Úradný vestník
Európskej únie

SK
Séria L

2025/2447

5.12.2025

VYKONÁVACIE NARIADENIE KOMISIE (EÚ) 2025/2447

zo 4. decembra 2025,

ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1727, pokiaľ ide o technické špecifikácie, opatrenia a iné požiadavky na zriadenie a využívanie decentralizovaného informačného systému na účely bezpečného spracúvania a poskytovania informácií

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na 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 ([1]), a najmä na jeho článok 22a ods. 3 a článok 22b ods. 1 písm. a), b), c) a d),

keďže:

(1) V nariadení (EÚ) 2018/1727 sa stanovuje rámec pre novú digitálnu vnútornú infraštruktúru Eurojustu a zriadenie decentralizovaného systému zabezpečenej digitálnej komunikácie medzi príslušnými vnútroštátnymi orgánmi členských štátov a Eurojustom.

(2) Zabezpečená digitálna komunikácia sa má vykonávať prostredníctvom decentralizovaného informačného systému. Na účely zriadenia decentralizovaného informačného systému treba stanoviť technické špecifikácie, v ktorých sa vymedzia metódy komunikácie a komunikačné protokoly, technické opatrenia zabezpečujúce minimálne normy informačnej bezpečnosti a minimálne ciele z hľadiska dostupnosti na prevádzkovanie tohto systému.

(3) Podľa článku 22a ods. 1 nariadenia (EÚ) 2018/1727 má decentralizovaný informačný systém pozostávať z informačných systémov členských štátov a Eurojustu a interoperabilných prístupových bodov e-CODEX, prostredníctvom ktorých sú tieto informačné systémy prepojené. Uvedený rámec by sa mal zohľadniť v technických špecifikáciách a iných požiadavkách decentralizovaného informačného systému stanovených v tomto nariadení.

(4) Prístupové body decentralizovaného informačného systému by mali byť založené na autorizovaných prístupových bodoch e-CODEX vymedzených v článku 3 ods. 3 nariadenia Európskeho parlamentu a Rady (EÚ) 2022/850 ([2]).

(5) Decentralizovaný informačný systém je implementovaný v rámci rozsiahlejšieho decentralizovaného informačného systému založeného na systéme e-CODEX, ktorý sa označuje ako digitálny systém na výmenu informácií v oblasti justície (JUDEX). Preto treba zabezpečiť účinnú výmenu informácií týkajúcich sa vývoja v horizontálnej rovine.

(6) V súlade s článkom 22a ods. 4 nariadenia (EÚ) 2018/1727 sa môžu členské štáty a Eurojust 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.

(7) Údaje týkajúce sa teroristických trestných činov a závažnej organizovanej trestnej činnosti by sa mali zasielať štruktúrovaným spôsobom, aby sa zlepšila kvalita a relevantnosť informácií, ako aj zabezpečilo efektívnejšie začlenenie informácií do systému správy vecí Eurojustu a ich lepšia krížová kontrola s informáciami, ktoré sú už v tomto systéme uložené. V prípade údajov o odtlačkoch prstov a fotografií, ktoré možno Eurojustu postupovať na účely identifikácie osôb, voči ktorým sa vedie trestné konanie v súvislosti s teroristickými trestnými činmi, by sa mal vymedziť formát a technické normy pre postupovanie.

([1]) Ú. v. EÚ L 295, 21.11.2018, s. 138, ELI: http://data.europa.eu/eli/reg/2018/1727/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).

(8) Eurojust uľahčuje a podporuje vydávanie a vykonávanie žiadostí o justičnú spoluprácu vrátane žiadostí a rozhodnutí vychádzajúcich z nástrojov, na základe ktorých nadobúda účinok zásada vzájomného uznávania. Príslušné vnútroštátne orgány by mali mať možnosť prostredníctvom decentralizovaného informačného systému požiadať Eurojust o pomoc a koordináciu.

(9) S cieľom zabezpečiť efektívnosť a konzistentnosť je dôležité, aby technické špecifikácie, ktoré sa majú stanoviť podľa nariadenia (EÚ) 2018/1727, boli zlučiteľné s technickými špecifikáciami stanovenými podľa nariadení Európskeho parlamentu a Rady (EÚ) 2023/2844 ([3]), (EÚ) 2023/1543 ([4]) a (EÚ) 2024/3011 ([5]), ako aj s budúcimi opatreniami v oblasti digitalizácie relevantnými z hľadiska mandátu Eurojustu týkajúceho sa podpory príslušných vnútroštátnych orgánov.

(10) Prostredníctvom decentralizovaného informačného systému by sa mala takisto umožniť akákoľvek iná komunikácia medzi Eurojustom a príslušnými vnútroštátnymi orgánmi, ako je napríklad poskytovanie informácií o výsledkoch spracúvania informácií vrátane existencie prepojení na prípady, ktoré sú už uložené v systéme správy vecí v súlade s článkom 22 nariadenia (EÚ) 2018/1727, keď Eurojust koná z vlastnej iniciatívy, alebo informácií postúpených Eurojustu na účely uchovania, analýzy a ukladania dôkazov týkajúcich sa genocídy, zločinov proti ľudskosti, vojnových zločinov a súvisiacich trestných činov v súlade s článkom 4 ods. 1 písm. j) uvedeného nariadenia.

(11) S cieľom zabezpečiť, aby sa v tomto nariadení zohľadnili operačné potreby Eurojustu, sa v súlade s článkom 22a ods. 3 nariadenia (EÚ) 2018/1727 uskutočnili konzultácie s Eurojustom.

(12) V súlade s článkom 4 Protokolu č. 21 o postavení Spojeného kráľovstva a Írska s ohľadom na priestor slobody, bezpečnosti a spravodlivosti, ktorý je pripojený k Zmluve o Európskej únii a Zmluve o fungovaní Európskej únie, Írsko listom z 9. septembra 2019 oznámilo želanie prijať nariadenie (EÚ) 2018/1727 a byť ním viazané. Rozhodnutím Komisie (EÚ) 2019/2006 ([6]) sa táto účasť potvrdzuje. Nariadením Európskeho parlamentu a Rady (EÚ) 2023/2131 ([7]) sa zmenilo nariadenie (EÚ) 2018/1727 s cieľom umožniť zriadenie zabezpečených digitálnych komunikačných kanálov medzi Eurojustom a príslušnými vnútroštátnymi orgánmi a predstavuje právny základ pre toto nariadenie. V situácii, keď Írsko neoznámilo svoje želanie zúčastniť sa na prijatí a uplatňovaní nariadenia (EÚ) 2023/2131 a neoznámilo svoje želanie prijať uvedené nariadenie a byť ním viazané, v súlade s článkami 1 a 2 a článkom 4a ods. 1 protokolu č. 21 nie je Írsko viazané nariadením (EÚ) 2023/2131, ani nepodlieha jeho uplatňovaniu. Írsko sa preto nezúčastňuje na prijatí tohto nariadenia.

(13) 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, sa Dánsko nezúčastnilo na prijatí nariadenia (EÚ) 2018/1727. Dánsko preto týmto nariadením nie je viazané ani nepodlieha jeho uplatňovaniu.

([3]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/2844 z 13. decembra 2023 o digitalizácii justičnej spolupráce a prístupu k spravodlivosti v cezhraničných občianskych, obchodných a trestných veciach a o zmene niektorých aktov v oblasti justičnej spolupráce (Ú. v. EÚ L, 2023/2844, 27.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2844/oj).

([4]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1543 z 12. júla 2023 o európskych príkazoch na predloženie elektronických dôkazov a európskych príkazoch na uchovanie elektronických dôkazov v trestnom konaní a na výkon trestu odňatia slobody v nadväznosti na trestné konanie (Ú. v. EÚ L 191, 28.7.2023, s. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

([5]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/3011 z 27. novembra 2024 o odovzdávaní trestného konania (Ú. v. EÚ L, 2024/3011, 18.12.2024, ELI: http://data.europa.eu/eli/reg/2024/3011/oj).

([6]) Rozhodnutie Komisie (EÚ) 2019/2006 z 29. novembra 2019 o účasti Írska na nariadení Európskeho parlamentu a Rady (EÚ) 2018/1727 o Agentúre Európskej únie pre justičnú spoluprácu v trestných veciach (Eurojust) (Ú. v. EÚ L 310, 2.12.2019, s. 59, ELI: http://data.europa.eu/eli/dec/2019/2006/oj).

([7]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/2131 zo 4. októbra 2023, ktorým sa mení nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1727 a rozhodnutie Rady 2005/671/SVV, pokiaľ ide o digitálnu výmenu informácií v prípadoch terorizmu (Ú. v. EÚ L, 2023/2131, 11.10.2023, ELI: http://data.europa.eu/eli/reg/2023/2131/oj).

(14) V súlade s článkom 42 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725 ([8]) sa uskutočnili konzultácie s európskym dozorným úradníkom pre ochranu údajov, ktorý vydal 21. októbra 2025 svoje stanovisko,

(15) Opatrenia stanovené v tomto nariadení sú v súlade so stanoviskom výboru zriadeného podľa článku 22c nariadenia (EÚ) 2018/1727,

PRIJALA TOTO NARIADENIE:

Článok 1

Technické špecifikácie decentralizovaného informačného systému

Technické špecifikácie, opatrenia a ciele decentralizovaného informačného systému uvedené v článku 22b ods. 1 písm. a), b), c) a d) nariadenia (EÚ) 2018/1727 sa stanovujú v prílohe I k tomuto nariadeniu.

Článok 2

Digitálne procesné štandardy

Digitálne procesné štandardy uplatniteľné na elektronickú komunikáciu prostredníctvom decentralizovaného informačného systému uvedené v článku 22a ods. 3 nariadenia (EÚ) 2018/1727 sú stanovené v prílohe II k tomuto nariadeniu.

Článok 3

Technické špecifikácie postupovania odtlačkov prstov a fotografií

Technické špecifikácie a formát na účely postupovania odtlačkov prstov a fotografií, ako sa uvádza v článku 22a ods. 3 nariadenia (EÚ) 2018/1727, sú stanovené v prílohe III k tomuto nariadeniu.

Článok 4

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 4. decembra 2025

Za Komisiu
predsedníčka
Ursula VON DER LEYEN

([8]) 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 I

TECHNICKÉ ŠPECIFIKÁCIE, OPATRENIA A CIELE DECENTRALIZOVANÉHO INFORMAČNÉHO SYSTÉMU

1. Úvod a rozsah pôsobnosti

V tejto prílohe sa stanovujú technické špecifikácie, opatrenia a ciele decentralizovaného informačného systému pre výmenu informácií podľa nariadenia (EÚ) 2018/1727.

Decentralizovaná povaha informačného systému umožňuje priamu a bezpečnú výmenu údajov medzi príslušnými vnútroštátnymi orgánmi a Eurojustom.

2. Vymedzenie pojmov

Na účely tejto prílohy sa uplatňuje toto 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, elektronické podpisy a elektronické pečate;

2.4. „prístupový protokol SOAP (Simple Object Access Protocol)“ 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 a dokumentov prostredníctvom decentralizovaného informačného systému.

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

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

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

2.11. „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;

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

2.13. „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 výmeny správ a dokumentov metódy komunikácie založené na službách, ako sú webové služby alebo iné opakovane použiteľné komponenty a softvérové riešenia.

3.2. Decentralizovaný informačný systém konkrétne zahŕňa 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.

4. **Komunikačné protokoly**

4.1. Decentralizovaný informačný systém využíva zabezpečené internetové protokoly na:

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

b) komunikáciu s databázou o príslušných orgánoch/súdoch, ako sa uvádza v bode 7.1.

4.2. Pokiaľ ide o vymedzenie a postupovanie štruktúrovaných údajov a metaúdajov, komponenty decentralizovaného informačného systému sa zakladajú na komplexných a všeobecne uznávaných odvetvových normách a protokoloch ako SOAP a REST.

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 využívajú príslušné normy alebo slovníky, ktoré sú potrebné na riadnu validáciu prvkov a typov definovaných v rámci tejto schémy. Uvedené normy alebo slovníky môžu zahŕňať:

a) slovník základných pojmov elektronickej justície EÚ;

b) neoprávnené dátové typy;

c) zoznam kódov jazykov Európskej únie.

4.6. 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) PKI (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 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 vedenia záznamov o bezpečnostných udalostiach v súlade s uznávanými medzinárodnými odporúčaniami pre bezpečnostné normy v oblasti informačných technológií ([1]);

e) 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 postupovanie 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. Ak sa v kontexte decentralizovaného informačného systému používa protokol TLS, použije sa najnovšia stabilná verzia protokolu alebo, ak to nie je možné, verzia bez známych bezpečnostných zraniteľností. Povolené sú len také dĺžky kľúča, ktoré zabezpečujú primeranú úroveň kryptografickej bezpečnosti, a nesmú sa používať šifrovacie súbory, o ktorých je známe, že nie sú bezpečné alebo sú zastaralé.

5.4. Digitálne certifikáty PKI používané na účely prevádzky decentralizovaného informačného systému vydávajú, pokiaľ je to možné, certifikačné orgány uznané za kvalifikovaných poskytovateľov dôveryhodných služieb v súlade s nariadením Európskeho parlamentu a Rady (EÚ) č. 910/2014 ([2]). Aby sa zabezpečilo, že takéto certifikáty sa používajú výlučne na zamýšľané účely, musia sa zaviesť opatrenia na požadovanej úrovni dôvery a v súlade s uplatniteľnými požiadavkami nariadenia (EÚ) č. 910/2014.

5.5. 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.

5.6. 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 v súlade s nariadením Európskeho parlamentu a Rady (EÚ) 2016/679 ([3]) a smernice (EÚ) 2016/680, podľa toho, čo sa uplatňuje.

([1]) Bez toho, aby bolo dotknuté vedenie záznamov na bezpečnostné účely, mechanizmy vedenia záznamov používané komponentmi decentralizovaného informačného systému podľa potreby umožňujú zabezpečiť súlad s požiadavkami stanovenými v článku 88 nariadenia (EÚ) 2018/1725 a prípadne v článku 25 smernice 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, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

([2]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (Ú. v. EÚ L 257, 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([3]) 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

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

5.8. Eurojust musí vykonať opatrenia potrebné na zabezpečenie toho, aby jeho backendový systém alebo príklad referenčného implementačného softvéru, ktorý používa, spĺňal požiadavky nariadení (EÚ) 2018/1725 a (EÚ) 2018/1727.

5.9. Členské štáty a Eurojust 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. **Ciele minimálnej dostupnosti**

6.1. Eurojust a členské štáty 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.

6.2. 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.

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

6.4. Členské štáty musia činnosti údržby oznámiť Komisii, Eurojustu a ostatným členským štátom 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.

6.5. Ak majú členské štáty stanovené pravidelné termíny údržby, informujú Komisiu, Eurojust a ostatné členské štáty o čase a dni (dňoch), keď sú tieto stanovené pravidelné termíny naplánované. Odchylne od povinností stanovených v prvej vete, ak sa komponenty decentralizovaného informačného systému, za ktoré zodpovedajú členské štáty, stanú nedostupnými počas takéhoto pravidelného stanoveného termínu, členské štáty sa môžu v jednotlivých prípadoch rozhodnúť neoznámiť to Komisii.

6.6. V prípade neočakávaného technického zlyhania komponentu decentralizovaného informačného systému, za ktorý zodpovedajú členské štáty, členské štáty musia bezodkladne informovať Komisiu a ostatné členské štáty o predmetnom zlyhaní a o predpokladanom časovom rámci obnovenia, ak je známy.

6.7. Eurojust musí činnosti údržby oznámiť Komisii a členským štátom 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.

6.8. Ak Eurojust stanovil pravidelné termíny údržby, Eurojust musí informovať Komisiu a členské štáty o čase a dni (dňoch), keď sú tieto stanovené pravidelné termíny naplánované. Odchylne od povinností stanovených v prvej vete, ak sa komponenty decentralizovaného informačného systému, za ktoré zodpovedá Eurojust, stanú nedostupnými počas takéhoto pravidelného stanoveného termínu, Eurojust sa môže v jednotlivých prípadoch rozhodnúť neoznámiť to Komisii.

6.9. V prípade neočakávaného technického zlyhania komponentu decentralizovaného informačného systému, za ktorý zodpovedá Eurojust, Eurojust musí bezodkladne informovať Komisiu a členské štáty o predmetnom zlyhaní a o predpokladanom časovom rámci obnovenia, ak je známy.

6.10. V prípade neočakávaného technického zlyhania databázy o príslušných orgánoch/súdoch Komisia bezodkladne informuje Eurojust a členské štáty o nedostupnosti a o predpokladanom časovom rámci obnovenia, ak je známy.

6.11. V prípade prerušenia prevádzky služieb členské štáty a Eurojust musia zabezpečiť rýchle obnovenie služby a minimálnu stratu údajov v súlade s cieľovým časom obnovenia a cieľovým bodom obnovenia.

6.12. Členské štáty a Eurojust zavedú vhodné opatrenia na dosiahnutie uvedených cieľov dostupnosti a stanovia postupy účinnej reakcie na incidenty.

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

7.1. Decentralizovaný informačný systém musí podľa článku 22a nariadenia (EÚ) 2018/1727 umožňovať elektronickú komunikáciu medzi príslušnými vnútroštátnymi orgánmi a Eurojustom. Vzhľadom na povinnosti podľa článkov 21, 21a a 22 týkajúce sa výmeny informácií medzi príslušnými vnútroštátnymi orgánmi a Eurojustom, ale aj vzhľadom na úlohu Eurojustu pri uľahčovaní a podpore vydávania a vybavovania akýchkoľvek žiadostí o vzájomnú právnu pomoc alebo vzájomné uznávanie v súlade s článkom 8 ods. 1 nariadenia (EÚ) 2018/1727, musia byť zapojené príslušné orgány pri používaní decentralizovaného informačného systému jasne identifikovateľné. Preto je nevyhnutné na účely decentralizovaného informačného systému zriadiť oficiálnu databázu informácií týchto orgánoch.

7.2. Táto databáza CDB musí obsahovať v štruktúrovanom formáte tieto informácie:

a) na účely článku 8 ods. 1, článku 8 ods. 3, článku 8 ods. 4, článku 21, článku 21a a článku 22 nariadenia (EÚ) 2018/1727 informácie o príslušných vnútroštátnych orgánoch vrátane národných spravodajcov stanovených v článku 20 uvedeného nariadenia, ako aj o národných členoch v súlade s článkom 7 ([4]) uvedeného nariadenia;

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

c) informácie potrebné na správne technické smerovanie správ v rámci decentralizovaného informačného systému.

7.3. Komisia zodpovedá za vývoj, údržbu, prevádzku a podporu databázy CDB.

7.4. Databáza CDB umožní členským štátom a Eurojustu aktualizovať informácie v nej uchovávané a príslušným vnútroštátnym orgánom a národným členom zapojeným do decentralizovaného informačného systému programový prístup k informáciám a získavanie informácií, ktoré sa v nej nachádzajú.

7.5. Prístup do databázy CDB je možný prostredníctvom spoločného komunikačného protokolu bez ohľadu na to, či príslušné orgány pripojené k decentralizovanému informačnému systému prevádzkujú vnútroštátny backendový systém alebo či bol zavedený referenčný implementačný softvér.

7.6. Členské štáty zabezpečia, aby informácie o ich príslušných orgánoch v databáze CDB, ako sa stanovuje v bode 7.2, boli úplné, presné a aktualizované.

([4]) Týmto nie je dotknuté delegovanie právomocí z národného člena na jeho zástupcu, ostatných zamestnancov národného zastúpenia alebo oprávnených zamestnancov Eurojustu.

PRÍLOHA II

DIGITÁLNE PROCESNÉ ŠTANDARDY

V článku 3 ods. 9 nariadenia (EÚ) 2022/850 sa digitálne procesné normy vymedzujú ako technické špecifikácie pre modely prevádzkových procesov a dátové schémy, ktorými sa stanovuje elektronická štruktúra údajov, ktoré sa vymieňajú prostredníctvom systému e-CODEX.

V tejto prílohe sa stanovujú technické špecifikácie pre modely prevádzkových procesov a technické špecifikácie pre dátové schémy.

1. **Technické špecifikácie pre modely prevádzkových procesov podľa nariadenia (EÚ) 2018/1727**

Technické špecifikácie pre modely prevádzkových procesov sú stanovené v bodoch 1.1 až 1.5. Vymedzujú sa v nich kľúčové aspekty potrebné na to, aby bola prostredníctvom decentralizovaného informačného systému možná elektronická komunikácia na účely nariadenia (EÚ) 2018/1727.

Decentralizovaný informačný systém musí umožňovať výmenu informácií len medzi príslušnými vnútroštátnymi orgánmi členského štátu a národným členom z daného členského štátu.

1.1. *Výmena informácií týkajúcich sa európskeho justičného registra na boj proti terorizmu (CTR) – článok 21a nariadenia (EÚ) 2018/1727*

1.1.1. Model postúpenia údajov CTR:

Príslušný vnútroštátny orgán postupuje národnému členovi údaje o konaniach súvisiacich s terorizmom určené pre CTR.

1.1.2. Model prijatia údajov CTR:

Národný člen prijíma údaje CTR.

1.1.3. Model žiadosti o súhlas:

Národný člen požiada svoj príslušný vnútroštátny orgán o súhlas.

1.1.4. Model prijatia žiadosti o súhlas:

Príslušný vnútroštátny orgán prijíma žiadosť o súhlas.

1.1.5. Model zasielania odpovede na žiadosť o súhlas:

Príslušný vnútroštátny orgán zasiela odpoveď na žiadosť o súhlas.

1.1.6. Model prijatia odpovede na žiadosť o súhlas:

Národný člen prijíma odpoveď na žiadosť o súhlas.

1.1.7. Model informovania o prepojení:

Národný člen informuje príslušný vnútroštátny orgán o prepojení s inou vecou.

1.1.8. Model aktualizácie údajov CTR:

Príslušný vnútroštátny orgán postupuje svojmu príslušnému národnému členovi údaje, ktoré si vyžadujú aktualizáciu alebo vymazanie.

1.1.9. Model prijatia aktualizovaných údajov CTR:

Národný člen prijíma údaje CTR, ktoré si vyžadujú aktualizáciu alebo vymazanie.

1.2. *Výmena informácií týkajúcich sa závažnej trestnej činnosti – článok 21 nariadenia (EÚ) 2018/1727*

1.2.1. Model postúpenia údajov o závažnej cezhraničnej trestnej činnosti:

Príslušný vnútroštátny orgán postupuje údaje o závažnej cezhraničnej trestnej činnosti Eurojustu.

1.2.2. Model prijatia údajov o závažnej cezhraničnej trestnej činnosti:

Národný člen prijíma údaje o závažnej cezhraničnej trestnej činnosti.

1.2.3. Model žiadosti o súhlas:

Národný člen požiada svoj príslušný vnútroštátny orgán o súhlas.

1.2.4. Model prijatia žiadosti o súhlas:

Príslušný vnútroštátny orgán prijíma žiadosť o súhlas.

1.2.5. Model zasielania odpovede na žiadosť o súhlas:

Príslušný vnútroštátny orgán zasiela odpoveď na žiadosť o súhlas.

1.2.6. Model prijatia odpovede na žiadosť o súhlas:

Národný člen prijíma odpoveď na žiadosť o súhlas.

1.2.7. Model informovania o prepojení:

Národný člen informuje príslušný vnútroštátny orgán o prepojení s inou vecou.

1.2.8. Model aktualizácie údajov o závažnej cezhraničnej trestnej činnosti:

Príslušný vnútroštátny orgán postupuje svojmu príslušnému národnému členovi údaje, ktoré si vyžadujú aktualizáciu alebo vymazanie.

1.2.9. Model aktualizovaných údajov o závažnej cezhraničnej trestnej činnosti:

Národný člen prijíma údaje o závažnej cezhraničnej trestnej činnosti, ktoré si vyžadujú aktualizáciu alebo vymazanie.

1.3. *Výmena všeobecných informácií*

1.3.1. Model zasielania informácií:

Národný člen zasiela informácie príslušnému vnútroštátnemu orgánu alebo naopak.

1.3.2. Model prijatia informácií:

Príslušný vnútroštátny orgán alebo národný člen prijímajú informácie.

1.3.3. Model odpovede na informácie:

Príslušný vnútroštátny orgán odpovedá na informácie prijaté od národného člena alebo naopak.

1.3.4. Model prijatia odpovede:

Národný člen prijíma odpoveď od príslušného vnútroštátneho orgánu.

1.3.5. Model zasielania informácií:

Príslušný vnútroštátny orgán zasiela informácie národnému členovi.

1.3.6. Model prijatia informácií:

Národný člen prijíma informácie.

1.3.7. Model odpovede na informácie:

Národný člen odpovedá na informácie prijaté od príslušného vnútroštátneho orgánu.

1.3.8. Model prijatia odpovede:

Príslušný vnútroštátny orgán prijíma odpoveď od národného člena.

1.4. *Uľahčenie a podpora – článok 8 ods. 1 nariadenia (EÚ) 2018/1727*

Poznámka: Ak modely týkajúce sa uľahčenia a podpory uvedené v bode 1.5 zahŕňajú výmenu zákonom stanovených formulárov uvedených v právnych aktoch Únie v oblasti justičnej spolupráce v trestných veciach, v modeloch sa musia použiť príslušné znázornenia štruktúrovaných údajov a schémy XML, ak sú k dispozícii, vypracované na účely týchto aktov, napríklad tie, ktoré boli vytvorené na účely vykonávacieho nariadenia (EÚ) 2023/2844 alebo iných relevantných nástrojov.

1.5. *Model žiadosti o uľahčenie alebo podporu*

1.5.1. Model postúpenia žiadosti o uľahčenie alebo podporu:

Príslušný vnútroštátny orgán postupuje žiadosť o uľahčenie alebo žiadosť o podporu svojmu príslušnému národnému členovi.

1.5.2. Model prijatia žiadosti o uľahčenie alebo podporu:

Národný člen prijíma žiadosť o uľahčenie alebo podporu a postúpi ju národnému členovi dožiadaného členského štátu mimo systému JUDEX.

1.5.3. Model predkladania žiadosti o uľahčenie alebo podporu príslušnému vnútroštátnemu orgánu:

Národný člen dožiadaného členského štátu zasiela žiadosť svojmu príslušnému vnútroštátnemu orgánu.

1.5.4. Model prijatia žiadosti o uľahčenie alebo podporu:

Príslušný vnútroštátny orgán prijíma žiadosť o uľahčenie alebo podporu.

1.5.5. Model zasielania odpovede na žiadosť o uľahčenie alebo podporu:

Príslušný vnútroštátny orgán zasiela odpoveď na žiadosť alebo informácie týkajúce sa žiadosti národnému členovi dožiadaného členského štátu.

1.5.6. Model prijatia odpovede na žiadosť o uľahčenie alebo podporu:

Národný člen prijíma odpoveď na žiadosť o uľahčenie alebo podporu alebo informácie týkajúce sa takejto žiadosti od príslušného vnútroštátneho orgánu a poskytne ju národnému členovi žiadajúceho členského štátu mimo systému JUDEX.

1.5.7. Model odpovede na žiadosť o uľahčenie alebo podporu:

Národný člen žiadajúceho členského štátu odpovedá na informácie týkajúce sa žiadosti príslušného vnútroštátneho orgánu o uľahčenie alebo podporu alebo ich zdieľa.

1.5.8. Model prijatia odpovede:

Príslušný vnútroštátny orgán prijíma odpoveď alebo informácie v súvislosti so žiadosťou o uľahčenie alebo podporu.

2. **Technické špecifikácie pre dátové schémy**

Technické špecifikácie, ktoré majú slúžiť ako základ pre vypracovanie schém XML (XSD) na účely digitalizácie nariadenia (EÚ) 2018/1727, sú stanovené v bodoch 2.1 a 2.2 tejto prílohy. V týchto špecifikáciách sa vymedzujú kľúčové komponenty a akékoľvek ďalšie informácie s cieľom poskytnúť komplexný opis tvorby týchto schém.

Opis má byť všeobecne použiteľný, aby sa vytvorené XSD dali upravovať a rozširovať bez potreby tieto špecifikácie podstatne meniť.

Špecifikácie sa uplatňujú na zákonom stanovenú formu schém pripojenú k nariadeniu (EÚ) 2018/1727, všetky vopred vymedzené správy alebo akékoľvek správy s voľným textom používané pri výmenách podľa uvedeného nariadenia.

2.1. *Všeobecné úvahy*

Pre všetky schémy, ktoré sa majú poskytnúť, sa uplatňujú tieto ustanovenia:

2.1.1. Verzie

Musí sa zahrnúť atribút verzie, ktorý uľahčuje správu verzií schém a umožňuje aktualizáciu schémy v budúcich iteráciách podľa prevádzkových požiadaviek. Atribút verzie musí uvádzať, či pri zavádzaní nových prvkov alebo vylepšení je nová verzia spätne kompatibilná.

2.1.2. Vyhlásenie o schéme a metaúdaje

— V náležitých prípadoch sa v schéme využívajú príslušné normy alebo slovníky, ktoré sa vyžadujú systémom e-CODEX na zabezpečenie interoperability a ktoré sú potrebné na riadnu validáciu prvkov a typov definovaných v rámci tejto schémy. Môže to zahŕňať:

  — slovník základných pojmov elektronickej justície EÚ,

  — neoprávnené dátové typy

  — zoznam kódov jazykov Európskej únie.

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

2.1.3. Poznámky a dokumentácia

— **Poznámky**: Ku každému prvku v schéme sa zvyčajne priložia poznámky. V poznámkach sa uvádzajú ľudským okom čitateľné informácie o prvku a často jasne a stručne sa v nich vymedzuje jeho účel alebo použitie.

2.1.4. Používanie a prispôsobiteľnosť

Schéma sa riadi pravidlami stanovenými v písmenách a) až d):

a) **Modulárna štruktúra**: Každý oddiel musí byť navrhnutý so špecifickými funkciami a môže sa opätovne použiť alebo upraviť nezávisle. Vďaka tomu sa dá schéma ľahko prispôsobiť rôznym prípadom použitia.

b) **Rozšíriteľnosť**: Schéma musí byť navrhnutá tak, aby podporovala začlenenie nových prvkov alebo atribútov, ak budú v budúcnosti potrebné dodatočné informácie. To sa dosiahne použitím voliteľných prvkov a sekvencií, ktoré možno rozšíriť bez narušenia existujúcich implementácií.

c) **Prispôsobiteľná štruktúra**: Schéma musí byť navrhnutá tak, aby podľa potreby umožňovala doplnenie alebo úpravu prvkov či dátových typov. Štruktúra schémy musí zohľadňovať zmeny v požiadavkách bez potreby zásadnejších zásahov do jej podoby.

d) **Nepovinné prvky**: Prvky v rámci schémy možno označiť za nepovinné, to znamená, že ich možno zahrnúť alebo vynechať na základe osobitných okolností.

Schéma musí byť navrhnutá tak, aby podporovala zber štruktúrovaných údajov v prípade konkrétnych žiadostí.

2.1.5. Zmeny

Návrh schémy sa musí vyznačovať flexibilitou, modularitou a jednoduchým prispôsobením sa. Komplexné typy a voliteľné prvky sa začlenia do návrhu tak, aby sa v ňom mohli odvíjať rôzne scenáre a zároveň, pričom sa bude dať ľahko upravovať a rozširovať.

2.2. *Výmena štruktúrovaných údajov*

Štruktúrované údaje uvedené v bodoch 2.2.1 a 2.2.2 sa poskytujú v súlade s článkom 22a ods. 3 nariadenia (EÚ) 2018/1727. Schéma musí takisto umožňovať označovanie dátových súborov, ktoré sa majú v budúcich aktualizáciách vymazať.

2.2.1. Údaje z Európskeho justičného registra na boj proti terorizmu

Nasledujúcimi technickými špecifikáciami pre dátovú schému sa stanovuje štruktúrovaný rámec na vytvorenie schémy vo formáte XML.

a) Oddiel najvyššej úrovne

Tento oddiel najvyššej úrovne zodpovedá informáciám stanoveným v prílohe III k nariadeniu (EÚ) 2018/1727 a určeným pre Európsky justičný register na boj proti terorizmu (CTR).

b) Štruktúra správy

Štruktúra údajov CTR pozostáva zo sekvencie prvkov a zahŕňa minimálne:

i) informácie na identifikáciu fyzických osôb:

— priezvisko,

— meno (mená),

— všetky prezývky,

— dátum narodenia,

— miesto narodenia (obec a štát),

— štátna príslušnosť alebo štátne príslušnosti,

— identifikačný doklad (druh a číslo dokladu),

— pohlavie,

— miesto bydliska;

ii) informácie na identifikáciu právnických osôb:

— obchodné meno,

— právna forma,

— sídlo;

iii) informácie na identifikáciu fyzických aj právnických osôb:

— telefónne čísla,

— e-mailové adresy,

— podrobnosti týkajúce sa bankových účtov alebo účtov v iných finančných inštitúciách,

— postavenie v rámci konania;

iv) informácie o trestnom čine:

— informácie o právnických osobách zapojených do prípravy alebo spáchania trestného činu terorizmu,

— právna kvalifikácia trestného činu podľa vnútroštátneho práva,

— príslušná forma závažného trestného činu zo zoznamu uvedeného v prílohe I,

— prípadná príslušnosť k teroristickej skupine,

— druh terorizmu, napríklad džihádista, separatista, ľavicový alebo pravicový extrémista,

— stručné zhrnutie prípadu;

v) informácie o vnútroštátnom konaní:

— stav takéhoto konania,

— zodpovedná prokuratúra,

— číslo veci,

— dátum začatia formálneho súdneho konania,

— prepojenia s inými relevantnými prípadmi;

vi) pole s doplňujúcimi informáciami (voľný text);

vii) kód predchádzajúceho súhlasu.

2.2.2. Údaje postúpené v súlade s článkom 21 nariadenia (EÚ) 2018/1727

a) Článok 21 ods. 4 nariadenia (EÚ) 2018/1727, ktorým sa zriaďujú spoločné vyšetrovacie tímy

i) oddiel najvyššej úrovne
Tento oddiel najvyššej úrovne zodpovedá informáciám stanoveným v článku 21 ods. 4 nariadenia (EÚ) 2018/1727, informáciám o zriadení spoločných vyšetrovacích tímov;

ii) štruktúra správy
Štruktúra údajov pozostáva zo sekvencie prvkov a zahŕňa minimálne:

— vnútroštátny súdny orgán zodpovedný za trestné konanie,

— vnútroštátne referenčné číslo trestného konania,

— stav trestného konania,

— vyšetrované trestné činy,

— ostatné krajiny, ktorých sa prípad týka,

— prípad, pre ktorý už Eurojust poskytol podporu?

— ak áno, uveďte identifikátor prípadu Eurojustu,

— ak nie, ide o žiadosť o podporu?

— prípad, pre ktorý Europol poskytol podporu?

— ak áno, operačná pracovná skupina (OTF) a/alebo sieťová aplikácia na zabezpečenú výmenu informácií (SIENA)?

— dohoda o spoločnom vyšetrovacom tíme:

— dotknuté štáty,

— strany zapojené do spoločného vyšetrovacieho tímu (vnútroštátne orgány zodpovedné za vyšetrovanie),

— vnútroštátne referenčné číslo trestného konania,

— dátum podpisu,

— trvanie,

— vyšetrované trestné činy,

— stručné zhrnutie prípadu,

— hlavné podozrivé osoby v trestnom konaní, ktorým sa zaoberá spoločný vyšetrovací tím (meno, priezvisko, dátum a miesto narodenia a prípadne iné relevantné a potrebné kategórie údajov podľa prílohy II),

— výsledky práce spoločných vyšetrovacích tímov:

— ťažkosti/zdržania pri:

— zriadení spoločného vyšetrovacieho tímu,

— požiadaní o/zdieľanie dôkazov v rámci spoločného vyšetrovacieho tímu,

— dohode o spoločnej stratégii v oblasti trestného stíhania/jej vykonávanie,

— prípustnosť/neprípustnosť/hodnotenie dôkazov spoločného vyšetrovacieho tímu v rámci vnútroštátnych konaní,

— výsledok súdneho konania (úspešné/neúspešné trestné stíhania a odsúdenia/oslobodenia spod obžaloby);

iii) kód predchádzajúceho súhlasu.

b) Článok 21 ods. 5 nariadenia (EÚ) 2018/1727, závažné zložité prípady

i) oddiel najvyššej úrovne
Tento oddiel najvyššej úrovne zodpovedá informáciám stanoveným v článku 21 ods. 5 nariadenia o Eurojuste, t. j. závažných zložitých prípadoch;

ii) štruktúra správy
Štruktúra údajov pozostáva zo sekvencie prvkov a zahŕňa minimálne tieto údaje:

— vnútroštátny súdny orgán zodpovedný za trestné konanie,

— vnútroštátne referenčné číslo trestného konania,

— stav trestného konania,

— vyšetrované trestné činy,

— ostatné krajiny, ktorých sa prípad týka,

— prípad, pre ktorý už Eurojust poskytol podporu?

— ak áno, uveďte identifikátor prípadu Eurojustu,

— ak nie, ide o žiadosť o podporu?

— prípad, pre ktorý Europol poskytol podporu?

— ak áno, operačná osobitná skupina a/alebo aplikácia SIENA?

— príslušná forma závažného trestného činu,

— zapojenie organizovanej zločineckej skupiny

— mafiánsky typ,

— nadnárodná organizovaná zločinecká skupina,

— následky na úrovni EÚ,

— hlavné podozrivé osoby v trestnom konaní (meno, priezvisko, dátum a miesto narodenia a prípadne iné relevantné a potrebné kategórie údajov podľa prílohy II),

— stručné zhrnutie prípadu,

— ostatné zúčastnené krajiny,

— krajiny, s ktorými sa už spolupráca začala,

— príslušné orgány zapojené v inej krajine,

— použité nástroje justičnej spolupráce,

— počet zaslaných/doručených žiadostí,

— existencia súvisiacich vyšetrovaní,

— krajiny, s ktorými sa má začať spolupráca/krajiny, na ktoré to môže mať vplyv,

— druh potrebnej spolupráce (napr. vydanie, zhromažďovanie dôkazov, iná spolupráca)

— existencia súvisiacich vyšetrovaní;

iii) kód predchádzajúceho súhlasu.

c) Článok 21 ods. 6 písm. a) nariadenia (EÚ) 2018/1727, spory o právomoc

i) Oddiel najvyššej úrovne

Tento oddiel najvyššej úrovne zodpovedá informáciám stanoveným v článku 21 ods. 6 písm. a) nariadenia (EÚ) 2018/1727, t. j. sporoch o právomoc.

ii) Štruktúra správy

Štruktúra údajov pozostáva zo sekvencie prvkov a zahŕňa minimálne tieto údaje:

— vnútroštátny súdny orgán zodpovedný za trestné konanie,

— vnútroštátne referenčné číslo trestného konania,

— stav trestného konania (napr. vyšetrovanie, trestné stíhanie, súdne konanie),

— vyšetrované trestné činy,

— ostatné krajiny, ktorých sa prípad týka,

— prípad, pre ktorý už Eurojust poskytol podporu?

— ak áno, uveďte identifikátor prípadu Eurojustu,

— ak nie, ide o žiadosť o podporu?

— prípad, pre ktorý Europol poskytol podporu?

— ak áno, operačná osobitná skupina a/alebo aplikácia SIENA?

— ostatné zúčastnené krajiny,

— príslušné vnútroštátne orgány v inej krajine, ak sú známe,

— vnútroštátne referenčné číslo trestného konania v inej krajine,

— fáza konania v inej krajine, ak je známa,

— kladný alebo záporný spor,

— skutočný alebo potenciálny spor,

— už vykonané koordinačné činnosti (napr. konzultácie podľa rámcového rozhodnutia Rady 2009/948/SVV ([1])),

— stručné zhrnutie prípadu,

— hlavné podozrivé osoby (meno, priezvisko, dátum a miesto narodenia a prípadne iné relevantné a potrebné kategórie údajov podľa prílohy II),

iii) Kód predchádzajúceho súhlasu;

d) Článok 21 ods. 6 písm. b), kontrolované dodávky

i) oddiel najvyššej úrovne
Tento oddiel najvyššej úrovne zodpovedá informáciám stanoveným v článku 21 ods. 6 písm. b) nariadenia (EÚ) 2018/1727: kontrolované dodávky;

ii) štruktúra správy
štruktúra údajov pozostáva zo sekvencie prvkov a zahŕňa minimálne tieto údaje:

— vnútroštátny súdny orgán zodpovedný za trestné konanie,

— vnútroštátne referenčné číslo trestného konania,

— stav trestného konania (napr. vyšetrovanie, trestné stíhanie, súdne konanie),

— vyšetrované trestné činy,

— ostatné krajiny, ktorých sa prípad týka,

— prípad, pre ktorý už Eurojust poskytol podporu?

— ak áno, uveďte identifikátor prípadu Eurojustu,

— ak nie, ide o žiadosť o podporu?

— prípad, pre ktorý Europol poskytol podporu?

— ak áno, operačná osobitná skupina a/alebo aplikácia SIENA?

— ostatné zúčastnené krajiny,

— krajina pôvodu/tranzitu/krajina konečného určenia,

— príslušné vnútroštátne orgány v iných krajinách,

— existencia súvisiacich vyšetrovaní v iných krajinách,

([1]) Rámcové rozhodnutie Rady 2009/948/SVV z 30. novembra 2009 o predchádzaní kolíziám pri výkone právomoci v trestných veciach a ich urovnávaní (Ú. v. EÚ L 328, 15.12.2009, s. 42, ELI: http://data.europa.eu/eli/dec_framw/2009/948/oj).

— druh dodaného tovaru (napr. drogy a ich typ/peniaze/zbrane/cigarety/iné),

— stav kontrolovanej dodávky (napr. plánovaná, prebiehajúca, dokončená),

— výsledok kontrolovanej dodávky, ak už bola vykonaná,

— použitý nástroj justičnej spolupráce,

— hlavné podozrivé osoby (meno, priezvisko, dátum a miesto narodenia a prípadne iné relevantné a potrebné kategórie údajov podľa prílohy II);

iii) kód predchádzajúceho súhlasu.

e) Článok 21 ods. 6 písm. c) nariadenia (EÚ) 2018/1727, opakované problémy súvisiace s nástrojmi justičnej spolupráce

i) oddiel najvyššej úrovne

Tento oddiel najvyššej úrovne zodpovedá informáciám stanoveným v článku 21 ods. 6 písm. c) nariadenia (EÚ) 2018/1727: opakované problémy súvisiace s nástrojmi justičnej spolupráce;

ii) štruktúra správy

Štruktúra údajov pozostáva zo sekvencie prvkov a zahŕňa minimálne tieto údaje:

— vnútroštátny súdny orgán zodpovedný za trestné konanie,

— vnútroštátne referenčné číslo trestného konania,

— stav trestného konania (napr. vyšetrovanie, trestné stíhanie, súdne konanie),

— vyšetrované trestné činy,

— ostatné krajiny, ktorých sa prípad týka,

— prípad, pre ktorý už Eurojust poskytol podporu?

— ak áno, uveďte identifikátor prípadu Eurojustu,

— ak nie, ide o žiadosť o podporu?

— prípad, pre ktorý Europol poskytol podporu?

— ak áno, operačná osobitná skupina a/alebo aplikácia SIENA?

— ostatné zúčastnené krajiny,

— príslušné vnútroštátne orgány, ak sú známe,

— konanie vo funkcii vydávajúceho alebo vykonávajúceho orgánu,

— uplatnený nástroj justičnej spolupráce (napr. európsky zatykač, európsky vyšetrovací príkaz, zaistenie a konfiškácia),

— dotknutá konkrétna žiadosť (t. j. ktoré vyšetrovacie opatrenie, aký druh zaistenia, európsky zatykač na výkon trestu alebo na trestné stíhanie),

— odmietnutie alebo opakované ťažkosti,

— v prípade zamietnutia, na aký konkrétny dôvod sa odvoláva?

— stručný opis problému,

— prípadne iné vnútroštátne orgány, ktoré čelia rovnakému problému;

iii) kód predchádzajúceho súhlasu.

2.3. *Kódy predchádzajúceho súhlasu*

Pri zdieľaní údajov s Eurojustom prostredníctvom systému JUDEX príslušné vnútroštátne orgány musia prostredníctvom kódov predchádzajúceho súhlasu oznámiť ďalšie spracovanie údajov, prístup k nim a ich prenos po identifikácii prepojenia. Kódy predchádzajúceho súhlasu musia označovať, či a do akej miery si možno informácie súvisiace s prepojením vymieňať s inými príslušnými vnútroštátnymi orgánmi, inými agentúrami a orgánmi Únie, tretími krajinami alebo medzinárodnými organizáciami.

2.4. *Vopred vymedzené správy*

Vopred vymedzené správy predstavujú výmeny informácií stanovené v nariadení (EÚ) 2018/1727, pre ktoré však v právnom akte nebola stanovená žiadna konkrétna forma. Ich druhy a počet sa určujú počas prevádzkovej a technickej analýzy.

Schémy XLM (XSD) pre vopred vymedzené správy musia byť navrhnuté tak, aby sa zabezpečila konzistentnosť, štruktúra a súlad s prevádzkovými potrebami.

Na tieto schémy sa vzťahujú tieto požiadavky:

a) oddiel najvyššej úrovne v tejto schéme sa musí pomenovať podľa konkrétneho typu správy, ktorý sa vymedzuje;

b) v rámci tejto štruktúry sa doplnia potrebné polia požadované pre konkrétny typ správy a vymedzia sa, čím sa zabezpečí náležité znázornenie dátových prvkov.

2.5. *Správy s voľným textom*

Správy s voľným textom predstavujú výmeny informácií, ktoré umožňujú neštruktúrovaný alebo čiastočne štruktúrovaný obsah, vďaka čomu je možná flexibilita a zároveň sa dodržiavajú regulačné a prevádzkové požiadavky. XSD pre správy s voľným textom musí byť navrhnutá tak, aby sa zabezpečila konzistentnosť a správne formátovanie.

Na tieto schémy sa vzťahujú tieto požiadavky:

a) oddiel najvyššej úrovne v tejto schéme sa musí pomenovať podľa konkrétneho typu správy s voľným textom, ktorý sa vymedzuje;

b) schéma musí vymedzovať potrebnú štruktúru pre správu s voľným textom, pričom podľa potreby umožňuje vhodné zoradenie prvkov;

c) v rámci tejto štruktúry sa doplnia potrebné polia požadované pre konkrétny typ správy s voľným textom a vymedzia sa, čím sa zabezpečí náležité znázornenie dátových prvkov.

PRÍLOHA III

TECHNICKÉ ŠPECIFIKÁCIE TÝKAJÚCE SA ODTLAČKOV PRSTOV A FOTOGRAFIÍ

K správam vymieňaným v rámci decentralizovaného informačného systému možno priložiť prílohy aj vo formáte súborov Národného inštitútu pre normy a technológie (ďalej len „NIST“), ktoré obsahujú odtlačky prstov a fotografie, v súlade s technickými špecifikáciami stanovenými v bodoch 1 a 2.

1. **Odtlačky prstov**

Odtlačky prstov, ktoré možno zdielať s Eurojustom na účely spoľahlivej identifikácie osôb, voči ktorým sa vedie trestné konanie v súvislosti s trestnými činmi terorizmu, musia spĺňať tieto podmienky:

a) odtlačky prstov sa poskytujú v jednom súbore obsahujúcom digitálne snímky odtlačkov prstov (súbor s odtlačkami prstov vo formáte NIST) a predložia sa v súlade s normou ANSI/NIST-ITL 1-2011 Update 2015 (alebo novšou verziou);

b) súbor s odtlačkami prstov vo formáte NIST pozostáva najviac z desiatich jednotlivých odtlačkov prstov: odvaľovaných, plošných alebo oboch typov;

c) všetky odtlačky prstov sú označené;

d) odtlačky prstov sú zachytené v podobe živých skenov (live scans) alebo v podobe atramentových odtlačkov na papieri pod podmienkou, že atramentové odtlačky na papieri boli skenované v požadovanom rozlíšení a v rovnakej kvalite;

e) súbor s odtlačkami prstov vo formáte NIST umožňuje zahrnutie doplňujúcich informácií, ako sú podmienky registrácie odtlačkov prstov a metóda použitá na získanie individuálnych snímok odtlačkov prstov;

f) odtlačky prstov majú nominálne rozlíšenie buď 500 alebo 1 000 ppi ([1]) (s prijateľnou odchýlkou +/– 10 ppi) s 256 úrovňami šedej;

g) algoritmus použitý na komprimovanie odtlačkov prstov sa riadi odporúčaniami Národného inštitútu pre normy a technológie (NIST). Údaje o odtlačkoch prstov s rozlíšením 500 ppi sa komprimujú za použitia algoritmu WSQ (ISO/IEC 19794-5:2005). Údaje o odtlačkoch prstov s rozlíšením 1 000 ppi sa komprimujú podľa normy pre kompresiu obrázkov JPEG 2 000 (ISO/IEC 15444-1) a príslušného kódovacieho systému. Cieľový kompresný pomer je 15:1.

2. **Fotografie**

Fotografie, ktoré možno zdielať s Eurojustom na účely spoľahlivej identifikácie osôb, voči ktorým sa vedie trestné konanie v súvislosti s trestnými činmi terorizmu, musia spĺňať tieto podmienky:

a) v súbore s fotografiami je uvedené len jedno vyobrazenie tváre (súbor s fotografiami vo formáte NIST) a predkladá sa v súlade s normou ANSI/NIST-ITL 1 – 2011 aktualizovanou v roku 2015 alebo akoukoľvek novšou dostupnou verziou;

b) fotografie sú buď v odtieňoch šedej, farebné alebo blízko infračervené;

c) kvalita fotografií vychádza z požiadaviek na snímku podľa normy ISO/IEC 19794-5:2011 pre frontálny typ snímky alebo akejkoľvek novšej dostupnej verzie);

d) súbor s fotografiami vo formáte NIST umožňuje zahrnúť doplňujúce informácie vrátane dátumu nasnímania;

([1]) Pixely na palec.

e) fotografie v portrétovom režime majú minimálne rozlíšenie 600 pixelov na 800 pixelov a maximálne rozlíšenie 1 200 pixelov na 1 600 pixelov;

f) tvár zaberá na fotografii taký priestor, ktorý zabezpečuje, že medzi stredmi očí je najmenej 120 pixelov;

g) algoritmus použitý na komprimovanie fotografií sa riadi odporúčaniami Národného inštitútu pre normy a technológie (NIST). Fotografie sa skomprimujú len raz podľa normy pre kompresiu obrázkov JPG (ISO/IEC 10918) alebo JPEG 2000 (ISO/IEC 15444) a príslušného kódovacieho systému, pri maximálnom povolenom kompresnom pomere obrázka 20:1.