IV.

**DŮVODOVÁ ZPRÁVA**

**Obecná část**

**Hodnocení dopadů regulace (RIA)**

Na základě výjimky udělené v souladu s čl. 76 odst. 2 Legislativních pravidel vlády a bodem 3. 8 písm. j) Obecných zásad pro hodnocení dopadů regulace (RIA) ministrem pro legislativu a předsedou Legislativní rady vlády (dopis č. j. 38988-2024-20439 ze dne 31. května 2024) nebylo hodnocení dopadů regulace zpracováno.

**Zhodnocení platného právního stavu, odůvodnění hlavních principů navrhované právní úpravy a vysvětlení nezbytnosti navrhované právní úpravy v jejím celku**

V rámci Evropské unie byl přijat tzv. balíček o e-důkazech, který tvoří nařízení Evropského parlamentu a Rady (EU) 2023/1543 ze dne 12. července 2023 o evropském vydávacím příkazu a evropském uchovávacím příkazu pro elektronické důkazy v trestním řízení a pro výkon trestu odnětí svobody po skončení trestního řízení (dále jen „nařízení“) a s ním související směrnice Evropského parlamentu a Rady (EU) 2023/1544 ze dne 12. července 2023, kterou se stanoví harmonizovaná pravidla pro určování určených provozoven a jmenování zástupců za účelem shromažďování elektronických důkazů v trestním řízení (dále jen „směrnice“). Cílem obou evropských předpisů je usnadnění a zrychlení přístupu policejních a justičních orgánů k elektronickým důkazům, které jsou uchovávány poskytovateli služeb sídlícími na území jiného státu, kteří nabízejí služby na území Evropské unie. Spolupráce podle nařízení se účastní Irsko a neúčastní se jí Dánsko.

Dosavadní evropský rámec pro přeshraniční získávání elektronických důkazů, jimiž mohou být např. e-maily, zprávy na sociálních sítích, údaje z různých aplikací nebo dokumenty uložené v cloudu, je založen na vzájemné právní pomoci v této oblasti, která je pro potřeby trestního řízení nepříliš vyhovující, neboť je relativně pomalá a komplikovaná, zatímco elektronické důkazy je s ohledem na jejich dočasnou a zranitelnou povahu třeba uchovat a zajistit co nejrychleji. Základem dosavadního právního rámce je směrnice Evropského parlamentu a Rady 2014/41/EU ze dne 3. dubna 2014 o evropském vyšetřovacím příkazu v trestních věcech, která umožňuje vydat evropský vyšetřovací příkaz za účelem získání důkazu v jiném členském státu Evropské unie (dále jen „členský stát EU“), a Úmluva o vzájemné pomoci v trestních věcech mezi členskými státy Evropské unie, vypracovaná Radou na základě článku 34 Smlouvy o Evropské unii (vyhl. pod č. 55/2006 Sb. m. s.). Získání elektronických důkazů prostřednictvím justiční spolupráce často s ohledem na formálnost řízení trvá dlouho, takže může dojít k tomu, že požadované elektronické důkazy již nejsou v době vyřízení žádosti nebo příkazu k dispozici, kromě toho neexistuje žádný harmonizovaný rámec pro spolupráci s poskytovateli služeb. V důsledku toho je ve stále větší míře využívána dobrovolná přímá spolupráce s poskytovateli služeb (někteří poskytovatelé z třetích zemí přijímají přímé žádosti o jiné než obsahové údaje, tak, jak jim to umožňuje jejich příslušné vnitrostátní právo) a používají se různé vnitrostátní nástroje, podmínky a postupy. Proto Evropská unie přistoupila k vytvoření jednotného rámce pro takovou přímou spolupráci s přeshraničními poskytovateli služeb při získávání elektronických důkazů.

Nařízení stanoví pravidla, na jejichž základě je orgán členského státu EU oprávněn vydat v trestním řízení evropský vydávací příkaz nebo evropský uchovávací příkaz a nařídit poskytovateli služeb, který tyto služby nabízí v Evropské unii a je usazen v jiném členském státě EU nebo, není-li usazen, je zastoupen zástupcem v jiném členském státě EU, aby vydal nebo uchoval pro účely trestního řízení elektronické důkazy bez ohledu na jejich umístění. Podle směrnice mají poskytovatelé služeb usazení v členských státech EU, které se neúčastní spolupráce podle nařízení, povinnost zajistit, aby poskytovatelé služeb nabízející služby na jejich území jmenovali jednoho nebo více zástupců v členských státech EU, které se těchto nástrojů účastní.

Nařízení se nevztahuje na vnitrostátní případy, kdy orgány členského státu EU požadují elektronické důkazy po poskytovateli usazeném nebo zastoupeném na jeho území.

Nařízení se vztahuje pouze na elektronické důkazy uložené poskytovatelem služeb v době obdržení evropského vydávacího příkazu nebo evropského uchovávacího příkazu a neukládá poskytovatelům služeb obecnou povinnost uchovávat určité údaje (data retention). Na základě nařízení nelze požadovat sledování určitých dat do budoucna. Předmětem evropského vydávacího příkazu nebo evropského uchovávacího příkazu mohou být údaje o účastníkovi, údaje o provozu nebo údaje o obsahu, nařízení stanoví podmínky, za kterých lze tyto údaje uchovat nebo vydat.

Nařízení předpokládá, že příslušné orgány a poskytovatelé služeb si budou zasílat osvědčení, příkazy a další informace prostřednictvím jednotného decentralizovaného informačního systému, který umožní rychlou, přímou, interoperabilní, udržitelnou, spolehlivou a bezpečnou přeshraniční elektronickou výměnu potřebných informací. Decentralizovaný informační systém by se měl skládat z informačních systémů členských států EU a agentur a subjektů Evropské unie a z interoperabilních přístupových bodů, jejichž prostřednictvím by měly být tyto systémy vzájemně propojeny.

Přístupové body decentralizovaného informačního systému by měly být založeny na informačním systému e-CODEX, který slouží jako backendová platforma určená pro zabezpečenou výměnu dat. Tento informační systém je upraven v nařízení Evropského parlamentu a Rady (EU) 2022/850 a je od června 2024 spravován Evropskou agenturou pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva eu-LISA (dále jen „eu-LISA“). Systém e-CODEX je členským státům EU poskytován bezplatně, v podobě instalačních balíčků, přičemž vývoj zajišťuje eu-LISA a Evropská komise (dále je „Komise“). Náklady na implementaci e-CODEX ze strany členských států EU spočívají v nasazení tohoto systému do architektury dané organizace/ministerstva v podobě tzv. „přístupového bodu e-CODEX“. Členské státy EU musí v průběhu nasazení systému zajistit všechny nutné integrace na informační systémy a bezpečnostní prvky, zároveň musí zajistit i hardware a dostupnost systému. Po úspěšné implementaci přístupového bodu e-CODEX je nutné na přístupový bod napojit národní informační systém spravující daný přeshraniční justiční nástroj (use-case), tj. informační systém, který je schopen zajistit správu a vydávání evropských vydávacích příkazů a evropských uchovávacích příkazů.

Požadavky nařízení lze buď implementovat do stávajícího národního informačního systému členských států EU, nebo lze využít informační systém, tzv. referenční rozhraní, poskytovaný Komisí členským státům EU. Referenční rozhraní poskytované Komisí je vhodné využít za situace, kdy národní informační systém není možné napojit nebo náklady na implementaci převažují nad přínosem takovéhoto napojení. Pro tyto případy vytváří Komise pro jednotlivé use-cases v přeshraniční justiční spolupráci jednoduché referenční rozhraní umožňující napojení na přístupové body systému e-CODEX, s jehož pomocí je možné daný use-case na národní úrovni realizovat. Referenční rozhraní je členským státům EU poskytováno bezplatně. Náklady na implementaci ze strany členských států EU spočívají v nasazení „referenčního rozhraní“ do architektury dané organizace/ministerstva, včetně nutných integrací na informační systémy a bezpečnostní prvky.

Předpokládá se, že pro přeshraniční use-cases, kde agenda není provozována na základech výstupu projektu „Vývoj a implementace eISIR a jeho společných částí“, tedy na plně elektronickém justičním spisu v podobě modulu eSpis, bude využito referenční rozhraní poskytované ze strany Komise. Pouze v případě use-cases, které spadají do oblasti působnosti státního zastupitelství, u kterého se připravuje nový informační agendový systém ELVIZ na základech výstupů projektu eISIR, se předpokládá přímá implementace do tohoto národního informačního systému bez využití referenčního rozhraní.

Cílem předloženého návrhu je zajistit nezbytnou míru adaptace nařízení, což je třeba provést do 18. srpna 2026. Povinnost příslušných orgánů a poskytovatelů služeb používat decentralizovaný informační systém pro vzájemnou komunikaci se použije po uplynutí jednoho roku od přijetí prováděcích aktů uvedených v článku 25 nařízení.

Pokud jde o českou právní úpravu, přeshraniční získávání důkazů v trestních věcech cestou justiční spolupráce je upraveno v zákoně č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních, ve znění pozdějších předpisů (dále jen „ZMJS“). Pro spolupráci v rámci Evropské unie se užije část pátá hlava XI ZMJS (evropský vyšetřovací příkaz), vůči nečlenským státům EU se použijí ustanovení o právní pomoci obsažená v části třetí hlavě I ZMJS, pokud se přednostně neužije mezinárodní smlouva. Tato ustanovení upravují postupy mezi justičními a ústředními orgány, nikoli přímou spolupráci se soukromými subjekty v jiném státu, kterou nařízení předpokládá. Vzhledem k uvedenému je třeba ZMJS doplnit o ustanovení umožňující řádnou aplikaci nařízení, která by upravila specifika tohoto nového druhu spolupráce, zejména je třeba vymezit příslušnost orgánů k vydávání příkazů a k uznání příkazů vydaných orgány jiných členských států EU, stanovit sankce za porušení povinností poskytovatelů služeb vyhovět příkazu apod.

Takové doplnění nevybočuje z předmětu úpravy ZMJS. Mezinárodní justiční spolupráci v trestních věcech lze vymezit jako součinnost poskytovanou jedním státem druhému státu při uskutečňování jeho trestní pravomoci. Uvedená součinnost zpravidla spočívá v aktivním provádění úkonů trestního řízení orgány jednoho státu na jeho území pro účely trestního řízení vedeného v druhém státu, může se však jednat i o součinnost pasivní, kdy jeden stát umožní, byť ve velmi omezeném rozsahu, na svém území provedení úkonů trestního řízení orgány druhého státu pro trestní řízení v něm vedené (např. u přeshraničního sledování, přeshraničního odposlechu či videokonference). Mezinárodní justiční spolupráci ve věcech trestních nelze chápat pouze jako spolupráci mezi justičními orgány, mezinárodní justiční spolupráce ve věcech trestních se běžně účastní i jiné orgány než justiční (typicky policejní orgány) i soukromé subjekty (např. u doručování písemností do ciziny poštou). Ostatně právním základem nařízení je článek 82 odst. 1 Smlouvy o fungování EU, který upravuje justiční spolupráci v trestních věcech. Spolupráce podle nařízení tak spadá pod pojem mezinárodní justiční spolupráce v trestních věcech.

Nařízení je doprovázeno směrnicí stanovující blíže specifikovaným poskytovatelům služeb povinnost zřídit si na území daného členského státu EU určenou provozovnu či jmenovat zástupce (dále jen „adresát“), a to v závislosti na místě usazení poskytovatele služby. Právě ten by měl v budoucnu přijímat a vykonávat příkazy k vydání a uchování elektronických důkazů. Tento adresát může provedení příkazu odmítnout pouze ze stanovených důvodů (např. pro rozpor s právem třetího státu), v případě odmítnutí příkazu pak bude do procesu zapojen i příslušný orgán státu, ve kterém má být příkaz vykonán. Členské státy EU by rovněž měly zavést účinné a přiměřené sankce k případnému vynucení provedení příkazu. Implementace této směrnice je předmětem návrhu Ministerstva průmyslu a obchodu na vydání zákona o určování provozoven a jmenování zástupců některých poskytovatelů služeb za účelem shromažďování elektronických důkazů v trestním řízení (č.j. MPO 59450/24/71600/01000). Předpokládá se, že aktualizovaný seznam určených provozoven a zástupců poskytovatelů služeb bude dostupný na internetových stránkách Evropské justiční sítě.

Kromě tzv. balíčku o e-důkazech Evropská unie v posledních letech přijala v oblasti digitalizace justice několik dalších předpisů, jež s nařízením úzce souvisí a které se týkají způsobu komunikace. Pro trestní oblast je relevantní zejména nařízení Evropského parlamentu a Rady (EU) 2023/2844 ze dne 13. prosince 2023 o digitalizaci justiční spolupráce a přístupu ke spravedlnosti v přeshraničních občanských, obchodních a trestních věcech a o změně některých aktů v oblasti justiční spolupráce (dále jen „nařízení o digitalizaci justiční spolupráce“) a s ním úzce související směrnice Evropského parlamentu a Rady (EU) 2023/2843 ze dne 13. prosince 2023, kterou se mění směrnice Evropského parlamentu a Rady 2011/99/EU a 2014/41/EU, směrnice Rady 2003/8/ES a rámcová rozhodnutí Rady 2002/584/SVV, 2003/577/SVV, 2005/214/SVV, 2006/783/SVV, 2008/909/SVV, 2008/947/SVV, 2009/829/SVV a 2009/948/SVV (dále jen „směrnice o digitalizaci justiční spolupráce“). Oba uvedené evropské předpisy představují harmonizovaný soubor pravidel pro digitalizaci justiční spolupráce, jehož cílem je zlepšit účinnost a odolnost komunikačních toků při spolupráci uskutečňované v rámci Evropské unie mezi justičními a jinými příslušnými orgány. V trestní oblasti přitom tyto předpisy upravují pouze způsob komunikace mezi příslušnými orgány účastnícími se justiční spolupráce ve věcech trestních, nedotýkají se způsobu komunikace mezi orgány ve vnitrostátních případech nebo způsobu komunikace s osobami zúčastněnými na řízení.

Účinná přeshraniční justiční spolupráce vyžaduje bezpečnou, spolehlivou a časově úspornou komunikaci mezi příslušnými orgány. Nařízení o digitalizaci justiční spolupráce proto zavádí při přeshraniční justiční spolupráci nový způsob digitální komunikace mezi příslušnými orgány. Směrnice o digitalizaci justiční spolupráce mění příslušné směrnice a rámcová rozhodnutí, aby spolupráce podle těchto předpisů probíhala způsobem uvedeným v článku 3 nařízení o digitalizaci justiční spolupráce. Podle tohoto ustanovení musí komunikace mezi příslušnými orgány členských států EU probíhat prostřednictvím decentralizovaného informačního systému (k tomu srov. viz výše). Výjimkou, kdy lze komunikaci vést alternativními prostředky, jsou případy, kdy komunikace prostřednictvím decentralizovaného informačního systému není možná v důsledku narušení decentralizovaného informačního systému (technická závada), fyzické nebo technické povahy předávaného materiálu (jedná se o důkaz, je potřeba listinný originál) nebo v důsledku zásahu vyšší moci. Jiné komunikační prostředky lze použít také tehdy, pokud není použití decentralizovaného informačního systému v dané situaci vhodné, např. je možné zvolit jednodušší a méně formální způsob komunikace jako je e-mail apod.

Nařízení o digitalizaci justiční spolupráce je přímo účinné a k jeho řádné aplikaci není zapotřebí český právní řád adaptovat. Směrnice o digitalizaci justiční spolupráce si vyžádá dílčí změny právního řádu, kdy je v ZMJS třeba u jednotlivých druhů justiční spolupráce stanovit, že justiční a ústřední orgány komunikují s příslušnými orgány jiných členských států EU v souladu s článkem 3 nařízení o digitalizaci justiční spolupráce, tj. primárně prostřednictvím decentralizovaného informačního systému, pokud není takový způsob komunikace vyloučen nebo není vhodný – směrnice o digitalizaci justiční spolupráce pak výslovně stanoví, v kterých případech se článek 3 nařízení o digitalizaci justiční spolupráce nepoužije (typicky u nejrůznějších konzultačních povinností). Datum, do kdy má být dosaženo souladu vnitrostátního práva s požadavky směrnice o digitalizaci justiční spolupráce, se odvíjí od data vstupu v platnost příslušného prováděcího aktu uvedeného v článku 10 odst. 3 nařízení o digitalizaci justiční spolupráce. Tyto prováděcí akty jsou přijímány postupně zvlášť k jednotlivým skupinám evropských předpisů upravujících justiční spolupráci ve věcech trestních, kdy jde v zásadě o technickou implementaci požadavků nařízení o digitalizaci justiční spolupráce − prováděcí akty stanoví např. technickou specifikaci způsobů komunikace elektronickými prostředky, technickou specifikaci komunikačních protokolů, bezpečnostní standardy, časový harmonogram aj. Prováděcí akty budou přijímány postupně v časovém období od 17. ledna 2026 do 17. ledna 2029, přičemž členské státy EU mají povinnost mít příslušnou implementační právní úpravu platnou vždy do dvou let od vstupu příslušného právního aktu v platnost. Tato dvouletá lhůta slouží k zajištění připravenosti vnitrostátních orgánů používat decentralizovaný informační systém (zajištění jejich připojení k systému, proškolení aj.). Implementační úprava pak bude účinná prvním dnem kalendářního měsíce následujícího po uplynutí této lhůty.

**Zhodnocení souladu navrhované právní úpravy s ústavním pořádkem České republiky, mezinárodními smlouvami, jimiž je Česká republika vázána, a s předpisy Evropské unie, judikaturou soudních orgánů Evropské unie nebo obecnými právními zásadami práva Evropské unie a judikaturou ESLP**

Navrhovaná právní úprava je v souladu s ústavním pořádkem České republiky, neboť v úpravou dotčené oblasti (v oblasti justiční spolupráce) nemění požadavky na zachování ochrany ústavně zaručených práv, zejména pokud jde o právo na ochranu nedotknutelnosti osoby a jejího soukromí podle článku 7 odst. 1 Listiny základních práv a svobod (dále jen „Listina“), právo na ochranu soukromého života a ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě podle článku 10 Listiny, právo na ochranu tajemství písemností a záznamů uchovávaných v soukromí nebo zasílaných poštou anebo jiným způsobem podle článku 13 Listiny a právo na soudní a jinou ochranu ve smyslu článků 36 až 40 Listiny.

Ve vztahu k článku 13 Listiny Ústavní soud uvedl, že ochrana poskytovaná tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením se netýká jen jejich vlastního obsahu, nýbrž i dalších údajů evidovaných při registraci telekomunikačního provozu ve vztahu ke konkrétním osobám [srov. např. nález ze dne 22. ledna 2001 sp. zn. II. ÚS 502/2000 (N 11/21 SbNU 83), nález ze dne 13. února 2001 sp. zn. IV. ÚS 536/2000 (N 29/21 SbNU 251), nález ze dne 27. srpna 2001 sp. zn. IV. ÚS 78/01 (N 123/23 SbNU 197), nález ze dne 13. září 2006 sp. zn. I. ÚS 191/05 (N 161/42 SbNU 327) nebo nález ze dne 27. září 2007 sp. zn. II. ÚS 789/06 (N 150/46 SbNU 489)].

Navrhovaná právní úprava ve spojení s nařízením zaručuje dotčené osobě, aby byla o zásazích do svého soukromého života informována a měla zaručený účinný prostředek nápravy proti takovému zásahu. Příkaz požadující údaje o obsahu nebo provozu musí vydat soudce.

Navrhovaná právní úprava je rovněž v souladu se závazky České republiky vyplývajícími z Evropské úmluvy o ochraně lidských práv a základních svobod (dále jen „Úmluva“) a jejích dodatkových protokolů, neboť nic nemění na zásadách, které se uplatňují v oblasti justiční spolupráce a trestního řízení již podle stávající právní úpravy.

Ve vztahu k mezinárodní justiční spolupráci jsou relevantní zejména rozsudky Evropského soudu pro lidská práva (dále jen „ESLP“) zabývající se právem na spravedlivý proces podle článku 6 Úmluvy, a to zejména ve vztahu k zajištění účinných práv obhajoby – uvést lze např. rozsudek ESLP ve věci Breukhoven proti České republice ze dne 21. 7. 2011, č. 44438/06, rozsudek ESLP ve věci Fąfrowicz proti Polsku ze dne 17. 4. 2012, č. 43609/07, rozsudek ESLP ve věci Damir Sibgatullin proti Rusku ze dne 24. 4. 2012, č. 1413/05, rozsudek ESLP ve věci Tseber proti České republice ze dne 22. 11. 2012, č. 46203/08, rozsudek ESLP ve věci Zhukovskyi proti Ukrajině ze dne 3. 3. 2011, č. 31240/03, rozsudek ESLP ve věci A. M. proti Itálii ze dne 14. 12.1 999, č. 37019/97 nebo rozsudek ESLP ve věci Solakov proti Bývalé jugoslávské republice Makedonii ze dne 31. 10. 2001, č. 47023/99.

Ve vztahu k ochraně soukromí je relevantní článek 8 Úmluvy zaručující právo na respektování soukromého a rodinného života, obydlí a korespondence. Zásah do tohoto práva musí být odůvodněn legitimním zájmem, jakým je ochrana národní bezpečnosti, veřejné bezpečnosti či hospodářského blahobytu země, zájem na předcházení nepokojům a zločinnosti, ochrana zdraví nebo morálky nebo ochrana práv a svobod jiných, musí být na základě zákona a musí být nezbytný v demokratické společnosti. Uvedené požadavky jsou v navrhované právní úpravě ve spojení s nařízením respektovány (údaje o provozu a obsahu mohou být vyžadovány pouze v souvislosti s řízením o trestných činech vyšší typové závažnosti, kdy sledovaným cílem je tak efektivní postihování závažné trestné činnosti).

Právo na soukromí a rodinný život je obecně chráněno také v článcích 17 a 23 Mezinárodního paktu o občanských a politických právech (vyhl. ve Sbírce zákonů pod č. 120/1976 Sb.). Ve vztahu k dítěti je pak právo na ochranu soukromí a rodinného života chráněno v článku 16 Úmluvy o právech dítěte (vyhl. ve Sbírce zákonů pod č. 104/1991 Sb.).

Pokud jde o mezinárodní smlouvy uzavřené v oblasti justiční spolupráce, vztah k nim vymezuje článek 32 nařízení, který uvádí, že nařízením nejsou dotčeny mezinárodní nástroje, dohody a ujednání o shromažďování důkazů, které spadají do oblasti působnosti tohoto nařízení. Členské státy EU jsou povinny do 18. srpna 2026 oznámit Komisi nástroje, dohody a ujednání, která budou i nadále používat. Členské státy EU rovněž oznámí Komisi nové dohody nebo ujednání do tří měsíců od jejich podpisu. Česká republika takové oznámení učiní, přičemž lze předpokládat, že obsahově bude podobné oznámení, které bylo učiněno v návaznosti na směrnici Evropského parlamentu a Rady 2014/41/EU ze dne 3. dubna 2014 o evropském vyšetřovacím příkazu v trestních věcech, kdy pouze budou případně zohledněny nové sjednávané smlouvy v této oblasti.

Relevantními smlouvami v oblasti přeshraničního získávání elektronických důkazů jsou zejména:

* Evropská úmluva Rady Evropy o vzájemné pomoci ve věcech trestních ze dne 20. dubna 1959 (vyhlášená pod č. 550/1992 Sb.), jakož i její dva dodatkové protokoly a dvoustranné dohody uzavřené podle článku 26 této úmluvy,
* Úmluva o vzájemné pomoci v trestních věcech mezi členskými státy Evropské unie, vypracovaná Radou na základě článku 34 Smlouvy o Evropské unii (vyhlášená pod č. 55/2006 Sb. m. s.) a její protokol,
* Úmluva Rady Evropy o počítačové kriminalitě, přijatá v Budapešti dne 23. listopadu 2001 (vyhlášená pod č. 104/2013 Sb. m. s.).

Aktuálně byl v rámci Rady Evropy sjednán Druhý dodatkový protokol k Úmluvě o počítačové kriminalitě o posílené spolupráci a zpřístupňování elektronických důkazů, který Česká republika podepsala dne 20. června 2024, a to s výhradou ratifikace. Předmětný dodatkový protokol upravuje mimo jiné přímou spolupráci se subjekty poskytujícími služby v oblasti registrace jmen domén spočívající v možnosti žádat údaje s cílem identifikovat držitele registrace jména domény. Dále je upravena možnost žádat po poskytovateli služby údaje o účastníkovi, které má uvedený poskytovatel služeb ve svém držení nebo pod svou kontrolou. Pokud jde o data o účastníkovi a data o provozu, je možné se obrátit na orgán jiného smluvního státu s žádostí o vymožení povinnosti poskytovatele taková data vydat.

Další iniciativou na poli přeshraničního získávání elektronických důkazů bylo přijetí rozhodnutí Rady EU dne 6. června 2019, kterým Rada zmocnila Komisi k zahájení jednání za účelem uzavření dohody mezi Evropskou unií a Spojenými státy americkými o přeshraničním přístupu k elektronickým důkazům pro justiční spolupráci v trestních věcech a dodatek k tomuto rozhodnutí obsahující vyjednávací směrnice. Dohoda má být tzv. *executive agreement* ve smyslu amerického zákona stručně označovaného jako US Cloud Act[[1]](#footnote-1) a jejím účelem má být řešení konfliktů právních úprav, resp. odstranění překážek, které by poskytovatelům služeb na území jedné strany bránily poskytovat údaje na základě příkazů orgánů druhé strany.

Uvedené smlouvy se uplatní paralelně vedle nařízení.

Pokud jde o bilaterální smlouvy uzavřené v oblasti justiční spolupráce v trestních věcech Českou republikou s jinými členskými státy EU, jde zejména o smlouvy uzavřené s Bulharskem, Chorvatskem, Itálií, Rakouskem, Rumunskem, Slovenskem, Slovinskem a Německem.

Z relevantních předpisů Evropské unie, které upravují oblast přeshraničního opatřování a zajištění důkazů, je zásadní směrnice Evropského parlamentu a Rady 2014/41/EU ze dne 3. dubna 2014 o evropském vyšetřovacím příkazu v trestních věcech, která se uplatní mezi členskými státy EU (implementační úprava je obsažena v části páté hlavě XI ZMJS). Této směrnice se neúčastní Irsko a Dánsko, vůči kterým se užije rámcové rozhodnutí Rady 2003/577/SVV ze dne 22. července 2003 o výkonu příkazů k zajištění majetku nebo důkazních prostředků v Evropské unii, pokud jde o zajištění důkazních prostředků (implementační úprava je obsažena v části páté hlavě III ZMJS). Nařízení se uplatní paralelně vedle uvedených předpisů EU, resp. vedle ustanovení tyto předpisy implementujících, neboť upravuje přímou spolupráci s poskytovateli služeb, která ale nijak nevylučuje využití tradiční cesty „klasické“ justiční spolupráce mezi orgány – viz i článek 32 nařízení, podle něhož nařízením nejsou dotčeny unijní předpisy o shromažďování důkazů, které spadá do oblasti působnosti nařízení. Vzhledem k tomu, že nařízení výše uvedenou směrnici a rámcové rozhodnutí neruší, ani nemodifikuje, a Česká republika je povinna provést tyto předpisy do svého právního řádu, je zřejmé, že musí umožnit jejich použitelnost vůči členským státům EU, které se budou těchto předpisů dovolávat.

Navrhovaná právní úprava dále zajišťuje implementaci směrnice o digitalizaci justiční spolupráce, s čímž souvisí přímo účinné nařízení o digitalizaci justiční spolupráce. Tato směrnice mění následující evropské předpisy:

* rámcové rozhodnutí Rady 2002/584/SVV ze dne 13. června 2002 o evropském zatýkacím rozkazu a postupech předávání mezi členskými státy,
* rámcové rozhodnutí Rady 2003/577/SVV ze dne 22. července 2003 o výkonu příkazů k zajištění majetku nebo důkazních prostředků v Evropské unii,
* rámcové rozhodnutí Rady 2009/829/SVV ze dne 23. října 2009 o uplatnění zásady vzájemného uznávání na rozhodnutí o opatřeních dohledu jakožto alternativy zajišťovací vazby mezi členskými státy Evropské unie,
* rámcové rozhodnutí Rady 2009/948/SVV ze dne 30. listopadu 2009 o předcházení kompetenčním sporům při výkonu pravomoci v trestním řízení a jejich řešení,
* rámcové rozhodnutí Rady 2005/214/SVV ze dne 24. února 2005 o uplatňování zásady vzájemného uznávání peněžitých trestů a pokut,
* rámcové rozhodnutí Rady 2006/783/SVV ze dne 6. října 2006 o uplatňování zásady vzájemného uznávání příkazů ke konfiskaci,
* rámcové rozhodnutí Rady 2008/909/SVV ze dne 27. listopadu 2008 o uplatňování zásady vzájemného uznávání rozsudků v trestních věcech, které ukládají trest odnětí svobody nebo opatření spojená se zbavením osobní svobody, za účelem jejich výkonu v Evropské unii,
* rámcové rozhodnutí Rady 2008/947/SVV ze dne 27. listopadu 2008 o uplatňování zásady vzájemného uznávání na rozsudky a rozhodnutí o probaci za účelem dohledu nad probačními opatřeními a alternativními tresty,
* směrnice 2011/99/EU ze dne 13. prosince 2011 o evropském ochranném příkazu,
* směrnice 2014/41/EU ze dne 3. dubna 2014 o evropském vyšetřovacím příkazu v trestních věcech.

V rámci judikatury Evropského soudního dvora v oblasti mezinárodní justiční spolupráce jsou ve vztahu k navržené právní úpravě relevantní zejména:

* rozsudek pátého senátu Soudního dvora EU ze dne 29. dubna 2021 ve věci C-665/20 PPU, z něhož vyplývá, že není v souladu s evropskými předpisy takové ustanovení právního řádu členského státu EU, které stanoví určitý důvod pro odmítnutí výkonu mezinárodní justiční spolupráce ve věcech trestních jako obligatorní, pokud je tento důvod v příslušném právním aktu Evropské unie formulován jako fakultativní, a
* rozsudek Soudního dvora EU ze dne 16. prosince 2021 ve věci C-724/19 HP, z něhož vyplývá, že pokud podle vnitrostátního práva členského státu EU má pravomoc nařídit vydání provozních a lokalizačních údajů v souvislosti s telekomunikačním provozem (podle českého trestního řádu jde o § 88a tr. ř.) výlučně soudce, pak není státní zástupce oprávněn sám vydat evropský vyšetřovací příkaz požadující provedení takového úkonu v jiném členském státu EU.

Pokud jde o druhý z uvedených rozsudků, členské státy EU jej aplikují různými způsoby, přičemž za rovnocenné vydání příkazu se považuje i udělení souhlasu soudce s příkazem nebo potvrzení příkazu soudcem (formu potvrzení příkazu zvolila i Česká republika).

Navržená úprava je s těmito rozhodnutími v souladu.

**Předpokládaný hospodářský a finanční dopad navrhované právní úpravy na státní rozpočet a ostatní veřejné rozpočty a na podnikatelské prostředí České republiky**

Finanční dopady spojené s technickou adaptací nařízení a směrnice o digitalizaci justiční spolupráce lze v době přípravy tohoto návrhu jen velmi obtížně odhadnout vzhledem k tomu, že jednání k těmto otázkám a příprava technických předpisů na úrovni Evropské unie, jakož i vnitrostátní technická realizace, teprve probíhají.

Náklady spojené s nařízením (nikoli tedy bezprostředně s adaptační úpravou) lze předpokládat jednak v souvislosti se zřízením přístupových bodů k decentralizovanému informačnímu systému, které budou sloužit k zasílání příkazů, a jednak se zajištěním interoperability národních informačních systémů s tímto systémem. Podle odhadů Komise budou v prvních dvou letech náklady každého členského státu EU na instalaci činit 100 000 EUR ročně, tj. cca 2 400 000 Kč. Tato částka zahrnuje náklady na zařízení a lidské zdroje potřebné k jeho konfiguraci. Přibližně 200 000 EUR, tj. cca 4 800 000 Kč, bude potřeba na zajištění podpory pro rostoucí počet uživatelů. Od třetího roku účinnosti se nepředpokládají žádné náklady na hardware a instalaci, pouze náklady spojené s podporou uživatelů a údržbou systému. Ty se odhadují na 300 000 EUR ročně, tj. cca 7 200 000 Kč.

Vzhledem k aktuálně na úrovni Evropské unie diskutovaným variantám architektonických řešení pro decentralizovaný informační systém pro e-důkazy lze nicméně spíše očekávat, že odhadované náklady jsou podhodnocené. Do celkových nákladů je nutné zahrnout také náklady na integraci dílčích informačních systémů k zajištění centralizace databáze justičních orgánů a následnou správu Ministerstvem spravedlnosti. Navíc, v závislosti na zvoleném řešení na úrovni Evropské unie, je třeba počítat s navýšenými náklady na správu integrací a dostupnost systému ze strany Ministerstva spravedlnosti a velikost úložiště dat. Dále je nutné zohlednit náklady spojené se správou a údržbou databáze CBD, kterou by měl dodavatel mít jako součást servisu a podpory. Předpokládá se tedy, že skutečné náklady mohou být vyšší, než uvádí Komise, konkrétně lze předpokládat jejich následující výši (bez DPH):

**Tabulka č. 1 - Předpokládaná výše nákladů (bez DPH)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **období** | **instalace + 30 %** | **podpora pro rostoucí počet uživatelů + 30 %** | **podpora uživatelů a údržba IS + 30 %** | **Celkem**  (v Kč) |
| 1. a 2. rok | 3 120 000 | 6 240 000 | 0 | 9 360 000 |
| 3. rok a následující léta – jde o trvalý výdaj | 0 | 0 | 9 360 000 | 9 360 000 |

Uvedený odhad výše nákladů se týká pouze nákladů spojených s technickou realizací nařízení (obdobné dopady lze očekávat i u směrnice o digitalizaci justiční spolupráce), nicméně před touto realizací je již třeba technicky implementovat (funkční požadavky) systému e-CODEX pro účely nařízení Evropského parlamentu a Rady (EU) 2020/1784 o doručování soudních a mimosoudních písemností ve věcech občanských a obchodních v členských státech (doručování písemností) a **nařízení Evropského parlamentu a Rady (EU) 2020/1783 o spolupráci soudů členských států při dokazování v občanských a obchodních věcech (dokazování),** která nabývají účinnosti dříve než nařízení.

Konečná výše finančních nákladů spojená s technickou implementací požadavků nařízení a směrnice o digitalizaci justiční spolupráce se proto bude odvíjet od zvoleného architektonického návrhu řešení technické implementace. Pokud bude využita již existující infrastruktura a přístupový bod e-CODEX zřízený pro citovaná nařízení o doručování a dokazování, mohlo by následně s účinností jednotlivých evropských předpisů v oblasti justiční spolupráce docházet pouze ke škálování existující infrastruktury a rozšiřování o jednotlivé přeshraniční nástroje za předpokladu, že to bude technicky možné. Takové řešení by bylo finančně mnohem méně nákladné, než pokud by se pro jednotlivé evropské předpisy realizovaly samostatné instance systému e-CODEX v podobě nasazení samostatného přístupového bodu systému e-CODEX a samostatného referenčního rozhraní, jak to uvádí ve svém odhadu Komise. Protože však dosud nejsou známy všechny technické požadavky a specifikace u jednotlivých evropských předpisů, v době přípravy této novely dosud není známo, která z variant bude přicházet v úvahu − zda méně náročné nebo více náročné finanční řešení.

Proto lze v tuto chvíli jen velmi obtížně odhadnout výši finančních nákladů spojených přímo s realizací nařízení a směrnice o digitalizaci přeshraniční justiční spolupráce. Pokud bude možné z větší části použít referenční rozhraní a infrastrukturu vytvořené pro výše uvedená nařízení o doručování a nařízení o dokazování, lze méně nákladnou finanční variantu odhadem vyčíslit pro nařízení a stejně tak pro směrnici o digitalizaci justiční spolupráce takto:

**Tabulka č. 2 – Předpokládaná výše nákladů spojená s projektem e-CODEX (bez DPH)**

|  |  |
| --- | --- |
| **Harmonogram projektu e-CODEX** | **Výše nákladů** (v Kč) |
| Realizace projektu (3. 11. 2024 - 30.4.2025) | 2 000 000 až 6 000 000 |
| Provoz/rozvoj po ukončení projektu (1. 5. 2025 – 31. 5. 2028) | 4 000 000 |
| Úprava stávajících národních informačních justičních systémů spojených s digitalizací přeshraničních justičních nástrojů | 1 000 000 |

Pokud nebude technicky možné použít již vytvořené referenční rozhraní a infrastrukturu pro účely nařízení a směrnice o digitalizaci justiční spolupráce, pak by byly náklady vyšší tak, jak je uvedeno v tabulce č. 1.

Vzhledem k tomu, že tyto náklady nelze v současné době přesněji vyčíslit, Ministerstvo spravedlnosti pokryje tyto náklady v rámci schválených a výdajových limitů své rozpočtové kapitoly bez navyšujících požadavků na státní rozpočet.

Pokud jde o způsob připojení policejních orgánů, dosud není známé přesné technické řešení. Pokud policejní orgány budou provozovat svůj vlastní přístupový bod k systému e-CODEX, podle článků 8 a 9 nařízení Evropského parlamentu a Rady (EU) 2022/850 o systému e-CODEX a podle článku 23 nařízení budou náklady na instalaci, provoz a údržbu přístupových bodů systému e-CODEX hrazeny z rozpočtové kapitoly Ministerstva vnitra (případně i jiných ministerstev, pokud by se k systému přímo připojovaly i jiné policejní orgány než Policie České republiky). Stejně tak, pokud se policejní orgány budou pouze připojovat na již existující přístupový bod nebo informační systém provozující use-case, budou náklady s tím spojené v souladu s recitálem 88 a články 14 a 23 nařízení rovněž hrazeny z rozpočtové kapitoly Ministerstva vnitra (případně jiných ministerstev). V tuto chvíli nelze přesně stanovit výši nákladů s tím spojených, protože technické řešení je stále předmětem diskuzí probíhajících jak na evropské, tak na národní úrovni. Lze tedy pouze odhadovat, že náklady s tím spojené mohou dosahovat výše jednotek milionů Kč. Vzhledem k tomu, že tyto náklady nelze v současné době přesněji vyčíslit, Ministerstvo vnitra (a případně jiné dotčené resorty) pokryje tyto náklady v rámci schválených výdajových limitů své rozpočtové kapitoly bez navyšujících požadavků na státní rozpočet.

Náklady spojené s instalací, provozem a údržbou přístupových bodů ponesou také poskytovatelé služeb, kteří se budou připojovat na území České republiky.

Podle článku 28 nařízení mají členské státy EU předávat Komisi statistické údaje v tomto článku specifikované. V odstavci 3 daného článku se stanoví, že ode dne 18. srpna 2026 (účinnost nařízení) mohou být statistické údaje v případě výměny údajů prováděné prostřednictvím decentralizovaného informačního systému shromažďovány vnitrostátními portály pomocí počítačového programu. Podle dostupných informací bude referenční rozhraní poskytované Komisí obsahovat většinu požadovaných statistických údajů a bude umožňovat stažení sledovaných dat do formátu XML a MS Excel. Ministerstvo spravedlnosti tak bude vynakládat pouze náklady spojené s rozvojem datového skladu, v němž se budou statistické údaje z referenčního rozhraní ukládat a z nějž se budou zasílat. Přesný výčet statistických údajů, které bude možné z referenčního rozhraní získat, není v současné chvíli znám, protože uvedená problematika bude teprve řešena v rámci vyjednávání dokumentů souvisejících s nařízením na úrovni pracovních skupin Evropské komise. Lze nicméně předpokládat, že referenční rozhraní by mělo statisticky zaznamenávat údaje v rozsahu článku 28 písm. a) až g) a i) nařízení. Ostatní požadované statistické údaje, tj. údaje obsažené v článku 28 písm. h) a j) nařízení (účinné prostředky nápravy a platby poskytovatelům služeb), referenční rozhraní nebude moci sledovat. Ve vztahu k těmto zbytkovým statistickým údajům (a ve vztahu k ostatním statistickým údajům do doby zprovoznění decentralizovaného informačního systému) vzniknou Ministerstvu spravedlnosti zvýšené finanční náklady spojené s úpravou informačních systémů (ISAS, ISYZ, ISVKS) a následnou úpravou datového skladu CSLAV, ve výši přibližně 1 milion Kč. Tyto zvýšené finanční náklady Ministerstvo spravedlnosti pokryje v rámci schválených výdajových limitů své rozpočtové kapitoly bez navyšujících požadavků na státní rozpočet.

Další dílčí náklady vzniknou v souvislosti s povinností proplácet náklady na vydání provozních údajů zahraničnímu poskytovateli služeb, pokud splní vnitrostátní podmínky pro jejich proplacení (článek 14 nařízení). Lze nicméně očekávat, že půjde o jednotky případů ročně, kdy při výši úhrady za vydání provozních údajů v jednom případu (podle stávající vyhlášky č. 462/2013 Sb. jde o úhrady v řádu stokorun) lze předpokládat, že tyto zvýšené náklady bude možné pokrýt v rámci schválených výdajových limitů své rozpočtové kapitoly bez navyšujících požadavků na státní rozpočet.

Jiné dopady na státní rozpočet a na ostatní veřejné rozpočty se nepředpokládají.

Navrhovaná právní úprava není spojena s dopady na podnikatelské prostředí v České republice.

**Zhodnocení sociálních dopadů, včetně dopadů na specifické skupiny obyvatel, zejména osoby sociálně slabé, osoby se zdravotním postižením a národnostní menšiny, dopadů na ochranu práv dětí a dopadů na rodiny, zejména s ohledem na plnění funkcí rodiny, s ohledem na počet vyživovaných členů, na případnou přítomnost hendikepovaných členů a rodiny samoživitelů, rodiny se třemi a více dětmi a další specifické životní situace, dále s ohledem na posílení integrity a stability rodiny a posílení rodinné harmonie, lepší rovnováhy mezi prací a rodinou a na posílení mezigeneračních a širších příbuzenských vztahů**

Navrhovaná právní úprava není spojena s žádnými negativními sociálními dopady, dopady na specifické skupiny obyvatel, děti a na rodiny.

**Zhodnocení dopadů na práva a povinnosti fyzických a právnických osob**

Navrhovaná právní úprava ve spojení s nařízením zavádí povinnost poskytovatelům služeb vyhovět přeshraničním příkazům orgánů činných v trestním řízení jiného členského státu EU na uchování nebo vydání určité kategorie dat, které má poskytovatel k dispozici. Za nedůvodné nesplnění této povinnosti hrozí poskytovateli sankce až do výše 2 % jeho celkového celosvětového ročního obratu za předchozí finanční rok. Podle stávající právní úpravy jsou stejné kategorie údajů po poskytovatelích vyžadovány cestou klasické justiční spolupráce mezi orgány států na základě evropského vyšetřovacího příkazu nebo žádosti o právní pomoc, případně přímo na základě dobrovolné spolupráce, nejedná se tedy o novou povinnost, nově se pouze jednotně stanoví výše sankce za nesplnění této povinnosti. Nařízení rovněž stanoví lhůty pro vyřízení příkazu.

Nařízení stanoví poskytovatelům služeb povinnost používat při komunikaci s orgány činnými v trestním řízení zabezpečený decentralizovaný informační systém zřízený jednotně na úrovni Evropské unie. Povinnost zajistit poskytovatelům přístup k tomuto systému mají jednotlivé členské státy EU. Poskytovatelé služeb jsou povinni nést náklady nezbytné pro úspěšnou integraci decentralizovaného informačního systému nebo jinou interakci s ním.

Navrhovaná právní úprava sama o sobě nemá nové bezprostřední dopady do práv a povinností fyzických osob, předmětné kategorie údajů o osobách mohou být vyžadovány již podle stávající právní úpravy. Nařízení pouze harmonizuje podmínky, za kterých mohou být tyto údaje vyžadovány a stanoví jednotný způsob komunikace mezi orgány a poskytovateli služeb prostřednictvím informačního systému, který bude povinně využíván.

V souvislosti s implementací směrnice o digitalizaci justiční spolupráce navržená úprava nezasahuje do práv a povinností fyzických a právnických osob, neboť se pouze upravuje způsob komunikace mezi příslušnými justičními orgány a ústředními orgány při přeshraniční spolupráci s orgány jiných členských států EU.

**Zhodnocení dopadů stávající úpravy a navrhovaného řešení ve vztahu k zákazu diskriminace a ve vztahu k rovnosti mužů a žen**

Stávající ani navrhovaná právní úprava nemá bezprostřední dopady na rovnost mužů a žen a nevede k diskriminaci jednoho z pohlaví, neboť nijak nerozlišuje, ani nezvýhodňuje jedno z pohlaví a nestanoví pro ně odlišné podmínky.

**Zhodnocení dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů**

Navrhovaná úprava není spojena s rozšířením okruhu dat zpracovávaných orgány činnými v trestním řízení a nepřináší žádný nový druh zpracování osobních údajů. Předmětné kategorie údajů podle nařízení již mohou orgány činné v trestním řízení vyžadovat podle stávající právní úpravy.

Orgány činné v trestním řízení zpracovávají osobní údaje osob zúčastněných na řízení v rozsahu nezbytném pro dané řízení, jehož smyslem je objasnit, zda byl spáchán trestný čin, a zjistit jeho pachatele. Zpracování osobních údajů v rozsahu nezbytném pro vedení trestního řízení je nezbytné a přiměřené sledovanému cíli, což vyplývá ze zásady přiměřenosti, kterou jsou orgány činné v trestním řízení vázány (§ 2 odst. 4 tr. ř.). Ve vztahu k mladistvým pachatelům je pak povinnost chránit jejich osobní údaje ještě zdůrazněna v základní zásadě uvedené v § 3 odst. 5 zákona o soudnictví ve věcech mládeže, podle níž je třeba v řízení podle tohoto zákona chránit osobní údaje osoby, proti níž se řízení vede, a její soukromí, aby každá taková osoba byla chráněna před škodlivými vlivy, a při dodržení zásady, že je považována za nevinnou, dokud její vina nebyla prokázána zákonným způsobem.

Navrhovaná právní úprava je v souladu se směrnicí 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.

Zvýšené dopady na problematiku ochrany soukromí a osobních údajů se nepředpokládají. Orgány činné v trestním řízení budou postupovat podle dosavadních procesních pravidel, která jim již nyní umožňují v zákonem stanovených případech v nezbytném rozsahu zasahovat do soukromí osob a pro potřeby příslušného řízení nakládat s jejich osobními údaji.

**Zhodnocení korupčních rizik**

Navrhovaná právní úprava není spojena s vyššími korupčními riziky, než kterým čelí státní orgány obecně již dnes. Korupční riziko pro ně tak není nové, je přítomno i při aplikaci stávající účinné právní úpravy. Prostředky ochrany proti tomuto riziku jsou tudíž obsaženy již ve stávající právní úpravě. Předně jsou to zákonné požadavky a postupy při výběru osoby státního zástupce a soudce, u nichž jsou kladeny zvýšené nároky na jejich morální integritu a osobnostní záruky. Dále jsou to pak určité mechanismy kontroly, jež v přípravném řízení spočívají zejména ve výkonu dozoru státního zástupce nad zákonností postupu policejního orgánu a ve výkonu dohledu vyššího státního zastupitelství nad nižším státním zastupitelstvím (a případně dohledu nad dohledem) a v soudní fázi řízení pak v systému řádných a mimořádných opravných prostředků.

Kromě těchto procesních pojistek se čelí tomuto riziku i hrozbou trestního stíhání toho, kdo úplatek nabídl, poskytl nebo slíbil, jakož i toho, kdo si dal úplatek slíbit nebo jej přijal. Je-li pachatelem trestného činu přijetí úplatku úřední osoba, jde o okolnost podmiňující použití vyšší trestní sazby, kde hrozí trest odnětí svobody ve výši tři léta až deset let (v případě, kdy byl tento trestný čin spáchán v úmyslu opatřit sobě nebo jinému značný prospěch, je dána trestní sazba pět až dvanáct let). V případě podplacení je rovněž skutečnost, že byl tento trestný čin spáchán vůči úřední osobě, okolností podmiňující použití vyšší trestní sazby (pachateli v tomto případě hrozí podle § 332 odst. 2 tr. zák. trest odnětí svobody ve výši jeden rok až šest let).

**Zhodnocení dopadů na bezpečnost nebo obranu státu**

Navrhovaná právní úprava nemá dopady na bezpečnost státu.

**Zhodnocení dopadů na životní prostředí**

Navrhovaná právní úprava není spojena s dopady na životní prostředí.

**Zhodnocení územních dopadů, včetně dopadů na územní samosprávné celky**

Navrhovaná právní úprava se nedotýká postavení územních samosprávných celků a nepřináší územní dopady.

**Zhodnocení souladu navrhovaného řešení se zásadami tvorby digitálně přívětivé legislativy, včetně zhodnocení rizika vyloučení nebo omezení možnosti přístupu specifických skupin osob k některým službám v důsledku digitalizace jejich poskytování (digitální vyloučení)**

Navrhovaná právní úprava neupravuje poskytování služeb konkrétním osobám jako takové, upravuje pouze způsob komunikace a spolupráci mezi orgány činnými v trestním řízení a poskytovateli služeb při uchování a vydání údajů, které slouží k důkazním účelům v trestním řízení, a dále způsob komunikace mezi justičními a ústředními orgány České republiky a orgány jiných členských států EU při přeshraniční spolupráci ve věcech trestních. Navrhovaná právní úprava tedy nesouvisí přímo s digitalizací služeb a nemá negativní dopady na možnosti přístupu specifických skupin osob k nim.

Na okraj lze uvést, že navrhovaná právní úprava přispívá k digitalizaci tím, že se předpokládá, že jak orgány činné v trestním řízení a poskytovatelé služeb, tak i justiční a ústřední orgány budou při přeshraniční komunikaci užívat jednotný zabezpečený decentralizovaný informační systém, tj. komunikace bude probíhat přednostně s využitím elektronických prostředků.

**Zhodnocení, zda návrh právního předpisu neobsahuje ustanovení, které by bylo svou povahou technickým předpisem podle právního předpisu upravujícího technické požadavky na výrobky, a informace o splnění oznamovací povinnosti podle tohoto právního předpisu**

Žádné ustanovení navržené právní úpravy nemá povahu technického předpisu.

**Zhodnocení, zda návrhem právního předpisu není zakládána veřejná podpora**

Návrh zákona nezakládá veřejnou podporu.

**Zvláštní část**

**K bodům 1 a 2 (poznámky pod čarou č. 1 a 53)**

Do výčtu předpisů EU, které jsou zapracovány do ZMJS, se doplňuje i nařízení a směrnice o digitalizaci justiční spolupráce.

**K bodu 3 (§ 65a odst. 1)**

Vzhledem k tomu, že v návaznosti na občas probíhající reorganizace Policie České republiky dochází ke změnám útvaru Policie České republiky, který plní roli kontaktního místa pro účely uchovávání elektronických důkazů v rámci přeshraniční spolupráce, a na tyto změny je třeba pružně reagovat, navrhuje se nově vymezit příslušný útvar Policie České republiky jako útvar, který je výkonem této agendy pověřený policejním prezidentem. Tímto útvarem je aktuálně Národní centrála proti terorismu, extremismu a kybernetické kriminalitě SKPV. Vnitrostátně došlo k jejímu vyčlenění z Národní centrály proti organizovanému zločinu SKPV, která byla původním kontaktním bodem pro účely Úmluvy o počítačové kriminalitě (tato změna zatím nebyla plně reflektována v prohlášení podle článku 35 Úmluvy o počítačové kriminalitě, nicméně sekretariát Úmluvy byl o změně vyrozuměn a v praxi je správný postup zajištěn).

**K bodům 4 až 17 (§ 189 odst. 3, § 226 odst. 3, § 256 odst. 4, § 260 odst. 3, § 261 odst. 3, § 273 odst. 4, § 278 odst. 5, § 292 odst. 3, § 298 odst. 3, § 314 odst. 3, § 323 odst. 6, § 336 odst. 5, § 340 odst. 3 a § 357 odst. 4)**

Předmětná ustanovení implementují relevantní články směrnice o digitalizaci justiční spolupráce ve vztahu k jednotlivým druhům justiční spolupráce, konkrétně jde o předávací řízení na základě evropského zatýkacího rozkazu (rámcové rozhodnutí 2002/584/SVV), výkon příkazů k zajištění majetku se státy, které nejsou vázány nařízením 2018/1805 (rámcové rozhodnutí 2003/577/SVV), uznání a výkon opatření nahrazujících vazbu (rámcové rozhodnutí 2009/829/SVV), postupy při řešení kompetenčních sporů (rámcové rozhodnutí 2009/948/SVV), uznání a výkon rozhodnutí ukládajících peněžité tresty a pokuty (rámcové rozhodnutí 2005/214/SVV), uznání a výkon rozhodnutí ukládajících propadnutí nebo zabrání majetku se státy, které nejsou vázány nařízením 2018/1805 (rámcové rozhodnutí 2006/783/SVV), uznání a výkon rozhodnutí ukládajících nepodmíněný trest odnětí svobody nebo ochranné opatření spojené se zbavením osobní svobody (rámcové rozhodnutí Rady 2008/909/SVV), uznání a výkon rozhodnutí ukládajících trest nespojený se zbavením osobní svobody, dohled nebo přiměřená omezením a povinnosti (rámcové rozhodnutí 2008/947/SVV), uznání evropského ochranného příkazu (směrnice 2011/99/EU) a zajištění výkonu evropského vyšetřovacího příkazu (směrnice 2014/41/EU).

U uvedených druhů justiční spolupráce se stanoví, že justiční orgány a ústřední orgány (Ministerstvo spravedlnosti a Nejvyšší státní zastupitelství, pokud plní úlohu ústředního orgánu) komunikují s příslušnými orgány jiného členského státu EU (justičními orgány nebo jinými orgány označenými členským státem EU jako příslušnými k justiční spolupráci a ústředními orgány, pokud napomáhají justičním a jiným orgánům nebo se účastní doručování písemností v rámci justiční spolupráce) v souladu s článkem 3 nařízení o digitalizaci justiční spolupráce. Uvedený požadavek se tedy netýká případů, kdy s jiným členským státem EU komunikuje jiný český orgán, který není v postavení justičního nebo ústředního orgánu – např. Ministerstvo financí při uzavírání dohody o sdílení propadlého nebo zabraného majetku, Úřad pro zastupování státu ve věcech majetkových při sdílení majetku s jiným členským státem EU, ale třeba i Ministerstvo spravedlnosti, pokud řeší regresní nároky nebo sdílí propadlé nebo zabrané peněžní prostředky nebo peněžní prostředky získané prodejem propadlého nebo zabraného majetku s jiným členským státem EU.

Článek 3 nařízení o digitalizaci justiční spolupráce stanoví, že se pro vzájemnou písemnou komunikaci použije přednostně decentralizovaný informační systém. Decentralizovaný informační systém by měl být vždy považován za nejvhodnější prostředek pro výměnu formulářů příkazů a osvědčení upravených v příslušných směrnicích a rámcových rozhodnutí (s výjimkou případu, kdy se zástupci příslušných orgánů členských států EU nacházejí na stejném místě v určitém členském státě EU za účelem pomoci při výkonu postupů justiční spolupráce, např. pokud vydávající orgán napomáhá při výkonu evropského vyšetřovacího příkazu ve vykonávajícím státě nebo pokud příslušné orgány různých členských států EU koordinují postupy justiční spolupráce za osobní účasti).

Tento způsob komunikace se neužije, pokud to není možné z důvodu narušení decentralizovaného informačního systému (technické závady), neumožňuje to povaha předávaného materiálu (např. jde o důkaz, je třeba předat listinný originál) nebo z důvodu zásahu vyšší moci (např. živelná pohroma) − v takovém případě se použije jiný bezpečný prostředek komunikace. Jiné komunikační prostředky lze použít také tehdy, pokud není použití decentralizovaného informačního systému v dané situaci vhodné, např. je možné zvolit jednodušší a méně formální způsob komunikace jako je e-mail v případě, kdy nejde o výměnu důvěrných materiálů (např. zjišťování, který orgán jiného členského státu EU je příslušný k poskytnutí spolupráce). Podle bodu 25 odůvodnění nařízení o digitalizaci justiční spolupráce by použití jiných komunikačních prostředků mohlo být vhodné také tehdy, pokud komunikace zahrnuje nakládání s citlivými údaji nebo pokud by převedení objemné dokumentace do elektronické podoby představovalo nepřiměřenou administrativní zátěž.

Směrnice o digitalizaci justiční spolupráce pak výslovně upravuje další výjimky, kdy se decentralizovaný informační systém k vzájemné komunikaci nepoužije, typicky jde o případy, kdy je pro uznání nebo výkon rozhodnutí či příkazu vyžadováno určité stanovisko nebo souhlas nebo kdy je jiný členský stát EU informován o tom, že nelze dodržet pořádkové lhůty stanovené pro uznání nebo výkon rozhodnutí či příkazu, tj. jde o určité konzultace nebo výměnu informací, jež lze provádět i méně formálními způsoby. Směrnice o digitalizaci justiční spolupráce umožňuje také zaslání žádosti o průvoz přes území třetího členského státu EU prostřednictvím zabezpečených komunikačních kanálů, čímž se má na mysli využití policejní spolupráce − tuto výjimku se navrhuje nevyužít, neboť v České republice o průvoz žádá Ministerstvo spravedlnosti, které tento způsob komunikace nevyužívá.

Pokud jde o nařízení 2018/1805 (příkazy k zajištění a ke konfiskaci), je měněno přímo nařízením o digitalizaci justiční spolupráce a také pro justiční spolupráci probíhající na jeho základě se použije článek 3 nařízení o digitalizaci justiční spolupráce se stanovenými výjimkami.

**K bodu 18 (§ 374 odst. 5)**

Předmětné ustanovení se navrhuje vypustit pro nadbytečnost a nepřesnost. Skutečnost, že obviněný (a jeho obhájce) má právo podávat návrhy, včetně návrhů na opatření důkazu, plyne dostatečně z § 33 tr. ř., který se subsidiárně použije i v řízení o evropském vyšetřovacím příkazu. Kromě toho toto právo nemá jen obviněný, ale také zadržený podezřelý a podezřelý ve zkráceném přípravném řízení (a jejich obhájci), u nichž lze dovodit, že je proti nim vedeno trestní řízení, což zakládá jejich určitá obhajovací práva (obdobná právům obviněného, když § 76 odst. 5 i § 179b odst. 2 tr. řádu odkazují na § 33 odst. 1 trestního řádu, kde je obsaženo i právo činit návrhy).

**K bodu 19 (hlava XII)**

Vzhledem k tomu, že nařízení upravuje nový typ spolupráce přímo mezi orgány vydávajícího státu a poskytovatelem služeb, je třeba do ZMJS zakotvit novou hlavu, která bude obsahovat adaptační úpravu k nařízení. Upravit je třeba zejména otázky týkající se příslušnosti k jednotlivým úkonům, sankcí za porušení povinností adresátem příkazu, úhrady nákladů poskytovateli služeb a některé další dílčí otázky.

**K dílu 1**

V tomto dílu jsou společně pro adaptační úpravu vymezeny některé pojmy v návaznosti na článek 3 nařízení, který je jinak přímo aplikovatelný.

**K § 396**

Definice pojmů obsahuje nařízení v článku 3. Vzhledem k tomu, že v trestním zákoníku a v § 7b tr. ř., který upravuje uchování dat, se používá pojem „data“, který je jednotně užíván i v rámci rekodifikace trestního práva procesního a předpokládá se jeho užití i u příkazu k vydání dat (stávající § 88a tr. ř.) v předpokládané novele trestního řádu, která naváže na tuto adaptační novelu, navrhuje se používat i v hlavě XII pojem „data“, a nikoli pojem „údaje“, který se používá v nařízení. Vzhledem k tomu se pak odkazuje na příslušné články nařízení, kde jsou jednotlivé typy dat vymezeny, nutno uvést, že poněkud odchylně od jejich vymezení v trestním řádu.

Předně jde o kategorii dat o účastníkovi (článek 3 odst. 9 nařízení), kterými se rozumí data, jež poskytovatel služeb shromáždil v souvislosti s poskytováním služeb (účastí na nich), která se týkají

* totožnosti účastníka nebo zákazníka (subsriber or customer), např. poskytnuté jméno, datum narození, poštovní nebo zeměpisná adresa, fakturační a platební údaje, telefonní číslo nebo e-mailová adresa,
* druhu služby a jejího trvání, včetně technických údajů a údajů identifikujících související technická opatření nebo rozhraní, která účastník nebo zákazník použil nebo mu byla poskytnuta v době počáteční registrace nebo aktivace, a údajů týkajících se potvrzení použití služby, kromě hesel nebo jiných autentizačních prostředků použitých místo hesla, poskytnutých uživatelem nebo vytvořených na žádost uživatele.

Z formuláře osvědčení obsaženého v příloze nařízení pak vyplývá, že do této kategorie dat spadají zejména následující data (nejde o uzavřený výčet):

* jméno a příjmení, datum narození, poštovní nebo zeměpisná adresa, kontaktní údaje   
  (e-mailová adresa, telefonní číslo) a další relevantní informace týkající se totožnosti účastníka,
* datum a čas úvodní registrace, typ registrace, kopie smlouvy, způsob ověření totožnosti během registrace, kopie dokumentů předložených účastníkem,
* druh služby a její trvání, včetně identifikátoru (identifikátorů), které účastník používá nebo které mu byly poskytnuty při úvodní registraci nebo aktivaci (např. telefonní číslo, číslo SIM karty, adresy MAC), a související zařízení,
* informace o profilu (např. uživatelské jméno, uživatelský pseudonym, profilová fotografie),
* údaje o potvrzení využívání služby, např. alternativní e-mailová adresa poskytnutá účastníkem,
* informace o debetní nebo kreditní kartě (poskytnuté účastníkem pro účely fakturace), včetně jiných platebních prostředků,
* kódy PUK.

Pokud jde o data týkající se služby, poskytovatel služeb by tedy měl v rámci této kategorie dat sdělit druh služby, kterou účastník nebo zákazník užívá, a dobu užívání služby jako takové (např. že uživatel má u poskytovatele od roku XXXX zřízenu e-mailovou schránku [XXX@XXX.XX](mailto:XXX@XXX.XX)). Oproti tomu v případě dotazu s odkazem na článek 3 odst. 11 nařízení (údaje o provozu) by měl poskytovatel služeb sdělit informace o relaci přístupu uživatele ke službě („session to a service“ – tedy, že uživatel přistupoval k zájmové e-mailové schránce [XXX@XXX.XX](mailto:XXX@XXX.XX) z IP adresy XXXXXX dne XX.XX.XXXX v čase od XX:XX do XX:XX).

Další kategorií dat, která je zavedena nově výlučně pro účely nařízení a dosud v mezinárodních dokumentech nebyla vymezena, jsou data požadovaná výhradně za účelem identifikace uživatele, kterými se rozumí adresy internetového protokolu a v případě potřeby příslušné zdrojové porty a časové razítko, konkrétně datum a čas, nebo technické ekvivalenty těchto identifikátorů a souvisejících informací, pokud je donucovací nebo justiční orgány požadují výhradně k identifikaci uživatele v rámci konkrétního trestního řízení.

Nařízení na tzv. IP adresy, přístupová čísla a související informace nahlíží dvojí optikou. Tato data jsou zpravidla součástí záznamu událostí, tzv. serverového logu, který uvádí začátek a ukončení přístupu uživatele ke službě. Často se jedná o individuální IP adresu, ať statickou nebo dynamickou, nebo jiný identifikátor, který identifikuje síťové rozhraní použité během přístupu. K informaci o zahájení a ukončení přístupu uživatele ke službě jsou zapotřebí i související informace, jako jsou zdrojový port a časové razítko, protože IP adresy jsou často sdíleny více uživateli, například je-li používána technologie Carrier Grade NAT (CGN) nebo technicky rovnocenná řešení. Podle *acquis* Unie se však IP adresy považují za osobní údaje a musí požívat plné ochrany v souladu s *acquis* Unie v oblasti ochrany údajů. Kromě toho mohou být IP adresy za určitých okolností považovány za data o provozu. Za data o provozu jsou v některých členských státech EU považována rovněž přístupová čísla a související informace. Pro účely konkrétního trestního řízení však mohou orgány za výhradním účelem identifikace uživatele požádat o IP adresu, jakož i přístupová čísla a související informace, předtím než lze od poskytovatele služeb vyžádat data o účastníkovi související s tímto identifikátorem. V takových případech stanoví nařízení pro vyžádání těchto dat stejný režim jako pro data o účastníkovi ve smyslu tohoto nařízení.

Pokud však IP adresy, přístupová čísla a související informace nejsou vyžadovány výhradně k identifikaci uživatele služby v konkrétním trestním řízení, jsou vyžadovány k získání informací, které více zasahují do soukromí, jako jsou informace o kontaktech a místu pobytu uživatele. Samy o sobě by mohly sloužit k vytvoření podrobného profilu dotčené osoby, avšak zároveň mohou být zpracovány a analyzovány snadněji než data o obsahu, neboť již mají strukturovaný a standardizovaný formát. Pro tyto případy nařízení stanoví pro IP adresy, přístupová čísla a související informace stejný režim jako pro data o provozu.

Daty o provozu se rozumí data, která se týkají poskytování služby nabízené poskytovatelem služeb a která slouží k poskytnutí kontextu nebo doplňujících informací o takové službě a jsou vytvářena nebo zpracovávána informačním systémem poskytovatele služeb, jako například zdroj a cíl zprávy nebo jiného typu interakce, data o umístění zařízení, datum, čas, trvání, velikost, trasa, formát, použitý protokol a typ komprese, a další metadata elektronických komunikací a data, jiná než data o účastníkovi, týkající se zahájení a ukončení relace přístupu uživatele ke službě, jako je datum a čas použití, čas přihlášení uživatele ke službě a čas jeho odhlášení.

Z formuláře osvědčení obsaženého v příloze nařízení pak vyplývá, že do této kategorie dat spadají zejména následující data (nejde o uzavřený výčet):

1. u (mobilních) telefonů:

* odchozí a příchozí identifikátory (telefonní číslo, IMSI, IMEI),
* čas a trvání připojení,
* pokusy o volání,
* ID základové stanice, včetně zeměpisných informací (souřadnic X/Y), v době začátku a ukončení spojení,
* použitý nositel / telefonní služba (např. UMTS, GPRS);

1. u internetu:

* informace o směrování (zdrojová IP adresa, cílová IP adresa či adresy, číslo či čísla portu, prohlížeče, informace o záhlaví v e-mailu, ID zpráva),
* ID základové stanice, včetně zeměpisných informací (souřadnic X/Y), v době začátku a ukončení spojení,
* objem dat,
* datum a čas připojení,
* trvání připojení nebo přístupu;

1. u hostingu:

* soubor protokolů,
* tikety;

1. jiné

* historie nákupů,
* historie dobíjení zůstatku předplacené služby.

Daty o obsahu se pak rozumí jakákoli data v digitálním formátu, jako je text, hlas, videa, obrázky a zvuk, a to jiná než data o účastníkovi nebo data o provozu. Z formuláře osvědčení obsaženého v příloze nařízení pak vyplývá, že do této kategorie dat spadají zejména následující data (nejde o uzavřený výčet):

* výpis (webové) poštovní schránky,
* výpis online úložiště (dat vygenerovaných uživatelem),
* výpis stránek,
* protokol/záloha zpráv,
* výpis hlasových zpráv,
* obsah serveru,
* zálohování zařízení,
* seznam kontaktů.

V odstavci 2 se zavádí součinnostní ustanovení obdobné jako u jiných nástrojů spolupráce mezi členskými státy EU pro účely statistického sledování a předávání relevantních údajů Komisi v souladu s článkem 28 nařízení.

**K dílu 2**

V tomto dílu jsou obsažena nezbytná adaptační ustanovení pro případ, že evropský vydávací příkaz nebo evropský uchovávací příkaz vydá příslušný orgán jiného členského státu EU a nařízení předpokládá určitou součinnost orgánu ve vykonávajícím státu (tj. v České republice) při přezkoumávání důvodů pro odmítnutí výkonu takového příkazu nebo za účelem zajištění výkonu příkazu.

**K § 397**

V tomto ustanovení se nastavuje příslušnost českých orgánů v případech, kdy nařízení předpokládá určitou aktivitu na straně orgánů vykonávajícího státu.

V odstavci 1 se jednotně nastavuje příslušnost ve vztahu k evropskému vydávacímu příkazu orgánu jiného členského státu EU.

Prvním z případů, kdy český orgán bude činný, je přijetí oznámení orgánu jiného členského státu EU o vydání evropského vydávacího příkazu (článek 8 nařízení) a následné přezkoumání osvědčení a případné uplatnění některého z důvodu pro odmítnutí výkonu evropského vydávacího příkazu (článek 12 nařízení). Druhým případem je pak samotné uznání a zajištění výkonu evropského vydávacího příkazu vydaného orgánem jiného členského státu EU podle článku 16 nařízení.

Za účelem zajištění jednotné příslušnosti k typově obdobným úkonům se pro uvedené případy nastavuje shodná příslušnost českých justičních orgánů jako pro přijetí žádosti o právní pomoc a její vyřízení (§ 48 odst. 5 věta první, § 48 odst. 6 až 9 a § 48a ZMJS) a pro zajištění výkonu evropského vyšetřovacího příkazu (§ 360 ZMJS), pokud je na jejich základě požadováno vydání obdobných dat. Evropský vydávací příkaz je rychlejší alternativou k evropskému vyšetřovacímu příkazu, proto je žádoucí nastavit jednotnou příslušnost.

V odstavci 2 je nastavena příslušnost českých orgánů ve vztahu k uznání a zajištění výkonu evropského uchovávacího příkazu a souvisejícím úkonům. V případě evropského uchovávacího příkazu se oznámení o jeho vydání orgánu vykonávajícího státu nezasílá, ingerence českého orgánu tak přichází v úvahu pouze v případě, kdy adresát nevyhověl příkazu k uchování dat a orgán jiného členského státu EU požaduje zajištění výkonu takového příkazu po příslušném orgánu ve vykonávajícím státu podle článku 16 nařízení. Příslušnost k zajištění výkonu takového příkazu se nastavuje shodně jako pro případy zajištění výkonu žádosti o uchování dat podle § 65b ZMJS, tj. příslušným orgánem je útvar Policie České republiky pověřený policejním prezidentem (aktuálně je tímto úvarem Národní centrála proti terorismu, extremismu a kybernetické kriminalitě SKPV).

Centralizace vyřizování žádostí o uchování dat a evropských uchovávacích příkazů u jednoho policejního útvaru zajistí nastavení jednotného postupu pro všechny případy a rychlý výkon žádostí a příkazů, což je v případě uchování dat s ohledem na zranitelnost takových dat a hrozbu jejich rychlé ztráty zapotřebí. Zohledňuje se dosavadní nastavený způsob přijímání žádostí podle Budapešťské úmluvy a nově i podle jejího druhého dodatkového protokolu, který v článku 9 předpokládá, že smluvní strana přijme taková legislativní a jiná opatření, která mohou být v případě mimořádné události nezbytná pro to, aby její kontaktní místo v rámci sítě, která funguje 24 hodin denně, 7 dnů v týdnu a která je uvedena v článku 35 úmluvy, mohlo kontaktnímu místu v jiné smluvní straně předat žádost a přijmout žádost od kontaktního místa v jiné smluvní straně s cílem získat okamžitou pomoc při zabezpečení toho, aby poskytovatel služeb na území uvedené smluvní strany urychleně uchoval a zpřístupnil specifikovaná uložená počítačová data, které má uvedený poskytoval služeb ve svém držení nebo pod svou kontrolou, a to bez žádosti o vzájemnou pomoc. V případě uchování dat má jít o urychlený typ spolupráce, čemuž má napomoci i předávání a vyřizování žádostí/příkazů přes jeden kontaktní bod.

Vzhledem k tomu, že se jedná o justiční spolupráci pro účely trestního řízení, vyžaduje se souhlas příslušného justičního orgánu – státního zástupce nebo soudu, který bude příslušný k uznání a zajištění výkonu evropského vydávacího příkazu týkajícího se uchovaných dat, pokud o to jiný členský stát EU požádá. Při udělení souhlasu justiční orgán posoudí, zda není dán důvod pro odmítnutí podle článku 16 odst. 5 nařízení.

V odstavci 3 je pak nastaven postup pro případ, že orgán jiného členského státu EU zašle příkaz nepříslušnému orgánu.

**K § 398**

V tomto ustanovení jsou obsažena adaptační ustanovení navazující na postup podle článků 8 až 12 nařízení. Jde o případ, kdy orgán jiného členského státu EU vydal evropský vydávací příkaz týkající se dat o provozu, s výjimkou dat požadovaných výhradně pro identifikaci uživatele, nebo dat o obsahu a nejsou dány důvody uvedené v článku 8 odst. 2 nařízení. Spolu s oznámením zašle příslušný orgán jiného členského státu EU také vyplněný formulář osvědčení (certifikátu) uvedený v příloze I nařízení přeložený do českého jazyka nebo jiného jazyka, v němž Česká republika prohlásí, že bude osvědčení přijímat (slovenský jazyk).

Samotný příkaz se automaticky nezasílá, lze si jej nicméně vyžádat podle článku 8 odst. 3 nařízení. Český orgán je povinen osvědčení přezkoumat nejpozději do 10 dnů (pořádková lhůta) a v naléhavých případech ve smyslu článku 3 odst. 18 nařízení do 96 hodin (pořádková lhůta) a v této lhůtě může uplatnit důvod pro odmítnutí výkonu příkazu.

Navržená úprava v odstavci 1 reaguje na to, že jedním z důvodů pro odmítnutí výkonu evropského vydávacího příkazu je podle článku 12 odst. 1 písm. a) nařízení i skutečnost, že požadované údaje jsou chráněny imunitami nebo výsadami podle práva vykonávajícího státu, které brání výkonu příkazu. Stejně jako u jiných typů justiční spolupráce se upravuje možnost, aby se v případě pochybností o tom, zda je taková imunita nebo výsada dána, justiční orgán obrátil na Nejvyšší soud.

V odstavci 2 se pak upravuje výsledek přezkoumání příkazu v případě, že justiční orgán neshledá žádný důvod pro odmítnutí (jde o obdobný postup jako u evropského vyšetřovacího příkazu). V takovém případě o tom učiní záznam do spisu, a pokud je možné takové vyrozumění provést před uplynutím desetidenní lhůty uvedené v článku 10 odst. 2 nařízení, informuje adresáta příkazu, že žádný důvod pro odmítnutí příkazu neshledal (článek 10 odst. 2 nařízení možnost takového vyrozumění nepřímo předpokládá, ale neupravuje je jako povinné). V naléhavých případech je justiční orgán povinen o tom vyrozumět orgán vydávajícího státu a adresáta nejpozději do 96 hodin od doručení oznámení (článek 10 odst. 4 nařízení).

**K § 399**

V tomto ustanovení je upraveno uznání a zajištění výkonu evropského vydávacího příkazu orgánu jiného členského státu EU. Jde o případ, kdy orgán jiného členského státu EU nebyl úspěšný při požadování dat přímo od poskytovatele služeb a ten mu bezdůvodně nebo z důvodů, které nařízení nepředpokládá, odmítl data poskytnout, nebo mu je neposkytl ve stanovené lhůtě. V takovém případě orgán jiného členského státu EU, který vydal evropský vydávací příkaz, může požádat příslušný český orgán, aby příkaz uznal a zajistil jeho výkon. Kromě evropského vydávacího příkazu zašle také formulář uvedený v příloze III nařízení a další potřebné informace – vše přeložené do českého jazyka nebo jiného jazyka, o kterém Česká republika prohlásí, že jej akceptuje (slovenský jazyk). Český justiční orgán, jehož příslušnost se stanoví podle § 397 odst. 1, pak přezkoumá, zda není dán důvod pro odmítnutí podle článku 16 odst. 4 nařízení. Pokud shledá, že je takový důvod dán, podle článku 16 odst. 2 nařízení o tom informuje adresáta příkazu a orgán vydávajícího státu. Pokud žádný důvod pro odmítnutí dán není, justiční orgán vydá příkaz, který bude obsahovat výrok o uznání příkazu jiného členského státu EU a výrok, kterým nařídí adresátovi příkazu, aby data poskytl, odůvodnění, v němž justiční orgán uvede, jakým způsobem posoudil podmínky pro výkon příkazu, tj. že nejsou dány důvody pro odmítnutí jeho výkonu, a poučení, v němž jsou obsaženy informace uvedené v článku 16 odst. 3 nařízení. Příkaz doručí adresátovi. Zároveň se staví najisto, že poskytovatel může žádat úhradu nákladů vzniklých v souvislosti výkonem evropského vydávacího příkazu pouze po státu, jehož orgán vydal evropský vydávací příkaz, a to za podmínek stanovených jeho právním řádem, i v případě, že český orgán vydal příkaz k zajištění jeho výkonu.

Vzhledem k tomu, že nařízení nastavuje soudní příslušnost k vydání evropského vydávacího příkazu v některých případech odlišně od trestního řádu, za účelem zachování jednotnosti soudního přezkumu při vyžadování dat na území České republiky se v odstavci 2 stanoví, že pokud by v obdobném vnitrostátním případu byl k vydání příkazu v přípravném řízení příslušný soudce, státní zástupce podá soudci návrh na vydání takového příkazu (příslušnost soudce se určí podle § 48a ZMJS). V odůvodnění svého návrhu musí státní zástupce rovněž uvést, jakým způsobem posoudil splnění podmínek pro výkon evropského vydávacího příkazu, tímto posouzením však soudce není vázán a v rámci hodnocení podmínek pro vydání příkazu, kterým se zajišťuje výkon evropského vydávacího příkazu, může dospět k jiným závěrům.

Pro výkon evropského vydávacího příkazu vydaného jiným členským státem EU se v přípravném řízení stanoví pouze jeden vykonávající orgán, a to státní zástupce (jde o obdobné řešení jako u vyřizování žádostí o právní pomoc či výkonu evropského vyšetřovacího příkazu). I když si státní zástupce za účelem zajištění výkonu evropského vydávacího příkazu u určité kategorie dat musí vyžádat příkaz soudce, soudce se nestává vykonávajícím orgánem, což je v souladu s vymezením vykonávajícího orgánu podle článku 3 bodu 17 nařízení, který odkazuje na orgán příslušný k obdržení evropského vydávacího příkazu. Tomu pak odpovídá navržená úprava, podle níž informace a konzultace pro účely rozhodnutí podle článku 16 odst. 7 nařízení vyžaduje státní zástupce.

Adresát příkazu, kterým se uznává a zajišťuje výkon evropského vydávacího příkazu, může proti takovému příkazu ve stanovené lhůtě podat námitky (článek 16 odst. 3 nařízení). V návaznosti na článek 16 odst. 6 nařízení se stanoví příslušnost orgánu k posouzení podaných námitek – je nastavena stejně jako pro vydání příkazu. Dále se stanoví postup při vyhovění námitce nebo při jejím shledáním nedůvodnou.

Navržená úprava v odstavci 3 reaguje na to, že jedním z důvodů pro odmítnutí výkonu evropského vydávacího příkazu je podle článku 16 odst. 4 písm. f) nařízení i skutečnost, že požadované údaje jsou chráněny imunitami nebo výsadami podle práva vykonávajícího státu, které brání výkonu příkazu. Stejně jako u jiných typů justiční spolupráce se upravuje možnost, aby se v případě pochybností o tom, zda je taková imunita nebo výsada dána, justiční orgán obrátil na Nejvyšší soud.

V odstavci 5 se upravuje postup v případě, že nelze nebo není třeba evropský vydávací příkaz jiného členského státu EU vykonat.

**K § 400**

V tomto ustanovení je upraveno uznání a zajištění výkonu evropského uchovávacího příkazu orgánu jiného členského státu EU. Jde o případ, kdy orgán jiného členského státu EU nebyl úspěšný s požadavkem na uchování dat přímo poskytovatelem služeb a ten bezdůvodně nebo z důvodů, které nařízení nepředpokládá, odmítl data uchovat, nebo je neuchoval ve stanovené lhůtě. V takovém případě orgán jiného členského státu EU, který vydal evropský uchovávací příkaz, může požádat příslušný český orgán, aby příkaz uznal a zajistil jeho výkon. Kromě evropského uchovávacího příkazu zašle také formulář uvedený v příloze III nařízení a další potřebné informace – vše přeložené do českého jazyka nebo jiného jazyka, o kterém Česká republika prohlásí, že jej akceptuje (slovenský jazyk). Útvar Policie České republiky, jehož příslušnost se stanoví v § 397 odst. 2, pak přezkoumá, zda není dán důvod pro odmítnutí podle článku 16 odst. 5 nařízení. Stejně tak přezkoumává tyto důvody i justiční orgán, který uděluje podle § 397 odst. 2 souhlas s uznáním a zajištěním výkonu evropského uchovávacího příkazu. Pokud příslušný útvar Policie České republiky nebo justiční orgán shledá, že je takový důvod dán, útvar Policie České republiky o tom podle článku 16 odst. 2 nařízení informuje adresáta příkazu a orgán vydávajícího státu. Pokud žádný důvod pro odmítnutí dán není, útvar Policie České republiky vydá příkaz, který bude obsahovat výrok o uznání příkazu jiného členského státu EU a výrok, kterým nařídí adresátovi příkazu, aby data uchoval, a poučení, v němž jsou obsaženy informace uvedené v článku 16 odst. 3 nařízení. Příkaz doručí adresátovi. Na rozdíl od příkazu, kterým se uznává a zajišťuje výkon evropského vydávacího příkazu, neobsahuje příkaz, kterým se uznává a zajišťuje výkon evropského uchovávacího příkazu, odůvodnění (stejně jako odůvodnění neobsahuje příkaz podle § 7b odst. 1 tr. ř.). Příkaz lze také uznat jen částečně – pak se vykoná ve zbylém rozsahu.

Adresát příkazu, kterým se uznává a zajišťuje výkon evropského uchovávacího příkazu, může proti takovému příkazu ve stanovené lhůtě podat námitky (článek 16 odst. 3 nařízení). V návaznosti na článek 16 odst. 6 nařízení se stanoví příslušnost orgánu k posouzení podaných námitek – námitku posoudí útvar Policie České republiky, který příkaz vydal. Dále se stanoví postup při vyhovění námitce nebo při jejím shledáním nedůvodnou. Útvar Policie České republiky má samostatnou pravomoc na základě námitky příkaz zúžit nebo odvolat, i když je k vydání příkazu potřeba souhlas justičního orgánu (jde o případy, kdy je výsledkem menší zásah do práv a soukromí osoby).

Pokud útvar Policie České republiky považuje námitku za nedůvodnou a na příkazu trvá, musí námitku se svým stanoviskem předložit k posouzení justičnímu orgánu uvedenému v § 397 odst. 2. Justiční orgán buď námitce zcela nebo zčásti vyhoví a uloží útvaru Policie České republiky, aby příkaz odvolal nebo změnil, nebo ji důvodnou neshledá a o důvodech neprodleně vyrozumí útvar Policie České republiky, který o tom následně informuje adresáta podle článku 16 odst. 8 nařízení.

Pokud justiční orgán potřebuje pro své posouzení další informace nebo konzultace, požádá o jejich zajištění útvar Policie České republiky, neboť vykonávajícím orgánem se podle článku 3 odst. 17 nařízení rozumí orgán ve vykonávajícím státě, který je v souladu s vnitrostátním právem tohoto státu příslušný k obdržení evropského uchovávacího příkazu.

Navržená úprava v odstavci 2 reaguje na to, že jedním z důvodů pro odmítnutí výkonu evropského uchovávacího příkazu je podle článku 16 odst. 5 písm. e) nařízení i skutečnost, že požadované údaje jsou chráněny imunitami nebo výsadami podle práva vykonávajícího státu, které brání výkonu příkazu. Stejně jako u jiných typů justiční spolupráce se upravuje možnost, aby se v případě pochybností o tom, zda je taková imunita nebo výsada dána, útvar Policie České republiky nebo justiční orgán obrátil na Nejvyšší soud.

V odstavci 4 se upravuje postup v případě, že nelze nebo není třeba evropský uchovávací příkaz jiného členského státu EU vykonat.

**K § 401**

Předmětné ustanovení provádí článek 15 nařízení, který stanoví povinnost členských států EU upravit ve svém právním řádu peněžité sankce za porušení článků 10 a 11 a článku 13 odst. 4 nařízení. Konkrétně se jedná o peněžité sankce za porušení povinnosti adresáta osvědčení uchovat požadovaná data a vydat je ve stanovené lhůtě na základě evropského vydávacího příkazu (článek 10), povinnosti uchovat požadovaná data po stanovenou dobu na základě evropského uchovávacího příkazu (článek 11) a za porušení povinnosti adresátů, a nejsou-li totožní, poskytovatelů služeb přijmout nezbytná nejmodernější provozní a technická opatření, aby zajistili důvěrnost, utajení a integritu vydaných osvědčení a vydaných nebo uchovaných dat.

K uložení pořádkové pokuty je příslušný orgán, který je příslušný k zajištění výkonu evropského vydávacího nebo evropského uchovávacího příkazu (tj. i v případě, že příkaz vydal v přípravném řízení na návrh státního zástupce soudce, je k uložení pořádkové pokuty příslušný státní zástupce jako vykonávající orgán). Podmínkou pro uložení pořádkové pokuty je, že není dán důvod pro odmítnutí zajištění výkonu evropského vydávacího nebo evropského uchovávacího příkazu podle článků 16 odst. 4 nebo 5 nařízení, tj. např. pokud dojde ke ztrátě požadovaných dat, je možné adresáta postihnout pořádkovou pokutou pouze tehdy, pokud adresát takovou ztrátu zavinil – pro takový případ nařízení předpokládá, že evropský vydávací příkaz nebo evropský uchovávací příkaz bude uznán, resp. z takového důvodu nelze odmítnout zajistit výkon příkazu. Lze mít za to, že to je právě z důvodu umožnění postihu adresáta.

Pořádkovou pokutu lze uložit ve dvou případech. V prvním případě jde o situaci, že adresát nesplnil povinnosti podle článků 10 nebo 11 nařízení, tj. zejména pokud příkaz neprovedl řádně a včas, aniž by k tomu měl důvod předpokládaný nařízením. V druhém případě nařízení v článku 13 odst. 4 požaduje postih za to, že adresáti, a nejsou-li totožní, poskytovatelé služeb nepřijmou nezbytná nejmodernější provozní a technická opatření, aby zajistili důvěrnost, utajení a integritu vydaných evropských vydávacích a uchovávacích příkazů a vydaných nebo uchovaných dat. Jde tedy o případy, kdy dojde k porušení důvěrnosti, utajení nebo integrity dat ve vztahu ke konkrétnímu příkazu – půjde např. o případ, kdy adresát vyzradí osobě, jejíchž dat se příkaz týká, že vůči ní byl takový příkaz vydán. Jedná se o obdobný případ, jako když dožádaný podle § 8 tr. ř. poruší povinnost mlčenlivosti a vyzradí dotčené osobě, že orgány činné v trestním řízení požadují informace týkající se této osoby.

Pokud jde o porušení této povinnosti obecně ve vztahu k osobním údajům, tj. pokud poskytovatel neprovede určitá systémová opatření, která má přijmout za účelem ochrany osobních údajů, lze využít také postih podle zákona o zpracování osobních údajů, konkrétně podle § 62 odst. 1 písm. a) zákona o zpracování osobních údajů [porušení povinnosti podle článku 32 nařízení Evropského parlamentu a Rady (EU) 2016/679 – GDPR]. Nařízení Evropského parlamentu a Rady (EU) 2016/679 za porušení povinnosti řádně zabezpečit data stanoví v článku 83 odst. 4 pokutu až do výše 10 000 000 EUR, nebo jedná-li se o podnik, až do výše 2 % celkového celosvětového ročního obratu za předchozí finanční rok, podle toho, která hodnota je vyšší.

Pořádkovou pokutu lze uložit i podle § 66 tr. ř. při splnění podmínek v něm uvedených, neboť trestní řád se uplatní subsidiárně.

Pořádková pokuta se ukládá adresátovi příkazu. Návrh zákona o určování provozoven a jmenování zástupců některých poskytovatelů služeb za účelem shromažďování elektronických důkazů v trestním řízení připravovaný souběžně s tímto návrhem na základě směrnice stanoví, že poskytovatel služeb a jím pověřená určená provozovna nebo jím jmenovaný zástupce (tj. adresát příkazu) odpovídají společně a nerozdílně za splnění povinností pro účely doručování, dodržování a vymáhání rozhodnutí a příkazů vydaných příslušnými orgány členských států EU za účelem shromažďování elektronických důkazů v trestním řízení, s výjimkou případu, kdy je porušení rozhodnutí nebo příkazu trestným činem.

Vzhledem k tomu, že nařízení požaduje, aby sankci za porušení uvedených povinností bylo možné uložit až do výše 2 % celkového celosvětového ročního obratu poskytovatele služeb za předchozí finanční rok, v odstavcích 2 a 3 se upravují procesní nástroje, které může orgán ukládající pořádkovou pokutu (popř. policejní orgán) využít při provádění potřebného šetření, aby takový obrat mohl zjistit. Při stanovení výše pokuty je třeba primárně vycházet z obchodních záznamů, např. auditované účetní závěrky, a pokud není k dispozici, lze požadovat po adresátovi sdělení alespoň kvalifikovaného odhadu. Pokud nelze zjistit takový odhad z důvodu nespolupráce adresáta příkazu, lze vycházet z posledních známých podkladů, např. informací o bankovních účtech, cenných papírech a investičních nástrojích, veřejně dostupných informací aj. Adresáta příkazu lze také vyzvat k učinění prohlášení o majetku. I zde se však uplatní zákaz sebeobviňování a adresáta příkazu nelze nutit k výpovědi nebo vydání podkladů proti němu. Vzhledem k tomu, že součástí šetření pro účely uložení pořádkové pokuty bude mj. prokázání naplnění jednání podle § 401 odst. 1 návrhu, nelze vyloučit ani potřebu výslechů osob a řešení odborných otázek, kdy by mohla vzniknout potřeba vyžádat odborné vyjádření nebo znalecký posudek.

Jelikož pro účely uložení pořádkové pokuty nelze využít mezinárodní justiční spolupráci ve věcech trestních a nařízení žádný mechanismus spolupráce pro tento účel nezakotvuje, může být zjištění celosvětového obratu v některých případech obtížné, proto se stanoví i postup pro případ, kdy celosvětový obrat nelze zjistit.

Proti rozhodnutí o uložení pořádkové pokuty lze podat stížnost k soudu. V případě, že rozhodnutí vydal státní zástupce, je příslušný soud, v jehož obvodu je činný státní zástupce, který napadené rozhodnutí vydal. V případě, kdy ukládá pořádkovou pokutu útvar Policie České republiky a věc je v jiném členském státu EU ve fázi přípravného řízení, je příslušný soud, v jehož obvodu je činný státní zástupce příslušný k vyslovení souhlasu s příkazem, kterým se uznává a vykonává evropský uchovávací příkaz. V případě, kdy ukládá pořádkovou pokutu útvar Policie České republiky a věc je v jiném členském státu EU ve fázi řízení před soudem, je příslušný soud, který je nejblíže vyššího stupně ve vztahu k soudu, který vyslovil souhlas s příkazem, kterým se uznává a vykonává evropský uchovávací příkaz.

**K dílu 3**

V tomto dílu je upraven postup pro případy, kdy české orgány činné v trestním řízení vydají evropský vydávací nebo uchovávací příkaz a jeho výkon je třeba zajistit v jiném členském státu EU. Řeší se zejména otázka příslušnosti k vydání těchto příkazů, otázka úhrady nákladů, informování dotčené osoby aj.

**K § 402**

V tomto ustanovení se upravuje příslušnost českých orgánů k vydání evropského vydávacího příkazu, vydání osvědčení o vydání tohoto příkazu a k dalším úkonům.

Nastavení příslušnosti k vydání evropského vydávacího příkazu zohledňuje skutečnost, že nařízení vymezuje kategorie dat poněkud odlišně než česká vnitrostátní úprava. Český trestní řád je totiž v některých směrech přísnější a požaduje soudní příkaz i tam, kde podle nařízení postačí příkaz státního zástupce. Např. v případě ustanovení IP adresy je v první fázi osloven typicky poskytovatel služby informační společnosti, aby poskytl data o IP adrese, z níž se v relevantní době uživatel přihlašoval k zájmové službě informační společnosti. V druhé fázi je IP adresa zjištěná v prvém kroku ustanovována u poskytovatele služby elektronických komunikací (u poskytovatele internetového připojení), jemuž jsou zaslána data o IP adrese zjištěné v prvním kroku s tím, že je žádáno o identifikaci účastníka služby přístupu k internetu. Podle nařízení jde v první fázi o dotaz na data požadovaná výhradně za účelem identifikace uživatele (nejde-li o dotaz, v jehož rámci jsou žádána i provozní data) a není vyžadován soudní příkaz. V druhé fázi jde pak o dotaz na data o účastníkovi a rovněž není vyžadován soudní příkaz. Podle české právní úpravy jde v první fázi o data, pro jejichž zjištění není vyžadován soudní příkaz, byť v některých případech může být i zde zapotřebí (§ 8 odst. 1 a 5 tr. ř.). V druhé fázi však jde o data vyžadovaná v režimu § 88a tr. ř. a je třeba soudní příkaz. V některých případech je naopak nařízení přísnější.

S ohledem na princip, že by důkazy pro účely trestního řízení vedeného v České republice měly být získávány, pokud možno, za shodných podmínek a při dodržení stejných právních záruk, navržená úprava požaduje soudní potvrzení příkazu vydaného státním zástupcem ve všech případech, kdy soudní příkaz vyžaduje pro vnitrostátní případy trestní řád, tj. i tehdy, pokud by podle nařízení postačil příkaz státního zástupce. Navržená úprava koresponduje s článkem 5 odst. 2 nařízení, který mj. předpokládá, že evropský vydávací příkaz „[…] *může být vydán pouze tehdy, pokud by podobný příkaz mohl být vydán za stejných podmínek v obdobném vnitrostátním případě*.“

Navrhuje se obdobná konstrukce jako u evropského vyšetřovacího příkazu, tj. nevyžaduje se, aby soudce v přípravném řízení příkaz přímo vydal, ale požaduje se, aby příkaz vydaný státním zástupcem potvrdil. Pokud by soudce byl přímo orgánem vydávajícím příkaz, měl by pak všechny povinnosti vydávajícího orgánu podle nařízení, tj. vyplňoval by i formulář osvědčení, příkaz by zasílal do jiného členského státu EU, poskytoval by doplňkové informace aj., což neodpovídá jeho roli v přípravném řízení. Ostatně pouhé potvrzení soudcem považuje za dostatečné i článek 4 odst. 2 písm. b) nařízení.

Ve zbylých případech pak příkaz v přípravném řízení může vydat státní zástupce nebo policejní orgán činný v trestním řízení, stejně jako podle vnitrostátní právní úpravy.

V odstavci 3 se provádí článek 4 odst. 5 nařízení, který se přizpůsobuje přísnější adaptační úpravě, tj. úprava je omezena na případy, kdy podle trestního řádu může příkaz vydat policejní orgán.

Vzhledem k tomu, že adresátovi se neposílá samotný evropský vydávací příkaz, ale pouze osvědčení, jehož formulář je obsažen v příloze I nařízení, stanoví se pro vyplnění osvědčení shodná příslušnost jako pro vydání příkazu. Požadavky na potvrzení osvědčení jsou pak rovněž shodné jako u evropského vydávacího příkazu.

V odstavci 5 se pak stanoví najisto, že úkony v řízení související s evropským vydávacím příkazem provádí orgán, který příkaz vydal a nikoli orgán, který jej potvrdil.

Oprávnění žádat o vydání evropského vydávacího příkazu má i obviněný, zadržený podezřelý a podezřelý ve zkráceném přípravném řízení, a to na základě článku 1 odst. 2 nařízení ve spojení s trestním řádem, neboť tento článek odkazuje na vnitrostátní právo. Nejde tedy o podezřelého v prověřování v materiálním smyslu. Pojem „podezřelý“ v nařízení totiž není totožný s pojmem „podezřelý“ v trestním řádu, v němž je užíván v různých souvislostech a významech. Zatímco u zadrženého podezřelého a podezřelého ve zkráceném přípravném řízení lze dovodit, že je proti nim vedeno trestní řízení, což zakládá jejich určitá obhajovací práva (obdobná obviněnému, když § 76 odst. 5 i § 179b odst. 2 tr. řádu odkazují na § 33 odst. 1 trestního řádu, kde je obsaženo i právo činit návrhy), u podezřelého v materiálním smyslu nelze tvrdit, že je osobou, proti níž je trestní řízení vedeno. Trestní řízení před zahájením trestního stíhání je vedeno tzv. „ve věci“ a materiální podezřelý ani (oficiálně) neví, že je materiálně podezřelý. Jestliže mu tato skutečnost není (oficiálně) známa, nelze od ní odvíjet oficiální procesní postavení a procesní práva.

**K § 403**

Podmínky pro vydání evropského vydávacího příkazu jsou primárně upraveny v článku 5 nařízení a jsou přímo použitelné. Přesto je zapotřebí je částečně provést v ZMJS, neboť článek 5 odst. 4 písm. b) a c) odkazuje na trestná jednání vymezená ve směrnicích, které nejsou přímo aplikovatelné, a je tak třeba odkázat na příslušné trestné činy podle českého trestního zákoníku. Vzhledem k tomu, že písmeno a) téhož ustanovení umožňuje vydat evropský vydávací příkaz pro všechny trestné činy s horní hranicí trestní sazby nejméně 3 roky, podle písmen b) a c) jsou relevantní pouze trestné činy s nižší horní hranicí – takové trestné činy se pak vyskytují pouze u písmene b). Přitom u těchto trestných činů platí podmínka uvedená v návětí článku 5 odst. 4 písm. b) nařízení, že tyto trestné činy musejí být spáchány zcela nebo zčásti prostřednictvím informačního systému.

S ohledem na článek 5 odst. 2 nařízení, který stanoví, že evropský vydávací příkaz „[…] *může být vydán pouze tehdy, pokud by podobný příkaz mohl být vydán za stejných podmínek v obdobném vnitrostátním případě*“, je nicméně třeba okruh trestných činů, pro které může být vydán evropský vydávací příkaz, dále omezit (obdobné omezení platí i pro vykonávací řízení). V případě, že jsou vyžadována data, která by vnitrostátně byla vyžadována podle § 88a tr. ř. (provozní a lokalizační údaje), lze i evropský vydávací příkaz vydat jen pro ty trestné činy, pro které to umožňuje § 88a tr. ř.

**K § 404**

V tomto ustanovení se upravuje příslušnost českých orgánů k vydání evropského uchovávacího příkazu, vydání osvědčení o vydání tohoto příkazu a k dalším úkonům. Příslušnost je nastavena shodně jako v § 7b tr. ř., nicméně vzhledem k tomu, že se jedná o mezinárodní justiční spolupráci v trestních věcech, v případě příkazu vydaného policejním orgánem se požaduje potvrzení příkazu státním zástupcem, což odpovídá i požadavku obsaženém v článku 4 odst. 3 písm. b) nařízení.

Vzhledem k tomu, že adresátovi se neposílá samotný evropský uchovávací příkaz, ale pouze osvědčení, jehož formulář je obsažen v příloze II nařízení, stanoví se pro vyplnění osvědčení shodná příslušnost jako pro vydání příkazu. Požadavky na potvrzení osvědčení jsou pak rovněž shodné jako u evropského uchovávacího příkazu. V článku 4 odst. 5 nařízení je pak stanoveno, že předchozí potvrzení se nevyžaduje v naléhavých případech.

**K § 405**

Vzhledem k tomu, že uchování dat vyžaduje urychlenou spolupráci, navrhuje se (stejně jako u žádostí o uchování dat podle § 65a ZMJS) koncentrace zasílání evropských uchovávacích příkazů, osvědčení a souvisejících písemností vydaných českými orgány činnými v trestním řízení do jiných členských států EU prostřednictvím útvaru Policie České republiky pověřeného policejním prezidentem. Tento útvar bude napojen na decentralizovaný informační systém. Aktuálně jím je Národní centrála proti terorismu, extremismu a kybernetické kriminalitě SKPV.

**K § 406**

V tomto ustanovení se provádí článek 17 nařízení ve vztahu k evropskému vydávacímu příkazu. Adresát příkazu může odmítnout výkon příkazu, pokud se domnívá, že v případě splnění evropského vydávacího příkazu by došlo k rozporu s povinností stanovenou příslušným právem třetí země. V takovém případě informuje vydávající a vykonávající orgán na formuláři uvedeném v příloze III nařízení. Přitom je povinen uvést všechny relevantní informace o právu třetí země. Nařízení vymezuje, co nemůže být obsahem odůvodněné námitky, a stanoví lhůtu pro podání odůvodněné námitky (10 dnů ode dne, kdy adresát příkazu obdržel osvědčení).

Odůvodněnou námitku přezkoumá orgán, který vydal evropský vydávací příkaz. Samostatně může námitce vyhovět. Pokud ji však považuje zcela nebo zčásti za nedůvodnou, musí být podán návrh na její přezkoumání k vrchnímu soudu, v jehož obvodu je vydávající orgán činný; v případě policejního orgánu se návrh podává prostřednictvím dozorujícího státního zástupce k vrchnímu soudu, v jehož obvodu je činný tento státní zástupce.

Postup soudu je pak upraven v článku 17 odst. 4 a násl. nařízení. Tento postup je v odstavci 3 doplněn o formu rozhodování soudu. Soud buď usnesením příkaz potvrdí, neshledá-li námitku důvodnou, nebo jej usnesením zruší, pokud námitce vyhoví. Pokud námitce vyhoví jen zčásti, může příkaz zrušit jen částečně pouze za předpokladu, že je příkaz ve zbylém rozsahu samostatně vykonatelný, jinak jej zruší celý. Vydávající orgán pak vydá nový příkaz ve zbylém rozsahu. Jedná se tedy o čistě kasační princip v souladu s článkem 17 nařízení.

**K § 407**

Předmětné ustanovení provádí článek 13 nařízení. Nařízení požaduje, aby dotčená osoba, jejíž data byla vyžádána na základě evropského vydávacího příkazu, o tom byla vydávajícím státem informována. Zároveň umožňuje v souladu s vnitrostátním právem informování odložit nebo omezit či od něj upustit z důvodů uvedených v článku 13 odst. 3 směrnice (EU) 2016/680. Těmito důvody jsou:

* zabránění maření úředních nebo právních šetření, vyšetřování nebo postupů,
* zabránění nepříznivému ovlivňování prevence, odhalování, vyšetřování či stíhání trestných činů nebo výkonu trestů,
* ochrana veřejné bezpečnosti,
* ochrana národní bezpečnosti a
* ochrana práv a svobod druhých.

Vzhledem k tomu, že článek 13 nařízení odkazuje na vnitrostátní právo, navrhuje se subsidiárně vycházet z úpravy informační povinnosti stanovené v § 88a tr. ř., včetně přezkumu příkazu podle § 314l a násl. tr. ř. Důvody pro neinformování osoby uvedené dnes v § 88a odst. 3 tr. ř. *(po přijetí tisku 861 v § 88a odst. 2 tr. ř. ve spojení s § 88 odst. 10 tr. ř.)* spadají mezi důvody upravené ve směrnici (EU) 2016/680. Informační povinnost se uplatní pro všechny kategorie dat, pokud je možné identifikovat osobu, která má být informována.

**K § 408**

Předmětné ustanovení provádí článek 14 nařízení, podle něhož může poskytovatel služeb v souladu s vnitrostátním právem vydávajícího státu požádat o náhradu svých nákladů vydávajícím státem, stanoví-li tuto možnost vnitrostátní právo vydávajícího státu pro vnitrostátní příkazy v obdobných situacích – to se netýká nákladů na decentralizovaný informační systém.

Ustanovení § 97 odst. 3 zákona o elektronických komunikacích (dále jen „ZEK“) obsahuje dva typy nákladů, jednak náklady na uchovávání provozních a lokalizačních údajů a jednak náklady na jejich poskytnutí. Jejich úhradu pak aktuálně upravuje prováděcí vyhláška č. 462/2013 Sb.

Vyhláška č. 462/2013 Sb. upravuje dva druhy nákladů. Jednak upravuje výši nákladů na poskytování provozních a lokalizačních údajů (viz § 2 odst. 3 této vyhlášky), přičemž v příloze této vyhlášky je uvedena „sazba“ za poskytnutí údajů v konkrétním případě. Náklady na poskytnutí provozních a lokalizačních údajů jsou jednorázové náklady, které přímo souvisí s vyhledáním vyžádané informace a jejím předáním. Náklady hradí subjekt, který podal žádost o poskytnutí provozních a lokalizačních údajů (§ 4 odst. 5 vyhlášky č. 462/2013 Sb.). O úhradu těchto nákladů může poskytovatel služeb požádat v rozsahu, v jakém jde o údaje hrazené podle vyhlášky (vyhláška v návaznosti na ZEK pracuje s kategoriemi provozních a lokalizačních údajů, návrh zákona v souladu s nařízením upravuje provozní údaje, které nicméně v zásadě odpovídají provozním a lokalizačním údajům podle ZEK) a pouze v případě, že má ve státě, v němž má sídlo, provozovnu nebo určeného zástupce, obdobnou povinnost uchovávat údaje (data retention), což je povinen doložit.

Dále předmětná vyhláška upravuje úhradu nákladů na uchovávání provozních a lokalizačních údajů. Tyto náklady vznikají nezávisle na množství poskytovaných informací, proto jsou hrazeny cestou jediného orgánu (Ministerstvem vnitra – viz § 4 odst. 4 vyhlášky č. 462/2013 Sb.) bez ohledu na to, že údaje si mohou vyžádat i jiné orgány. Tyto náklady tedy nesouvisí s konkrétní žádostí o uchování údajů, a poskytovatelům služeb tedy hrazeny nebudou.

V návaznosti na změnu právní úpravy v důsledku přijetí zákona č. 23/2025 Sb., kterým se mění ZEK, by měla být nově výše a způsob úhrady příspěvku na plnění povinnosti uchovávat provozní a lokalizační údaje stanovena nařízením vlády (§ 97 odst. 11 zákona o elektronických komunikacích, ve znění zákona č. 23/2025 Sb.) a výše a způsob úhrady efektivně a účelně vynaložených nákladů na poskytnutí provozních a lokalizačních údajů má stanovit vyhláška ČTÚ, s tím, že vyhláška č. 462/2013 Sb. je přímo zákonem č. 23/2025 Sb. s účinností od 1. července 2025 rušena (na základě přechodných ustanovení k zákonu č. 23/2025 Sb. se ale bude do doby nabytí účinnosti této nové vyhlášky při stanovení výše a způsobu úhrady efektivně a účelně vynaložených nákladů za poskytnutí informace z databáze účastníků veřejně dostupné služby elektronických komunikací a za poskytnutí provozních a lokalizačních údajů postupovat podle dosavadní vyhlášky č. 462/2013 Sb.). Uvedené principy by se nicméně měly uplatnit i nadále.

**K článku II**

Datum nabytí účinnosti je ve vztahu k nařízení navázáno na datum, které nařízení stanoví pro adaptaci do vnitrostátních právních řádů členských států EU.

Pokud jde o úpravu implementující směrnici o digitalizaci justiční spolupráce, datum, do kdy má být tato směrnice provedena do vnitrostátních právních řádů, se odvíjí od data vstupu v platnost příslušného prováděcího aktu uvedeného v článku 10 odst. 3 nařízení o digitalizaci justiční spolupráce. Tyto prováděcí akty budou přijímány postupně v časovém období od 17. ledna 2026 do 17. ledna 2029, přičemž příslušná implementační právní úprava má být platná vždy do dvou let od vstupu příslušného právního aktu v platnost. Tato dvouletá lhůta slouží k zajištění připravenosti vnitrostátních orgánů používat decentralizovaný informační systém (zajištění jejich připojení k systému, proškolení aj.). Implementační úprava pak bude účinná prvním dnem kalendářního měsíce následujícího po uplynutí uvedené lhůty.

Do 17. ledna 2026 by měl být přijat prováděcí akt týkající se evropského zatýkacího rozkazu a evropského vyšetřovacího příkazu, do 17. ledna 2027 by měl být přijat prováděcí akt týkající se rozhodnutí ukládajících nepodmíněný trest odnětí svobody nebo ochranné opatření spojené se zbavením osobní svobody a evropského ochranného příkazu, do 17. ledna 2028 by měl být přijat prováděcí akt týkající se příkazů k zajištění majetku, kompetenčních sporů, rozhodnutí ukládajících peněžité tresty a pokuty a rozhodnutí ukládajících propadnutí nebo zabrání majetku a do 17. ledna 2029 by měl být přijat prováděcí akt týkající se opatření nahrazujících vazbu a rozhodnutí ukládajících trest nespojený se zbavením osobní svobody, dohled nebo přiměřená omezení a povinnosti.

Všechny výše uvedené prováděcí akty jsou standardním způsobem zveřejněny v Úředním věstníku EU a jsou dohledatelné na portálu eur-lex.

1. The Clarifying Lawful Overseas Use of Data Act (CLOUD Act). [↑](#footnote-ref-1)