích nebo obsahu získané evropským předávacím příkazem chráněny imunitami nebo výsadami udělenými podle práva členského státu adresáta nebo pokud mají dopad na základní zájmy tohoto členského státu, jako je národní bezpečnost a obrana, zajistí soud ve vydávajícím státě během trestního řízení, pro které byl příkaz vydán, aby tyto důvody byly brány v úvahu stejně, jako kdyby byly stanoveny podle jeho vnitrostátního práva při posuzování relevantnosti a přípustnosti dotčených důkazů. Soud může konzultovat orgány příslušného členského státu, Evropskou soudní síť v trestních věcech nebo Eurojust.

Kapitola 5: Závěrečná ustanovení

Článek 19

Monitorování a podávání zpráv

1. Nejpozději do dne *[datum použitelnosti tohoto nařízení]* zřídí Komise podrobný program pro monitorování výstupů, výsledků a dopadů tohoto nařízení. Program monitorování stanoví prostředky a intervaly shromažďování údajů a dalších potřebných důkazů. Specifikuje opatření, která mají být přijata Komisí a členskými státy při shromažďování a analýze údajů a dalších důkazů.
2. Členské státy sbírají v každém případě statistické údaje a vedou souhrnné statistiky příslušných orgánů. Shromážděné údaje za předchozí kalendářní rok se každý rok zasílají Komisi do 31. března a obsahují:
 - (a) počet vydaných certifikátů EPOC a EPOC-PR podle typu požadovaných údajů, oslovených poskytovatelů služeb a situace (naléhavý případ či nikoli);
 - (b) počet splněných a nesplněných certifikátů EPOC podle typu požadovaných údajů, oslovených poskytovatelů služeb a situace (naléhavý případ či nikoli);
 - (c) u splněných certifikátů EPOC průměrnou dobu pro získání požadovaných údajů od okamžiku jeho vydání do okamžiku získání údajů podle typu požadovaných údajů, oslovených poskytovatelů služeb a situace (naléhavý případ či nikoli);
 - (d) počet odeslaných a obdržených evropských předávacích příkazů k vymáhání vymáhajícímu státu podle typu požadovaných údajů, oslovených poskytovatelů služeb a situace (naléhavý případ či nikoli) a počet splněných příkazů;

- (e) počet právních prostředků proti evropským předávacím příkazům ve vydávajícím státě a ve vymáhajícím státě podle typu požadovaných údajů.

Článek 20 *Změny certifikátů a formulářů*

Komise přijme akty v přenesené pravomoci v souladu s článkem 21 za účelem změn přílohy I, II a III, aby účinně řešila případnou potřebu zlepšení obsahu formulářů EPOC a EPOC-PR a formulářů používaných k poskytnutí informací o nemožnosti provést certifikáty EPOC nebo EPOC-PR.

Článek 21 *Výkon přenesené pravomoci*

1. Pravomoc přijímat akty v přenesené pravomoci je svěřena Komisi za podmínek stanovených v tomto článku.
2. Přenesení pravomoci uvedené v článku 20 je svěřeno Komisi na dobu neurčitou ode dne *[datum použitelnosti tohoto nařízení]*.
3. Evropský parlament nebo Rada mohou přenesení pravomocí uvedených v článku 20 kdykoli zrušit. Rozhodnutím o zrušení se ukončuje přenesení pravomoci v něm blíže určené. Rozhodnutí nabývá účinku prvním dnem po zveřejnění v *Úředním věstníku Evropské unie*, nebo k pozdějšímu dni, který je v něm upřesněn. Nedotýká se platnosti již platných aktů v přenesené pravomoci.
4. Před přijetím aktu v přenesené pravomoci vede Komise konzultace s odborníky ustanovenými jednotlivými členskými státy v souladu se zásadami stanovenými v interinstitucionální dohodě o zdokonalení tvorby právních předpisů ze dne 13. dubna 2016⁵⁰.
5. Přijetí aktu v přenesené pravomoci Komise neprodleně oznámí současně Evropskému parlamentu a Radě.
6. Akt v přenesené pravomoci přijatý podle článku 20 vstoupí v platnost, pouze pokud proti němu Evropský parlament nebo Rada nevysloví námitky ve lhůtě dvou měsíců ode dne, kdy jim byl tento akt oznámen, nebo pokud Evropský parlament i Rada před uplynutím této lhůty informují Komisi o tom, že námitky nevysloví. Z podnětu Evropského parlamentu nebo Rady se tato lhůta prodlouží o dva měsíce.

Článek 22 *Oznámení*

1. Do dne *[datum použitelnosti tohoto nařízení]* sdělí každý členský stát Komisi:
 - (a) orgány, které jsou v souladu s vnitrostátním právem příslušné v souladu s článkem 4 k vydávání a/nebo potvrzování evropských předávacích příkazů a evropských uchovávacích příkazů;
 - (b) vymáhající orgán či orgány, které jsou příslušné k vymáhání evropských předávacích příkazů a evropských uchovávacích příkazů za jiný členský stát;

⁵⁰ Úř. věst. L 123, 12.5.2016, s. 13.

- (c) soudy, které jsou příslušné k vyřízení odůvodněných námitek adresátů v souladu s články 15 a 16.
2. Komise zveřejní informace, které obdrží podle tohoto článku, buď na zvláštní webové stránce, nebo na webové stránce Evropské soudní sítě podle článku 9 rozhodnutí Rady 2008/976/SVV⁵¹.

Článek 23

Vztah k evropským vyšetřovacím příkazům

Orgány členských států mohou i nadále vydávat evropské vyšetřovací příkazy v souladu se směrnicí 2014/41/EU ke shromažďování důkazů, které by spadaly též do oblasti působnosti tohoto nařízení.

Článek 24

Hodnocení

Nejpozději do *[pěti let od data použitelnosti tohoto nařízení]* provede Komise hodnocení tohoto nařízení a předloží Evropskému parlamentu a Radě zprávu o jeho fungování, která zahrnuje posouzení potřeby rozšířit jeho oblast působnosti. V případě potřeby zprávu doplní legislativními návrhy. Toto hodnocení bude provedeno v souladu s pokyny Komise pro zlepšování právní úpravy. Členské státy poskytnou Komisi informace nezbytné pro přípravu této zprávy.

Článek 25

Vstup v platnost

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Použije se ode dne *[šest měsíců po vstupu v platnost]*.

Toto nařízení je závazné v celém rozsahu a přímo použitelné v členských státech v souladu se Smlouvami.

V Bruselu dne

*Za Evropský parlament
předseda / předsedkyně*

*Za Radu
předseda / předsedkyně*

⁵¹ Rozhodnutí Rady 2008/976/SVV ze dne 16. prosince 2008 o Evropské soudní síti (Úř. věst. L 348, 24.12.2008, s. 130).