2025/2447

5.12.2025.

PROVEDBENA UREDBA KOMISIJE (EU) 2025/2447

od 4. prosinca 2025.

o utvrđivanju pravila za primjenu Uredbe (EU) 2018/1727 Europskog parlamenta i Vijeća u pogledu tehničkih specifikacija, mjera i drugih zahtjeva za uspostavu i upotrebu decentraliziranog IT sustava za sigurnu obradu i priopćavanje informacija

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu (EU) 2018/1727 Europskog parlamenta i Vijeća od 14. studenoga 2018. o Agenciji Europske unije za suradnju u kaznenom pravosuđu (Eurojust) te zamjeni i stavljanju izvan snage Odluke Vijeća 2002/187/PUP ([1]), a posebno njezin članak 22.a stavak 3. i članak 22.b stavak 1. točke (a), (b), (c) i (d),

budući da:

(1) Uredbom (EU) 2018/1727 utvrđuje se okvir za novu digitalnu unutarnju infrastrukturu Eurojusta i uspostavu decentraliziranog sigurnog digitalnog komunikacijskog sustava između nadležnih nacionalnih tijela država članica i Eurojusta.

(2) Sigurna digitalna komunikacija provodi se putem decentraliziranog IT sustava. Kako bi se uspostavio decentralizirani IT sustav, potrebno je utvrditi tehničke specifikacije u kojima se definiraju komunikacijske metode i komunikacijski protokoli, tehničke mjere kojima se osiguravaju minimalni standardi informacijske i opće sigurnosti te minimalni ciljevi dostupnosti za provedbu tog sustava.

(3) U skladu s člankom 22.a stavkom 1. Uredbe (EU) 2018/1727 decentralizirani IT sustav sastoji se od IT sustava država članica i Eurojusta i interoperabilnih pristupnih točaka e-CODEX-a koje ih povezuju. Taj bi okvir trebalo uzeti u obzir u tehničkim specifikacijama i drugim zahtjevima decentraliziranog IT sustava utvrđenima u ovoj Uredbi.

(4) Pristupne točke decentraliziranog IT sustava trebale bi se temeljiti na odobrenim pristupnim točkama e-CODEX-a kako su definirane u članku 3. točki 3. Uredbe (EU) 2022/850 Europskog parlamenta i Vijeća ([2]).

(5) Decentralizirani IT sustav uvodi se u okviru većeg decentraliziranog IT sustava koji se temelji na sustavu e-CODEX pod nazivom Sustav digitalne razmjene podataka o pravosuđu (JUDEX). Stoga je potrebno osigurati djelotvornu razmjenu informacija o horizontalnim kretanjima.

(6) U skladu s člankom 22.a stavkom 4. Uredbe (EU) 2018/1727 države članice i Eurojust mogu umjesto nacionalnog IT sustava kao svoj pozadinski sustav upotrebljavati referentni implementacijski softver koji je izradila Komisija. Da bi se osigurala interoperabilnost, nacionalni IT sustavi i referentni implementacijski softver trebali bi biti sukladni s istim tehničkim specifikacijama i zahtjevima.

(7) Podaci koji se odnose na kaznena djela terorizma i teški organizirani kriminal trebali bi se strukturirano prenositi kako bi se poboljšala kvaliteta i relevantnost informacija i osigurala učinkovitija integracija informacija u Eurojustov sustav vođenja predmeta i bolja unakrsna provjera s informacijama koje su već pohranjene u tom sustavu. Za podatke o otiscima prstiju i fotografije, koji se mogu poslati Eurojustu u svrhu identifikacije pojedinaca koji podliježu kaznenom postupku koji je povezan s kaznenim djelima terorizma, trebalo bi utvrditi format i tehničke standarde za njihov prijenos.

([1]) SL L 295, 21.11.2018., str. 138., ELI: http://data.europa.eu/eli/reg/2018/1727/oj.
([2]) Uredba (EU) 2022/850 Europskog parlamenta i Vijeća od 30. svibnja 2022. o računalnom sustavu za prekograničnu elektroničku razmjenu podataka u području pravosudne suradnje u građanskim i kaznenim stvarima (sustav e-CODEX) i izmjeni Uredbe (EU) 2018/1726 (SL L 150, 1.6.2022., str. 1., ELI: http://data.europa.eu/eli/reg/2022/850/oj).

(8) Eurojust olakšava i podupire izdavanje i izvršavanje zahtjeva za pravosudnu suradnju, među ostalim zahtjeva i odluka koji se temelje na instrumentima kojima se provodi načelo uzajamnog priznavanja. Nacionalna nadležna tijela trebala bi moći zatražiti pomoć i koordinaciju od Eurojusta putem decentraliziranog IT sustava.

(9) Kako bi se osigurale djelotvornost i dosljednost, važno je da tehničke specifikacije koje treba utvrditi na temelju Uredbe (EU) 2018/1727 budu kompatibilne s tehničkim specifikacijama utvrđenima na temelju uredaba (EU) 2023/2844 ([3]), (EU) 2023/1543 ([4]) i (EU) 2024/3011 ([5]) Europskog parlamenta i Vijeća, kao i s budućim mjerama digitalizacije relevantnima za mandat Eurojusta za potporu nacionalnim nadležnim tijelima.

(10) Svaku drugu komunikaciju između Eurojusta i nadležnih nacionalnih tijela, kao što je priopćavanje informacija o rezultatima obrade informacija, među ostalim o postojanju poveznica s predmetima koji su već pohranjeni u sustavu vođenja predmeta u skladu s člankom 22. Uredbe (EU) 2018/1727 kad Eurojust djeluje na vlastitu inicijativu, ili informacija prenesenih Eurojustu u svrhu očuvanja, analize i pohrane dokaza u vezi s genocidom, zločinima protiv čovječnosti, ratnim zločinima i povezanim kaznenim djelima u skladu s člankom 4. stavkom 1. točkom (j) te uredbe, također bi trebalo omogućiti putem decentraliziranog IT sustava.

(11) Kako bi se osiguralo da se ovom Uredbom uzimaju u obzir operativne potrebe Eurojusta, provedeno je savjetovanje s Eurojustom u skladu s člankom 22.a stavkom 3. Uredbe (EU) 2018/1727.

(12) U skladu s člankom 4. Protokola br. 21 o stajalištu Ujedinjene Kraljevine i Irske s obzirom na područje slobode, sigurnosti i pravde, priloženog Ugovoru o Europskoj uniji i Ugovoru o funkcioniranju Europske unije, Irska je dopisom od 9. rujna 2019. obavijestila o svojoj želji da prihvati Uredbu (EU) 2018/1727 i da ta uredba za nju bude obvezujuća. Odlukom Komisije (EU) 2019/2006 ([6]) potvrđeno je to sudjelovanje. Uredbom (EU) 2023/2131 Europskog parlamenta i Vijeća ([7]) izmijenjena je Uredba (EU) 2018/1727 kako bi se omogućila uspostava sigurnih digitalnih komunikacijskih kanala između Eurojusta i nadležnih nacionalnih tijela i ona čini pravnu osnovu za ovu Uredbu. U okolnostima u kojima Irska nije obavijestila o svojoj želji da sudjeluje u donošenju i primjeni Uredbe (EU) 2023/2131 niti da je prihvati ili bude obvezana njome, u skladu s člancima 1. i 2. i člankom 4.a stavkom 1. Protokola br. 21 Uredba (EU) 2023/2131 ne obvezuje Irsku niti se na nju primjenjuje. Stoga Irska ne sudjeluje u donošenju ove Uredbe.

(13) U skladu s člancima 1. i 2. Protokola br. 22 o stajalištu Danske, koji je priložen Ugovoru o Europskoj uniji i Ugovoru o funkcioniranju Europske unije, Danska nije sudjelovala u donošenju Uredbe (EU) 2018/1727. Stoga ova Uredba nije obvezujuća za Dansku niti se na nju primjenjuje.

([3]) Uredba (EU) 2023/2844 Europskog parlamenta i Vijeća od 13. prosinca 2023. o digitalizaciji pravosudne suradnje i pristupa pravosuđu u prekograničnim građanskim, trgovačkim i kaznenim stvarima te o izmjeni određenih akata u području pravosudne suradnje (SL L, 2023/2844, 27.12.2023., ELI: http://data.europa.eu/eli/reg/2023/2844/oj).

([4]) Uredba (EU) 2023/1543 Europskog parlamenta i Vijeća od 12. srpnja 2023. o europskim nalozima za dostavljanje i europskim nalozima za čuvanje elektroničkih dokaza u kaznenim postupcima i za izvršenje kazni zatvora nakon kaznenog postupka (SL L 191, 28.7.2023., str. 118., ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

([5]) Uredba (EU) 2024/3011 Europskog parlamenta i Vijeća od 27. studenog 2024. o prijenosu postupaka u kaznenim stvarima (SL L, 2024/3011, 18.12.2024., ELI: http://data.europa.eu/eli/reg/2024/3011/oj).

([6]) Odluka Komisije (EU) 2019/2006 od 29. studenoga 2019. o sudjelovanju Irske u Uredbi (EU) 2018/1727 Europskog parlamenta i Vijeća o Agenciji Europske unije za suradnju u kaznenom pravosuđu (Eurojust) (SL L 310, 2.12.2019., str. 59., ELI: http://data.europa.eu/eli/dec/2019/2006/oj).

([7]) Uredba (EU) 2023/2131 Europskog parlamenta i Vijeća od 4. listopada 2023. o izmjeni Uredbe (EU) 2018/1727 Europskog parlamenta i Vijeća i Odluke Vijeća 2005/671/PUP u pogledu digitalne razmjene podataka u predmetima povezanima s terorizmom (SL L, 2023/2131, 11.10.2023., ELI: http://data.europa.eu/eli/reg/2023/2131/oj).

(14) Provedeno je savjetovanje s Europskim nadzornikom za zaštitu podataka u skladu s člankom 42. stavkom 1. Uredbe (EU) 2018/1725 Europskog parlamenta i Vijeća ([8]) koji je dostavio mišljenje 21. listopada 2025.

(15) Mjere predviđene u ovoj Uredbi u skladu su s mišljenjem Odbora osnovanog člankom 22.c Uredbe (EU) 2018/1727,

DONIJELA JE OVU UREDBU:

Članak 1.

Tehničke specifikacije decentraliziranog IT sustava

Tehničke specifikacije, mjere i ciljevi decentraliziranog IT sustava iz članka 22.b stavka 1. točaka (a), (b), (c) i (d) Uredbe (EU) 2018/1727 utvrđeni su u Prilogu I. ovoj Uredbi.

Članak 2.

Digitalni postupovni standardi

Digitalni postupovni standardi koji se primjenjuju na elektroničku komunikaciju putem decentraliziranog IT sustava iz članka 22.a stavka 3. Uredbe (EU) 2018/1727 utvrđeni su u Prilogu II. ovoj Uredbi.

Članak 3.

Tehničke specifikacije za prijenos otisaka prstiju i fotografija

Tehničke specifikacije i format za prijenos otisaka prstiju i fotografija iz članka 22.a stavka 3. Uredbe (EU) 2018/1727 utvrđeni su u Prilogu III. ovoj Uredbi.

Članak 4.

Stupanje na snagu

Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u državama članicama u skladu s Ugovorima.

Sastavljeno u Bruxellesu 4. prosinca 2025.

Za Komisiju
Predsjednica
Ursula VON DER LEYEN

([8]) Uredba (EU) 2018/1725 Europskog parlamenta i Vijeća od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ (SL L 295, 21.11.2018., str. 39., ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

PRILOG I.

TEHNIČKE SPECIFIKACIJE, MJERE I CILJEVI DECENTRALIZIRANOG IT SUSTAVA

1. **Uvod i područje primjene**

U ovom se Prilogu utvrđuju tehničke specifikacije, mjere i ciljevi decentraliziranog IT sustava za razmjenu podataka na temelju Uredbe (EU) 2018/1727.

Decentraliziranost IT sustava omogućuje izravnu i sigurnu razmjenu podataka između nadležnih nacionalnih tijela i Eurojusta.

2. **Definicije**

Za potrebe ovog Priloga primjenjuju se sljedeće definicije:

2.1. „Hypertext Transport Protocol Secure" odnosno „HTTPS" znači šifrirani komunikacijski kanali sa sigurnom vezom;

2.2. „neosporivost podrijetla" znači dokazivanje cjelovitosti i podrijetla podataka metodama kao što su digitalna certifikacija, infrastruktura javnih ključeva te elektronički potpisi i pečati;

2.3. „neosporivost primitka podataka" znači dokazivanje osobi od koje prijenos potječe da je predviđeni primatelj primio podatke metodama kao što su digitalna certifikacija, infrastruktura javnih ključeva te elektronički potpisi i pečati;

2.4. „SOAP" (*Simple Object Access Protocol*) znači, prema standardima konzorcija World Wide Web, specifikacija protokola za prijenos poruka radi razmjene strukturiranih informacija prilikom provedbe *web*-usluga u računalnim mrežama;

2.5. „REST" (*Representational State Transfer*) znači vrstu arhitekture za projektiranje umreženih aplikacija koja se temelji na modelu komunikacije između korisnika i poslužitelja bez očuvanja stanja, standardnim metodama za obavljanje operacija nad resursima, koji su obično u strukturiranim formatima;

2.6. „web-usluga" znači softverski sustav projektiran tako da podržava interoperabilne mrežne interakcije stroj-stroj i koji ima sučelje opisano u strojno obradivom obliku;

2.7. „razmjena podataka" znači razmjena poruka i dokumenata putem decentraliziranog IT sustava;

2.8. „e-CODEX" znači sustav e-CODEX kako je definiran u članku 3. stavku 1. Uredbe (EU) 2022/850;

2.9. „temeljni rječnici e-pravosuđa EU-a" znači temeljni rječnici e-pravosuđa EU-a kako su definirani u točki 4. Priloga Uredbi (EU) 2022/850;

2.10. „ebMS" odnosi se na *ebXML Message Service*, protokol za razmjenu poruka razvijen u okviru OASIS-a koji omogućuje sigurnu, pouzdanu i interoperabilnu razmjenu elektroničkih poslovnih dokumenata SOAP-om. Podupire integraciju među poduzećima u različitim sustavima;

2.11. „AS4" znači *Applicability Statement 4*, standard OASIS-a na temelju kojeg je definiran protokol ebMS 3.0, kojim se pojednostavnjuje sigurna i interoperabilna razmjena poruka među poduzećima korištenjem otvorenih standarda kao što su SOAP i WS-Security;

2.12. „ciljano vrijeme oporavka” znači maksimalno dopušteno vrijeme da se usluga ponovno uspostavi nakon incidenta;

2.13. „ciljana točka oporavka” znači maksimalna prihvatljiva količina izgubljenih podataka u slučaju kvara.

3. **Načini komunikacije elektroničkim sredstvima**

3.1. Decentralizirani IT sustav koristi se komunikacijskim metodama utemeljenima na uslugama, poput *web*-usluga ili drugih ponovno iskoristivih komponenata i softvera za razmjenu poruka i dokumenata.

3.2. Konkretno, za decentralizirani IT sustav bit će potrebna komunikacija putem pristupnih točaka e-CODEX-a, kako je utvrđeno u članku 5. stavku 2. Uredbe (EU) 2022/850. Stoga, kako bi se osigurala djelotvorna i interoperabilna prekogranična razmjena podataka, decentralizirani IT sustav mora podržavati komunikaciju e-CODEX-om.

4. **Komunikacijski protokoli**

4.1. Decentralizirani IT sustav koristi sigurne internetske protokole za:

(a) komunikaciju unutar decentraliziranog IT sustava između nadležnih tijela i Eurojusta;

(b) komunikaciju s bazom podataka nadležnih tijela / sudova kako je navedeno u točki 7.1.

4.2. U kontekstu definiranja i prenošenja strukturiranih podataka i metapodataka komponente decentraliziranog IT sustava temelje se na sveobuhvatnim i opće prihvaćenim industrijskim standardima i protokolima, kao što su SOAP i REST.

4.3. Prijenos podataka i razmjena poruka putem decentraliziranog IT sustava temelji se na sigurnim protokolima utemeljenim na standardima kao što su:

(a) AS4 Profile za prekograničnu razmjenu podataka, koji jamči sigurnu i pouzdanu razmjenu poruka sa šifriranjem i neosporivosti;

(b) API-ji HTTPS/RESTful za komunikaciju u formatima JSON i XML;

(c) SOAP za interakcije visoke pouzdanosti sa standardom WS-Security za autentifikaciju i šifriranje.

4.4. Da bi razmjena podataka bila glatka i interoperabilna, komunikacijski protokoli decentraliziranog IT sustava u skladu su s relevantnim standardima za interoperabilnost.

4.5. Ako je primjenjivo, XML sheme koriste relevantne standarde ili rječnike potrebne za pravilno potvrđivanje valjanosti elemenata i vrsta definiranih u shemi. Ti standardi ili rječnici mogu uključivati:

(a) temeljni rječnik e-pravosuđa EU-a;

(b) nekvalificirane vrste podataka;

(c) popis oznaka za oznake jezika Europske unije.

4.6. Protokoli koje decentralizirani IT sustav koristi za sigurnost i autentifikaciju temelje se na protokolima utemeljenima na standardima kao što su:

(a) TLS (sigurnost transportnog sloja) za šifriranu i autentificiranu mrežnu komunikaciju, koji podržava uzajamnu autentifikaciju na temelju digitalnih certifikata X.509;

(b) OAuth/OpenID Connect (OIDC) za sigurnu autentifikaciju i autorizaciju;

(c) PKI (infrastruktura javnih ključeva) i digitalni potpisi za sigurnu razmjenu ključeva i provjeru cjelovitosti poruka na temelju digitalnih certifikata (X.509) koje su izdala pouzdana certifikacijska tijela.

5. **Ciljevi informacijske sigurnosti i relevantne tehničke mjere**

5.1. Tehničke mjere za potrebe ispunjavanja minimalnih sigurnosnih standarda informacijske tehnologije u razmjeni informacija decentraliziranim IT sustava obuhvaćaju:

(a) mjere za osiguravanje povjerljivosti informacija, među ostalim korištenje sigurnih komunikacijskih kanala;

(b) mjere za osiguravanje cjelovitosti podataka u mirovanju i u prijenosu;

(c) mjere za osiguravanje neosporivosti podrijetla pošiljatelja informacija unutar decentraliziranog IT sustava i neosporivosti primitka informacija;

(d) mjere za osiguravanje bilježenja sigurnosnih događaja u skladu s priznatim međunarodnim preporukama za sigurnosne standarde informacijske tehnologije ([1]);

(e) mjere za osiguravanje autentifikacije i autorizacije korisnika i mjere za provjeru identiteta sustava povezanih s decentraliziranim IT sustavom.

5.2. Komponente decentraliziranog IT sustava omogućuju sigurnu komunikaciju i prijenos podataka koji se temelje na šifriranju, infrastrukturi javnih ključeva s digitalnim certifikatima za autentifikaciju i sigurnu razmjenu ključeva te sigurnim protokolima za razmjenu poruka, kao što su AS4 (ebMS), API-ji RESTful i SOAP, kako bi se održala povjerljivost i cjelovitost poruka.

5.3. Ako se TLS koristi u kontekstu decentraliziranog IT sustava, koristi se najnovija stabilna verzija protokola ili, ako to nije moguće, verzija bez poznatih sigurnosnih nedostataka. Dopuštene su samo duljine ključeva kojima se osigurava odgovarajuća razina kriptografske sigurnosti, a ne koriste se sljedovi šifri za koje je poznato da su nesigurni ili zastarjeli.

5.4. U mjeri u kojoj je to moguće, digitalne certifikate PKI-ja koji se koriste za rad decentraliziranog IT sustava izdaju certifikacijska tijela priznata kao kvalificirani pružatelji usluga povjerenja u skladu s Uredbom (EU) br. 910/2014 Europskog parlamenta i Vijeća ([2]). Provode se mjere kako bi se osiguralo da se takvi certifikati upotrebljavaju isključivo u predviđene svrhe, na potrebnoj razini povjerenja i u skladu s primjenjivim zahtjevima Uredbe (EU) br. 910/2014.

5.5. Komponente decentraliziranog IT sustava razvijaju se u skladu s načelom tehničke i integrirane zaštite podataka i provode se odgovarajuće administrativne, organizacijske i tehničke mjere kako bi se osigurala visoka razina kibernetičke sigurnosti.

5.6. Komisija izrađuje, razvija i održava referentni implementacijski softver u skladu sa zahtjevima i načelima za zaštitu podataka utvrđenima u Uredbi (EU) 2018/1725. Referentni implementacijski softver koji Komisija stavlja na raspolaganje državama članicama omogućuje da ispune svoje obveze u skladu s Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća ([3]) i Direktivom (EU) 2016/680, ovisno o slučaju.

([1]) Ne dovodeći u pitanje bilježenje radi sigurnosti, mehanizmi bilježenja koje upotrebljavaju komponente decentraliziranog IT sustava osiguravaju, prema potrebi, usklađenost sa zahtjevima utvrđenima u članku 88. Uredbe (EU) 2018/1725 i, ako je primjenjivo, članku 25. Direktive (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podatakate o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP (SL L 119, 4.5.2016., str. 89., ELI: http://data.europa.eu/eli/dir/2016/680/oj).

([2]) Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (SL L 257, 28.8.2014., str. 73., ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([3]) Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1., ELI: http://data.europa.eu/eli/reg/2016/679/oj).

5.7. Države članice koje upotrebljavaju nacionalni pozadinski sustav koji nije referentni implementacijski softver dužne su primjenjivati mjere potrebne za osiguravanje njegove usklađenosti sa zahtjevima iz Uredbe (EU) 2016/679 i Direktive (EU) 2016/680, ovisno o slučaju.

5.8. Eurojust poduzima potrebne mjere kako bi osigurao da njegov pozadinski sustav ili primjerak referentnog implementacijskog softvera koji koristi ispunjava zahtjeve iz uredaba (EU) 2018/1725 i (EU) 2018/1727.

5.9. Države članice i Eurojust dužni su uspostaviti pouzdane mehanizme za otkrivanje prijetnji i odgovaranje na incidente radi pravovremenog utvrđivanja, ublažavanja i oporavka od sigurnosnih incidenata, u skladu sa svojim relevantnim politikama za IT sustave za koje su odgovorni i koji su dio decentraliziranog IT sustava.

6. **Minimalni ciljevi dostupnosti**

6.1. Eurojust i države članice dužni su se pobrinuti da komponente decentraliziranog IT sustava za koje su odgovorni budu dostupne 24 sata dnevno sedam dana u tjednu, pri čemu ciljana tehnička dostupnost na godišnjoj razini mora biti najmanje 98 %, ne računajući planirano održavanje.

6.2. Komisija je dužna pobrinuti se da baza podataka sudova bude dostupna 24 sata dnevno sedam dana u tjednu, pri čemu ciljana tehnička dostupnost na godišnjoj razini mora biti veća od 99 %, ne računajući planirano održavanje.

6.3. U mjeri u kojoj je to moguće, aktivnosti održavanja zakazuju se izvan radnog vremena (između 20 sati i 7 sati po srednjoeuropskom vremenu).

6.4. Države članice obavješćuju Komisiju, Eurojust i druge države članice o aktivnostima održavanja kako slijedi:

(a) 5 radnih dana unaprijed za aktivnosti održavanja koje mogu uzrokovati nedostupnost dulju od 4 sata;

(b) 10 radnih dana unaprijed za aktivnosti održavanja koje mogu uzrokovati nedostupnost od 4 do 12 sati;

(c) 30 radnih dana unaprijed za aktivnosti održavanja koje mogu uzrokovati nedostupnost dulju od 12 sati.

6.5. Ako države članice imaju fiksna razdoblja unutar kojih vrše redovno održavanje, obavješćuju Komisiju, Eurojust i druge države članice o danima i vremenu takvih redovitih fiksnih razdoblja. Odstupajući od obveza utvrđenih u prvoj rečenici, ako komponente decentraliziranog IT sustava za koje su odgovorne države članice u takvom redovitom fiksnom razdoblju budu nedostupne, države članice mogu odlučiti da neće o tome svaki put obavijestiti Komisiju.

6.6. U slučaju neočekivanog tehničkog kvara komponente decentraliziranog IT sustava za koje su odgovorne države članice, o tom kvaru i o predviđenom roku za oporavak, ako je poznat, države članice bez odgode obavješćuju Komisiju i druge države članice.

6.7. Eurojust obavješćuje Komisiju i druge države članice o aktivnostima održavanja kako slijedi:

(a) 5 radnih dana unaprijed za aktivnosti održavanja koje mogu uzrokovati nedostupnost dulju od 4 sata;

(b) 10 radnih dana unaprijed za aktivnosti održavanja koje mogu uzrokovati nedostupnost od 4 do 12 sati;

(c) 30 radnih dana unaprijed za aktivnosti održavanja koje mogu uzrokovati nedostupnost dulju od 12 sati.

6.8. Ako Eurojust ima fiksna razdoblja unutar kojih vrši redovno održavanje, obavješćuje Komisiju i države članice o danima i vremenu takvih planiranih redovitih fiksnih razdoblja. Odstupajući od obveza utvrđenih u prvoj rečenici, ako komponente decentraliziranog IT sustava za koje je odgovoran Eurojust u takvom redovitom fiksnom razdoblju budu nedostupne, Eurojust može odlučiti da neće o tome svaki put obavijestiti Komisiju.

6.9. U slučaju neočekivanog tehničkog kvara komponente decentraliziranog IT sustava za koju je odgovoran, o tom kvaru i o predviđenom roku za oporavak, ako je poznat, Eurojust bez odgode obavješćuje Komisiju i države članice.

6.10. U slučaju neočekivanog tehničkog kvara u bazi podataka nadležnih tijela / sudova Komisija bez odgode obavješćuje Eurojust i države članice o nedostupnosti i o predviđenom roku za oporavak, ako je poznat.

6.11. U slučaju prekida pružanja usluge države članice i Eurojust dužni su se pobrinuti za brzo ponovno uspostavljanje usluge s minimalnim gubitkom podataka, u skladu s ciljanim vremenom oporavka i ciljanom točkom oporavka.

6.12. Države članice i Eurojust dužni su uvesti odgovarajuće mjere za postizanje prethodno navedenih ciljeva dostupnosti i uspostaviti postupke za djelotvoran odgovor na incidente.

7. **Baza podataka nadležnih tijela / sudova (CDB)**

7.1. U skladu s člankom 22.a Uredbe (EU) 2018/1727 decentralizirani IT sustav omogućuje elektroničku komunikaciju između nadležnih nacionalnih tijela i Eurojusta. Uzimajući u obzir obveze razmjene informacija između nadležnih nacionalnih tijela i Eurojusta na temelju članaka 21., 21.a i 22., ali i ulogu Eurojusta u olakšavanju i podupiranju izdavanja i izvršenja svih zahtjeva za uzajamnu pravnu pomoć ili uzajamno priznavanje u skladu s člankom 8. stavkom 1. Uredbe (EU) 2018/1727, potrebno je da se uključena nadležna tijela mogu jasno identificirati pri upotrebi decentraliziranog IT sustava. Stoga je važno uspostaviti mjerodavnu bazu podataka s informacijama tih tijela za potrebe decentraliziranog IT sustava.

7.2. CDB uključuje sljedeće informacije u strukturiranom obliku:

(a) za potrebe članka 8. stavaka 1., 3. i 4. te članaka 21., 21.a i 22. Uredbe (EU) 2018/1727 informacije o nadležnim nacionalnim tijelima, uključujući nacionalne korespondente kako je utvrđeno u članku 20. te uredbe, kao i o nacionalnim članovima u skladu s člankom 7. ([4]) te uredbe;

(b) informacije potrebne za određivanje geografskih ili materijalnih područja nadležnosti nadležnih tijela ili druge relevantne kriterije potrebne za utvrđivanje njihove nadležnosti, prema potrebi;

(c) informacije potrebne za pravilno tehničko usmjeravanje poruka u okviru decentraliziranog IT sustava.

7.3. Komisija je odgovorna za razvoj, održavanje, rad i potporu CDB-u.

7.4. CDB omogućuje državama članicama i Eurojustu da ažuriraju informacije u njemu, a nadležnim nacionalnim tijelima i nacionalnim članovima koji sudjeluju u decentraliziranom IT sustavu programski pristup informacijama u tom sustavu i njihovo preuzimanje.

7.5. Pristup CDB-u moguć je putem zajedničkog komunikacijskog protokola, neovisno o tome koriste li nadležna tijela povezana s decentraliziranim IT sustavom nacionalni pozadinski sustav ili su uvela referentni implementacijski softver.

7.6. Države članice osiguravaju da su informacije o njihovim nadležnim tijelima u CDB-u kako je utvrđeno u točki 7.2. potpune, točne i ažurirane.

([4]) Time se ne dovodi u pitanje delegiranje ovlasti nacionalnog člana njegovu zamjeniku, drugom osoblju nacionalnog ureda ili ovlaštenom osoblju Eurojusta.

PRILOG II.

DIGITALNI POSTUPOVNI STANDARDI

U članku 3. stavku 9. Uredbe (EU) 2022/850 digitalni postupovni standardi definirani su kao tehničke specifikacije za modele poslovnih procesa i sheme podataka kojima se određuje elektronička struktura podataka razmijenjenih putem sustava e-CODEX.

U ovom se Prilogu određuju tehničke specifikacije za modele poslovnih procesa i tehničke specifikacije za sheme podataka.

1. **Tehničke specifikacije za modele poslovnih procesa na temelju Uredbe (EU) 2018/1727**

Tehničke specifikacije za modele poslovnih procesa određene su u točkama od 1.1. do 1.5. U njima se utvrđuju glavni aspekti potrebni za omogućivanje elektroničke komunikacije u smislu Uredbe (EU) 2018/1727 putem decentraliziranog IT sustava.

Decentralizirani IT sustav omogućuje razmjenu informacija samo između nadležnih nacionalnih tijela države članice i nacionalnog člana iz te države članice.

1.1. *Razmjena informacija povezanih s Europskim pravosudnim registrom za borbu protiv terorizma (CTR) na temelju članka 21.a Uredbe (EU) 2018/1727*

1.1.1. Model za prijenos podataka CTR-a:

nadležno nacionalno tijelo nacionalnom članu prosljeđuje podatke CTR-a o postupcima povezanima s terorizmom.

1.1.2. Model za primanje podataka CTR-a:

nacionalni član prima podatke CTR-a.

1.1.3. Model zahtjeva za suglasnost:

nacionalni član traži suglasnost svojeg nadležnog nacionalnog tijela.

1.1.4. Model za primanje zahtjeva za suglasnost:

nadležno nacionalno tijelo prima zahtjev za suglasnost.

1.1.5. Model za slanje odgovora na zahtjev za suglasnost:

nadležno nacionalno tijelo šalje odgovor na zahtjev za suglasnost.

1.1.6. Model za primanje odgovora na zahtjev za suglasnost:

nacionalni član prima odgovor na zahtjev za suglasnost.

1.1.7. Model za informacije o povezanosti s drugim predmetom:

nacionalni član obavješćuje nadležno nacionalno tijelo o povezanosti s drugim predmetom.

1.1.8. Model za ažuriranje podataka CTR-a:

nadležno nacionalno tijelo prosljeđuje svojem nacionalnom članu podatke koje je potrebno ažurirati ili izbrisati.

1.1.9. Model za primanje ažuriranih podataka CTR-a:

nacionalni član prima podatke CTR-a koje je potrebno ažurirati ili izbrisati.

1.2. *Razmjena informacija povezanih s teškim kaznenim djelima na temelju članka 21. Uredbe (EU) 2018/1727*

1.2.1. Model za prijenos podataka o teškom prekograničnom kriminalu:

nacionalno nadležno tijelo prosljeđuje Eurojustu podatke o teškom prekograničnom kriminalu.

1.2.2. Model za primanje podataka o teškom prekograničnom kriminalu:

nacionalni član prima podatke o teškom prekograničnom kriminalu.

1.2.3. Model zahtjeva za suglasnost:

nacionalni član zahtijeva suglasnost svojeg nadležnog nacionalnog tijela.

1.2.4. Model za primanje zahtjeva za suglasnost:

nadležno nacionalno tijelo prima zahtjev za suglasnost.

1.2.5. Model za slanje odgovora na zahtjev za suglasnost:

nadležno nacionalno tijelo šalje odgovor na zahtjev za suglasnost.

1.2.6. Model za primanje odgovora na zahtjev za suglasnost:

nacionalni član prima odgovor na zahtjev za suglasnost.

1.2.7. Model za informacije o povezanosti s drugim predmetom:

nacionalni član obavješćuje nadležno nacionalno tijelo o povezanosti s drugim predmetom.

1.2.8. Model za ažuriranje podataka o teškom prekograničnom kriminalu:

nadležno nacionalno tijelo prosljeđuje svojem nacionalnom članu podatke koje je potrebno ažurirati ili izbrisati.

1.2.9. Model za primanje ažuriranih podataka o teškom prekograničnom kriminalu:

nacionalni član prima podatke o teškom prekograničnom kriminalu koje je potrebno ažurirati ili izbrisati.

1.3. *Razmjena općih informacija*

1.3.1. Model za slanje informacija:

nacionalni član šalje informacije nadležnom nacionalnom tijelu ili obrnuto.

1.3.2. Model za primanje informacija:

nadležno nacionalno tijelo ili nacionalni član prima informacije.

1.3.3. Model za odgovaranje na informacije:

nadležno nacionalno tijelo odgovara na informacije primljene od nacionalnog člana ili obrnuto.

1.3.4. Model za primanje odgovora na informacije:

nacionalni član prima odgovor nadležnog nacionalnog tijela.

1.3.5. Model za slanje informacija:

nadležno nacionalno tijelo šalje nacionalnom članu informacije.

1.3.6. Model za primanje informacija:

nacionalni član prima informacije.

1.3.7. Model za odgovaranje na informacije:

nacionalni član odgovara na primljene informacije nadležnog nacionalnog tijela.

1.3.8. Model za primanje odgovora na informacije:

nadležno nacionalno tijelo prima odgovor nacionalnog člana.

1.4. *Uloga olakšavanja i potpore na temelju članka 8. stavka 1. Uredbe (EU) 2018/1727*

Napomena: Ako modeli olakšavanja i potpore navedeni u točki 1.5. uključuju razmjenu propisanih obrazaca uspostavljenih pravnim aktima Unije u području pravosudne suradnje u kaznenim stvarima, u modelima se, ako su dostupni, upotrebljavaju relevantni strukturirani prikazi podataka i sheme XML izrađene za te akte, na primjer oni uspostavljeni za potrebe provedbe Uredbe (EU) 2023/2844 ili drugih relevantnih instrumenata.

1.5. *Model zahtjeva za olakšavanje ili potporu*

1.5.1. Model za prijenos zahtjeva za olakšavanje ili potporu:

nacionalno nadležno tijelo svojem nacionalnom članu prenosi zahtjev za olakšavanje ili zahtjev za potporu.

1.5.2. Model za primanje zahtjeva za olakšavanje ili potporu:

nacionalni član prima zahtjev za olakšavanje ili potporu i prosljeđuje ga nacionalnom članu države članice kojoj se upućuje zahtjev izvan JUDEX-a.

1.5.3. Model za prosljeđivanje zahtjeva za olakšavanje ili potporu nadležnom nacionalnom tijelu:

nacionalni član države članice kojoj se upućuje zahtjev šalje zahtjev svojem nadležnom nacionalnom tijelu.

1.5.4. Model za primanje zahtjeva za olakšavanje ili potporu:

nadležno nacionalno tijelo prima zahtjev za olakšavanje ili potporu.

1.5.5. Model za slanje odgovora na zahtjev za olakšavanje ili potporu:

nadležno nacionalno tijelo nacionalnom članu države članice kojoj se upućuje zahtjev šalje odgovor ili informacije o zahtjevu.

1.5.6. Model za primanje odgovora na zahtjev za olakšavanje ili potporu:

nacionalni član od nadležnog nacionalnog tijela prima odgovor na zahtjev za olakšavanje ili zahtjev za potporu ili informacije vezane uz njega i dijeli ih s nacionalnim članom države članice koja upućuje zahtjev izvan JUDEX-a.

1.5.7. Model za odgovaranje na zahtjev za olakšavanje ili potporu:

nacionalni član države članice koja upućuje zahtjev odgovara ili dijeli informacije o zahtjevu za olakšavanje ili potporu koji je uputilo nadležno nacionalno tijelo.

1.5.8. Model za primanje odgovora:

nadležno nacionalno tijelo prima odgovor ili informacije o zahtjevu za olakšavanje ili potporu.

2. **Tehničke specifikacije za sheme podataka**

Tehničke specifikacije koje će služiti kao osnova za razvoj definicija XML sheme (XSD) za digitalizaciju Uredbe (EU) 2018/1727 utvrđene su u točkama 2.1. i 2.2. ovog Priloga. U tim se specifikacijama definiraju glavne komponente i sve druge informacije kako bi se pružio potpun opis u svrhu stvaranja tih shema.

Opis bi trebao biti općenit kako bi omogućio izmjenu i proširenje proizvedenih XSD-ova bez potrebe za bitnim promjenama tih specifikacija.

Specifikacije se primjenjuju na propisane obrasce shema priloženih Uredbi (EU) 2018/1727, sve unaprijed definirane poruke ili poruke za slobodan unos teksta koje se upotrebljavaju u razmjenama na temelju te uredbe.

2.1. *Opća razmatranja*

Za sve sheme primjenjuju se sljedeće odredbe:

2.1.1. Verzije

Dodaje se atribut verzija koji olakšava upravljanje verzijama sheme i omogućuje ažuriranje sheme u budućim izdanjima u skladu s poslovnim zahtjevima. Atribut verzija navodi je li nova verzija povratno kompatibilna pri uvođenju novih značajki ili poboljšanja.

2.1.2. Izjava o shemi i metapodaci

— Ako je primjenjivo, u shemi se koriste relevantni standardi ili rječnici koji se zahtijevaju u sustavu e-CODEX radi interoperabilnosti, a potrebni su za pravilno potvrđivanje valjanosti elemenata i vrsta definiranih u toj shemi. To može uključivati:

  — temeljni rječnik e-pravosuđa EU-a,

  — nekvalificirane vrste podataka,

  — popis oznaka za oznake jezika Europske unije.

— Osim toga, ako je primjenjivo, shema može uključivati relevantne ETSI-jeve norme kako bi se iskoristile njihove definicije.

2.1.3. Napomene i dokumentacija

— **Napomene**: Uz svaki element sheme obično se prilažu napomene. Napomene pružaju ljudima čitljive informacije o elementu i često jasno i sažeto definiraju njegovu svrhu ili uporabu.

2.1.4. Korištenje i prilagodljivost

Shema mora biti u skladu s pravilima utvrđenima u točkama od (a) do (d):

(a) **Modularna struktura**: svaki odjeljak ima posebnu funkciju i može se neovisno ponovno upotrijebiti ili prilagoditi. To će olakšati prilagodbu sheme za različite primjere uporabe.

(b) **Proširenje**: shema je koncipirana kao potpora uključivanju novih elemenata ili atributa ako u budućnosti budu potrebne dodatne informacije. To se postiže neobveznim elementima i sljedovima koji se mogu proširiti bez prekidanja postojećih primjena.

(c) **Prilagodljiva struktura**: shema mora biti osmišljena tako da omogućuje dodavanje ili izmjenu elemenata ili vrsta podataka, prema potrebi. Struktura sheme mora se prilagođavati promjenama zahtjeva bez potrebe za većim preoblikovanjem.

(d) **Neobvezni elementi**: elementi unutar sheme mogu se označiti kao neobvezni, odnosno mogu biti uključeni ili izostavljeni na temelju posebnih okolnosti.

Shema je osmišljena kao potpora prikupljanju strukturiranih podataka za posebne zahtjeve.

2.1.5. Izmjene

Shemu odlikuje fleksibilnost, modularnost i lakoća prilagodbe. Složeni tipovi i neobvezni elementi uključeni su u dizajn tako da funkcioniraju u različitim scenarijima, a da ih je i dalje lako izmijeniti i proširiti.

2.2. *Razmjena strukturiranih podataka*

Strukturirani podaci iz točaka 2.2.1. i 2.2.2. dostavljaju se u skladu s člankom 22.a stavkom 3. Uredbe (EU) 2018/1727. Shema omogućuje i navođenje skupova podataka koje treba izbrisati u budućim ažuriranjima.

2.2.1. Podaci Europskog pravosudnog registra za borbu protiv terorizma

Sljedeće tehničke specifikacije za shemu podataka uspostavljaju strukturirani okvir za izradu sheme u formatu XML.

(a) Odjeljak na najvišoj razini

Ovaj odjeljak na najvišoj razini odgovara informacijama utvrđenima u Prilogu III. Uredbi (EU) 2018/1727, informacijama za Europski pravosudni registar za borbu protiv terorizma (CTR).

(b) Struktura poruke

Struktura podataka CTR-a sastoji se od niza elemenata i uključuje barem sljedeće:

i. informacije za identifikaciju fizičkih osoba:

— prezime,

— imena,

— eventualni pseudonimi,

— datum rođenja,

— mjesto rođenja (grad i zemlja),

— državljanstvo ili državljanstva,

— identifikacijski dokument (vrsta i broj dokumenta),

— spol,

— mjesto boravišta;

ii. informacije za identifikaciju fizičkih osoba:

— naziv poduzeća,

— pravni oblik,

— sjedište;

iii. informacije za identifikaciju fizičkih i pravnih osoba:

— brojevi telefona,

— e-adrese,

— informacije o računima u bankama ili drugim financijskim institucijama,

— status u postupcima;

iv. informacije o kaznenom djelu:

— informacije o pravnim osobama uključenima u pripremu ili počinjenje kaznenog djela terorizma,

— pravna kvalifikacija kaznenog djela na temelju nacionalnog prava,

— primjenjivi oblik teškog kaznenog djela iz popisa u Prilogu I.,

— svaka povezanost s terorističkom skupinom,

— vrsta terorizma, kao što su džihadistički, separatistički, ljevičarski ili desničarski,

— kratak sažetak predmeta;

v. informacije o nacionalnom postupku:

— status takvog postupka,

— nadležni ured javnog tužitelja,

— broj predmeta,

— datum pokretanja službenog sudskog postupka,

— poveznice s drugim relevantnim predmetima;

vi. polje za dodatne informacije (slobodan tekst);

vii. oznaka prethodnog odobrenja.

2.2.2. Podaci preneseni u skladu s člankom 21. Uredbe (EU) 2018/1727

(a) Članak 21. stavak 4. Uredbe (EU) 2018/1727 o osnivanju zajedničkih istražnih timova

i. Odjeljak na najvišoj razini
Ovaj odjeljak na najvišoj razini odgovara informacijama iz članka 21. stavka 4. Uredbe (EU) 2018/1727 o osnivanju zajedničkih istražnih timova.

ii. Struktura poruke
Struktura podataka sastoji se od niza elemenata i uključuje barem sljedeće:

— nacionalno pravosudno tijelo nadležno za kazneni postupak

— nacionalni referentni broj kaznenog postupka

— status kaznenog postupka

— istražena kaznena djela

— druge zemlje uključene u predmet

— Eurojust je već podržao predmet?

— Ako je odgovor potvrdan, koja je Eurojustova identifikacijska oznaka predmeta?

— Ako je odgovor niječan, je li ovo zahtjev za potporu?

— Podupire li Europol predmet?

— Ako je odgovor potvrdan, podupire li ga pomoću operativne radne skupine (OTF) i/ili mrežne aplikacije za sigurnu razmjenu informacija (SIENA)?

— sporazum o zajedničkom istražnom timu:

— uključene zemlje

— stranke zajedničkog istražnog tima (nacionalna tijela zadužena za istrage)

— nacionalni referentni broj kaznenog postupka u nadležnosti zajedničkog istražnog tima

— datum potpisivanja

— trajanje

— istražena kaznena djela

— kratak sažetak predmeta

— glavni osumnjičenici u kaznenom postupku koji pokriva zajednički istražni tim (ime, prezime, datum i mjesto rođenja i eventualno druge relevantne i potrebne kategorije podataka iz Priloga II.)

— rezultati rada zajedničkih istražnih timova:

— poteškoće/kašnjenja u:

— uspostavi zajedničkog istražnog tima

— traženju/razmjeni dokaza unutar zajedničkog istražnog tima

— dogovaranju/provedbi zajedničke strategije kaznenog progona

— dopuštenost/nedopuštenost/evaluacija dokaza zajedničkog istražnog tima u nacionalnim postupcima

— ishod sudskih postupaka (uspješni/neuspješni kazneni progoni i osuđujuće/oslobađajuće presude)

iii. Oznaka prethodnog odobrenja

(b) Članak 21. stavak 5. Uredbe (EU) 2018/1727, ozbiljni složeni predmeti

i. Odjeljak na najvišoj razini

Ovaj odjeljak na najvišoj razini odgovara informacijama utvrđenima u članku 21. stavku 5. Uredbe o Eurojustu, tj. ozbiljnim složenim predmetima.

ii. Struktura poruke

Struktura podataka sastoji se od niza elemenata i uključuje barem sljedeće:

— nacionalno pravosudno tijelo nadležno za kazneni postupak

— nacionalni referentni broj kaznenog postupka

— status kaznenog postupka

— istražena kaznena djela

— druge zemlje uključene u predmet

— Eurojust je već podržao predmet?

— Ako je odgovor potvrdan, koja je Eurojustova identifikacijska oznaka predmeta?

— Ako je odgovor niječan, je li ovo zahtjev za potporu?

— Podupire li Europol predmet?

— Ako je odgovor potvrdan, podupire li ga pomoću operativne radne skupine i/ili SIENA-e?

— primjenjivi oblik teškog kaznenog djela

— uključenost mreže organiziranog kriminala

— vrsta mafije

— prekogranična mreža organiziranog kriminala

— posljedice na razini EU-a

— glavni osumnjičenici u kaznenom postupku (ime, prezime, datum i mjesto rođenja i eventualno druge relevantne i potrebne kategorije podataka iz Priloga II.)

— kratak sažetak predmeta

— druge uključene zemlje

— zemlje s kojima je suradnja već započela

— uključena nadležna tijela u drugoj zemlji

— korišteni instrumenti za pravosudnu suradnju

— broj poslanih/primljenih zahtjeva

— povezane istrage

— zemlje s kojima će se pokrenuti suradnja / moguće pogođene zemlje

— vrsta potrebne suradnje (kao što su izručenje, prikupljanje dokaza, druga suradnja)

— povezane istrage

iii. Oznaka prethodnog odobrenja

(c) Članak 21. stavak 6. točka (a) Uredbe (EU) 2018/1727, sukobi nadležnosti

i. Odjeljak na najvišoj razini

Ovaj odjeljak na najvišoj razini odgovara informacijama iz članka 21. stavka 6. Uredbe (EU) 2018/1727, tj. sukobi nadležnosti.

ii. Struktura poruke

Struktura podataka sastoji se od niza elemenata i uključuje barem sljedeće:

— nacionalno pravosudno tijelo nadležno za kazneni postupak

— nacionalni referentni broj kaznenog postupka

— status kaznenog postupka (npr. istraga, kazneni progon, suđenje)

— istražena kaznena djela

— druge zemlje uključene u predmet

— Eurojust je već podržao predmet?

— Ako je odgovor potvrdan, koja je Eurojustova identifikacijska oznaka predmeta?

— Ako je odgovor niječan, je li ovo zahtjev za potporu?

— Podupire li Europol predmet?

— Ako je odgovor potvrdan, podupire li ga pomoću operativne radne skupine i/ili SIENA-e?

— druge uključene zemlje

— nadležna nacionalna tijela u drugoj zemlji, ako su poznata

— nacionalni referentni broj kaznenog postupka u drugoj zemlji

— faza postupka u drugoj zemlji, ako je poznata

— pozitivni ili negativni sukob

— stvarni ili mogući sukob

— već poduzete koordinacijske aktivnosti (npr. savjetovanja na temelju Okvirne odluke Vijeća 2009/948/PUP ([1]))

— kratak sažetak predmeta

— glavni zajednički osumnjičenici (ime, prezime, datum i mjesto rođenja i eventualno druge relevantne i potrebne kategorije podataka iz Priloga II.)

iii. Oznaka prethodnog odobrenja

(d) Članak 21. stavak 6. točka (b), kontrolirane isporuke

i. Odjeljak na najvišoj razini

Ovaj odjeljak na najvišoj razini odgovara informacijama iz članka 21. stavka 6. točke (b) Uredbe (EU) 2018/1727: kontrolirane isporuke.

ii. Struktura poruke

Struktura podataka sastoji se od niza elemenata i uključuje barem sljedeće:

— nacionalno pravosudno tijelo nadležno za kazneni postupak

— nacionalni referentni broj kaznenog postupka

— status kaznenog postupka (npr. istraga, kazneni progon, suđenje)

— istražena kaznena djela

— druge zemlje uključene u predmet

— Eurojust je već podržao predmet?

— Ako je odgovor potvrdan, koja je Eurojustova identifikacijska oznaka predmeta?

— Ako je odgovor niječan, je li ovo zahtjev za potporu?

— Podupire li Europol predmet?

— Ako je odgovor potvrdan, podupire li ga pomoću operativne radne skupine i/ili SIENA-e?

— druge uključene zemlje

— zemlja podrijetla / tranzita / odredišta

— nadležna nacionalna tijela u drugim zemljama

— povezani ispitni postupci u drugim zemljama

([1]) Okvirna odluka Vijeća 2009/948/PUP od 30. studenoga 2009. o sprečavanju i rješavanju sporova o izvršavanju nadležnosti u kaznenim postupcima (SL L 328, 15.12.2009., str. 42., ELI: http://data.europa.eu/eli/dec_framw/2009/948/oj).

— vrsta isporučene robe (npr. droge i koja vrsta, novac, oružje, cigarete, ostalo)

— status kontrolirane isporuke (npr. planirana, u tijeku, dovršena)

— ishod kontrolirane isporuke, ako je već izvršena

— korišteni instrument za pravosudnu suradnju

— glavni zajednički osumnjičenici (ime, prezime, datum i mjesto rođenja i eventualno druge relevantne i potrebne kategorije podataka iz Priloga II.)

iii. Oznaka prethodnog odobrenja

(e) Članak 21. stavak 6. točka (c) Uredbe (EU) 2018/1727, opetovani problemi s instrumentima pravosudne suradnje

i. Odjeljak na najvišoj razini

Ovaj odjeljak na najvišoj razini odgovara informacijama iz članka 21. stavka 6. točke (c) Uredbe (EU) 2018/1727: opetovani problemi s instrumentima pravosudne suradnje.

ii. Struktura poruke

Struktura podataka sastoji se od niza elemenata i uključuje barem sljedeće:

— nacionalno pravosudno tijelo nadležno za kazneni postupak

— nacionalni referentni broj kaznenog postupka

— status kaznenog postupka (npr. istraga, kazneni progon, suđenje)

— istražena kaznena djela

— druge zemlje uključene u predmet

— Eurojust je već podržao predmet?

— Ako je odgovor potvrdan, koja je Eurojustova identifikacijska oznaka predmeta?

— Ako je odgovor niječan, je li ovo zahtjev za potporu?

— Podupire li Europol predmet?

— Ako je odgovor potvrdan, podupire li ga pomoću operativne radne skupine i/ili SIENA-e?

— druge uključene zemlje

— nadležna nacionalna tijela, ako su poznata

— djelovanje u svojstvu tijela izdavatelja ili izvršitelja

— uključeni instrument pravosudne suradnje (npr. europski uhidbeni nalog, europski istražni nalog, zamrzavanje i oduzimanje)

— konkretni predmetni zahtjev (tj. koja je istražna mjera, koja vrsta zamrzavanja, europski uhidbeni nalog za izvršenje kazne ili za kazneni progon)

— odbijanje ili ponovljena poteškoća

— U slučaju odbijanja, na koji se konkretan razlog poziva?

— kratak opis problema

— druga nacionalna tijela s istim problemom, ako postoje

iii. Oznaka prethodnog odobrenja

2.3. *Oznake prethodnog odobrenja*

Pri razmjeni podataka s Eurojustom putem JUDEX-a nadležna nacionalna tijela navode putem oznaka prethodnog odobrenja daljnje postupanje, pristup i prijenos podataka nakon identifikacije poveznice. U oznakama prethodnog odobrenja navodi se mogu li se i u kojoj mjeri informacije povezane s poveznicom podijeliti s drugim nadležnim nacionalnim tijelima, drugim agencijama i tijelima Unije, trećim zemljama ili međunarodnim organizacijama.

2.4. *Unaprijed definirane poruke*

Unaprijed definirane poruke predstavljaju razmjene utvrđene Uredbom (EU) 2018/1727, ali za koje u pravnom aktu nije predviđen poseban oblik. Njihove vrste i broj određuju se tijekom poslovne i tehničke analize.

Definicije XLM sheme (XSD) za unaprijed definirane poruke koncipirane su tako da osiguraju dosljednost, strukturu i usklađenost s poslovnim potrebama.

Na te sheme primjenjuje se sljedeće:

(a) odjeljak na najvišoj razini u ovoj shemi imenuje se prema posebnoj vrsti poruke koja se definira;

(b) unutar te strukture dodaju se i definiraju polja potrebna za posebnu vrstu poruke, čime se osigurava odgovarajući prikaz podatkovnih elemenata.

2.5. *Poruke za slobodan unos teksta*

Poruke za slobodan unos teksta su prikazi razmjena koje omogućuju nestrukturirani ili djelomično strukturirani sadržaj, čime se omogućuje fleksibilnost uz poštovanje regulatornih i poslovnih zahtjeva. XSD za poruke za slobodan unos teksta osmišljen je tako da se osigura dosljednost i pravilno formatiranje.

Na te sheme primjenjuje se sljedeće:

(a) odjeljak na najvišoj razini u ovoj shemi imenuje se prema posebnoj vrsti poruke za slobodan unos teksta koja se definira;

(b) shemom se definira struktura poruke za slobodan unos teksta, čime se, prema potrebi, omogućuje ispravan redoslijed elemenata;

(c) unutar te strukture dodaju se i definiraju polja potrebna za posebnu vrstu poruke za slobodan unos teksta, čime se osigurava odgovarajući prikaz podatkovnih elemenata.

PRILOG III.

TEHNIČKE SPECIFIKACIJE OTISAKA PRSTIJU I FOTOGRAFIJA

Poruke koje se razmjenjuju putem decentraliziranog IT sustava mogu biti popraćene prilozima, uključujući datoteke Nacionalnog instituta za norme i tehnologiju („NIST”) koje sadržavaju otiske prstiju i fotografije, u skladu s tehničkim specifikacijama utvrđenima u točkama 1. i 2.

1. **Otisci prstiju**

Otisci prstiju koji se mogu podijeliti s Eurojustom u svrhu pouzdane identifikacije pojedinaca u kaznenom postupku povezanom s kaznenim djelima terorizma, moraju ispunjavati sljedeće uvjete:

(a) otisci prstiju navode se u jednoj datoteci koja sadržava digitalne slike otisaka prstiju (datoteka NIST s otiscima prstiju) i šalju se u skladu s normom ANSI/NIST-ITL 1-2011, verzijom 2015. (ili novijom verzijom);

(b) datoteka NIST-a s otiscima prstiju sastoji se od najviše deset pojedinačnih otisaka prstiju: valjanih otisaka prstiju, ravnih otisaka prstiju ili oboje;

(c) svi otisci prstiju označeni su;

(d) otisci prstiju bilježe se izravnim skeniranjem ili pomoću tinte na papiru, pod uvjetom da su otisci prstiju otisnuti tintom na papiru skenirani u odgovarajućoj rezoluciji i iste kvalitete;

(e) datoteka NIST-a s otiscima prstiju omogućuje uključivanje dodatnih informacija kao što su uvjeti registracije otisaka prstiju i metoda korištena za dobivanje pojedinačnih slika otisaka prstiju;

(f) otisci prstiju imaju nominalnu razlučivost od 500 ili 1 000 ppi ([1]) (uz prihvatljivo odstupanje od +/– 10 ppi) s 256 razina sive boje;

(g) algoritam za kompresiju otisaka prstiju koji će se upotrebljavati u skladu je s preporukama Nacionalnog instituta za norme i tehnologiju (NIST). Podaci o otiscima prstiju razlučivosti od 500 ppi komprimiraju se pomoću algoritma WSQ (ISO/IEC 19794-5:2005). Podaci o otiscima prstiju razlučivosti od 1 000 ppi komprimiraju se pomoću norme za komprimiranje JPEG 2000 (ISO/IEC 15444-1) i sustava kodiranja. Ciljni omjer kompresije je 15:1.

2. **Fotografije**

Fotografije koje se mogu podijeliti s Eurojustom u svrhu pouzdane identifikacije pojedinaca u kaznenom postupku povezanom s kaznenim djelima terorizma, moraju ispunjavati sljedeće uvjete:

(a) datoteka fotografije (datoteka NIST-a s fotografijom) sadržava samo jedan prikaz lica, koji se podnosi u skladu s normom ANSI/NIST-ITL 1-2011, verzijom 2015. ili bilo kojom novijom dostupnom verzijom;

(b) fotografije su crno-bijele, u boji ili snimljene u blisko infracrvenom području;

(c) kvaliteta fotografija temelji se na zahtjevima za vrstu frontalnog prikaza u skladu s normom ISO/IEC 19794-5:2011 ili bilo kojom novijom dostupnom verzijom;

(d) datoteka NIST-a s fotografijom omogućuje uključivanje dopunskih informacija, uključujući datum na koji je slika snimljena;

([1]) Pikseli po inču.

(e) fotografije, u formatu portreta, imaju razlučivost od najmanje 600 x 800 piksela do najviše 1 200 x 1 600 piksela;

(f) lice mora na fotografiji zauzimati dovoljnu površinu da između središta svakog oka bude najmanje 120 piksela;

(g) algoritam za kompresiju fotografija koji će se upotrebljavati u skladu je s preporukama Nacionalnog instituta za norme i tehnologiju (NIST). Fotografije se samo jednom komprimiraju pomoću norme za komprimiranje JPG (ISO/IEC 10918) ili JPEG 2000 (ISO/IEC 15444) i sustava kodiranja, pri najvećem dopuštenom omjeru kompresije slike od 20:1.