Úradný vestník
Európskej únie

SK
Séria L

2025/1550

29.7.2025

VYKONÁVACIE NARIADENIE KOMISIE (EÚ) 2025/1550

z 28. júla 2025,

ktorým sa stanovujú technické špecifikácie a iné požiadavky pre decentralizovaný informačný systém uvedený v nariadení Európskeho parlamentu a Rady (EÚ) 2023/1543

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1543 z 12. júla 2023 o európskych príkazoch na predloženie elektronických dôkazov a európskych príkazov na uchovanie elektronických dôkazov v trestnom konaní a na výkon trestu odňatia slobody v nadväznosti na trestné konanie ([1]), a najmä na jeho článok 25 ods. 1 písm. a), b), c) a d),

keďže:

(1) Na zriadenie decentralizovaného informačného systému uvedeného v nariadení (EÚ) 2023/1543 je potrebné vymedziť a prijať technické špecifikácie, opatrenia a ciele na implementáciu uvedeného systému.

(2) Podľa nariadenia (EÚ) 2023/1543 by mal decentralizovaný informačný systém zahŕňať informačné systémy členských štátov a agentúr a orgánov Únie a interoperabilné prístupové body e-CODEX, prostredníctvom ktorých sú tieto informačné systémy prepojené. Technické špecifikácie a iné požiadavky decentralizovaného informačného systému by preto mali odrážať tento rámec.

(3) V súlade s nariadením (EÚ) 2023/1543 by prístupové body decentralizovaného informačného systému mali byť založené na autorizovaných prístupových bodoch e-CODEX vymedzených v článku 3 ods. 3 nariadenia Európskeho parlamentu a Rady (EÚ) 2022/850 ([2]).

(4) Členské štáty sa môžu rozhodnúť, že namiesto vnútroštátneho informačného systému budú ako svoj backendový systém používať referenčný implementačný softvér vyvinutý Komisiou. V záujme zabezpečenia interoperability by vnútroštátne informačné systémy aj referenčný implementačný softvér mali podliehať rovnakým technickým špecifikáciám a požiadavkám stanoveným v tomto nariadení.

(5) S cieľom zmierniť potenciálne technické problémy týkajúce sa kapacity a spoľahlivosti decentralizovaného informačného systému je potrebné stanoviť prahovú hodnotu pre objem elektronických dôkazov zasielaných prostredníctvom tohto systému. Po spustení systému by sa mala monitorovať frekvencia a objem takýchto prenosov a prahová hodnota by sa mala v prípade potreby upraviť, aby sa maximalizovala efektívnosť systému.

(6) V záujme posilnenia interoperability a efektívnosti decentralizovaného informačného systému by malo byť používanie príslušných noriem ETSI povinné. Mal by sa sledovať budúci vývoj a v prípade potreby by sa malo zvážiť prijatie ďalších noriem ETSI.

(7) Írsko je viazané nariadením (EÚ) 2023/1543, a preto sa zúčastňuje na prijatí tohto nariadenia.

(8) V súlade s článkami 1 a 2 Protokolu č. 22 o postavení Dánska, ktorý je pripojený k Zmluve o Európskej únii a Zmluve o fungovaní Európskej únie, Dánsko týmto nariadením nie je viazané ani nepodlieha jeho uplatňovaniu.

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

([2]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/850 z 30. mája 2022 o počítačovom systéme na cezhraničnú elektronickú výmenu údajov v oblasti justičnej spolupráce v občianskych a trestných veciach (systém e-CODEX) a o zmene nariadenia (EÚ) 2018/1726 (Ú. v. EÚ L 150, 1.6.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/850/oj).

(9) V súlade s článkom 42 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725 ([3]) sa uskutočnili konzultácie s európskym dozorným úradníkom pre ochranu údajov, ktorý 25. júna 2025 vydal svoje stanovisko.

(10) Opatrenia stanovené v tomto nariadení sú v súlade so stanoviskom výboru zriadeného podľa článku 26 nariadenia (EÚ) 2023/1543,

PRIJALA TOTO NARIADENIE:

Článok 1

Technické špecifikácie decentralizovaného informačného systému

Technické špecifikácie a požiadavky, opatrenia a ciele decentralizovaného informačného systému uvedeného v článku 25 ods. 1 nariadenia (EÚ) 2023/1543 na komunikáciu v zmysle článku 19 uvedeného nariadenia sú stanovené v prílohe k tomuto nariadeniu.

Článok 2

Nadobudnutie účinnosti

Toto nariadenie nadobúda účinnosť dvadsiatym dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné v členských štátoch v súlade so zmluvami.

V Bruseli 28. júla 2025

Za Komisiu
predsedníčka
Ursula VON DER LEYEN

([3]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (Ú. v. EÚ L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

PRÍLOHA

TECHNICKÉ ŠPECIFIKÁCIE DECENTRALIZOVANÉHO INFORMAČNÉHO SYSTÉMU

(v zmysle článku 1)

1. Úvod a rozsah pôsobnosti

V tejto prílohe sa stanovujú technické špecifikácie, opatrenia a ciele decentralizovaného informačného systému pre postupy podľa nariadenia (EÚ) 2023/1543.

Podľa nariadenia (EÚ) 2023/1543, a najmä jeho článku 19, má decentralizovaný informačný systém umožniť písomnú komunikáciu medzi príslušnými orgánmi a určenými prevádzkarňami alebo právnymi zástupcami, medzi príslušnými orgánmi navzájom, ako aj medzi príslušnými orgánmi a príslušnými agentúrami alebo orgánmi Únie.

2. Vymedzenie pojmov

2.1. „zabezpečený hypertextový prenosový protokol“ (Hypertext Transfer Protocol Secure) alebo „HTTPS“ je šifrovaná komunikácia a bezpečné prepojovacie kanály;

2.2. „nepopretie pôvodu“ sú opatrenia poskytujúce dôkaz o integrite a dôkaz o pôvode údajov takými metódami, ako je napríklad elektronická certifikácia, infraštruktúra verejného kľúča a elektronické podpisy a elektronické pečate;

2.3. „nepopretie prijatia“ sú opatrenia poskytujúce pôvodcovi údajov dôkaz o prijatí údajov zamýšľaným príjemcom údajov takými metódami, ako je napríklad elektronická certifikácia, infraštruktúra verejného kľúča a elektronické podpisy a elektronické pečate;

2.4. „SOAP“ je podľa noriem Konzorcia World Wide Web špecifikácia protokolu zasielania správ na výmenu štruktúrovaných informácií pri zavádzaní webových služieb v počítačových sieťach;

2.5. „REST“ (*Representational State Transfer* – reprezentácia stavu prenosu) je architektonický štýl na navrhovanie sieťových aplikácií, ktorý sa opiera o bezstavový komunikačný model klient-server a využíva štandardné metódy na vykonávanie operácií so zdrojmi, ktoré sú zvyčajne reprezentované v štruktúrovaných formátoch;

2.6. „webová služba“ je softvérový systém určený na podporu interoperabilnej interakcie medzi zariadeniami prostredníctvom siete a ktorý má rozhranie popísané v strojovo spracovateľnom formáte;

2.7. „výmena údajov“ je výmena správ, formulárov, dokumentov a elektronických dôkazov prostredníctvom decentralizovaného informačného systému;

2.8. „API“ je aplikačné programovacie rozhranie založené na spoločnej norme pre výmenu údajov, ktoré poskytovateľom služieb, ktorí na účely výmeny informácií a údajov súvisiacich so žiadosťami o elektronické dôkazy využívajú individualizované IT riešenia, umožňuje automatizovaný prístup k decentralizovaným informačným systémom;

2.9. „webové rozhranie“ je používateľské rozhranie dostupné prostredníctvom HTTPS na internete, ktoré umožňuje poskytovateľom služieb manuálny prístup k decentralizovanému informačnému systému na účely bezpečnej komunikácie s orgánmi a na účely výmeny informácií a údajov súvisiacich so žiadosťami o elektronické dôkazy bez toho, aby museli vytvoriť vlastnú špecializovanú infraštruktúru;

2.10. „normy ETSI“ sú technické špecifikácie a normy vypracované Európskym inštitútom pre telekomunikačné normy (ETSI) s cieľom zaistiť interoperabilitu, bezpečnosť a efektívnosť informačných a komunikačných technológií. Poskytujú rámce, protokoly a najlepšie postupy pre širokú škálu technológií vrátane mobilných sietí, rádiovej komunikácie, kybernetickej bezpečnosti a internetovej infraštruktúry;

2.11. „hašovací výstup“ (*hash digest*) je výstup s pevnou dĺžkou generovaný kryptografickou hašovacou funkciou pri použití na vstup ľubovoľnej dĺžky. Kryptografická hašovacia funkcia je navrhnutá tak, aby spĺňala základné bezpečnostné vlastnosti vrátane odolnosti voči nájdeniu vzoru, odolnosti voči nájdeniu druhého vzoru a odolnosti voči kolízii, čím sa zaisťuje jej odolnosť voči útokom prostredníctvom inverzie a kolízie;

2.12. „systém e-CODEX“ je systém e-CODEX vymedzený v článku 3 bode 1 nariadenia (EÚ) 2022/850;

2.13. „slovníky základných pojmov elektronickej justície EÚ“ sú slovníky základných pojmov elektronickej justície EÚ vymedzené v bode 4 prílohy k nariadeniu (EÚ) 2022/850;

2.14. „ebMS“ je služba výmeny správ ebXML, čo je protokol na výmenu správ vyvinutý podľa rámca OASIS, ktorý umožňuje bezpečnú, spoľahlivú a interoperabilnú výmenu elektronických obchodných dokumentov pomocou protokolu SOAP a podporuje medzipodnikovú integráciu v rámci rôznych systémov;

2.15. „AS4“ (*Applicability Statement 4* – vyhlásenie o aplikovateľnosti 4) je norma OASIS, ktorou sa profiluje ebMS 3.0, pričom zjednodušuje bezpečnú a interoperabilnú medzipodnikovú výmenu správ pomocou otvorených noriem ako SOAP a WS-Security;

2.16. „cieľový čas obnovenia“ (*Recovery Time Objective*) je maximálne akceptovaný čas na obnovenie služby po incidente;

2.17. „cieľový bod obnovenia“ (*Recovery Point Objective*) je maximálna prijateľná miera straty údajov v prípade zlyhania.

3. **Spôsoby komunikácie elektronickými prostriedkami**

3.1. Decentralizovaný informačný systém využíva na účely písomnej komunikácie medzi príslušnými orgánmi členských štátov, medzi príslušnými orgánmi a určenými prevádzkarňami alebo právnymi zástupcami poskytovateľov služieb, ako aj medzi príslušnými orgánmi a agentúrami alebo orgánmi Únie metódy komunikácie založené na službách, ako napríklad webové služby alebo iné opätovne použiteľné komponenty a softvérové riešenia na účely výmeny údajov. Konkrétne bude zahŕňať komunikáciu prostredníctvom prístupových bodov e-CODEX, ako sa stanovuje v článku 5 ods. 2 nariadenia (EÚ) 2022/850. Na zabezpečenie účinnej a interoperabilnej cezhraničnej výmeny údajov preto musí decentralizovaný informačný systém podporovať komunikáciu prostredníctvom systému e-CODEX.

3.2. Vzhľadom na predpokladaný veľký objem elektronických dôkazov, ktoré sa majú zasielať na základe európskeho príkazu na predloženie dôkazov prostredníctvom decentralizovaného informačného systému, ako sa uvádza v článku 19 ods. 1 a 4 nariadenia (EÚ) 2023/1543, čo môže viesť k obmedzeniam technickej kapacity, ktoré by mohli mať na decentralizovaný informačný systém nepriaznivý vplyv, sa elektronické dôkazy zasielajú prostredníctvom tohto systému, pokiaľ nepresiahnu prahovú hodnotu 25 megabajtov (25 600 kilobajtov). Zasielanie elektronických dôkazov presahujúcich uvedenú prahovú hodnotu sa uskutočňuje v súlade s článkom 19 ods. 5 uvedeného nariadenia.

3.3. So zreteľom na článok 19 ods. 6 nariadenia (EÚ) 2023/1543, ak sa zasielanie uskutočňuje alternatívnymi prostriedkami, ako sa stanovuje v uvedenom odseku, pretože decentralizovaný informačný systém nemožno použiť z niektorého z dôvodov uvedených v článku 19 ods. 5 uvedeného nariadenia:

3.3.1. Ak je predmetom zaslania písomná komunikácia vrátane výmeny formulárov medzi príslušnými orgánmi a poskytovateľmi služieb v zmysle článku 19 ods. 1 nariadenia (EÚ) 2023/1543, pôvodca zaslania zaznamená toto zaslanie vo svojom vnútroštátnom informačnom systéme, ktorý je súčasťou decentralizovaného informačného systému. Zaznamenané informácie zahŕňajú minimálne referenčné číslo veci alebo spisu, dátum a čas, odosielateľa a príjemcu, názov súboru a jeho veľkosť.

3.3.2. Ak je predmetom zaslania písomná komunikácia vrátane výmeny formulárov medzi príslušnými orgánmi, ako aj písomná komunikácia s príslušnými agentúrami alebo orgánmi Únie v zmysle článku 19 ods. 4 nariadenia (EÚ) 2023/1543, pôvodca zaslania zaznamená toto zaslanie v decentralizovanom informačnom systéme, najmä v rámci svojho vnútroštátneho informačného systému alebo prípadne v informačných systémoch prevádzkovaných príslušnou agentúrou alebo orgánom Únie. Zaznamenané informácie zahŕňajú minimálne referenčné číslo veci alebo spisu, dátum a čas zaslania, odosielateľa a príjemcu, názov súboru a jeho veľkosť.

3.3.3. Ak sa zaslanie elektronických dôkazov na základe európskeho príkazu na predloženie dôkazov uskutočnilo prostredníctvom alternatívnych prostriedkov komunikácie medzi poskytovateľmi služieb a príslušnými orgánmi vo vydávajúcom štáte ([1]) alebo ak vykonávajúci orgán zasiela elektronické dôkazy prostredníctvom alternatívnych prostriedkov príslušným orgánom vo vydávajúcom štáte v rámci postupu vykonávania, ako sa stanovuje v článku 16 ods. 9 nariadenia (EÚ) 2023/1543, pôvodca:

a) zaznamená a pošle orgánu, ktorému bol elektronický dôkaz zaslaný alebo sprístupnený, nasledujúce informácie ako súčasť zoznamu:

1. informácie o odosielateľovi a príjemcovi;

2. metaúdaje, ktorými sa poskytnuté elektronické dôkazy spájajú s konkrétnym európskym príkazom na predloženie dôkazov alebo na uchovanie dôkazov;

3. dátum a čas zaslania alebo informácie o tom, kedy bol daný elektronický dôkaz sprístupnený príjemcovi;

4. informácie o spôsobe zaslania (napr. záznam o zabezpečenom prepojení, prostredníctvom ktorého bol elektronický dôkaz sprístupnený, doklad od poštových služieb o prijatí alebo doručení atď. ([2]));

5. úplný (-é) názov (-y) súboru (-ov) elektronických dôkazov, ktoré boli zaslané alebo inak sprístupnené zamýšľanému príjemcovi vo vydávajúcom štáte;

6. veľkosť údajov elektronických dôkazov, ktoré boli zaslané alebo inak sprístupnené zamýšľanému príjemcovi vo vydávajúcom štáte;

7. aspoň jeden hašovací výstup zaslaných alebo sprístupnených údajov a informácie o použitom (-ých) hašovacom (-ích) algoritme (-och). Hašovacie algoritmy použité na výpočet daných hašovacích výstupov musia byť kryptograficky silné, bežne používané a nesmú podliehať verejne známym slabým miestam, ako sú kolízie (napríklad SHA-512, SHA3-512, BLAKE2 alebo RIPEMD-160, ale potenciálne aj silnejšie v závislosti od technologického vývoja);

b) v náležitých prípadoch uvedie ako súčasť zoznamu uvedeného v písmene a) dátum a čas, do ktorého budú elektronické dôkazy prístupné. Táto lehota poskytuje príslušnému orgánu vo vydávajúcom štáte primeraný časový rámec na získanie elektronických dôkazov, pričom nesmie byť kratšia ako desať kalendárnych dní a dlhšia ako 45 kalendárnych dní od okamihu sprístupnenia elektronických dôkazov. Lehota uvedená pôvodcom sa na žiadosť príslušného orgánu vydávajúceho štátu môže v individuálnom prípade predĺžiť;

c) môže zaznamenať a zaslať orgánu, ktorému boli elektronické dôkazy zaslané alebo sprístupnené, akékoľvek doplňujúce informácie alebo poznámky týkajúce sa veci ako súčasť zoznamu uvedeného v písmene a).

3.4. So zreteľom na článok 28 nariadenia (EÚ) 2023/1543 referenčný implementačný softvér programovo zhromažďuje a zasiela štatistiky uvedené v odseku 2 uvedeného článku alebo inak poskytuje prístup k týmto štatistikám v štruktúrovaných (napr. XML) aj neštruktúrovaných (napr. PDF) formátoch údajov. V súlade s článkom 28 ods. 3 nariadenia (EÚ) 2023/1543 môžu tieto štatistiky automatizovaným postupom zasielať alebo poskytovať Komisii aj vnútroštátne portály ([3]) prevádzkované členskými štátmi, ak sú na to technicky vybavené. Komisia vydá usmernenie k štruktúre údajov a metóde zhromažďovania a oznamovania týchto štatistík.

([1]) V záujme väčšej jasnosti sa odkazy na príslušné vnútroštátne orgány chápu *mutatis mutandis* aj ako odkazy na národných členov Eurojustu, európskych prokurátorov a európskych delegovaných prokurátorov, pokiaľ sú oprávnení vykonávať rovnaké funkcie podľa práva EÚ a vnútroštátneho práva.

([2]) Treba pripomenúť, že v súlade s článkom 19 ods. 5 musí zasielanie prostredníctvom takýchto alternatívnych prostriedkov komunikácie spĺňať požiadavky, pokiaľ ide o rýchlosť, bezpečnosť a spoľahlivosť, ako aj možnosť príjemcu potvrdiť pravosť.

([3]) „Vnútroštátne portály“ sa majú chápať ako vnútroštátne „informačné systémy“, ktoré sú súčasťou decentralizovaného informačného systému, ako sa vymedzuje v článku 3 bode 21 nariadenia (EÚ) 2023/1543.

4. **Komunikačné protokoly**

4.1. Decentralizovaný informačný systém využíva zabezpečené internetové protokoly na:

a) komunikáciu v rámci decentralizovaného informačného systému medzi príslušnými orgánmi;

b) komunikáciu v rámci decentralizovaného informačného systému medzi príslušnými orgánmi a agentúrami a orgánmi Únie;

c) komunikáciu medzi príslušnými orgánmi a poskytovateľmi služieb prostredníctvom API a webového rozhrania a

d) komunikáciu s databázou o súdoch.

4.2. Pokiaľ ide o vymedzenie a zasielanie štruktúrovaných údajov a metaúdajov, komponenty decentralizovaného informačného systému sa zakladajú na komplexných a všeobecne uznávaných odvetvových normách a protokoloch ako SOAP a REST, najmä na takých, ktoré uvádzajú európske normalizačné organizácie, napríklad ETSI.

4.3. Pokiaľ ide o protokoly pre prenos a výmenu správ, decentralizovaný informačný systém vychádza zo zabezpečených protokolov založených na normách, ako sú:

a) profil AS4 na cezhraničnú výmenu údajov, ktorý zaisťuje bezpečnú a spoľahlivú výmenu správ so šifrovaním a s nepopretím;

b) rozhrania API HTTPS/RESTful na komunikáciu podporujúce formáty JSON a XML;

c) SOAP na vysoko spoľahlivé interakcie so zahrnutím normy WS-Security na overovanie a šifrovanie.

4.4. Na účely plynulej a interoperabilnej výmeny údajov musia komunikačné protokoly používané decentralizovaným informačným systémom spĺňať príslušné normy interoperability.

4.5. V náležitých prípadoch sa v schémach XML pre elektronické dôkazy využívajú príslušné normy alebo slovníky, ktoré sú potrebné na riadnu validáciu prvkov a typov definovaných v rámci tejto schémy. Môže ísť o:

a) slovník základných pojmov elektronickej justície EÚ;

b) neoprávnené dátové typy;

c) zoznam kódov jazykov Európskej únie.

V náležitých prípadoch môžu schémy XML obsahovať aj príslušné normy ETSI s cieľom využiť ich definície.

4.6. Komisia vymedzí špecifikácie spoločného API, ktoré vykonávajúce štáty sprístupnia poskytovateľom služieb ako prostriedok prístupu k decentralizovanému informačnému systému. Toto API je v rozsahu, v akom je to možné a rozumné, založené na norme ETSI TS 104 144 [„Interface definition for the e-Evidence Regulation (EU) 2023/1543 for National Authorities and Service Providers“] [Definícia rozhrania na účely nariadenia (EÚ) 2023/1543 o elektronických dôkazoch pre vnútroštátne orgány a poskytovateľov služieb].

4.7. Pokiaľ ide o bezpečnostné protokoly a protokoly na overovanie, decentralizovaný informačný systém vychádza z protokolov založených na normách, ako sú:

a) TLS (zabezpečenie transportnej vrstvy) na šifrovanú a overovanú komunikáciu v sieťach s podporou vzájomného overovania prostredníctvom digitálnych certifikátov X.509;

b) OAuth/OpenID Connect (OIDC) na bezpečné overovanie a autorizáciu;

c) Infraštruktúra verejného kľúča a digitálne podpisy na zabezpečenú výmenu kľúčov a overovanie integrity správ pomocou digitálnych certifikátov (X.509) vydaných dôveryhodnými certifikačnými orgánmi.

5. **Ciele informačnej bezpečnosti a príslušné technické opatrenia**

5.1. Na účely výmeny informácií prostredníctvom decentralizovaného informačného systému musia technické opatrenia na zaistenie minimálnych bezpečnostných noriem v oblasti informačných technológií zahŕňať:

a) opatrenia na zabezpečenie dôvernosti informácií, a to aj prostredníctvom zabezpečených kanálov komunikácie;

b) opatrenia na zabezpečenie integrity údajov (správ, formulárov, dokumentov a elektronických dôkazov) v pokoji a pri prenose;

c) opatrenia na zabezpečenie nepopretia pôvodu odosielateľa informácií v rámci decentralizovaného informačného systému a nepopretia prijatia informácií;

d) opatrenia na zabezpečenie dostupnosti zaistením nepretržitého prístupu k službám a údajom, ktoré zabránia narušeniam v dôsledku kybernetických útokov alebo zlyhaní;

e) opatrenia na zabezpečenie vedenia záznamov o bezpečnostných udalostiach v súlade s uznávanými medzinárodnými odporúčaniami pre bezpečnostné normy v oblasti informačných technológií;

f) opatrenia na zabezpečenie overovania a autorizácie používateľa a opatrenia na overenie identity systémov pripojených k decentralizovanému informačnému systému.

5.2. Komponenty decentralizovaného informačného systému zaisťujú zabezpečenú komunikáciu a zasielanie údajov pomocou šifrovania, infraštruktúry verejného kľúča s digitálnymi certifikátmi na overovanie a zabezpečenú výmenu kľúčov a zabezpečených protokolov na výmenu správ, ako sú AS4 (ebMS), API RESTful a SOAP na zachovanie dôvernosti a integrity správ.

5.3. Komponenty decentralizovaného informačného systému sú vyvinuté v súlade so zásadou špecificky navrhnutej a štandardnej ochrany údajov, pričom sú zavedené vhodné administratívne, organizačné a technické opatrenia na zaistenie vysokej úrovne kybernetickej bezpečnosti.

5.4. Komisia navrhne, vyvinie a udržiava referenčný implementačný softvér v súlade s požiadavkami a zásadami ochrany údajov stanovenými v nariadení (EÚ) 2018/1725. Referenčný implementačný softvér poskytnutý Komisiou umožní členským štátom plniť si povinnosti podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 ([4]) a smernice Európskeho parlamentu a Rady (EÚ) 2016/680 ([5]), podľa toho, čo sa uplatňuje.

5.5. Členské štáty, ktoré používajú vnútroštátny informačný systém odlišný od referenčného implementačného softvéru, zavedú potrebné opatrenia na zabezpečenie toho, aby spĺňal požiadavky nariadenia (EÚ) 2016/679 a smernice (EÚ) 2016/680, podľa toho, čo sa uplatňuje.

5.6. Eurojust a Európska prokuratúra so zreteľom na svoju účasť v decentralizovanom informačnom systéme zavedú potrebné opatrenia na zabezpečenie toho, aby ich príslušné informačné systémy spĺňali požiadavky nariadenia (EÚ) 2018/1725 a ich zakladajúcich aktov.

5.7. Členské štáty, Eurojust a Európska prokuratúra zavedú v súvislosti s informačnými systémami, ktoré sú súčasťou decentralizovaného informačného systému a za ktoré zodpovedajú, spoľahlivé mechanizmy na odhaľovanie hrozieb a reakciu na incidenty s cieľom zaistiť včasnú identifikáciu bezpečnostných incidentov, ich zmiernenie a obnovu po nich, a to v súlade so svojimi príslušnými politikami.

6. **Šifrovanie elektronických dôkazov** ([6])

6.1. Bez toho, aby boli dotknuté bezpečnostné opatrenia poskytované decentralizovaným informačným systémom, môžu príslušné orgány pri vydávaní európskeho príkazu na predloženie dôkazov dodatočne predložiť osobitný verejný certifikát X.509 na asymetrické šifrovanie elektronických dôkazov.

([4]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1).

([5]) Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV (Ú. v. EÚ L 119, 4.5.2016, s. 89).

([6]) S cieľom predísť pochybnostiam sa pojem „elektronické dôkazy“ obmedzuje na vymedzenie tohto pojmu v článku 3 bode 8 nariadenia (EÚ) 2023/1543.

6.2. Za vydávanie, správu, overovanie a všetky súvisiace aspekty certifikátov uvedených v bode 6.1 spolu s príslušnou infraštruktúrou verejného kľúča zodpovedá výlučne vydávajúci štát.

6.3. Bez toho, aby bol dotknutý budúci technologický vývoj, verejné certifikáty podporujú šifrovacie algoritmy založené na odvetvových normách, ako napríklad RSA (Rivest-Shamir-Adleman) alebo ECDH (*Elliptic Curve Diffie-Hellman* – Diffie – Helmannova eliptická krivka) pre ECC (*Elliptic Curve Cryptography* – kryptografia podľa eliptickej krivky).

6.4. Verejné certifikáty musia mať príslušné rozšírenie na atribút „keyUsage“, ako je „keyEncipherment“ alebo „dataEncipherment“ v prípade certifikátov založených na RSA a „keyAgreement“ v prípade certifikátov založených na ECC. Certifikáty musia byť poskytnuté vo formáte PEM (*Privacy-Enhanced Mail*) alebo DER (*Distinguished Encoding Rules*).

6.5. Ak vydávajúci orgán predložil verejný certifikát X.509 a ak poskytovateľ služieb posiela predložené elektronické dôkazy na základe európskeho príkazu na predloženie dôkazov, poskytovateľ pred zaslaním daných údajov prostredníctvom decentralizovaného informačného systému zašifruje elektronické dôkazy na základe príslušného verejného certifikátu X.509, ktorý predložil vydávajúci štát.

6.6. Ak vydávajúci orgán predložil verejný certifikát X.509, ale zaslanie elektronických dôkazov v zašifrovanej forme nie je možné z technických alebo iných opodstatnených dôvodov, a bez toho, aby bolo dotknuté ustanovenie podľa článku 19 ods. 5 nariadenia (EÚ) 2023/1543, poskytovateľ služieb môže údaje zaslať bez šifrovania obsahu. V takýchto prípadoch poskytovateľ služieb poskytne vydávajúcemu orgánu odôvodnené vysvetlenie.

7. **Ciele minimálnej dostupnosti**

7.1. Členské štáty, Eurojust a Európska prokuratúra zabezpečia nepretržitú dostupnosť (24 hodín denne, 7 dní v týždni) komponentov decentralizovaného informačného systému, za ktoré sú zodpovedné, pričom cieľová miera technickej dostupnosti je najmenej 98 % ročne bez zahrnutia plánovanej údržby.

7.2. Komisia zabezpečí nepretržitú dostupnosť (24 hodín denne, 7 dní v týždni) databázy o súdoch, pričom cieľová miera technickej dostupnosti je viac ako 99 % ročne bez zahrnutia plánovanej údržby.

7.3. Pokiaľ je to možné, operácie údržby sa počas pracovných dní plánujú v rámci časového úseku 20.00 – 7.00 hod. SEČ.

7.4. Členské štáty, Eurojust a Európska prokuratúra oznámia Komisii a ostatným členským štátom činnosti údržby takto:

a) 5 pracovných dní vopred v prípade operácií údržby, ktoré môžu spôsobiť nedostupnosť systému v trvaní najviac 4 hodín;

b) 10 pracovných dní vopred v prípade operácií údržby, ktoré môžu spôsobiť nedostupnosť systému v trvaní od 4 do 12 hodín;

c) 30 pracovných dní vopred v prípade operácií údržby, ktoré môžu spôsobiť nedostupnosť systému v trvaní viac ako 12 hodín.

7.5. Ak majú členské štáty, Eurojust alebo Európska prokuratúra stanovené pravidelné termíny údržby, informujú Komisiu a účastníkov decentralizovaného informačného systému o čase a dni (dňoch), keď sú tieto stanovené pravidelné termíny naplánované. Bez ohľadu na povinnosti stanovené v bode 7.4, ak sa komponenty decentralizovaného informačného systému, za ktoré zodpovedajú členské štáty, Eurojust alebo Európska prokuratúra, stanú nedostupnými počas takéhoto pravidelného stanoveného termínu, môžu sa v jednotlivých prípadoch rozhodnúť neoznámiť to Komisii.

7.6. V prípade neočakávaného technického zlyhania komponentov decentralizovaného informačného systému, za ktoré zodpovedajú členské štáty, Eurojust alebo Európska prokuratúra, tieto subjekty bezodkladne informujú Komisiu a účastníkov decentralizovaného informačného systému o predmetnom zlyhaní a o predpokladanom časovom rámci obnovenia, ak je známy.

7.7. V prípade činností údržby alebo neočakávaného technického zlyhania komponentov decentralizovaného informačného systému, za ktoré zodpovedá členský štát, s nepriaznivým vplyvom na dostupnosť API a/alebo webového rozhrania pre poskytovateľov služieb dotknutý členský štát bez zbytočného odkladu sprístupní tieto informácie na webovom sídle a/alebo ich oznámi poskytovateľom služieb pôsobiacim na jeho území.

7.8. V prípade neočakávaného technického zlyhania databázy o súdoch Komisia bezodkladne informuje členské štáty, Eurojust a Európsku prokuratúru o tejto nedostupnosti a o predpokladanom časovom rámci obnovenia, ak je známy.

7.9. V prípade prerušenia prevádzky služieb členské štáty, Eurojust a Európska prokuratúra zabezpečia rýchle obnovenie služieb a minimálnu stratu údajov v súlade s cieľovým časom obnovenia a cieľovým bodom obnovenia.

7.10. Členské štáty, Eurojust a Európska prokuratúra zavedú vhodné opatrenia na dosiahnutie uvedených cieľov dostupnosti a stanovia postupy účinnej reakcie na incidenty.

8. **Databáza o príslušných orgánoch/súdoch (CDB)**

8.1. So zreteľom na článok 19 nariadenia (EÚ) 2023/1543 je na účely fungovania decentralizovaného informačného systému nevyhnutné vytvoriť oficiálnu databázu o poskytovateľoch služieb a príslušných orgánoch.

8.2. Oficiálna databáza o príslušných orgánoch obsahuje tieto informácie v štruktúrovanom formáte:

a) na účely článku 19 nariadenia (EÚ) 2023/1543 informácie o príslušných orgánoch oznámených podľa článku 31 ods. 1 písm. a) až c) uvedeného nariadenia vrátane informácií o:

1. národných členoch Eurojustu s uvedením, či sú podľa vnútroštátneho práva oprávnení vydávať európske príkazy na predloženie dôkazov a európske príkazy na uchovanie dôkazov v súlade s článkom 8 ods. 3 a 4 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1727 ([7]);

2. európskych delegovaných prokurátoroch a európskych prokurátoroch, pokiaľ ich členské štáty oznámili v súlade s článkom 105 ods. 3 nariadenia Rady (EÚ) 2017/1939 ([8]) ako príslušný vydávajúci orgán v zmysle nariadenia (EÚ) 2023/1543;

b) v príslušných prípadoch informácie potrebné na určenie zemepisných oblastí pôsobnosti orgánov alebo iné relevantné kritériá potrebné na určenie ich pôsobnosti;

c) informácie potrebné na správne fungovanie decentralizovaného informačného systému a technické smerovanie správ pri výmene údajov v rámci neho.

8.2.1. Informácie uvedené v bode 8.2 písm. c) musia zahŕňať:

a) informácie o členskom štáte, v ktorom je zriadená určená prevádzkareň poskytovateľa služieb alebo v ktorom má sídlo jeho právny zástupca:

1. členský štát;

2. ústredný orgán;

([7]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1727 zo 14. novembra 2018 o Agentúre Európskej únie pre justičnú spoluprácu v trestných veciach (Eurojust) a o nahradení a zrušení rozhodnutia Rady 2002/187/SVV (Ú. v. EÚ L 295, 21.11.2018, s. 138).

([8]) Nariadenie Rady (EÚ) 2017/1939 z 12. októbra 2017, ktorým sa vykonáva posilnená spolupráca na účely zriadenia Európskej prokuratúry (Ú. v. EÚ L 283, 31.10.2017, s. 1).

b) informácie o poskytovateľovi služieb:

1. názov/meno;
2. adresa/sídlo;
3. registračné číslo;
4. právna forma;
5. telefónne číslo;
6. e-mailová adresa;

c) informácie o určenej prevádzkarni/právnom zástupcovi:

1. typ subjektu (určená prevádzkareň/právny zástupca);
2. názov/meno;
3. adresa/sídlo;
4. telefónne číslo;
5. e-mailová adresa;
6. všeobecná kontaktná osoba/subjekt;
7. úradný (-é) jazyk (-y) akceptovaný (-é) poskytovateľom služieb/určenou prevádzkarňou/právnym zástupcom;
8. služby uvedené v článku 2 ods. 1 smernice Európskeho parlamentu a Rady (EÚ) 2023/1544 ([9]) ponúkané v Únii;
9. typ právnych nástrojov EÚ, pre ktoré je daná určená prevádzkareň/právny zástupca určená/určený (v situáciách, keď sa členské štáty nezúčastňujú na všetkých príslušných právnych nástrojoch EÚ);
10. územná pôsobnosť určenia/vymenovania;

d) overenie pravosti informácií:

1. meno splnomocneného zástupcu;
2. pracovné zaradenie;
3. adresa;
4. telefónne číslo;
5. e-mailová adresa;
6. dátum.

8.2.2. Informácie uvedené v bode 8.2 písm. c) môžu zahŕňať tieto údaje, ak sú dostupné:

a) informácie o poskytovateľovi služieb:

1. kontaktná osoba pre otázky týkajúce sa oznámení (ak sa líši od podpisujúcej osoby);
2. webové sídlo;

b) typy dostupných údajov:

1. pri každej dotknutej službe:

— typy dostupných údajov,

— kategória údajov,

— identifikátory,

— obdobie dostupnosti údajov;

([9]) Smernica Európskeho parlamentu a Rady (EÚ) 2023/1544 z 12. júla 2023, ktorou sa stanovujú harmonizované pravidlá určovania určených prevádzkarní a vymenúvania právnych zástupcov na účely zhromažďovania dôkazov v trestnom konaní (Ú. v. EÚ L 191, 28.7.2023, s. 181, ELI: http://data.europa.eu/eli/dir/2023/1544/oj).

2. doplňujúce informácie o údajoch;
3. doplňujúce informácie o službe (napr. o subdodávateľských vzťahoch);

c) informácie o určenej prevádzkarni/právnom zástupcovi:
1. ďalší poskytovatelia služieb, pre ktorých je daná určená prevádzkareň alebo právny zástupca určený;
2. kontaktné informácie o technickej pomoci;
3. kontakt pre prípad mimoriadnej situácie;

d) technické informácie:
1. názov technického kontaktného miesta;
2. telefónne číslo technického kontaktného miesta;
3. e-mailová adresa technického kontaktného miesta;
4. URL adresa API pre dynamické získavanie informácií o tomto type údajov;
5. typ pripojenia k vnútroštátnemu informačnému systému:
— webové rozhranie,
— API,
— Push API URL.

8.3. Pokiaľ ide o prevádzkové potreby decentralizovaného informačného systému:

a) Komisia zodpovedá za vývoj, údržbu, prevádzku a podporu oficiálnej databázy;

b) Komisia umožní prístup do oficiálnej databázy prostredníctvom API sprístupneného príslušným orgánom, Eurojustu a Európskej prokuratúre na účely účasti v decentralizovanom informačnom systéme;

c) členské štáty zabezpečia, aby informácie o ich príslušných orgánoch stanovené v bode 8.2 písm. a) a b) v oficiálnej databáze boli úplné, presné a aktualizované;

d) oficiálna databáza umožňuje členským štátom poskytovať a aktualizovať informácie o svojich poskytovateľoch služieb, ktoré sú v nej uvedené, a orgánom zúčastneným v decentralizovanom informačnom systéme umožňuje programový prístup k týmto informáciám a ich vyhľadávanie;

e) členské štáty a poskytovatelia služieb zabezpečia, aby informácie stanovené v bode 8.2 písm. c) v oficiálnej databáze boli úplné, presné a aktualizované.