Úřední věstník
Evropské unie

CS
Řada L

2025/1550

29.7.2025

PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2025/1550

ze dne 28. července 2025,

kterým se stanoví technické specifikace a další požadavky pro decentralizovaný informační systém uvedené v nařízení Evropského parlamentu a Rady (EU) 2023/1543

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na 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 ([1]), a zejména na čl. 25 odst. 1 písm. a), b) c) a d) uvedeného nařízení,

vzhledem k těmto důvodům:

(1) Pro zavedení decentralizovaného informačního systému uvedeného v nařízení (EU) 2023/1543 je nezbytné vymezit a přijmout technické specifikace, opatření a cíle pro zavedení tohoto systému.

(2) V souladu s nařízením (EU) 2023/1543 by se měl decentralizovaný informační systém skládat z informačních systémů členských států a agentur a subjektů Unie a interoperabilních přístupových bodů systému e-CODEX, jejichž prostřednictvím jsou tyto systémy vzájemně propojeny. Technické specifikace a další požadavky decentralizovaného informačního systému by proto měly tento rámec odrážet.

(3) V souladu s nařízením (EU) 2023/1543 by přístupové body decentralizovaného informačního systému měly být založeny na oprávněných přístupových bodech systému e-CODEX, které jsou definovány v čl. 3 bodu 3 nařízení Evropského parlamentu a Rady (EU) 2022/850 ([2]).

(4) Členské státy se mohou rozhodnout, že budou jako svůj koncový systém namísto vnitrostátního informačního systému používat referenční prováděcí software vyvinutý Komisí. V zájmu zajištění interoperability by se na vnitrostátní informační systémy i referenční prováděcí software měly vztahovat stejné technické specifikace a požadavky stanovené v tomto nařízení.

(5) Za účelem zmírnění možných technických otázek souvisejících s kapacitou a spolehlivostí decentralizovaného informačního systému je nutné stanovit prahovou hodnotu pro předávání elektronických důkazů prostřednictvím tohoto systému. Po spuštění systému by měly být sledovány četnost a objem těchto výměn a tato prahová hodnota případně upravena v zájmu maximalizace účinnosti systému.

(6) Za účelem posílení interoperability a účinnosti decentralizovaného informačního systému je vhodné stanovit povinné používání příslušných norem ETSI. Je třeba monitorovat další vývoj a případě nutnosti zvážit přijetí dalších norem ETSI.

(7) Irsko je vázáno nařízením (EU) 2023/1543, a proto se účastní přijímání tohoto nařízení.

(8) V souladu s články 1 a 2 Protokolu č. 22 o postavení Dánska, připojeného ke Smlouvě o Evropské unii a Smlouvě o fungování Evropské unie, není Dánsko vázáno tímto nařízením a používání tohoto nařízení se na ně nevztahuje.

([1]) Úř. věst. L 191, 28.7.2023, s. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj.

([2]) Nařízení Evropského parlamentu a Rady (EU) 2022/850 ze dne 30. května 2022 o počítačovém systému pro přeshraniční elektronickou výměnu údajů v oblasti justiční spolupráce v občanských a trestních věcech (systém e-CODEX) a o změně nařízení (EU) 2018/1726 (Úř. věst. L 150, 1.6.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/850/oj).

(9) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ([3]) byl konzultován evropský inspektor ochrany údajů, který vydal stanovisko dne 25. června 2025.

(10) Opatření stanovená tímto nařízením jsou v souladu se stanoviskem výboru zřízeného článkem 26 nařízení (EU) 2023/1543,

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Technické specifikace decentralizovaného informačního systému

Technické specifikace a požadavky, opatření a cíle decentralizovaného informačního systému uvedeného v čl. 25 odst. 1 nařízení (EU) 2023/1543 pro účely komunikace ve smyslu článku 19 uvedeného nařízení jsou stanoveny v příloze tohoto nařízení.

Článek 2

Vstup v platnost

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

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

V Bruselu dne 28. července 2025.

Za Komisi
předsedkyně
Ursula VON DER LEYEN

([3]) Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Úř. věst. L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

PŘÍLOHA

TECHNICKÉ SPECIFIKACE DECENTRALIZOVANÉHO INFORMAČNÍHO SYSTÉMU

(uvedené v článku 1)

1. Úvod a rozsah působnosti

Tato příloha stanoví technické specifikace, opatření a cíle decentralizovaného informačního systému pro účely postupů podle nařízení (EU) 2023/1543.

Podle nařízení (EU) 2023/1543, a zejména jeho článku 19, má decentralizovaný informační systém umožnit písemnou komunikaci mezi příslušnými orgány a určenými provozovnami nebo zástupci, mezi příslušnými orgány navzájem, jakož i mezi příslušnými orgány a příslušnými agenturami nebo subjekty Unie.

2. Definice

2.1. Protokolem „Hypertext Transfer Protocol Secure“ nebo „HTTPS“ se rozumí šifrovaná komunikace a zabezpečené kanály propojení;

2.2. „nepopiratelností původu“ se rozumí opatření poskytující důkaz o integritě a důkaz o původu údajů prostřednictvím metod, jako jsou elektronická certifikace, infrastruktura veřejných klíčů a elektronické podpisy a elektronické pečeti;

2.3. „nepopiratelností přijetí“ se rozumí opatření poskytující původci údajů důkaz o přijetí údajů zamýšleným příjemcem prostřednictvím metod, jako jsou elektronická certifikace, infrastruktura veřejných klíčů a elektronické podpisy a elektronické pečeti;

2.4. protokolem „SOAP“ (Simple Object Access Protocol) se rozumí, podle norem konsorcia World Wide Web Consortium, specifikace komunikačního protokolu pro výměnu strukturovaných informací při zavádění webových služeb v počítačových sítích;

2.5. architekturou „Representational State Transfer“ nebo „REST“ se rozumí architektonický styl pro navrhování síťových aplikací, který se opírá o bezstavový komunikační model klient-server a používá standardní metody pro provádění operací se zdroji, které jsou obvykle reprezentovány ve strukturovaných formátech;

2.6. „webovou službou“ se rozumí softwarový systém určený k podpoře interoperabilní interakce mezi počítači prostřednictvím počítačové sítě, který má rozhraní popsané ve strojově zpracovatelném formátu;

2.7. „výměnou údajů“ se rozumí výměna zpráv, formulářů, dokumentů a elektronických důkazů prostřednictvím decentralizovaného informačního systému;

2.8. rozhraním „API“ se rozumí aplikační programové rozhraní založené na společném standardu pro výměnu údajů, které umožňuje poskytovatelům služeb, kteří využívají na míru šitá řešení IT pro účely výměny informací a údajů souvisejících s žádostmi o elektronické důkazy, automatizovaný přístup k decentralizovaným informačním systémům;

2.9. „internetovým rozhraním“ se rozumí uživatelské rozhraní, které je k dispozici na internetu prostřednictvím protokolu HTTPS a které umožňuje poskytovatelům služeb manuální přístup k decentralizovanému informačnímu systému za účelem bezpečné komunikace s orgány a výměny informací a údajů souvisejících s žádostmi o elektronické důkazy, aniž by museli zřizovat vlastní vyhrazenou infrastrukturu;

2.10. „normami ETSI“ se rozumí technické specifikace a normy vypracované Evropským ústavem pro telekomunikační normy (ETSI) za účelem zajištění interoperability, bezpečnosti a účinnosti informačních a komunikačních technologií. Poskytují rámce, protokoly a osvědčené postupy pro širokou škálu technologií, včetně mobilních sítí, rádiové komunikace, kybernetické bezpečnosti a internetové infrastruktury;

2.11. výstupem „hash digest“ se rozumí výstup pevné délky generovaný kryptografickou hašovací funkcí použitou na vstup libovolné délky. Kryptografická hašovací funkce je navržena tak, aby splňovala základní bezpečnostní vlastnosti, včetně odolnosti proti nalezení vzoru, odolnosti proti nalezení druhého vzoru a odolnosti proti kolizi, čímž je zajištěna její odolnost proti inverzním a kolizním útokům;

2.12. „systémem e-CODEX“ se rozumí systém e-CODEX ve smyslu čl. 3 bodu 1 nařízení Evropského parlamentu a Rady (EU) 2022/850;

2.13. „slovníky základních pojmů v oblasti e-justice EU“ se rozumí slovníky základních pojmů v oblasti e-justice EU definované v bodě 4 přílohy nařízení (EU) 2022/850;

2.14. protokolem „ebMS“ se rozumí ebXML Message Service, což je protokol pro zasílání zpráv vyvinutý podle rámce OASIS, který umožňuje bezpečnou, spolehlivou a interoperabilní výměnu elektronických obchodních dokumentů pomocí protokolu SOAP a podporuje mezipodnikovou integraci mezi různými systémy;

2.15. protokolem „AS4“ se rozumí Applicability Statement 4, což je standard OASIS, který profiluje ebMS 3.0; přičemž zjednodušuje bezpečné a interoperabilní zasílání zpráv mezi podniky pomocí otevřených standardů, jako jsou SOAP a WS-Security;

2.16. „cílovou dobou obnovy funkce“ se rozumí maximální přijatelná doba pro obnovu služby po incidentu;

2.17. „cílovým okamžikem obnovy funkce“ znamená maximální přijatelnou míru ztráty údajů v případě selhání.

3. **Způsoby komunikace elektronickými prostředky**

3.1. Pro účely písemné komunikace mezi příslušnými orgány členských států, mezi příslušnými orgány a určenými provozovnami nebo zástupci poskytovatelů služeb, jakož i mezi příslušnými orgány a agenturami nebo subjekty Unie, využívá decentralizovaný informační systém metody komunikace založené na službách, jako jsou webové služby nebo jiné opakovaně použitelné komponenty a softwarová řešení pro účely výměny údajů. Konkrétně bude zahrnovat komunikaci prostřednictvím přístupových bodů systému e-CODEX, jak je stanoveno v čl. 5 odst. 2 nařízení (EU) 2022/850. Aby byla proto zajištěna účinná a interoperabilní přeshraniční výměna údajů, musí decentralizovaný informační systém podporovat komunikaci pomocí systému e-CODEX.

3.2. Vzhledem k předpokládanému velkému objemu elektronických důkazů, které mají být dále předávány v rámci evropského vydávacího příkazu prostřednictvím decentralizovaného informačního systému, jak je uvedeno v čl. 19 odst. 1 a 4 nařízení (EU) 2023/1543, což může vést k omezením technické kapacity, která by mohla mít na decentralizovaný informační systém negativní dopad, smí být elektronické důkazy předávány prostřednictvím tohoto systému, pokud nepřesáhnou prahovou hodnotu 25 megabajtů (25 600 kilobajtů). Předávání elektronických důkazů přesahujících výše uvedenou prahovou hodnotu se musí provádět v souladu s čl. 19 odst. 5 uvedeného nařízení.

3.3. S ohledem na čl. 19 odst. 6 nařízení (EU) 2023/1543 v případě, že se předání provádí alternativními prostředky podle uvedeného odstavce z důvodu nemožnosti použít decentralizovaný informační systém z některého z důvodů uvedených v čl. 19 odst. 5 uvedeného nařízení:

3.3.1. Pokud se předání týká písemné komunikace, včetně výměny formulářů, mezi příslušnými orgány a poskytovateli služeb ve smyslu čl. 19 odst. 1 nařízení (EU) 2023/1543, zaznamená původce údajů informace o tomto předání ve svém vnitrostátním informačním systému, který je součástí decentralizovaného informačního systému. Zaznamenané informace musí obsahovat alespoň referenční číslo případu nebo spisu, datum a čas, odesílatele a příjemce, název souboru a jeho velikost.

3.3.2. Pokud se předání týká písemné komunikace, včetně výměny formulářů, mezi příslušnými orgány, jakož i písemné komunikace s příslušnými agenturami nebo subjekty Unie ve smyslu čl. 19 odst. 4 nařízení (EU) 2023/1543, zaznamená původce údajů informace o tomto předání v decentralizovaném informačním systému, zejména v rámci svého vnitrostátního informačního systému nebo případně v informačních systémech provozovaných příslušnou agenturou nebo subjektem Unie. Zaznamenané informace musí obsahovat alespoň referenční číslo případu nebo spisu, datum a čas předání, odesílatele a příjemce, název souboru a jeho velikost.

3.3.3. Pokud byly elektronické důkazy podle evropského vydávacího příkazu předány prostřednictvím alternativních komunikačních prostředků mezi poskytovateli služeb a příslušnými orgány ve vydávajícím státě ([1]), nebo pokud jsou elektronické důkazy předány alternativními prostředky vykonávajícím orgánem příslušným orgánům ve vydávajícím státě v rámci postupu pro výkon podle čl. 16 odst. 9 nařízení (EU) 2023/1543, původce údajů:

a) zaznamená a předá orgánu, kterému byly elektronické důkazy předány nebo zpřístupněny, následující informace jako součást záznamu:

1) informace o odesílateli a příjemci;

2) metadata spojující poskytnuté elektronické důkazy s konkrétním evropským vydávacím příkazem nebo evropským uchovávacím příkazem;

3) datum a čas předání nebo údaj o tom, kdy byl elektronický důkaz zpřístupněn příjemci;

4) informace o způsobu předání (např. záznam o zabezpečeném spojení, jehož prostřednictvím byl elektronický důkaz zpřístupněn, doklad o přijetí nebo doručení od poštovních služeb atd. ([2]));

5) úplný název (názvy) souboru (souborů) elektronických důkazů, které byly předány nebo jinak zpřístupněny zamýšlenému příjemci ve vydávajícím státě;

6) velikost dat elektronických důkazů, které byly předány nebo jinak zpřístupněny zamýšlenému příjemci ve vydávajícím státě;

7) alespoň jeden výstup hash digest údajů, které byly předány nebo zpřístupněny, a údaj o použitém hašovacím algoritmu (hašovacích algoritmech). Hašovací algoritmus (hašovací algoritmy) použitý (použité) pro výpočet těchto výstupů hash digest musí být kryptograficky silný (silné), běžně používaný (používané) a nepodléhající veřejně známým slabinám, jako jsou kolize (například SHA-512, SHA3-512, BLAKE2 nebo RIPEMD-160, případně silnější, v závislosti na technologickém vývoji);

b) případně uvede jako součást záznamu uvedeného v písmenu a) výše datum a čas, do kterého budou elektronické důkazy přístupné. Tato lhůta poskytne příslušnému orgánu ve vydávajícím státě přiměřenou lhůtu k získání elektronických důkazů, která nesmí být kratší než 10 kalendářních dnů a delší než 45 kalendářních dnů od okamžiku, kdy jsou elektronické důkazy zpřístupněny. Na žádost příslušného orgánu vydávajícího státu může být lhůta uvedená původcem údajů v jednotlivých případech prodloužena;

c) může zaznamenat a předat orgánu, jemuž byly elektronické důkazy předány nebo zpřístupněny, veškeré další informace nebo poznámky týkající se případu, které jsou součástí záznamu uvedeného v písmenu a) výše.

3.4. S ohledem na článek 28 nařízení (EU) 2023/1543 referenční prováděcí software programově shromažďuje, předává nebo jinak poskytuje přístup ke statistikám uvedeným v odstavci 2 uvedeného článku ve strukturovaných (např. XML) i nestrukturovaných (např. PDF) datových formátech. V souladu s čl. 28 odst. 3 nařízení (EU) 2023/1543 mohou vnitrostátní portály ([3]) provozované členskými státy, pokud jsou k tomu technicky vybaveny, tyto statistiky rovněž předávat nebo poskytovat Komisi prostřednictvím automatizovaného procesu. Komise vydá pokyny ke struktuře údajů a způsobu shromažďování a sdělování těchto statistik.

([1]) Pro větší srozumitelnost se odkazy na příslušné vnitrostátní orgány *obdobně* vztahují rovněž na vnitrostátní členy Eurojustu, evropské žalobce a evropské pověřené žalobce, pokud jsou podle práva EU a vnitrostátního práva oprávněni vykonávat stejné funkce.

([2]) Je třeba připomenout, že v souladu s čl. 19 odst. 5 musí předání prostřednictvím těchto alternativních komunikačních prostředků splňovat požadavky na rychlost, bezpečnost a spolehlivost a umožnit příjemci ověřit pravost.

([3]) „Vnitrostátními portály“ je třeba rozumět vnitrostátní „informační systémy“, které jsou součástí decentralizovaného informačního systému, který je definován v čl. 3 bodu 21 nařízení (EU) 2023/1543.

4. **Komunikační protokoly**

4.1. Decentralizovaný informační systém používá zabezpečené internetové protokoly pro:

a) komunikaci v rámci decentralizovaného informačního systému mezi příslušnými orgány,

b) komunikaci v rámci decentralizovaného informačního systému mezi příslušnými orgány a agenturami a subjekty Unie,

c) komunikaci mezi příslušnými orgány a poskytovateli služeb prostřednictvím rozhraní API a internetového rozhraní a

d) komunikaci s databází soudů.

4.2. Pro účely definice a předávání strukturovaných údajů a metadat musí být komponenty decentralizovaného informačního systému založeny na komplexních a široce uznávaných průmyslových normách a protokolech, jako jsou SOAP a REST, zejména těch, na které odkazují evropské normalizační organizace, jako je ETSI.

4.3. Pokud jde o transportní protokoly a protokoly pro přenos a zprávy, decentralizovaný informační systém musí být založen na protokolech založených na standardech, jako jsou například:

a) profil AS4 pro přeshraniční výměnu údajů, který zajišťuje bezpečnou a spolehlivou výměnu zpráv se šifrováním a nepopiratelností;

b) rozhraní HTTPS/RESTful API pro komunikaci podporující formáty JSON a XML;

c) protokol SOAP pro vysoce spolehlivé interakce, se zahrnutím WS-Security pro ověřování a šifrování.

4.4. Pro účely bezproblémové a interoperabilní výměny údajů musí komunikační protokoly používané decentralizovaným informačním systémem splňovat příslušné normy interoperability.

4.5. Schémata XML elektronických důkazů případně využívají příslušné normy nebo slovníky, které jsou nezbytné pro řádné ověření prvků a typů definovaných v rámci tohoto schématu. Může se jednat o:

a) slovník základních pojmů v oblasti e-justice EU;

b) nekvalifikované datové typy;

c) seznam kódů jazyků Evropské unie.

V případě potřeby mohou schémata XML zahrnovat také příslušné normy ETSI a využívat jejich definice.

4.6. Komise vymezí specifikace společného rozhraní API, které vykonávající státy zpřístupní poskytovatelům služeb jako prostředek přístupu k decentralizovanému informačnímu systému. Toto rozhraní API musí v co největší možné a odůvodněné míře vycházet z normy ETSI TS 104 144 („Definice rozhraní pro nařízení o elektronických důkazech (EU) 2023/1543 pro vnitrostátní orgány a poskytovatele služeb“).

4.7. Pokud jde o bezpečnostní a autentizační protokoly, decentralizovaný informační systém musí být založen na protokolech založených na standardech, jako jsou například:

a) TLS (Transport Layer Security) pro šifrovanou a autentizovanou komunikaci v sítích, podporující vzájemné ověřování pomocí digitálních certifikátů X.509;

b) OAuth / OpenID Connect (OIDC) pro bezpečnou autentizaci a autorizaci;

c) Infrastruktura veřejných klíčů a digitální podpisy pro bezpečnou výměnu klíčů a ověření integrity zpráv pomocí digitálních certifikátů (X.509) vydaných důvěryhodnými certifikačními autoritami.

5. **Cíle bezpečnosti informací a příslušná technická opatření**

5.1. Pro výměnu informací prostřednictvím decentralizovaného informačního systému musí technická opatření zajišťující minimální bezpečnostní standardy informačních technologií zahrnovat:

a) opatření k zajištění důvěrnosti informací, a to i prostřednictvím používání zabezpečených komunikačních kanálů;

b) opatření k zajištění integrity údajů (zpráv, formulářů, dokumentů a elektronických důkazů) v úložišti („at rest“) a při přenosu („in transit“);

c) opatření k zajištění nepopiratelnosti původu odesílatele informací v rámci decentralizovaného informačního systému a nepopiratelnosti přijetí informací;

d) opatření k zajištění dostupnosti tím, že zajistí nepřetržitý přístup ke službám a datům a zabrání se narušením v důsledku kybernetických útoků nebo selhání;

e) opatření k zajištění protokolování bezpečnostních událostí v souladu s uznávanými mezinárodními doporučeními pro bezpečnostní standardy informačních technologií;

f) opatření k zajištění autentizace a autorizace uživatelů a opatření k ověření totožnosti systémů připojených k decentralizovanému informačnímu systému.

5.2. Komponenty decentralizovaného informačního systému zajišťují bezpečnou komunikaci a přenos údajů pomocí šifrování, infrastruktury veřejných klíčů s digitálními certifikáty pro autentizaci a bezpečnou výměnu klíčů a bezpečných protokolů pro zasílání zpráv, jako je AS4 (ebMS), RESTful API a SOAP, aby byla zachována důvěrnost a integrita zpráv.

5.3. Komponenty decentralizovaného informačního systému musí být vyvinuty v souladu se zásadou ochrany údajů již od návrhu a jako standardní nastavení a musí být zavedena vhodná administrativní, organizační a technická opatření k zajištění vysoké úrovně kybernetické bezpečnosti.

5.4. Komise navrhne, vyvine a udržuje referenční prováděcí software v souladu s požadavky a zásadami ochrany údajů stanovenými v nařízení (EU) 2018/1725. Referenční prováděcí software poskytnutý Komisí umožní členským státům splnit jejich povinnosti podle nařízení Evropského parlamentu a Rady (EU) 2016/679 ([4]), resp. směrnice Evropského parlamentu a Rady (EU) 2016/680 ([5]).

5.5. Členské státy, které používají jiný vnitrostátní informační systém než referenční prováděcí software, zavedou nezbytná opatření, aby zajistily jeho soulad s požadavky nařízení (EU) 2016/679 a případně směrnice (EU) 2016/680.

5.6. S ohledem na svou účast v decentralizovaném informačním systému provedou Eurojust a Úřad evropského veřejného žalobce opatření nezbytná k zajištění toho, aby jejich příslušné informační systémy splňovaly požadavky nařízení (EU) 2018/1725 a jejich zřizovacích aktů.

5.7. Členské státy, Eurojust a Úřad evropského veřejného žalobce zavedou pro informační systémy, které jsou součástí decentralizovaného informačního systému, za nějž odpovídají, spolehlivé mechanismy pro odhalování hrozeb a reakci na incidenty, aby zajistily včasnou identifikaci a zmírnění bezpečnostních incidentů a obnovu po nich v souladu se svými příslušnými politikami.

6. **Šifrování elektronických důkazů** ([6])

6.1. Aniž jsou dotčena bezpečnostní opatření poskytovaná decentralizovaným informačním systémem, mohou příslušné orgány při vydávání evropského vydávacího příkazu dodatečně dodat zvláštní veřejný certifikát X.509 pro asymetrické šifrování elektronických důkazů.

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

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

([6]) Pro vyloučení pochybností se pojem „elektronické důkazy“ omezuje na definici uvedenou v čl. 3 bodu 8 nařízení (EU) 2023/1543.

6.2. Za vydávání, správu, ověřování a všechny související aspekty certifikátů uvedených v bodě 6.1 a za odpovídající infrastrukturu veřejných klíčů odpovídá výhradně členský stát příslušného orgánu vydávajícího státu.

6.3. Aniž je dotčen budoucí technologický vývoj, veřejné certifikáty musí podporovat standardní šifrovací algoritmy, jako je RSA (Rivest-Shamir-Adleman) nebo ECDH (Elliptic Curve Diffie-Hellman) pro ECC (kryptografie na bázi eliptických křivek).

6.4. Veřejné certifikáty musí obsahovat rozšiřující atribut „keyUsage“ s vhodnou hodnotou, jako je „keyEncipherment“ nebo „dataEncipherment“ v případě certifikátů založených na RSA a „keyAgreement“ v případě certifikátů založených na ECC. Certifikáty musí být poskytnuty ve formátu PEM (Privacy-Enhanced Mail) nebo DER (Distinguished Encoding Rules).

6.5. Pokud vydávající orgán dodal veřejný certifikát X.509 a pokud poskytovatel služeb zasílá vydané elektronické důkazy na základě evropského vydávacího příkazu, zašifruje před předáním těchto údajů prostřednictvím decentralizovaného informačního systému elektronické důkazy za použití příslušného veřejného certifikátu X.509, který dodal vydávající stát.

6.6. Pokud vydávající orgán dodal veřejný certifikát X.509, ale pokud předání elektronických důkazů v zašifrované podobě není z technických nebo jiných oprávněných důvodů možný, a aniž je dotčeno ustanovení čl. 19 odst. 5 nařízení (EU) 2023/1543, může poskytovatel služeb předávat údaje bez zašifrování obsahu. V takových případech poskytovatel služeb poskytne vydávajícímu orgánu odůvodněné vysvětlení.

7. **Minimální cíle dostupnosti**

7.1. Členské státy, Eurojust a Úřad evropského veřejného žalobce zajistí nepřetržitou dostupnost komponent decentralizovaného informačního systému, za které odpovídají, přičemž cílová technická dostupnost musí bez plánované údržby činit nejméně 98 % ročně.

7.2. Komise zajistí nepřetržitou dostupnost databáze soudů, přičemž cílová technická dostupnost musí bez plánované údržby činit více než 99 % ročně.

7.3. Pokud je to možné, operace údržby během pracovních dnů musí být plánovány na dobu mezi 20:00–7:00 SEČ.

7.4. Členské státy, Eurojust a Úřad evropského veřejného žalobce informují Komisi a ostatní členské státy o činnostech údržby následovně:

a) 5 pracovních dnů předem v případě údržby, která může způsobit nedostupnost o délce až 4 hodin;

b) 10 pracovních dnů předem v případě údržby, která může způsobit nedostupnost o délce 4 až 12 hodin;

c) 30 pracovních dnů předem v případě údržby, která může způsobit nedostupnost o délce překračující 12 hodin.

7.5. Pokud mají členské státy, Eurojust nebo Úřad evropského veřejného žalobce stanoveny termíny pravidelné údržby, informují Komisi a účastníky decentralizovaného informačního systému o čase a dni (dnech), na kdy jsou tyto termíny pravidelné údržby plánovány. Bez ohledu na povinnosti stanovené v bodě 7.4 se mohou členské státy, Eurojust nebo Úřad evropského veřejného žalobce rozhodnout, že v případě nedostupnosti komponent decentralizovaného informačního systému, za které odpovídají, během těchto termínů pravidelné údržby nebudou Komisi pokaždé informovat.

7.6. Členské státy, Eurojust nebo Úřad evropského veřejného žalobce v případě neočekávaného technického selhání komponent decentralizovaného informačního systému, za které odpovídají, informují neprodleně Komisi a účastníky decentralizovaného informačního systému o tomto selhání, a pokud je znám, i o předpokládaném časovém rámci obnovy.

7.7. V případě údržby nebo neočekávaného technického selhání komponent decentralizovaného informačního systému, za které odpovídá členský stát, s nepříznivým dopadem na dostupnost rozhraní API a/nebo internetového rozhraní pro poskytovatele služeb, dotčený členský stát neprodleně zpřístupní tyto informace na internetových stránkách a/nebo je sdělí poskytovatelům služeb působícím na jeho území, a to bez zbytečného odkladu.

7.8. V případě neočekávaného technického selhání databáze soudů Komise neprodleně informuje členské státy, Eurojust a Úřad evropského veřejného žalobce o této nedostupnosti, a pokud je znám, i o předpokládaném časovém rámci obnovy.

7.9. V případě přerušení poskytování služeb zajistí členské státy, Eurojust a Úřad evropského veřejného žalobce rychlou obnovu služby a minimální ztrátu údajů v souladu s cílovou dobou obnovy funkce a cílovým okamžikem obnovy funkce.

7.10. Členské státy, Eurojust a Úřad evropského veřejného žalobce zavedou vhodná opatření k dosažení výše uvedených cílů dostupnosti a stanoví postupy pro účinnou reakci na incidenty.

8. **Databáze příslušných orgánů / soudů (CDB)**

8.1. S ohledem na článek 19 nařízení (EU) 2023/1543 je pro účely fungování decentralizovaného informačního systému nezbytné vytvořit závaznou databázi poskytovatelů služeb a příslušných orgánů.

8.2. Závazná databáze příslušných orgánů obsahuje následující informace ve strukturovaném formátu:

a) pro účely článku 19 nařízení (EU) 2023/1543 informace o příslušných orgánech oznámených podle čl. 31 odst. 1 písm. a) až c) uvedeného nařízení, včetně informací o:

1) vnitrostátních členech Eurojustu, společně s uvedení, zda mají oprávnění podle vnitrostátního práva vydávat evropské vydávací příkazy a evropské uchovávací příkazy ve smyslu čl. 8 odst. 3 a 4 nařízení Evropského parlamentu a Rady (EU) 2018/1727 ([7]);

2) evropských pověřených žalobcích a evropských žalobcích, pokud je členské státy oznámí v souladu s čl. 105 odst. 3 nařízení Rady (EU) 2017/1939 ([8]) jako příslušný vydávající orgán ve smyslu nařízení (EU) 2023/1543;

b) případně informace nezbytné k určení zeměpisných oblastí působnosti orgánů nebo jiná relevantní kritéria nezbytná k určení jejich působnosti;

c) informace, které jsou nezbytné pro řádné fungování a technické směrování zpráv při výměnách údajů v rámci decentralizovaného informačního systému.

8.2.1. Součástí informací uvedených v bodě 8.2 písm. c) jsou:

a) informace o členském státě, v němž je usazena určená provozovna poskytovatele služeb nebo kde má bydliště či sídlo jeho zástupce:

1) členský stát;

2) ústřední orgán;

([7]) Nařízení Evropského parlamentu a Rady (EU) 2018/1727 ze dne 14. listopadu 2018 o Agentuře Evropské unie pro justiční spolupráci v trestních věcech (Eurojust) a o nahrazení a zrušení rozhodnutí Rady 2002/187/SVV (Úř. věst. L 295, 21.11.2018, s. 138).

([8]) Nařízení Rady (EU) 2017/1939 ze dne 12. října 2017, kterým se provádí posílená spolupráce za účelem zřízení Úřadu evropského veřejného žalobce (Úř. věst. L 283, 31.10.2017, s. 1).

b) informace o poskytovateli služeb:

1) název/jméno;

2) adresa/sídlo;

3) registrační číslo;

4) právní forma,

5) telefonní číslo;

6) e-mail;

c) informace o určené provozovně / zástupci:

1) typ subjektu (určená provozovna / zástupce);

2) název/jméno;

3) adresa/sídlo;

4) telefonní číslo;

5) e-mail;

6) obecná kontaktní osoba / obecný kontaktní subjekt;

7) úřední jazyk (jazyky) akceptovaný (akceptované) poskytovatelem služeb / určenou provozovnou / zástupcem;

8) služby uvedené v čl. 2 bodu 1 směrnice Evropského parlamentu a Rady (EU) 2023/1544 ([9]) nabízené v Unii;

9) typ právních nástrojů EU, pro které jsou určené provozovny / zástupci určeni (v situacích, kdy se členské státy neúčastní všech příslušných právních nástrojů EU);

10) územní působnost určení/jmenování;

d) ověření informací:

1) název (jméno) oprávněného zástupce:

2) pracovní pozice;

3) adresa;

4) telefonní číslo;

5) e-mail;

6) datum.

8.2.2 Informace uvedené v bodě 8.2 písm. c) mohou zahrnovat, pokud jsou k dispozici:

a) informace o poskytovateli služeb:

1) kontaktní osoba pro dotazy týkající se oznámení (pokud se liší od podepisující osoby);

2) webové stránky;

b) typy dostupných údajů;

1) v případě každé dotčené služby:

— typy dostupných údajů,

— kategorie údajů,

— identifikátory,

— doba dostupnosti údajů;

([9]) 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 (Úř. věst. L 191, 28.7.2023, s. 181, ELI: http://data.europa.eu/eli/dir/2023/1544/oj).

2) další informace o údajích;

3) další informace o službě (např. subdodavatelské vztahy);

c) informace o určené provozovně / zástupci:

1) další poskytovatelé služeb, pro které jsou tyto určené provozovny nebo zástupci určeni;

2) kontaktní údaje technické pomoci;

3) kontaktní osoba pro případ nouze;

d) technické informace:

1) jméno/název technického kontaktního místa:

2) telefonní číslo technického kontaktního místa;

3) e-mail technického kontaktního místa;

4) adresa URL API pro dynamické získávání informací o typech údajů;

5) typ připojení k vnitrostátnímu informačnímu systému:

— internetové rozhraní,

— rozhraní API,

— adresa URL API Push.

8.3. S ohledem na provozní potřeby decentralizovaného informačního systému:

a) Komise odpovídá za vývoj, údržbu, provoz a podporu závazné databáze;

b) Komise umožní přístup do závazné databáze prostřednictvím rozhraní API, které je k dispozici příslušným orgánům, Eurojustu a Úřadu evropského veřejného žalobce pro účely jejich účasti v decentralizovaném informačním systému;

c) členské státy zajistí, aby informace o jejich příslušných orgánech uvedené v bodě 8.2 písm. a) a b) v závazné databázi byly úplné, přesné a aktualizované;

d) závazná databáze umožní členským státům poskytovat a aktualizovat informace o svých poskytovatelích služeb, které jsou v ní obsaženy, a orgánům účastnícím se decentralizovaného informačního systému umožní programový přístup k těmto informacím a jejich vyhledávání;

e) členské státy a poskytovatelé služeb zajistí, aby informace uvedené v bodě 8.2 písm. c) byly v závazné databázi úplné, přesné a aktualizované.