2025/2447

5.12.2025

PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2025/2447

ze dne 4. prosince 2025,

kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) 2018/1727, pokud jde o technické specifikace, opatření a další požadavky pro zavedení a používání decentralizovaného informačního systému pro zabezpečené zpracovávání a předávání informací

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na 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 ([1]), a zejména na čl. 22a odst. 3 a čl. 22b odst. 1 písm. a), b), c) a d) uvedeného nařízení,

vzhledem k těmto důvodům:

(1) Nařízení (EU) 2018/1727 stanoví rámec pro novou vnitřní digitální infrastrukturu Eurojustu a zřízení decentralizovaného systému zabezpečené digitální komunikace mezi příslušnými vnitrostátními orgány členských států a Eurojustem.

(2) Tato zabezpečená digitální komunikace má probíhat prostřednictvím decentralizovaného informačního systému. Pro zřízení decentralizovaného informačního systému je nezbytné stanovit technické specifikace, které vymezují způsoby komunikace a komunikační protokoly, technická opatření, která zajišťují minimální standardy bezpečnosti informací a bezpečnost, a minimální cíle dostupnosti pro zavedení tohoto systému.

(3) V souladu s čl. 22a odst. 1 nařízení (EU) 2018/1727 se má decentralizovaný informační systém skládat z informačních systémů členských států a Eurojustu a interoperabilních přístupových bodů systému e-CODEX, jejichž prostřednictvím jsou tyto systémy vzájemně propojeny. Technické specifikace a další požadavky decentralizovaného informačního systému stanovené v tomto nařízení by měly tento rámec zohlednit.

(4) Přístupové body decentralizovaného informačního systému by měly být založeny na oprávněných přístupových bodech systému e-CODEX, které jsou definovány v čl. 3 bodě 3 nařízení Evropského parlamentu a Rady (EU) 2022/850 ([2]).

(5) Decentralizovaný informační systém je zaveden v rámci většího decentralizovaného informačního systému založeného na systému e-CODEX, označovaného jako digitální systém pro výměnu informací v oblasti justice (JUDEX). Je proto nezbytné zajistit účinnou výměnu informací o horizontálním vývoji.

(6) V souladu s čl. 22a odst. 4 nařízení (EU) 2018/1727 se členské státy a Eurojust mohou rozhodnout používat referenční prováděcí software vyvinutý Komisí jako svůj koncový systém namísto vnitrostátního informačního systému. V zájmu zajištění interoperability by se na vnitrostátní informační systémy i referenční prováděcí software měly vztahovat stejné technické specifikace a požadavky.

(7) Údaje týkající se teroristických trestných činů a závažné organizované trestné činnosti by měly být předávány strukturovaným způsobem, aby se zlepšila kvalita a relevantnost těchto informací a zajistilo se efektivnější začlenění informací do systému řízení případů Eurojustu a jejich lepší porovnávání s informacemi již uloženými v tomto systému. Pro údaje o otiscích prstů a fotografie, které mohou být předány Eurojustu za účelem identifikace osob, proti nimž je vedeno trestní řízení v souvislosti s teroristickými trestnými činy, by měl být stanoven formát a technické normy pro předávání.

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

(8) Eurojust usnadňuje a podporuje vydávání a výkon žádostí o justiční spolupráci, včetně žádostí a rozhodnutí, které se zakládají na nástrojích provádějících zásadu vzájemného uznávání. Příslušné vnitrostátní orgány by měly mít možnost požádat Eurojust o pomoc a koordinaci prostřednictvím decentralizovaného informačního systému.

(9) V zájmu zajištění účinnosti a soudržnosti je důležité, aby technické specifikace, které mají být stanoveny podle nařízení (EU) 2018/1727, byly slučitelné s technickými specifikacemi stanovenými podle nařízení Evropského parlamentu a Rady (EU) 2023/2844 ([3]), (EU) 2023/1543 ([4]) a (EU) 2024/3011 ([5]), jakož i s budoucími opatřeními v oblasti digitalizace, která jsou relevantní pro pravomoci Eurojustu týkající se podpory příslušných vnitrostátních orgánů.

(10) Prostřednictvím decentralizovaného informačního systému by měla být rovněž umožněna jakákoli jiná komunikace mezi Eurojustem a příslušnými vnitrostátními orgány, jako je předávání informací o výsledcích zpracování informací, včetně existence vazeb na případy již uložené v systému správy případů v souladu s článkem 22 nařízení (EU) 2018/1727, jedná-li Eurojust z vlastního podnětu, nebo informací předaných Eurojustu za účelem uchovávání, analýzy a ukládání důkazů týkajících se genocidy, zločinů proti lidskosti, válečných zločinů a souvisejících trestných činů v souladu s čl. 4 odst. 1 písm. j) uvedeného nařízení.

(11) Aby se zajistilo, že toto nařízení zohledňuje operativní potřeby Eurojustu, byl Eurojust konzultován v souladu s čl. 22a odst. 3 nařízení (EU) 2018/1727.

(12) V souladu s článkem 4 Protokolu č. 21 o postavení Spojeného království a Irska s ohledem na prostor svobody, bezpečnosti a práva, připojeného ke Smlouvě o Evropské unii a ke Smlouvě o fungování Evropské unie, oznámilo Irsko dopisem ze dne 9. září 2019 své přání přijmout nařízení (EU) 2018/1727 a být jím vázáno. Rozhodnutí Komise (EU) 2019/2006 ([6]) tuto účast potvrdilo. Nařízením (EU) 2023/2131 bylo nařízení (EU) 2018/1727 změněno s cílem umožnit zřízení kanálů zabezpečené digitální komunikace mezi Eurojustem a příslušnými vnitrostátními orgány a poskytnout právní základ pro toto nařízení. V situaci, kdy Irsko neoznámilo své přání účastnit se přijímání a používání nařízení Evropského parlamentu a Rady (EU) 2023/2131 ([7]) a neoznámilo své přání přijmout uvedené nařízení a být jím vázáno, v souladu s články 1 a 2 a čl. 4a odst. 1 Protokolu č. 21 není nařízení (EU) 2023/2131 pro Irsko závazné ani použitelné. Irsko se tudíž neúčastní přijímání tohoto nařízení.

(13) V souladu s články 1 a 2 Protokolu č. 22 o postavení Dánska, připojeného ke Smlouvě o Evropské unii a ke Smlouvě o fungování Evropské unie, se Dánsko neúčastnilo přijímání nařízení (EU) 2018/1727. Toto nařízení proto není pro Dánsko závazné ani použitelné.

([3]) Nařízení Evropského parlamentu a Rady (EU) 2023/2844 ze dne 13. prosince 2023 o digitalizaci justiční spolupráce a přístupu ke spravedlnosti v přeshraničních občanských, obchodních a trestních věcech a o změně některých aktů v oblasti justiční spolupráce (Úř. věst. L, 2023/2844, 27.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2844/oj).

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

([5]) Nařízení Evropského parlamentu a Rady (EU) 2024/3011 ze dne 27. listopadu 2024 o předávání trestního řízení (Úř. věst. L, 2024/3011, 18.12.2024, ELI: http://data.europa.eu/eli/reg/2024/3011/oj).

([6]) Rozhodnutí Komise (EU) 2019/2006 ze dne 29. listopadu 2019 o účasti Irska na provádění nařízení Evropského parlamentu a Rady (EU) 2018/1727 o Agentuře Evropské unie pro justiční spolupráci v trestních věcech (Eurojust) (Úř. věst. L 310, 2.12.2019, s. 59, ELI: http://data.europa.eu/eli/dec/2019/2006/oj).

([7]) Nařízení Evropského parlamentu a Rady (EU) 2023/2131 ze dne 4. října 2023, kterým se mění nařízení Evropského parlamentu a Rady (EU) 2018/1727 a rozhodnutí Rady 2005/671/SVV, pokud jde o elektronickou výměnu informací v případech terorismu (Úř. věst. L, 2023/2131, 11.10.2023, ELI: http://data.europa.eu/eli/reg/2023/2131/oj).

(14) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ([8]) byl konzultován evropský inspektor ochrany údajů, který vydal stanovisko dne 21. října 2025.

(15) Opatření stanovená tímto nařízením jsou v souladu se stanoviskem výboru zřízeného podle článku 22c nařízení (EU) 2018/1727,

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Technické specifikace decentralizovaného informačního systému

Technické specifikace, opatření a cíle decentralizovaného informačního systému uvedené v čl. 22b odst. 1 písm. a), b), c) a d) nařízení (EU) 2018/1727 jsou stanoveny v příloze I tohoto nařízení.

Článek 2

Digitální procesní normy

Digitální procesní normy platné pro elektronickou komunikaci prostřednictvím decentralizovaného informačního systému uvedené v čl. 22a odst. 3 nařízení (EU) 2018/1727 jsou stanoveny v příloze II tohoto nařízení.

Článek 3

Technické specifikace pro předávání fotografií a otisků prstů

Technické specifikace a formát pro předávání fotografií a otisků prstů uvedené v čl. 22a odst. 3 nařízení (EU) 2018/1727 jsou stanoveny v příloze III tohoto nařízení.

Článek 4

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 4. prosince 2025.

Za Komisi
předsedkyně
Ursula VON DER LEYEN

([8]) 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 I

TECHNICKÉ SPECIFIKACE, OPATŘENÍ A CÍLE DECENTRALIZOVANÉHO INFORMAČNÍHO SYSTÉMU

1. **Úvod a rozsah působnosti**

Tato příloha stanoví technické specifikace, opatření a cíle decentralizovaného informačního systému pro účely výměny informací podle nařízení (EU) 2018/1727.

Decentralizovaná povaha informačního systému umožňuje přímou a bezpečnou výměnu informací mezi příslušnými vnitrostátními orgány a Eurojustem.

2. **Definice**

Pro účely této přílohy se použijí tyto 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 „REST“ (Representational State Transfer) 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 a dokumentů prostřednictvím decentralizovaného informačního systému;

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

2.9. „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;

2.10. 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. Podporuje mezipodnikovou integraci napříč různými systémy;

2.11. 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;

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

2.13. „cílovým okamžikem obnovy funkce“ se rozumí maximální přijatelná míra ztráty údajů v případě selhání.

3. **Způsoby komunikace elektronickými prostředky**

3.1. Decentralizovaný informační systém využívá pro účely výměny zpráv a dokumentů metody komunikace založené na službách, jako jsou webové služby nebo jiné opakovaně použitelné komponenty a softwarová řešení.

3.2. Decentralizovaný informační systém bude konkrétně 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.

4. **Komunikační protokoly**

4.1. Decentralizovaný informační systém používá zabezpečené internetové protokoly pro:

a) komunikaci v rámci decentralizovaného informačního systému mezi příslušnými orgány a Eurojustem;

b) komunikaci s databází příslušných orgánů / soudů podle bodu 7.1.

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.

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 případně využívají příslušné normy nebo slovníky, které jsou nezbytné pro řádné ověření prvků a typů definovaných v rámci tohoto schématu. Tyto normy nebo slovníky mohou zahrnovat:

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

b) nekvalifikované datové typy;

c) seznam kódů jazyků Evropské unie.

4.6. 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 (PKI) 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 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 protokolování bezpečnostních událostí v souladu s uznávanými mezinárodními doporučeními pro bezpečnostní standardy informačních technologií ([1]);

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

5.2. Komponenty decentralizovaného informačního systému musí zajišťovat 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. Pokud se v rámci decentralizovaného informačního systému používá TLS, použije se nejnovější stabilní verze protokolu, nebo případně verze bez známých bezpečnostních zranitelností. Povoleny jsou pouze délky klíčů, které zajišťují odpovídající úroveň kryptografické bezpečnosti, a nesmí se používat sady šifer, o nichž je známo, že jsou nezabezpečené nebo zastaralé.

5.4. Digitální certifikáty PKI používané pro účely provozu decentralizovaného informačního systému vydávají pokud možno certifikační autority uznané jako kvalifikovaní poskytovatelé služeb vytvářejících důvěru v souladu s nařízením Evropského parlamentu a Rady (EU) č. 910/2014 ([2]). Musí být zavedena opatření, která zajistí, aby se tyto certifikáty používaly výhradně k účelům, pro něž byly zamýšleny, na požadované úrovni důvěry a v souladu s příslušnými požadavky nařízení (EU) č. 910/2014.

5.5. 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.

5.6. 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 v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679 ([3]) nebo se směrnicí (EU) 2016/680 (dle příslušného případu).

([1]) Aniž je dotčeno protokolování pro bezpečnostní účely, musí mechanismy protokolování používané komponentami decentralizovaného informačního systému vhodným způsobem umožňovat zajištění souladu s požadavky stanovenými v článku 88 nařízení (EU) 2018/1725 a v příslušných případech v článku 25 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, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

([2]) Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (Úř. věst. L 257, 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

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

5.7. Členské státy, které používají jiný vnitrostátní koncový systém než referenční prováděcí software, zavedou nezbytná opatření, aby zajistily soulad svého vnitrostátního koncového systému s požadavky nařízení (EU) 2016/679 a směrnice (EU) 2016/680 (dle příslušného případu).

5.8. Eurojust provede nezbytná opatření, aby zajistil, že jeho koncový systém nebo instance referenčního prováděcího softwaru, který používá, splňuje požadavky nařízení (EU) 2018/1725 a (EU) 2018/1727.

5.9. Členské státy a Eurojust 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. **Minimální cíle dostupnosti**

6.1. Eurojust a členské státy zajistí nepřetržitou dostupnost komponent decentralizovaného informačního systému, za které odpovídají, přičemž cílová technická dostupnost musí bez plánované údržby činit nejméně 98 % ročně.

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

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

6.4. Členské státy informují Komisi, Eurojust 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.

6.5. Pokud mají členské státy stanoveny termíny pravidelné údržby, informují Komisi, Eurojust a ostatní členské státy o čase a dni (dnech), na kdy jsou tyto termíny pravidelné údržby plánovány. Odchylně od povinností stanovených v první větě se členské státy mohou rozhodnout, že v případě nedostupnosti komponent decentralizovaného informačního systému, za které odpovídají, během těchto termínů pravidelné údržby nebudou Komisi pokaždé informovat.

6.6. Členské státy v případě neočekávaného technického selhání některé komponenty decentralizovaného informačního systému, za kterou odpovídají, informují neprodleně Komisi a ostatní členské státy o tomto selhání, a pokud je znám, i o předpokládaném časovém rámci obnovy.

6.7. Eurojust informuje Komisi a 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.

6.8. Pokud má Eurojust stanoven termíny pravidelné údržby, informuje Komisi a členské státy o čase a dni (dnech), na kdy jsou tyto termíny pravidelné údržby plánovány. Odchylně od povinností stanovených v první větě se Eurojust může rozhodnout, že v případě nedostupnosti komponent decentralizovaného informačního systému, za které odpovídá, během těchto termínů pravidelné údržby nebude Komisi pokaždé informovat.

6.9. Eurojust v případě neočekávaného technického selhání některé komponenty decentralizovaného informačního systému, za kterou odpovídá, informuje neprodleně Komisi a členské státy o tomto selhání, a pokud je znám, i o předpokládaném časovém rámci obnovy.

6.10. V případě neočekávaného technického selhání databáze příslušných orgánů / soudů informuje Komise neprodleně Eurojust a členské státy o tomto selhání, a pokud je znám, i o předpokládaném časovém rámci obnovy.

6.11. V případě přerušení poskytování služeb zajistí členské státy a Eurojust rychlou obnovu služby a minimální ztrátu údajů v souladu s cílovou dobou obnovy funkce a cílovým okamžikem obnovy funkce.

6.12. Členské státy a Eurojust zavedou vhodná opatření k dosažení výše uvedených cílů dostupnosti a stanoví postupy pro účinnou reakci na incidenty.

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

7.1. Podle článku 22a nařízení (EU) 2018/1727 umožňuje decentralizovaný informační systém elektronickou komunikaci mezi příslušnými vnitrostátními orgány a Eurojustem. Vzhledem k povinnostem týkajícím se výměny informací mezi příslušnými vnitrostátními orgány a Eurojustem podle článků 21, 21a a 22, ale také vzhledem k úloze Eurojustu při usnadňování a podpoře podávání a výkonu žádostí o vzájemnou právní pomoc nebo vzájemné uznávání v souladu s čl. 8 odst. 1 nařízení (EU) 2018/1727 je třeba, aby byly zapojené příslušné orgány při používání decentralizovaného informačního systému jasně identifikovatelné. Proto je pro účely decentralizovaného informačního systému nezbytné vytvořit závaznou databázi informací o těchto orgánech.

7.2. Databáze CDB obsahuje následující informace ve strukturovaném formátu:

a) pro účely čl. 8 odst. 1, 3 a 4, článku 21, článku 21a a článku 22 nařízení (EU) 2018/1727 informace o příslušných vnitrostátních orgánech, včetně národních zpravodajů podle článku 20 uvedeného nařízení, jakož i o národních členech v souladu s článkem 7 ([4]) uvedeného nařízení;

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

c) informace, které jsou nezbytné pro řádné technické směrování zpráv v rámci decentralizovaného informačního systému.

7.3. Komise odpovídá za vývoj, údržbu, provoz a podporu databází CDB.

7.4. Databáze CDB umožní členským státům a Eurojustu aktualizovat informace, které jsou v ní obsaženy, a příslušným vnitrostátním orgánům a národním členům účastnícím se decentralizovaného informačního systému umožní programový přístup k těmto informacím a jejich vyhledávání.

7.5. Přístup do databáze CDB musí být možný prostřednictvím společného komunikačního protokolu bez ohledu na to, zda příslušné orgány připojené k decentralizovanému informačnímu systému provozují vnitrostátní koncový systém nebo nasazení referenčního prováděcího softwaru.

7.6. Členské státy zajistí, aby informace o jejich příslušných orgánech v databázi CDB uvedené v bodě 7.2 byly úplné, přesné a aktualizované.

([4]) Tím není dotčeno přenesení pravomocí národního člena na jeho zástupce, ostatní zaměstnance národního zastoupení nebo oprávněné zaměstnance Eurojustu.

PŘÍLOHA II

DIGITÁLNÍ PROCESNÍ NORMY

Ustanovení čl. 3 bodu 9 nařízení (EU) 2022/850 definuje digitální procesní normy jako technické specifikace modelů provozních procesů a datových schémat, stanovující elektronickou strukturu údajů vyměňovaných prostřednictvím systému e-CODEX.

Tato příloha stanoví technické specifikace modelů provozních procesů a technické specifikace datových schémat.

1. **Technické specifikace modelů provozních procesů podle nařízení (EU) 2018/1727**

Technické specifikace modelů provozních procesů jsou uvedeny v bodech 1.1 až 1.5. Definují klíčové aspekty nezbytné pro umožnění elektronické komunikace pro účely nařízení (EU) 2018/1727 prostřednictvím decentralizovaného informačního systému.

Decentralizovaný informační systém umožňuje výměnu informací pouze mezi příslušnými vnitrostátními orgány členského státu a národním členem z tohoto členského státu.

1.1. *Výměna informací souvisejících s evropským justičním rejstříkem pro boj proti terorismu (CTR), článek 21a nařízení (EU) 2018/1727*

1.1.1. Model předání údajů CTR:

Příslušný vnitrostátní orgán předá národnímu členovi údaje o řízeních týkajících se teroristických trestných činů pro účely CTR.

1.1.2. Model příjmu údajů CTR:

Národní člen obdrží údaje pro účely CTR.

1.1.3. Model žádosti o souhlas:

Národní člen žádá o souhlas svého příslušného vnitrostátního orgánu.

1.1.4. Model příjmu žádosti o souhlas:

Příslušný vnitrostátní orgán obdrží žádost o souhlas.

1.1.5. Model zaslání odpovědi na žádost o souhlas:

Příslušný vnitrostátní orgán zašle odpověď na žádost o souhlas.

1.1.6. Model příjmu odpovědi na žádost o souhlas:

Národní člen obdrží odpověď na žádost o souhlas.

1.1.7. Model informování o vazbě:

Národní člen informuje příslušný vnitrostátní orgán o vazbě na jiný případ.

1.1.8. Model aktualizace údajů CTR:

Příslušný vnitrostátní orgán předá údaje, které vyžadují aktualizaci nebo výmaz, svému příslušnému národnímu členovi.

1.1.9. Model příjmu aktualizovaných údajů CTR:

Národní člen obdrží údaje CTR, které vyžadují aktualizaci nebo výmaz.

1.2. *Výměna informací týkajících se závažné trestné činnosti, článek 21 nařízení (EU) 2018/1727*

1.2.1. Model předání údajů o závažné přeshraniční trestné činnosti:

Příslušný vnitrostátní orgán předá údaje o závažné přeshraniční trestné činnosti Eurojustu.

1.2.2. Model příjmu údajů o závažné přeshraniční trestné činnosti:

Národní člen obdrží údaje o závažné přeshraniční trestné činnosti.

1.2.3. Model žádosti o souhlas:

Národní člen žádá o souhlas svého příslušného vnitrostátního orgánu.

1.2.4. Model příjmu žádosti o souhlas:

Příslušný vnitrostátní orgán obdrží žádost o souhlas.

1.2.5. Model zaslání odpovědi na žádost o souhlas:

Příslušný vnitrostátní orgán zašle odpověď na žádost o souhlas.

1.2.6. Model příjmu odpovědi na žádost o souhlas:

Národní člen obdrží odpověď na žádost o souhlas.

1.2.7. Model informování o vazbě:

Národní člen informuje příslušný vnitrostátní orgán o vazbě na jiný případ.

1.2.8. Model aktualizace údajů o závažné přeshraniční trestné činnosti:

Příslušný vnitrostátní orgán předá údaje, které vyžadují aktualizaci nebo výmaz, svému příslušnému národnímu členovi.

1.2.9. Model příjmu aktualizovaných údajů o závažné přeshraniční trestné činnosti:

Národní člen obdrží údaje o závažné přeshraniční trestné činnosti, které vyžadují aktualizaci nebo výmaz.

1.3. *Výměna všeobecných informací*

1.3.1. Model zaslání informací:

Národní člen zašle informace příslušnému vnitrostátnímu orgánu, nebo naopak.

1.3.2. Model příjmu informací:

Příslušný vnitrostátní orgán nebo národní člen obdrží informace.

1.3.3. Model odpovědi na informace:

Příslušný vnitrostátní orgán odpoví na informace obdržené od národního člena, nebo naopak.

1.3.4. Model příjmu odpovědi:

Národní člen obdrží odpověď od příslušného vnitrostátního orgánu.

1.3.5. Model zaslání informací:

Příslušný vnitrostátní orgán zašle informace národnímu členovi.

1.3.6. Model příjmu informací:

Národní člen obdrží informace.

1.3.7. Model odpovědi na informace:

Národní člen odpoví na informace obdržené od příslušného vnitrostátního orgánu.

1.3.8. Model příjmu odpovědi:

Příslušný vnitrostátní orgán obdrží odpověď od národního člena.

1.4. *Usnadňující a podpůrná úloha, čl. 8 odst. 1 nařízení (EU) 2018/1727*

Pozn.: Pokud modely pro usnadnění a podporu uvedené v bodě 1.5 zahrnují výměnu povinných formulářů určených právními akty Unie v oblasti justiční spolupráce v trestních věcech, používají tyto modely, pokud jsou k dispozici, příslušné strukturované datové reprezentace a XML schémata vytvořená pro tyto akty, například pro účely provádění nařízení (EU) 2023/2844 nebo jiných příslušných nástrojů.

1.5. *Model žádosti o usnadnění nebo podporu:*

1.5.1. Model předání žádosti o usnadnění nebo podporu:

Příslušný vnitrostátní orgán předá žádost o usnadnění nebo podporu svému příslušnému národnímu členovi.

1.5.2. Model příjmu žádosti o usnadnění nebo podporu:

Národní člen obdrží žádost o usnadnění nebo podporu a předá ji národnímu členovi dožádaného členského státu mimo systém JUDEX.

1.5.3. Model přeposlání žádosti o usnadnění nebo podporu příslušnému vnitrostátnímu orgánu:

Národní člen dožádaného členského státu zašle žádost svému příslušnému vnitrostátnímu orgánu.

1.5.4. Model příjmu žádosti o usnadnění nebo podporu:

Příslušný vnitrostátní orgán obdrží žádost o usnadnění nebo podporu.

1.5.5. Model zaslání odpovědi na žádost o usnadnění nebo podporu:

Příslušný vnitrostátní orgán zašle odpověď nebo informace týkající se žádosti národnímu členovi dožádaného členského státu.

1.5.6. Model příjmu odpovědi na žádost o usnadnění nebo podporu:

Národní člen obdrží odpověď nebo informace týkající se žádosti o usnadnění nebo podporu od příslušného vnitrostátního orgánu a předá ji národnímu členovi žádajícího členského státu mimo systém JUDEX.

1.5.7. Model odpovědi na žádost o usnadnění nebo podporu:

Národní člen žádajícího členského státu odpoví na žádost o usnadnění nebo podporu od příslušného vnitrostátního orgánu nebo mu předá informace týkající se této žádosti.

1.5.8. Model příjmu odpovědi:

Příslušný vnitrostátní orgán obdrží odpověď nebo informace týkající se žádosti o usnadnění nebo podporu.

2. **Technické specifikace datových schémat**

Technické specifikace, které mají sloužit jako základ pro vývoj definic schématu XML (XSD) pro účely digitalizace nařízení (EU) 2018/1727, jsou uvedeny v bodech 2.1 a 2.2 této přílohy. Tyto specifikace definují klíčové komponenty a veškeré další informace a poskytují tak komplexní popis pro tvorbu těchto schémat.

Popis má být obecný, aby bylo možné vytvořená schémata XSD upravovat a rozšiřovat, aniž by bylo nutné tyto specifikace výrazně měnit.

Specifikace se vztahují na povinnou podobu schémat podle příloh nařízení (EU) 2018/1727, na všechny předdefinované zprávy a na všechny zprávy s volným textem používané při výměně informací podle uvedeného nařízení.

2.1. *Obecné poznámky*

Pro všechna schémata, která mají být poskytnuta, platí následující ustanovení:

2.1.1. Správa verzí

Uvede se atribut verze, který usnadňuje správu verzí schématu a umožňuje jeho aktualizaci v budoucích iteracích v souladu s provozními požadavky. Atribut verze udává, zda je nová verze při zavádění nových funkcí nebo vylepšení zpětně kompatibilní.

2.1.2. Deklarace schématu a metadata

— Schémata případně využívají příslušné normy nebo slovníky požadované systémem e-CODEX za účelem zajištění interoperability, které jsou nezbytné pro řádné ověření prvků a typů definovaných v rámci tohoto schématu. To může zahrnovat:

  — slovník základních pojmů v oblasti e-justice EU,

  — nekvalifikované datové typy,

  — seznam kódů jazyků Evropské unie.

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

2.1.3. Anotace a dokumentace

— **Anotace**: Každý prvek ve schématu je obvykle doplněn anotacemi. Anotace poskytují člověkem čitelnou informaci o daném prvku, často jasně a stručně vymezují jeho účel nebo způsob použití.

2.1.4. Použití a přizpůsobitelnost

Schéma se řídí pravidly uvedenými v písmenech a) až d):

a) **Modulární struktura**: Každá sekce musí být navržena s konkrétní funkcionalitou a může být znovu použita nebo upravena samostatně. Tím se zajistí snadná přizpůsobitelnost schématu pro různé případy užití.

b) **Rozšiřitelnost:** Schéma musí být navrženo tak, aby umožňovalo začlenění nových prvků nebo atributů, pokud bude v budoucnu potřeba doplnit další informace. Toho se dosáhne použitím volitelných prvků a sekvencí, které lze rozšířit bez narušení stávajících implementací.

c) **Přizpůsobitelná struktura**: Schéma musí být navrženo tak, aby umožňovalo přidávání nebo úpravu prvků či datových typů podle potřeby. Struktura schématu musí být schopna reagovat na změny požadavků bez nutnosti zásadních změn návrhu.

d) **Nepovinné prvky:** Prvky ve schématu mohou být označeny jako nepovinné, což znamená, že mohou být zahrnuty nebo vynechány v závislosti na konkrétních okolnostech.

Schéma musí být navrženo tak, aby podporovalo sběr strukturovaných údajů pro konkrétní požadavky.

2.1.5. Úpravy

Návrh schématu se musí vyznačovat flexibilitou, modularitou a snadnou přizpůsobitelností. Složité typy a volitelné prvky musí být do návrhu začleněny takovým způsobem, aby schéma zvládlo různorodé scénáře a zároveň zůstalo snadno upravitelné a rozšiřitelné.

2.2. *Výměna strukturovaných údajů*

Strukturované údaje uvedené v bodech 2.2.1 a 2.2.2 se poskytují v souladu s čl. 22a odst. 3 nařízení (EU) 2018/1727. Schéma rovněž umožňuje označit soubory údajů, které mají být při budoucích aktualizacích vymazány.

2.2.1. Údaje z evropského justičního rejstříku pro boj proti terorismu

Následující technické specifikace datového schématu stanoví strukturovaný rámec pro vytvoření schématu ve formátu XML.

a) Sekce nejvyšší úrovně

Tato sekce nejvyšší úrovně odpovídá informacím pro evropský justiční rejstřík pro boj proti terorismu (CTR) uvedeným v příloze III nařízení (EU) 2018/1727.

b) Struktura zprávy

Struktura údajů CTR se skládá z posloupnosti prvků a zahrnuje alespoň následující:

i) informace k určení totožnosti fyzických osob:

— příjmení,

— jména (rodná jména),

— případné přezdívky,

— datum narození,

— místo narození (obec a země),

— státní příslušnost nebo příslušnosti,

— doklad totožnosti (druh a číslo dokladu),

— pohlaví,

— bydliště;

ii) informace k určení totožnosti právnických osob:

— obchodní firma,

— právní forma,

— sídlo;

iii) informace k určení totožnosti fyzických i právnických osob:

— telefonní čísla,

— e-mailové adresy,

— údaje o účtech u bank nebo jiných finančních institucí,

— postavení v řízení;

iv) informace o trestném činu:

— informace o právnických osobách podílejících se na přípravě nebo spáchání teroristického trestného činu,

— právní kvalifikace trestného činu podle vnitrostátního práva,

— příslušná forma závažné trestné činnosti ze seznamu uvedeného v příloze I,

— příslušnost k teroristické skupině,

— druh terorismu, například džihádistický, separatistický, levicový nebo pravicový,

— stručné shrnutí případu;

v) informace o vnitrostátním řízení:

— stav řízení,

— odpovědné státní zastupitelství,

— spisová značka,

— datum zahájení formálního řízení vedeného justičním orgánem,

— vazby na jiné relevantní případy;

vi) pole pro doplňující informace (volný text);

vii) kód předchozího povolení.

2.2.2. Údaje předávané v souladu s článkem 21 nařízení (EU) 2018/1727

a) Ustanovení čl. 21 odst. 4 nařízení (EU) 2018/1727, zřízení společných vyšetřovacích týmů

i) Sekce nejvyšší úrovně
Tato sekce nejvyšší úrovně odpovídá informacím uvedeným v čl. 21 odst. 4 nařízení (EU) 2018/1727, informování o zřízení společných vyšetřovacích týmů.

ii) Struktura zprávy
Struktura údajů se skládá z posloupnosti prvků a zahrnuje alespoň následující:

— Vnitrostátní soudní orgán pověřený trestním řízením

— Vnitrostátní referenční číslo trestního řízení

— Stav trestního řízení

— Vyšetřované trestné činy

— Další země zapojené do případu

— Jde o případ, na který již Eurojust poskytl podporu?

— Pokud ano, identifikátor případu Eurojustu?

— Pokud ne, jedná se o žádost o podporu?

— Jde o případ, na který poskytl podporu Europol?

— Pokud ano, operativní pracovní skupina („OTF“) a/nebo aplikace sítě pro bezpečnou výměnu informací („SIENA“)?

— Dohoda o společném vyšetřovacím týmu (SVT):

— Zapojené země

— Strany SVT (vnitrostátní orgány pověřené vyšetřováním)

— Vnitrostátní referenční číslo trestního řízení, kterým se SVT zabývá

— Datum podpisu

— Doba trvání

— Vyšetřované trestné činy

— Stručné shrnutí případu

— Hlavní podezřelí v trestním řízení, kterým se SVT zabývá (jméno, příjmení, datum a místo narození a případně další relevantní a nezbytné kategorie údajů podle přílohy II)

— Výsledky práce SVT:

— Obtíže/zpoždění při:

— zřízení SVT

— žádání o důkazy / sdílení důkazů v rámci SVT

— dohodě o společné strategii trestního stíhání / její realizaci

— Přípustnost/nepřípustnost/hodnocení důkazů SVT ve vnitrostátním řízení

— Výsledek soudního řízení (úspěšné/neúspěšné stíhání a odsouzení / zproštění viny)

iii) Kód předchozího povolení

b) Ustanovení čl. 21 odst. 5 nařízení (EU) 2018/1727, závažné složité případy

i) Sekce nejvyšší úrovně

Tato sekce nejvyšší úrovně odpovídá informacím uvedeným v čl. 21 odst. 5 nařízení o Eurojustu, tj. závažné složité případy.

ii) Struktura zprávy

Struktura údajů se skládá z posloupnosti prvků a zahrnuje alespoň následující:

— Vnitrostátní soudní orgán pověřený trestním řízením

— Vnitrostátní referenční číslo trestního řízení

— Stav trestního řízení

— Vyšetřované trestné činy

— Další země zapojené do případu

— Jde o případ, na který již Eurojust poskytl podporu?

— Pokud ano, identifikátor případu Eurojustu?

— Pokud ne, jedná se o žádost o podporu?

— Jde o případ, na který poskytl podporu Europol?

— Pokud ano, operativní pracovní skupina a/nebo SIENA?

— Příslušná forma závažné trestné činnosti

— Zapojení organizované zločinecké skupiny

— Typ mafie

— Nadnárodní organizovaná zločinecká skupina

— Dopady na úrovni EU

— Hlavní podezřelí v trestním řízení (jméno, příjmení, datum a místo narození a případně další relevantní a nezbytné kategorie údajů podle přílohy II)

— Stručné shrnutí případu

— Další zapojené země

— Země, se kterými již byla zahájena spolupráce

— Příslušné orgány zapojené v jiné zemi

— Využité nástroje justiční spolupráce

— Počet zaslaných/obdržených žádostí

— Existence souvisejících vyšetřování

— Země, s nimiž má být spolupráce aktivována / země, jichž se to může týkat

— Typ potřebné spolupráce (např. vydání, shromažďování důkazů, jiná spolupráce)

— Existence souvisejících vyšetřování

iii) Kód předchozího povolení

c) Ustanovení čl. 21 odst. 6 písm. a) nařízení (EU) 2018/1727, kompetenční spory

i) Sekce nejvyšší úrovně

Tato sekce nejvyšší úrovně odpovídá informacím uvedeným v čl. 21 odst. 6 písm. a) nařízení (EU) 2018/1727, tj. kompetenční spory

ii) Struktura zprávy

Struktura údajů se skládá z posloupnosti prvků a zahrnuje alespoň následující:

— Vnitrostátní soudní orgán pověřený trestním řízením

— Vnitrostátní referenční číslo trestního řízení

— Stav trestního řízení (např. vyšetřování, trestní stíhání, soudní řízení)

— Vyšetřované trestné činy

— Další země zapojené do případu

— Jde o případ, na který již Eurojust poskytl podporu?

— Pokud ano, identifikátor případu Eurojustu?

— Pokud ne, jedná se o žádost o podporu?

— Jde o případ, na který poskytl podporu Europol?

— Pokud ano, operativní pracovní skupina a/nebo SIENA?

— Další zapojené země

— Příslušné vnitrostátní orgány v jiné zemi, pokud jsou známy

— Vnitrostátní referenční číslo trestního řízení v jiné zemi

— Fáze řízení v jiné zemi, je-li známa

— Pozitivní nebo negativní spor

— Skutečný nebo potenciální spor

— Již provedené koordinační činnosti (např. konzultace podle rámcového rozhodnutí Rady 2009/948/SVV ([1]))

— Stručné shrnutí případu

— Hlavní společní podezřelí (jméno, příjmení, datum a místo narození a případně další relevantní a nezbytné kategorie údajů podle přílohy II)

iii) Kód předchozího povolení

d) Ustanovení čl. 21 odst. 6 písm. b), sledované zásilky

i) Sekce nejvyšší úrovně

Tato sekce nejvyšší úrovně odpovídá informacím uvedeným v čl. 21 odst. 6 písm. b) nařízení (EU) 2018/1727: sledované zásilky

ii) Struktura zprávy

Struktura údajů se skládá z posloupnosti prvků a zahrnuje alespoň následující:

— Vnitrostátní soudní orgán pověřený trestním řízením

— Vnitrostátní referenční číslo trestního řízení

— Stav trestního řízení (např. vyšetřování, trestní stíhání, soudní řízení)

— Vyšetřované trestné činy

— Další země zapojené do případu

— Jde o případ, na který již Eurojust poskytl podporu?

— Pokud ano, identifikátor případu Eurojustu?

— Pokud ne, jedná se o žádost o podporu?

— Jde o případ, na který poskytl podporu Europol?

— Pokud ano, operativní pracovní skupina a/nebo SIENA?

— Další zapojené země

— Země původu/tranzitu/konečného určení

— Příslušné vnitrostátní orgány v jiných zemích

— Existence souvisejících vyšetřování v jiných zemích

([1]) Rámcové rozhodnutí Rady 2009/948/SVV ze dne 30. listopadu 2009 o předcházení kompetenčním sporům při výkonu pravomoci v trestním řízení a jejich řešení (Úř. věst. L 328, 15.12.2009, s. 42, ELI: http://data.europa.eu/eli/dec_framw/2009/948/oj).

— Typ zasílaného zboží (např. drogy a jejich druh / peníze/zbraně/cigarety/jiné)

— Stav sledované zásilky (např. plánovaná, probíhající, dokončená)

— Výsledek sledované zásilky, pokud již byla provedena

— Využitý nástroj justiční spolupráce

— Hlavní společní podezřelí (jméno, příjmení, datum a místo narození a případně další relevantní a nezbytné kategorie údajů podle přílohy II)

iii) Kód předchozího povolení

e) Ustanovení čl. 21 odst. 6 písm. c) nařízení (EU) 2018/1727, opakované obtíže s nástroji justiční spolupráce

i) Sekce nejvyšší úrovně

Tato sekce nejvyšší úrovně odpovídá informacím uvedeným v čl. 21 odst. 6 písm. c) nařízení (EU) 2018/1727: opakované obtíže s nástroji justiční spolupráce

ii) Struktura zprávy

Struktura údajů se skládá z posloupnosti prvků a zahrnuje alespoň následující:

— Vnitrostátní soudní orgán pověřený trestním řízením

— Vnitrostátní referenční číslo trestního řízení

— Stav trestního řízení (např. vyšetřování, trestní stíhání, soudní řízení)

— Vyšetřované trestné činy

— Další země zapojené do případu

— Jde o případ, na který již Eurojust poskytl podporu?

— Pokud ano, identifikátor případu Eurojustu?

— Pokud ne, jedná se o žádost o podporu?

— Jde o případ, na který poskytl podporu Europol?

— Pokud ano, operativní pracovní skupina a/nebo SIENA?

— Další zapojené země

— Příslušné vnitrostátní orgány, jsou-li známy

— Jednající jako vydávající nebo vykonávající orgán

— Zapojený nástroj justiční spolupráce (např. evropský zatýkací rozkaz, evropský vyšetřovací příkaz, zajištění a konfiskace)

— Dotčená konkrétní žádost (tj. jaké vyšetřovací opatření, jaký druh zajištění, evropský zatýkací rozkaz pro výkon trestu nebo pro trestní stíhání)

— Odmítnutí nebo opakované obtíže

— V případě odmítnutí, jaký konkrétní důvod je uveden?

— Stručný popis problému

— Případné další vnitrostátní orgány, kterých se týká stejný problém

iii) Kód předchozího povolení

2.3. *Kódy předchozích povolení*

Při sdílení údajů s Eurojustem prostřednictvím systému JUDEX uvedou příslušné vnitrostátní orgány prostřednictvím kódů předchozích povolení další nakládání s údaji, přístup k nim a jejich předávání po zjištění vazby. Kódy předchozích povolení uvádějí, zda a v jakém rozsahu mohou být informace týkající se vazby sdíleny s jinými příslušnými vnitrostátními orgány, jinými agenturami a subjekty Unie, třetími zeměmi nebo mezinárodními organizacemi.

2.4. *Předdefinované zprávy*

Předdefinované zprávy představují formy výměny informací stanovené nařízením (EU) 2018/1727, pro které však tento právní akt nestanovil konkrétní podobu. Jejich typy a počet jsou určeny během provozní a technické analýzy.

Definice schémat XML (XSD) pro předdefinované zprávy musí být navrženy tak, aby zajišťovaly konzistenci, strukturu a soulad s provozními požadavky.

Na tato schémata se vztahují následující pravidla:

a) sekce nejvyšší úrovně v tomto schématu musí být pojmenována podle konkrétního typu zprávy, který je definován;

b) nezbytná pole požadovaná pro konkrétní typ zprávy musí být do této struktury přidána a definována tak, aby správně reprezentovala datové prvky.

2.5. *Zprávy s volným textem*

Zprávy s volným textem představují formy výměny informací, které umožňují nestrukturovaný nebo částečně strukturovaný obsah, čímž poskytují flexibilitu při zachování souladu s regulatorními a provozními požadavky. Schéma XSD pro zprávy s volným textem musí být navrženo tak, aby zajišťovalo konzistenci a správné formátování.

Na tato schémata se vztahují následující pravidla:

a) sekce nejvyšší úrovně ve schématu musí být pojmenována podle konkrétního typu zprávy s volným textem, který je definován;

b) schéma musí definovat potřebnou strukturu zprávy s volným textem a zároveň umožnit vhodné uspořádání prvků podle potřeby;

c) nezbytná pole požadovaná pro konkrétní typ zprávy s volným textem musí být do této struktury přidána a definována tak, aby správně reprezentovala datové prvky.

PŘÍLOHA III

TECHNICKÉ SPECIFIKACE OTISKŮ PRSTŮ A FOTOGRAFIÍ

Zprávy vyměňované prostřednictvím decentralizovaného informačního systému mohou být doplněny přílohami, včetně souborů Národního ústavu pro normalizaci a technologie („NIST“) obsahujících otisky prstů a fotografie, v souladu s technickými specifikacemi uvedenými v bodech 1 a 2.

1. **Otisky prstů**

Otisky prstů, které mohou být sdíleny s Eurojustem za účelem spolehlivého určení totožnosti osob, proti nimž je vedeno trestní řízení v souvislosti s teroristickými trestnými činy, musí splňovat tyto podmínky:

a) otisky prstů se poskytují v jednom souboru obsahujícím digitální snímky otisků prstů (soubor NIST s otisky prstů) a předkládají se v souladu s normou ANSI/NIST-ITL 1-2011 Update 2015 (nebo její novější verzí);

b) soubor NIST s otisky prstů se skládá z maximálně deseti jednotlivých otisků prstů: válených, píchaných nebo obou druhů;

c) všechny otisky prstů jsou označeny;

d) otisky prstů se snímají pomocí přímého skenování nebo inkoustem na papír, pokud byly otisky prstů inkoustem na papír naskenovány v požadovaném rozlišení a ve stejné kvalitě;

e) soubor NIST s otisky prstů umožňuje zahrnout doplňující informace, jako jsou podmínky registrace otisků prstů a metoda použitá pro pořízení jednotlivých snímků otisků prstů;

f) otisky prstů mají jmenovité rozlišení 500 nebo 1 000 ppi [1] (s přípustnou odchylkou +/– 10 ppi) s 256 úrovněmi šedi;

g) algoritmus komprese otisků prstů, který se má použít, se řídí doporučeními Národního ústavu pro normalizaci a technologie („NIST“). Údaje o otiscích prstů s rozlišením 500 ppi se komprimují pomocí algoritmu WSQ (ISO/IEC 19794-5:2005). Údaje o otiscích prstů s rozlišením 1 000 ppi se komprimují pomocí normy pro kompresi zobrazení JPEG 2000 (ISO/IEC 15444-1) a kódovacího systému. Cílový poměr komprese je 15:1.

2. **Fotografie**

Fotografie, které mohou být sdíleny s Eurojustem za účelem spolehlivého určení totožnosti osob, proti nimž je vedeno trestní řízení v souvislosti s teroristickými trestnými činy, musí splňovat tyto podmínky:

a) v souboru s fotografií (soubor NIST s fotografií) je zahrnuto pouze jedno zobrazení obličeje, které se předkládá v souladu s normou ANSI/NIST-ITL 1-2011 Update 2015 nebo jakoukoli její novější dostupnou verzí;

b) fotografie jsou buď v odstínech šedi, v barvě, nebo v blízkém infračerveném spektru;

c) kvalita fotografií je založena na požadavcích na zobrazení pro frontální obraz podle normy ISO/IEC 19794-5:2011 nebo jakékoli její novější dostupné verze;

d) soubor NIST s fotografií umožňuje zahrnout doplňující informace, včetně data, kdy bylo zobrazení pořízeno;

[1] Pixely na palec.

e) fotografie v režimu portrétu mají minimální rozlišení 600 × 800 pixelů a maximální rozlišení 1 200 × 1 600 pixelů;

f) obličej zabírá na fotografii tolik místa, aby minimální vzdálenost mezi středy očí činila 120 pixelů;

g) použitý kompresní algoritmus fotografie se řídí doporučeními Národního institutu pro standardy a technologie („NIST“). Fotografie se komprimují pouze jednou podle normy komprese obrazu JPG (ISO/IEC 10918) nebo JPEG 2000 (ISO/IEC 15444), přičemž maximální povolený poměr komprese zobrazení činí 20:1.