Uradni list
Evropske unije

SL
Serija L

2025/2447

5.12.2025

IZVEDBENA UREDBA KOMISIJE (EU) 2025/2447

z dne 4. decembra 2025

o določitvi pravil za uporabo Uredbe (EU) 2018/1727 Evropskega parlamenta in Sveta v zvezi s tehničnimi specifikacijami, ukrepi in drugimi zahtevami za vzpostavitev in uporabo decentraliziranega sistema IT za varno obdelavo in sporočanje informacij

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) 2018/1727 Evropskega parlamenta in Sveta z dne 14. novembra 2018 o Agenciji Evropske unije za pravosodno sodelovanje v kazenskih zadevah (Eurojust) ter nadomestitvi in razveljavitvi Sklepa Sveta 2002/187/PNZ ([1]) in zlasti člena 22a(3) ter člena 22b(1), točke (a), (b), (c) in (d), Uredbe,

ob upoštevanju naslednjega:

(1) Uredba (EU) 2018/1727 določa okvir za Eurojustovo novo digitalno notranjo infrastrukturo in vzpostavitev decentraliziranega varnega digitalnega komunikacijskega sistema med pristojnimi nacionalnimi organi držav članic in Eurojustom.

(2) Varna digitalna komunikacija bo potekala prek decentraliziranega sistema IT. Za vzpostavitev decentraliziranega sistema IT je treba opredeliti tehnične specifikacije, ki določajo načine komunikacije, tehnične specifikacije za komunikacijske protokole, tehnične ukrepe, ki zagotavljajo minimalne standarde informacijske varnosti in minimalno varnost, ter minimalne cilje glede razpoložljivosti za izvajanje sistema.

(3) V skladu s členom 22a(1) Uredbe (EU) 2018/1727 bi morali decentralizirani sistem IT sestavljati sistemi IT držav članic ter Eurojusta, pa tudi interoperabilne dostopovne točke e-CODEX, prek katerih bi bili ti sistemi IT med seboj povezani. Tehnične specifikacije in druge zahteve decentraliziranega sistema IT iz te uredbe bi morale upoštevati navedeni okvir.

(4) Točke za dostop do decentraliziranega sistema IT bi morale temeljiti na odobrenih dostopovnih točkah e-CODEX, kot so opredeljene v členu 3(3) Uredbe (EU) 2022/850 Evropskega parlamenta in Sveta ([2]).

(5) Decentralizirani sistem IT se izvaja v okviru širšega decentraliziranega sistema IT, ki temelji na sistemu e-CODEX in se imenuje JUDEX (JUstice Digital Exchange – sistem za digitalno izmenjavo podatkov na področju pravosodja). Zato je treba zagotoviti učinkovito izmenjavo informacij o horizontalnem razvoju.

(6) V skladu s členom 22a(4) Uredbe (EU) 2018/1727 se lahko države članice in Eurojust odločijo, da bodo namesto nacionalnega sistema IT kot zaledni sistem uporabljale referenčno izvedbeno programsko opremo, ki jo je razvila Komisija. Da bi zagotovili interoperabilnost, bi morale za nacionalne sisteme IT in referenčno izvedbeno programsko opremo veljati enake tehnične specifikacije in zahteve.

(7) Podatke v zvezi s terorističnimi kaznivimi dejanji in hudimi oblikami organiziranega kriminala bi bilo treba pošiljati strukturirano, da se izboljšata kakovost in ustreznost informacij ter da se zagotovi učinkovitejše vključevanje informacij v Eurojustov sistem vodenja zadev in izboljša navzkrižno preverjanje z informacijami, že shranjenimi v njem. Za podatke o prstnih odtisih in fotografije, ki se lahko pošljejo Eurojustu za namene identifikacije posameznikov, ki so v kazenskem postopku v zvezi s terorističnimi kaznivimi dejanji, bi bilo treba opredeliti obliko in tehnične standarde za pošiljanje.

([1]) UL L 295, 21.11.2018, str. 138, ELI: http://data.europa.eu/eli/reg/2018/1727/oj.
([2]) Uredba (EU) 2022/850 Evropskega parlamenta in Sveta z dne 30. maja 2022 o računalniško podprtem sistemu za čezmejno elektronsko izmenjavo podatkov na področju pravosodnega sodelovanja v civilnih in kazenskih zadevah (sistem e-CODEX) ter spremembi Uredbe (EU) 2018/1726 (UL L 150, 1.6.2022, str. 1, ELI: http://data.europa.eu/eli/reg/2022/850/oj).

(8) Eurojust lajša in podpira izvrševanje zaprosil za pravosodno sodelovanje in odločitev o njem, tudi zaprosil in odločitev na podlagi pravnih aktov, ki dajejo učinek načelu vzajemnega priznavanja. Pristojni nacionalni organi bi morali imeti možnost, da Eurojust zaprosijo za pomoč in usklajevanje prek decentraliziranega sistema IT.

(9) Za zagotovitev učinkovitosti in doslednosti je pomembno, da so tehnične specifikacije, ki se določijo na podlagi Uredbe (EU) 2018/1727, združljive s tehničnimi specifikacijami, določenimi na podlagi uredb (EU) 2023/2844 ([3]), (EU) 2023/1543 ([4]) in (EU) 2024/3011 ([5]) Evropskega parlamenta in Sveta, ter s prihodnjimi ukrepi digitalizacije, pomembnimi za Eurojustovo pooblastilo za podporo pristojnim nacionalnim organom.

(10) Vsa druga komunikacija med Eurojustom in pristojnimi nacionalnimi organi, kot je sporočanje informacij o rezultatih obdelave informacij, vključno z obstojem povezav z zadevami, ki so že shranjene v sistemu vodenja zadev v skladu s členom 22 Uredbe (EU) 2018/1727, kadar Eurojust deluje na lastno pobudo, ali informacij, poslanih Eurojustu za namene zavarovanja, analiziranja in hranjenja dokazov, povezanih z genocidom, hudodelstvi zoper človečnost, vojnimi zločini in povezanimi kaznivimi dejanji v skladu s členom 4(1), točka (j), navedene uredbe, bi morala biti omogočena tudi prek decentraliziranega sistema IT.

(11) Za zagotovitev, da se v tej uredbi upoštevajo operativne potrebe Eurojusta, je bilo z Eurojustom opravljeno posvetovanje v skladu s členom 22a(3) Uredbe (EU) 2018/1727.

(12) V skladu s členom 4 Protokola št. 21 o stališču Združenega kraljestva in Irske glede območja svobode, varnosti in pravice, ki je priložen Pogodbi o Evropski uniji in Pogodbi o delovanju Evropske unije, je Irska s pismom z dne 9. septembra 2019 podala uradno obvestilo, da sprejme Uredbo (EU) 2018/1727 Evropskega parlamenta in Sveta in da jo ta zavezuje. To sodelovanje je potrjeno s Sklepom Komisije (EU) 2019/2006 ([6]). Uredba (EU) 2023/2131 Evropskega parlamenta in Sveta ([7]) je spremenila Uredbo (EU) 2018/1727, da se omogoči vzpostavitev varnih digitalnih komunikacijskih kanalov med Eurojustom in pristojnimi nacionalnimi organi, ter zagotavlja pravno podlago za to uredbo. Glede na to, da Irska ni podala uradnega obvestila, da želi sodelovati pri sprejetju in uporabi Uredbe (EU) 2023/2131, ter ni podala uradnega obvestila, da želi sprejeti navedeno uredbo in da jo ta zavezuje, Uredba (EU) 2023/2131 v skladu s členoma 1 in 2 ter členom 4a(1) Protokola št. 21 zanjo ni zavezujoča in se v njej ne uporablja. Zato Irska ne sodeluje pri sprejetju te uredbe.

(13) V skladu s členoma 1 in 2 Protokola št. 22 o stališču Danske, ki je priložen Pogodbi o Evropski uniji in Pogodbi o delovanju Evropske unije, Danska ni sodelovala pri sprejetju Uredbe (EU) 2018/1727. Ta uredba za Dansko zato ni zavezujoča in se v njej ne uporablja.

([3]) Uredba (EU) 2023/2844 Evropskega parlamenta in Sveta z dne 13. decembra 2023 o digitalizaciji pravosodnega sodelovanja in dostopa do sodnega varstva v čezmejnih civilnih, gospodarskih in kazenskih zadevah ter o spremembi nekaterih aktov s področja pravosodnega sodelovanja (UL L, 2023/2844, 27.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2844/oj).

([4]) Uredba (EU) 2023/1543 Evropskega parlamenta in Sveta z dne 12. julija 2023 o evropskem nalogu za posredovanje in evropskem nalogu za zavarovanje elektronskih dokazov v kazenskih postopkih ter za izvrševanje zapornih kazni po kazenskem postopku (UL L 191, 28.7.2023, str. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

([5]) Uredba (EU) 2024/3011 Evropskega parlamenta in Sveta z dne 27. novembra 2024 o prenosu postopkov v kazenskih zadevah (UL L, 2024/3011, 18.12.2024, ELI: http://data.europa.eu/eli/reg/2024/3011/oj).

([6]) Sklep Komisije (EU) 2019/2006 z dne 29. novembra 2019 o sodelovanju Irske pri Uredbi (EU) 2018/1727 Evropskega parlamenta in Sveta o Agenciji Evropske unije za pravosodno sodelovanje v kazenskih zadevah (Eurojust) (UL L 310, 2.12.2019, str. 59, ELI: http://data.europa.eu/eli/dec/2019/2006/oj).

([7]) UREDBA (EU) 2023/2131 Evropskega parlamenta in Sveta z dne 4. oktobra 2023 o spremembi Uredbe (EU) 2018/1727 Evropskega parlamenta in Sveta ter Sklepa Sveta 2005/671/PNZ v zvezi z digitalno izmenjavo informacij v primerih terorizma (UL L, 2023/2131, 11.10.2023, ELI: http://data.europa.eu/eli/reg/2023/2131/oj).

(14) V skladu s členom 42(1) Uredbe (EU) 2018/1725 Evropskega parlamenta in Sveta ([8]) je bilo opravljeno posvetovanje z Evropskim nadzornikom za varstvo podatkov, ki je mnenje podal 21. oktobra 2025.

(15) Ukrepi iz te uredbe so v skladu z mnenjem odbora, ustanovljenega na podlagi člena 22c Uredbe (EU) 2018/1727 –

SPREJELA NASLEDNJO UREDBO:

Člen 1

Tehnične specifikacije decentraliziranega sistema IT

Tehnične specifikacije, ukrepi in cilji decentraliziranega sistema IT iz člena 22b(1), točke (a), (b), (c) in (d), Uredbe (EU) 2018/1727 so določeni v Prilogi I k tej uredbi.

Člen 2

Digitalni postopkovni standardi

Digitalni postopkovni standardi, ki se uporabljajo za elektronsko komunikacijo prek decentraliziranega sistema IT iz člena 22a(3) Uredbe (EU) 2018/1727, so določeni v Prilogi II k tej uredbi.

Člen 3

Tehnične specifikacije za prenos prstnih odtisov in fotografij

Tehnične specifikacije in format za prenos prstnih odtisov in fotografij iz člena 22a(3) Uredbe (EU) 2018/1727, so določeni v Prilogi III k tej uredbi.

Člen 4

Začetek veljavnosti

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v državah članicah v skladu s Pogodbama.

V Bruslju, 4. decembra 2025

Za Komisijo
predsednica
Ursula VON DER LEYEN

([8]) Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

PRILOGA I

TEHNIČNE SPECIFIKACIJE, UKREPI IN CILJI DECENTRALIZIRANEGA SISTEMA IT

1. **Uvod in področje uporabe**

Ta priloga določa tehnične specifikacije, ukrepe in cilje decentraliziranega sistema IT za izmenjavo informacij na podlagi Uredbe (EU) 2018/1727.

Decentralizirana narava sistema IT omogoča neposredno in varno izmenjavo podatkov med pristojnimi nacionalnimi organi in Eurojustom.

2. **Opredelitev pojmov**

V tej prilogi se uporabljajo naslednje opredelitve pojmov:

2.1. „Hypertext Transport Protocol Secure“ ali „HTTPS“ pomeni kanale za šifrirano komunikacijo in varno povezavo;

2.2. „nezatajljivost porekla“ pomeni ukrepe za zagotavljanje dokazov o celovitosti in dokazov o poreklu podatkov z metodami, kot so digitalno certificiranje, infrastruktura javnih ključev ter elektronski podpisi in elektronski žigi;

2.3. „nezatajljivost prejema“ pomeni ukrepe za zagotavljanje dokazov o prejemu podatkov s strani predvidenega prejemnika podatkov subjektu izvora podatkov z metodami, kot so digitalno certificiranje, infrastruktura javnih ključev, elektronski podpisi in elektronski žigi;

2.4. „SOAP“ (Simple Object Access Protocol) pomeni, v skladu s standardi Konzorcija za svetovni splet, specifikacijo protokola sporočanja za izmenjavo strukturiranih informacij pri izvajanju spletnih storitev v računalniških omrežjih;

2.5. „REST“ (Representational State Transfer) pomeni način arhitekture za oblikovanje omrežnih aplikacij, ki temelji na komunikacijskem modelu odjemalec-strežnik brez stanja in uporablja standardne metode za izvajanje operacij na virih, ki so običajno predstavljeni v strukturiranih oblikah;

2.6. „spletna storitev“ pomeni sistem programske opreme, ki je zasnovan za podpiranje interoperabilne interakcije med strojno opremo znotraj mreže in ima vmesnik, opisan v obliki, primerni za strojno obdelavo;

2.7. „izmenjava podatkov“ pomeni izmenjavo sporočil in dokumentov prek decentraliziranega sistema IT;

2.8. „e-CODEX“ pomeni sistem e-CODEX, kot je opredeljen v členu 3(1) Uredbe (EU) 2022/850;

2.9. „osnovno besedišče e-pravosodja EU“ pomeni osnovno besedišče e-pravosodja EU, kot je opredeljeno v točki 4 Priloge k Uredbi (EU) 2022/850;

2.10. „ebMS“ pomeni storitev sporočanja ebXML, ki je protokol sporočanja, razvit v okviru OASIS, ki omogoča varno, zanesljivo in interoperabilno izmenjavo elektronskih poslovnih dokumentov z uporabo SOAP. Podpira povezovanje med podjetji po različnih sistemih;

2.11. „AS4“ pomeni komunikacijski protokol Applicability Statement 4, ki je standard organizacije OASIS, ki profilira ebMS 3.0; poenostavlja varno in interoperabilno sporočanje med podjetji z uporabo odprtih standardov, kot sta SOAP in WS-Security;

2.12. „ciljni čas ponovne vzpostavitve delovanja“ pomeni najdaljši sprejemljiv čas za ponovno vzpostavitev storitve po incidentu;

2.13. „ciljna točka ponovne vzpostavitve delovanja“ pomeni največjo sprejemljivo količino izgube podatkov v primeru izpada delovanja.

3. **Načini komunikacije z elektronskimi sredstvi**

3.1. Decentralizirani sistem IT za izmenjavo sporočil in dokumentov uporablja načine komunikacije, ki temeljijo na storitvah, kot so spletne storitve ali druge večkratno uporabne komponente in programske rešitve.

3.2. Natančneje, decentralizirani sistem IT vključuje komunikacijo prek dostopovnih točk e-CODEX, kot so določene v členu 5(2) Uredbe (EU) 2022/850. Zato za zagotovitev učinkovite in interoperabilne čezmejne izmenjave podatkov decentralizirani sistem IT podpira komunikacijo prek sistema e-CODEX.

4. **Komunikacijski protokoli**

4.1. Decentralizirani sistem IT uporablja varne internetne protokole za:

(a) komunikacijo v okviru decentraliziranega sistema IT med pristojnimi organi in Eurojustom;

(b) komunikacijo s pristojnim organom / podatkovno zbirko sodišč iz točke 7.1.

4.2. Kar zadeva opredelitev in prenos strukturiranih podatkov in metapodatkov, komponente decentraliziranega sistema IT temeljijo na celovitih in splošno sprejetih standardih in protokolih, kot sta SOAP in REST.

4.3. Kar zadeva protokole za promet in pošiljanje sporočil, decentralizirani sistem IT temelji na varnih protokolih, ki temeljijo na standardih, kot so:

(a) profil AS4 za čezmejno izmenjavo podatkov, ki zagotavlja varno in zanesljivo pošiljanje sporočil s šifriranjem in nezatajljivostjo;

(b) HTTPS/RESTful vmesniki API za komunikacijo, ki podpira formata JSON in XML;

(c) SOAP za interakcije z visoko zanesljivostjo, ki vključuje protokol WS-Security za avtentikacijo in šifriranje.

4.4. Za namene nemotene in interoperabilne izmenjave podatkov komunikacijski protokoli, ki jih uporablja decentralizirani sistem IT, ustrezajo zadevnim standardom interoperabilnosti.

4.5. Po potrebi sheme XML uporabljajo ustrezne standarde ali besedišča, ki so potrebni za ustrezno validacijo elementov in tipov, opredeljenih v tej shemi. Ti standardi ali besedišča lahko vključujejo:

(a) osnovno besedišče e-pravosodja EU;

(b) nekvalificirane vrste podatkov;

(c) šifrant jezikovnih oznak Evropske unije.

4.6. Za varnostne in avtentikacijske protokole decentralizirani sistem IT temelji na varnih protokolih, ki temeljijo na standardih, kot so:

(a) TLS (varnost transportne plasti) za šifrirano in avtenticirano komunikacijo prek omrežij, ki podpira vzajemno avtentikacijo prek digitalnih potrdil X.509;

(b) OAuth/OpenID Connect (OIDC) za varno avtentikacijo in avtorizacijo;

(c) PKI (infrastruktura javnih ključev) in digitalni podpisi za varno izmenjavo ključev in preverjanje celovitosti sporočil z uporabo digitalnih potrdil (X.509), ki jih izdajo certifikacijski organi.

5. **Cilji informacijske varnosti in zadevni tehnični ukrepi**

5.1. Za izmenjavo informacij prek decentraliziranega sistema IT tehnični ukrepi za zagotavljanje minimalnih varnostnih standardov informacijske tehnologije vključujejo naslednje:

(a) ukrepe za zagotavljanje zaupnosti informacij, tudi z uporabo varnih komunikacijskih kanalov;

(b) ukrepe za zagotavljanje celovitosti podatkov v mirovanju in med prenosom;

(c) ukrepe za zagotavljanje nezatajljivosti porekla pošiljatelja informacij znotraj decentraliziranega sistema IT in nezatajljivosti prejema informacij;

(d) ukrepe za zagotavljanje beleženja varnostnih dogodkov v skladu s priznanimi mednarodnimi priporočili za varnostne standarde informacijske tehnologije ([1]);

(e) ukrepe za zagotavljanje avtentikacije in avtorizacije uporabnikov ter ukrepe za preverjanje identitete sistemov, povezanih z decentraliziranim sistemom IT.

5.2. Komponente decentraliziranega sistema IT zagotavljajo varno komunikacijo in prenos podatkov z uporabo šifriranja, infrastrukture javnih ključev z digitalnimi potrdili za avtentikacijo in varno izmenjavo ključev ter protokolov za varno pošiljanje sporočil, kot so AS4 (ebMS), RESTful vmesniki API in SOAP, da se ohranita zaupnost in celovitost sporočil.

5.3. Kadar se v okviru decentraliziranega sistema IT uporablja TLS, se uporabi najnovejša stabilna različica protokola, če to ni mogoče, pa različica brez znanih varnostnih ranljivosti. Dovoljene so samo dolžine ključev, ki zagotavljajo ustrezno raven kriptografske varnosti, nabori algoritmov, za katere je znano, da so nezanesljivi ali zastareli, pa se ne smejo uporabljati.

5.4. Kolikor je mogoče, digitalna potrdila PKI, ki se uporabljajo za namene delovanja decentraliziranega sistema IT, izdajajo certifikacijski organi, priznani kot ponudniki kvalificiranih storitev zaupanja v skladu z Uredbo (EU) št. 910/2014 Evropskega parlamenta in Sveta ([2]). Izvajajo se ukrepi za zagotovitev, da se taka potrdila uporabljajo izključno za predvidene namene, na ustrezni ravni zaupanja in v skladu z veljavnimi zahtevami iz Uredbe (EU) št. 910/2014.

5.5. Komponente decentraliziranega sistema IT se razvijejo v skladu z načelom vgrajenega in privzetega varstva podatkov, za zagotovitev visoke ravni kibernetske varnosti pa se izvajajo ustrezni upravni, organizacijski in tehnični ukrepi.

5.6. Komisija oblikuje, razvija in vzdržuje referenčno izvedbeno programsko opremo v skladu z zahtevami in načeli varstva podatkov iz Uredbe (EU) 2018/1725. Referenčna izvedbena programska oprema, ki jo zagotovi Komisija, državam članicam omogoča, da izpolnijo svoje obveznosti v skladu z Uredbo (EU) 2016/679 ([3]) oziroma Direktivo (EU) 2016/680.

([1]) Brez poseganja v beleženje za varnostne namene mehanizmi beleženja, ki jih uporabljajo komponente decentraliziranega sistema IT, kot je ustrezno, omogočajo zagotavljanje skladnosti z zahtevami iz člena 88 Uredbe (EU) 2018/1725 in po potrebi člena 25 Direktive (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (UL L 119, 4.5.2016, str. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

([2]) Uredba (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES (UL L 257, 28.8.2014, str. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([3]) Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

5.7. Države članice, ki uporabljajo nacionalni zaledni sistem, ki ni referenčna izvedbena programska oprema, izvedejo potrebne ukrepe za zagotovitev, da je njihov nacionalni zaledni sistem skladen z zahtevami iz Uredbe (EU) 2016/679 oziroma Direktive (EU) 2016/680.

5.8. Eurojust izvede potrebne ukrepe za zagotovitev, da je njegov zaledni sistem ali primerek referenčne izvedbene programske opreme, ki jo uvaja, skladen z zahtevami iz uredb (EU) 2018/1725 in (EU) 2018/1727.

5.9. Države članice in Eurojust vzpostavijo zanesljive mehanizme za odkrivanje groženj in odzivanje na incidente, da bi za informacijske sisteme v njihovi pristojnosti, ki so del decentraliziranega sistema IT, v skladu s svojimi ustreznimi politikami zagotovili pravočasno prepoznavanje, blažitev in ponovno vzpostavitev delovanja po varnostnih incidentih.

6. **Minimalni cilji glede razpoložljivosti**

6.1. Eurojust in države članice zagotovijo, da so komponente decentraliziranega sistema IT v njihovi pristojnosti na voljo ves čas, vse dni v tednu, pri čemer je ciljna stopnja tehnične razpoložljivosti sistema vsaj 98 % na letni ravni, brez načrtovanega vzdrževanja.

6.2. Komisija zagotovi razpoložljivost podatkovne zbirke sodišč ves čas, vse dni v tednu, pri čemer je ciljna stopnja tehnične razpoložljivosti več kot 99 % na letni ravni, brez načrtovanega vzdrževanja.

6.3. Kolikor je mogoče, se vzdrževalna dela ob delovnih dneh načrtujejo med 20:00 in 7:00 po srednjeevropskem času.

6.4. Države članice obvestijo Komisijo, Eurojust in druge države članice o dejavnostih vzdrževanja, kot sledi:

(a) 5 delovnih dni vnaprej za vzdrževalna dela, ki lahko povzročijo nedostopnost do 4 ure;

(b) 10 delovnih dni vnaprej za vzdrževalna dela, ki lahko povzročijo nedostopnost med 4 in 12 ur;

(c) 30 delovnih dni vnaprej za vzdrževalna dela, ki lahko povzročijo nedostopnost nad 12 ur.

6.5. Kadar imajo države članice določena redna obdobja vzdrževanja, Komisijo, Eurojust in druge države članice obvestijo o času in dnevih, ko se načrtujejo taka določena redna obdobja. Države članice se lahko z odstopanjem od obveznosti iz prvega stavka odločijo, da ne bodo obvestile Komisije o vsakem posameznem primeru nedostopnosti komponent decentraliziranega sistema IT, za katere so odgovorne, v takem določenem rednem obdobju.

6.6. Države članice v primeru nepričakovane tehnične okvare komponent decentraliziranega sistema IT, za katere so odgovorne, o njej nemudoma obvestijo Komisijo in druge države članice ter jih obvestijo tudi o predvidenem času, potrebnem za ponovno vzpostavitev delovanja, če je znan.

6.7. Eurojust obvesti Komisijo in druge države članice o dejavnostih vzdrževanja, kot sledi:

(a) 5 delovnih dni vnaprej za vzdrževalna dela, ki lahko povzročijo nedostopnost do 4 ure;

(b) 10 delovnih dni vnaprej za vzdrževalna dela, ki lahko povzročijo nedostopnost med 4 in 12 ur;

(c) 30 delovnih dni vnaprej za vzdrževalna dela, ki lahko povzročijo nedostopnost nad 12 ur.

6.8. Kadar ima Eurojust določena redna obdobja vzdrževanja, Komisijo, Eurojust in države članice obvesti o času in dnevih, ko se načrtujejo taka določena redna obdobja. Eurojust se lahko z odstopanjem od obveznosti iz prvega stavka odloči, da ne bo obvestil Komisije o vsakem posameznem primeru nedostopnosti komponent decentraliziranega sistema IT, za katere je odgovoren, v takem določenem rednem obdobju.

6.9. Eurojust v primeru nepričakovane tehnične okvare komponent decentraliziranega sistema IT, za katere je odgovoren, o njej nemudoma obvesti Komisijo in države članice ter jih obvesti tudi o predvidenem času, potrebnem za ponovno vzpostavitev delovanja, če je znan.

6.10. Komisija v primeru nepričakovane tehnične okvare podatkovne zbirke pristojnih organov/sodišč nemudoma obvesti Eurojust in države članice o tej nerazpoložljivosti in o predvidenem času, potrebnem za ponovno vzpostavitev delovanja, če je znan.

6.11. Države članice in Eurojust v primeru motenj v storitvah hitro poskrbijo za ponovno vzpostavitev delovanja storitev ter minimalno izgubo podatkov v skladu s ciljnim časom ponovne vzpostavitve delovanja in ciljno točko ponovne vzpostavitve delovanja.

6.12. Države članice in Eurojust izvedejo ustrezne ukrepe za doseganje zgoraj navedenih ciljev glede razpoložljivosti in vzpostavijo postopke za učinkovito odzivanje na incidente.

7. **Podatkovna zbirka pristojnih organov/sodišč (CDB)**

7.1. V skladu s členom 22a Uredbe (EU) 2018/1727 decentralizirani sistem IT omogoča elektronsko komunikacijo med pristojnimi nacionalnimi organi in Eurojustom. Glede na obveznosti izmenjave informacij med pristojnimi nacionalnimi organi in Eurojustom na podlagi členov 21, 21a in 22, pa tudi vlogo Eurojusta pri lajšanju in podpiranju izdajanja in izvrševanja zaprosil za medsebojno pravno pomoč ali vzajemno priznavanje v skladu s členom 8(1) Uredbe (EU) 2018/1727, morajo biti zadevni pristojni organi pri uporabi decentraliziranega sistema IT jasno določljivi. Zato je bistveno, da se za namene decentraliziranega sistema IT vzpostavi verodostojna podatkovna zbirka informacij o teh organih.

7.2. CDB vključuje naslednje informacije v strukturirani obliki:

(a) za namene členov 8(1), 8(3), 8(4), 21, 21a in 22 Uredbe (EU) 2018/1727 informacije o pristojnih nacionalnih organih, vključno z nacionalnimi korespondenti, kot je določeno v členu 20 navedene uredbe, in nacionalnih članih v skladu s členom 7 ([4]) navedene uredbe;

(b) po potrebi informacije, potrebne za določitev geografskih območij ali vsebinskih področij, za katera so pristojni organi pristojni, ali druga ustrezna merila, potrebna za določitev njihove pristojnosti;

(c) informacije, potrebne za pravilno tehnično usmerjanje sporočil v okviru decentraliziranega sistema IT.

7.3. Komisija je odgovorna za razvoj, vzdrževanje in delovanje CDB ter za podporo zanjo.

7.4. CDB državam članicam in Eurojustu omogoča posodabljanje informacij v njej, pristojnim nacionalnim organom in nacionalnim članom, ki sodelujejo v decentraliziranem sistemu IT, pa programski dostop do informacij v njej in njihovo pridobitev.

7.5. Dostop do CDB je mogoč prek skupnega komunikacijskega protokola, ne glede na to, ali pristojni organi, povezani z decentraliziranim sistemom IT, uporabljajo nacionalni zaledni sistem ali referenčno izvedbeno programsko opremo.

7.6. Države članice zagotovijo, da so informacije o njihovih pristojnih organih, ki so vključene v CDB, kot je določeno v točki 7.2, popolne, točne in posodobljene.

([4]) To ne posega v prenos pooblastil za nacionalnega člana na njegovega namestnika, drugo osebje nacionalnega urada ali pooblaščeno osebje Eurojusta.

PRILOGA II

DIGITALNI POSTOPKOVNI STANDARDI

V členu 3(9) Uredbe (EU) 2022/850 so digitalni postopkovni standardi opredeljeni kot tehnične specifikacije za modele poslovnih procesov in podatkovne sheme, ki določajo elektronsko strukturo podatkov, izmenjanih prek sistema e-CODEX.

V tej prilogi so določene tehnične specifikacije za modele poslovnih procesov in tehnične specifikacije za podatkovne sheme.

1. **Tehnične specifikacije za modele poslovnih procesov v skladu z Uredbo (EU) 2018/1727**

Tehnične specifikacije za modele poslovnih procesov so določene v točkah 1.1 do 1.5. V njih so opredeljeni ključni vidiki, potrebni za omogočanje elektronske komunikacije za namene Uredbe (EU) 2018/1727 prek decentraliziranega sistema IT.

Decentralizirani sistem IT omogoča izmenjavo informacij samo med pristojnimi nacionalnimi organi države članice in nacionalnim članom iz te države članice.

1.1. *Izmenjava informacij v zvezi z evropsko pravosodno protiteroristično evidenco (CTR), člen 21a Uredbe (EU) 2018/1727*

1.1.1. Model za pošiljanje podatkov CTR:

pristojni nacionalni organ pošlje podatke o postopkih v zvezi s terorizmom za CTR nacionalnemu članu.

1.1.2. Model za prejemanje podatkov CTR:

nacionalni član prejme podatke CTR.

1.1.3. Model za zaprosilo za soglasje:

nacionalni član zaprosi za soglasje svoj pristojni nacionalni organ.

1.1.4. Model za prejetje zaprosila za soglasje:

pristojni nacionalni organ prejme zaprosilo za soglasje.

1.1.5. Model za pošiljanje odgovora na zaprosilo za soglasje:

pristojni nacionalni organ pošlje odgovor na zaprosilo za soglasje.

1.1.6. Model za prejetje odgovora na zaprosilo za soglasje:

nacionalni član prejme odgovor na zaprosilo za soglasje.

1.1.7. Model za obveščanje o povezavi:

nacionalni član obvesti pristojni nacionalni organ o povezavi z drugo zadevo.

1.1.8. Model za posodabljanje podatkov CTR:

pristojni nacionalni organ pošlje podatke, ki jih je treba posodobiti ali izbrisati, svojemu nacionalnemu članu.

1.1.9. Model za prejemanje posodobljenih podatkov CTR:

nacionalni član prejme podatke CTR, ki jih je treba posodobiti ali izbrisati.

1.2. *Izmenjava informacij v zvezi s hudimi kaznivimi dejanji, člen 21 Uredbe (EU) 2018/1727*

1.2.1. Model za pošiljanje podatkov o hudih čezmejnih kaznivih dejanjih:

pristojni nacionalni organ pošlje podatke o hudih čezmejnih kaznivih dejanjih Eurojustu.

1.2.2. Model za prejemanje podatkov o hudih čezmejnih kaznivih dejanjih:

nacionalni član prejme podatke o hudih čezmejnih kaznivih dejanjih.

1.2.3. Model za zaprosilo za soglasje:

nacionalni član zaprosi za soglasje svoj pristojni nacionalni organ.

1.2.4. Model za prejetje zaprosila za soglasje:

pristojni nacionalni organ prejme zaprosilo za soglasje.

1.2.5. Model za pošiljanje odgovora na zaprosilo za soglasje:

pristojni nacionalni organ pošlje odgovor na zaprosilo za soglasje.

1.2.6. Model za prejetje odgovora na zaprosilo za soglasje:

nacionalni član prejme odgovor na zaprosilo za soglasje.

1.2.7. Model za obveščanje o povezavi:

nacionalni član obvesti pristojni nacionalni organ o povezavi z drugo zadevo.

1.2.8. Model za posodabljanje podatkov o hudih čezmejnih kaznivih dejanjih:

pristojni nacionalni organ pošlje podatke, ki jih je treba posodobiti ali izbrisati, svojemu nacionalnemu članu.

1.2.9. Model za prejemanje posodobljenih podatkov o hudih čezmejnih kaznivih dejanjih:

nacionalni član prejme podatke o hudih čezmejnih kaznivih dejanjih, ki jih je treba posodobiti ali izbrisati.

1.3. *Izmenjava splošnih informacij*

1.3.1. Model za pošiljanje informacij:

nacionalni član pošlje informacije pristojnemu nacionalnemu organu ali obratno.

1.3.2. Model za prejemanje informacij:

pristojni nacionalni organ ali nacionalni član prejme informacije.

1.3.3. Model za odzivanje na informacije:

pristojni nacionalni organ se odzove na informacije, prejete od nacionalnega člana, ali obratno.

1.3.4. Model za prejetje odziva na informacije:

nacionalni član prejme odziv pristojnega nacionalnega organa.

1.3.5. Model za pošiljanje informacij:

pristojni nacionalni organ pošlje informacije nacionalnemu članu.

1.3.6. Model za prejemanje informacij:

nacionalni član prejme informacije.

1.3.7. Model za odzivanje na informacije:

nacionalni član se odzove na informacije, prejete od pristojnega nacionalnega organa.

1.3.8. Model za prejetje odziva:

pristojni nacionalni organ prejme odziv nacionalnega člana.

1.4. *Vloga pri lajšanju in podpori, člen 8(1) Uredbe (EU) 2018/1727*

Opomba: Kadar modeli za lajšanje in podporo iz točke 1.5 vključujejo izmenjavo predpisanih obrazcev, določenih s pravnimi akti Unije s področja pravosodnega sodelovanja v kazenskih zadevah, se v modelih, kadar je ustrezno, uporabijo ustrezne strukturirane predstavitve podatkov in sheme XML, razvite za zadevne akte, na primer kot so vzpostavljene za namene Izvedbene uredbe (EU) 2023/2844 ali drugih ustreznih instrumentov.

1.5. *Model za zaprosilo za lajšanje ali podporo*

1.5.1. Model za pošiljanje prošenj za lajšanje ali podporo:

pristojni nacionalni organ pošlje zaprosilo za lajšanje ali podporo svojemu nacionalnemu članu.

1.5.2. Model za prejetje zaprosila za lajšanje ali podporo:

nacionalni član prejme zaprosilo za lajšanje ali podporo in jo posreduje nacionalnemu članu zaprošene države članice zunaj sistema JUDEX.

1.5.3. Model za posredovanje zaprosila za lajšanje ali podporo pristojnemu nacionalnemu organu:

nacionalni član zaprošene države članice pošlje zaprosilo svojemu pristojnemu nacionalnemu organu.

1.5.4. Model za prejetje zaprosila za lajšanje ali podporo:

pristojni nacionalni organ prejme zaprosilo za lajšanje ali podporo.

1.5.5. Model za pošiljanje odziva na zaprosilo za lajšanje ali podporo:

pristojni nacionalni organ pošlje odziv na zaprosilo ali pošlje informacije v zvezi z njim nacionalnemu članu zaprošene države članice.

1.5.6. Model za prejetje odziva na zaprosilo za lajšanje ali podporo:

nacionalni član prejme odziv na zaprosilo za lajšanje ali podporo oziroma informacije v zvezi z njim od pristojnega nacionalnega organa in jih deli z nacionalnim članom države članice prosilke zunaj sistema JUDEX.

1.5.7. Model za odzivanje na prošnjo za lajšanje ali podporo:

nacionalni član države članice prosilke se odzove na zaprosilo pristojnega nacionalnega organa za lajšanje ali podporo ali deli informacije v zvezi z njim.

1.5.8. Model za prejetje odziva:

pristojni nacionalni organ prejme odziv na zaprosilo za lajšanje ali podporo ali informacije v zvezi z njim.

2. **Tehnične specifikacije za podatkovne sheme**

Tehnične specifikacije, ki bodo služile kot podlaga za razvoj opredelitev sheme XML (XSD) za digitalizacijo iz Uredbe (EU) 2018/1727, so določene v točkah 2.1 in 2.2 te priloge. Te specifikacije opredeljujejo ključne sestavne dele in vse druge informacije, da se zagotovi celovit opis za izdelavo teh shem.

Opis je namerno generičen, da omogoča spremembe in razširitve izdelanih XSD, ne da bi bile potrebne bistvene spremembe teh specifikacij.

Te specifikacije se uporabljajo za predpisani obrazec shem, kot je priložen Uredbi (EU) 2018/1727, ter za morebitna vnaprej določena sporočila ali sporočila s poljubnim besedilom, ki se uporabljajo pri izmenjavah na podlagi navedene uredbe.

2.1. *Splošne ugotovitve*

Za vse sheme, ki jih je treba zagotoviti, se uporabljajo naslednje določbe:

2.1.1. Upravljanje različic

Vključi se atribut za različice, ki olajšuje upravljanje različic sheme in omogoča posodobitev sheme v prihodnjih različicah v skladu s poslovnimi zahtevami. Atribut za različice označuje, ali je nova različica ob uvedbi novih lastnosti ali izboljšav združljiva s predhodnimi različicami.

2.1.2. Opredelitev sheme in metapodatki

— Po potrebi shema uporablja ustrezne standarde ali besedišča, ki jih e-CODEX potrebuje za interoperabilnost in so potrebni za ustrezno validacijo elementov in tipov, opredeljenih v tej shemi. To lahko vključuje:

  — osnovno besedišče e-pravosodja EU,

  — nekvalificirane vrste podatkov,

  — šifrant jezikovnih oznak Evropske unije.

— Poleg tega lahko po potrebi shema vključuje ustrezne standarde ETSI za uporabo njihovih opredelitev.

2.1.3. Opombe in dokumentacija

— **Opombe**: vsak element sheme je običajno opremljen z opombami. Opombe zagotavljajo človeku berljive informacije o elementu ter pogosto jasno in jedrnato opredeljujejo njegov namen ali uporabo.

2.1.4. Uporaba in prilagodljivost

Shema je v skladu s pravili iz točk (a) do (d):

(a) **Modularna struktura**: vsak oddelek je zasnovan s posebno funkcionalnostjo in se lahko samostojno ponovno uporabi ali prilagodi. To omogoča enostavno prilagajanje sheme različnim primerom uporabe.

(b) **Razširljivost**: shema je zasnovana tako, da podpira vključitev novih elementov ali atributov, če bodo v prihodnosti potrebne dodatne informacije. To se doseže z uporabo neobveznih elementov in zaporedij, ki se lahko razširijo, ne da bi se prekinile obstoječe izvedbe.

(c) **Prilagodljiva struktura**: shema je zasnovana tako, da po potrebi omogoča dodajanje ali spreminjanje elementov ali vrst podatkov. Struktura sheme omogoča spremembe zahtev, ne da bi bile potrebno večje preoblikovanje.

(d) **Neobvezni elementi**: elementi sheme se lahko označijo kot neobvezni, kar pomeni, da se lahko glede na konkretne okoliščine vključijo ali izpustijo.

Shema je zasnovana tako, da podpira zbiranje strukturiranih podatkov za posebna zaprosila.

2.1.5. Spremembe

Za zasnovo sheme so značilne prožnost, modularnost in enostavnost prilagoditev. Kompleksne vrste in neobvezni elementi se vključijo v zasnovo tako, da se lahko obravnavajo različni scenariji, hkrati pa se zasnova zlahka spremeni in razširi.

2.2. *Izmenjava strukturiranih podatkov*

Strukturirani podatki iz točk 2.2.1 in 2.2.2 se zagotovijo v skladu s členom 22a(3) Uredbe (EU) 2018/1727. Shema omogoča tudi opredelitev podatkovnih nizov, ki jih je ob prihodnjih posodobitvah treba izbrisati.

2.2.1. Podatki evropske pravosodne protiteroristične evidence

Naslednje tehnične specifikacije za podatkovno shemo vzpostavljajo strukturiran okvir za oblikovanje sheme v obliki XML.

(a) Najvišja raven

Najvišja raven obsega informacije iz Priloge III k Uredbi (EU) 2018/1727 za evropsko pravosodno protiteroristično evidenco (CTR).

(b) Struktura sporočila

Struktura podatkov CTR je sestavljena iz zaporedja elementov, ki vključuje najmanj naslednje:

(i) informacije za identifikacijo fizičnih oseb:

— priimek,

— ime (imena),

— vsi vzdevki,

— datum rojstva,

— kraj rojstva (mesto in država),

— državljanstvo ali državljanstva,

— identifikacijski dokument (vrsta in številka dokumenta),

— spol,

— kraj prebivališča;

(ii) informacije za identifikacijo pravnih oseb:

— ime podjetja,

— pravna oblika,

— kraj sedeža;

(iii) informacije za identifikacijo fizičnih in pravnih oseb:

— telefonske številke,

— elektronski naslovi,

— podatki o računih pri bankah ali drugih finančnih ustanovah,

— status v postopku;

(iv) informacije o terorističnem kaznivem dejanju:

— informacije o pravnih osebah, ki sodelujejo pri pripravi ali storitvi terorističnega kaznivega dejanja,

— pravna kvalifikacija kaznivega dejanja na podlagi nacionalnega prava,

— ustrezna oblika hudega kaznivega dejanja s seznama iz Priloge I,

— morebitna pripadnost teroristični skupini,

— vrsta terorizma, na primer džihadistični, separatistični, levičarski ali desničarski,

— kratek povzetek zadeve;

(v) informacije o nacionalnem postopku:

— status takih postopkov,

— pristojno državno tožilstvo,

— številka zadeve,

— datum začetka formalnega sodnega postopka,

— povezave z drugimi zadevnimi primeri;

(vi) polje za dodatne informacije (poljubno besedilo);

(vii) oznaka predhodnega dovoljenja.

2.2.2. Podatki, poslani v skladu s členom 21 Uredbe (EU) 2018/1727

(a) Člen 21(4) Uredbe (EU) 2018/1727 o ustanovitvi skupnih preiskovalnih skupin (JIT)

(i) Najvišja raven
Najvišja raven obsega informacije iz člena 21(4) Uredbe (EU) 2018/1727 o ustanovitvi JIT.

(ii) Struktura sporočila
Struktura podatkov je sestavljena iz zaporedja elementov, ki vključuje najmanj naslednje:

— nacionalni pravosodni organ, pristojen za kazenski postopek,

— nacionalna referenčna številka kazenskega postopka,

— status kazenskega postopka,

— preiskana kazniva dejanja,

— druge države, vključene v zadevo,

— ali je zadevo že podprl Eurojust?

— če je: Eurojustova identifikacijska številka zadeve,

— če ni: ali je to zaprosilo za podporo?

— ali je zadevo podprl Europol?

— če je: operativna projektna skupina (OTF) in/ali mrežna aplikacija za varno izmenjavo informacij (SIENA)?

— sporazum o ustanovitvi JIT:

— vključene države,

— pogodbenice JIT (nacionalni organi, pristojni za preiskave),

— nacionalna referenčna številka kazenskega postopka, ki ga zajema JIT,

— datum podpisa,

— trajanje,

— preiskana kazniva dejanja,

— kratek povzetek zadeve,

— glavni osumljenci v kazenskem postopku, ki ga zajema JIT (ime, priimek, datum in kraj rojstva ter po možnosti druge ustrezne in potrebne kategorije podatkov iz Priloge II),

— rezultati dela JIT:

— težave/zamude pri:

— ustanovitvi JIT,

— zaprosilu/izmenjavi dokazov v JIT,

— dogovoru o skupni strategiji pregona ali njenem izvajanju,

— dopustnost/nedopustnost/presoja dokazov JIT v nacionalnih postopkih,

— izid sodnega postopka (uspešen/neuspešen pregon in obsodbe/oprostitve).

(iii) Oznaka predhodnega dovoljenja

(b) Člen 21(5) Uredbe (EU) 2018/1727, zapletene zadeve v zvezi s hudimi kaznivimi dejanji

(i) Najvišja raven

Najvišja raven obsega informacije iz člena 21(5) Uredbe o Eurojustu, tj. o zapletenih zadevah v zvezi s hudimi kaznivimi dejanji.

(ii) Struktura sporočila

Struktura podatkov je sestavljena iz zaporedja elementov, ki vključuje najmanj naslednje:

— nacionalni pravosodni organ, pristojen za kazenski postopek,

— nacionalna referenčna številka kazenskega postopka,

— status kazenskega postopka,

— preiskana kazniva dejanja,

— druge države, vključene v zadevo,

— ali je zadevo že podprl Eurojust?

— če je: Eurojustova identifikacijska številka zadeve,

— če ni: ali je to zaprosilo za podporo?

— ali je zadevo podprl Europol?

— če ni: operativna projektna skupina in/ali SIENA?

— zadevna oblika hudega kaznivega dejanja,

— vpletenost mreže organiziranega kriminala:

— vrsta mafije,

— mednarodna mreža organiziranega kriminala,

— posledice na ravni EU,

— glavni osumljenci v kazenskem postopku (ime, priimek, datum in kraj rojstva ter po možnosti druge ustrezne in potrebne kategorije podatkov iz Priloge II),

— kratek povzetek zadeve,

— druge vključene države:

— države, s katerimi se je sodelovanje že začelo:

— vključeni pristojni organi v drugi državi,

— uporabljeni instrumenti pravosodnega sodelovanja,

— število poslanih/prejetih zaprosil,

— obstoj povezanih preiskav,

— države, s katerimi se bo aktiviralo sodelovanje / morebiti prizadete države:

— vrsta potrebnega sodelovanja (kot so izročitev, zbiranje dokazov, drugo sodelovanje),

— obstoj povezanih preiskav.

(iii) Oznaka predhodnega dovoljenja

(c) Člen 21(6), točka (a), Uredbe (EU) 2018/1727, spori o pristojnosti

(i) Najvišja raven

Najvišja raven obsega informacije iz člena 21(6), točka (a), Uredbe (EU) 2018/1727, tj. spori o pristojnosti.

(ii) Struktura sporočila

Struktura podatkov je sestavljena iz zaporedja elementov, ki vključuje najmanj naslednje:

— nacionalni pravosodni organ, pristojen za kazenski postopek,

— nacionalna referenčna številka kazenskega postopka,

— status kazenskega postopka (npr. preiskava, pregon, sojenje),

— preiskana kazniva dejanja,

— druge države, vključene v zadevo,

— ali je zadevo že podprl Eurojust?

— če je: Eurojustova identifikacijska številka zadeve,

— če ni: ali je to zaprosilo za podporo?

— ali je zadevo podprl Europol?

— če ni: operativna projektna skupina in/ali SIENA?

— druge vključene države:

— pristojni nacionalni organi v drugi državi, če so znani,

— nacionalna referenčna številka kazenskega postopka v drugi državi,

— faza postopka v drugi državi, če je znana,

— pozitivni ali negativni spor,

— dejanski ali morebiten spor:

— že izvedene usklajevalne dejavnosti (npr. posvetovanja v skladu z Okvirnim sklepom Sveta 2009/948/PNZ ([1])),

— kratek povzetek zadeve,

— glavni skupni osumljenci (ime, priimek, datum in kraj rojstva ter po možnosti druge ustrezne in potrebne kategorije podatkov iz Priloge II).

(iii) Oznaka predhodnega dovoljenja

(d) Člen 21(6), točka (b), nadzorovane pošiljke

(i) Najvišja raven

Najvišja raven obsega informacije iz člena 21(6), točka (b), Uredbe (EU) 2018/1727: nadzorovane pošiljke.

(ii) Struktura sporočila

Struktura podatkov je sestavljena iz zaporedja elementov, ki vključuje najmanj naslednje:

— nacionalni pravosodni organ, pristojen za kazenski postopek,

— nacionalna referenčna številka kazenskega postopka,

— status kazenskega postopka (npr. preiskava, pregon, sojenje),

— preiskana kazniva dejanja,

— druge države, vključene v zadevo,

— ali je zadevo že podprl Eurojust?

— če je: Eurojustova identifikacijska številka zadeve,

— če ni: ali je to zaprosilo za podporo?

— ali je zadevo podprl Europol?

— če ni: operativna projektna skupina in/ali SIENA?

— druge vključene države:

— država porekla/tranzita / namembna država,

— pristojni nacionalni organi v drugih državah,

— obstoj povezanih preiskav v drugih državah,

([1]) Okvirni Sklep Sveta 2009/948/PNZ z dne 30. novembra 2009 o preprečevanju in reševanju sporov o izvajanju pristojnosti v kazenskih postopkih (UL L 328, 15.12.2009, str. 42, ELI: http://data.europa.eu/eli/dec_framw/2009/948/oj).

— vrsta dobavljenega blaga (npr. droge in vrsta/denar/orožje/cigarete/drugo),

— status nadzorovane pošiljke (npr. načrtovana, tekoča, končana),

— rezultat nadzorovane pošiljke, če je že izvedena,

— uporabljeni instrument pravosodnega sodelovanja,

— glavni skupni osumljenci (ime, priimek, datum in kraj rojstva ter po možnosti druge ustrezne in potrebne kategorije podatkov iz Priloge II).

(iii) Oznaka predhodnega dovoljenja

(e) Člen 21(6), točka (c), Uredbe (EU) 2018/1727, ponavljajoče se težave z instrumenti pravosodnega sodelovanja.

(i) Najvišja raven

Najvišja raven obsega informacije iz člena 21(6), točka (c), Uredbe (EU) 2018/1727: ponavljajoče se težave z instrumenti pravosodnega sodelovanja.

(ii) Struktura sporočila

Struktura podatkov je sestavljena iz zaporedja elementov, ki vključuje najmanj naslednje:

— nacionalni pravosodni organ, pristojen za kazenski postopek,

— nacionalna referenčna številka kazenskega postopka,

— status kazenskega postopka (npr. preiskava, pregon, sojenje),

— preiskana kazniva dejanja,

— druge države, vključene v zadevo,

— ali je zadevo že podprl Eurojust?

— če je: Eurojustova identifikacijska številka zadeve,

— če ni: ali je to zaprosilo za podporo?

— ali je zadevo podprl Europol?

— če ni: operativna projektna skupina in/ali SIENA?

— druge vključene države:

— pristojni nacionalni organi, če so znani,

— v vlogi odreditvenega ali izvršitvenega organa,

— zadevni instrument pravosodnega sodelovanja (npr. evropski nalog za prijetje, EPN, zamrznitev in zaplemba):

— zadevno posebno zaprosilo (tj. kateri preiskovalni ukrep, katera vrsta zamrznitve, evropski nalog za prijetje za izvršitev kazni ali pregon),

— zavrnitev ali ponavljajoče se težave:

— če gre za zavrnitev: kateri konkretni razlog je bil naveden?

— kratek opis težave,

— drugi nacionalni organi, ki jih zadeva ista težava, če obstajajo.

(iii) Oznaka predhodnega dovoljenja

2.3. *Oznake predhodnega dovoljenja*

Pri izmenjavi podatkov z Eurojustom prek sistema JUDEX pristojni nacionalni organi z oznakami predhodnega dovoljenja označijo nadaljnje ravnanje s podatki, dostop do njih in njihov prenos po odkritju povezave. Oznake predhodnega dovoljenja označujejo, ali in v kakšnem obsegu se lahko informacije v zvezi s povezavo izmenjujejo z drugimi pristojnimi nacionalnimi organi, drugimi agencijami in organi Unije, tretjimi državami ali mednarodnimi organizacijami.

2.4. *Vnaprej določena sporočila*

Vnaprej določena sporočila so primeri izmenjav, ki so določene v Uredbi (EU) 2018/1727, vendar zanje tam ni določen poseben obrazec. Njihovi vrste in število se določijo med poslovno in tehnično analizo.

Opredelitve shem XLM (XSD) za vnaprej določena sporočila so zasnovane tako, da zagotavljajo doslednost, strukturo in skladnost s poslovnimi potrebami.

Za te sheme velja naslednje:

(a) najvišja raven sheme se imenuje v skladu s posebno vrsto sporočila, ki se opredeljuje;

(b) v tej strukturi se dodajo in opredelijo polja, potrebna za določeno vrsto sporočila, da se zagotovi ustrezna predstavitev podatkovnih elementov.

2.5. *Sporočila s poljubnim besedilom*

Sporočila s poljubnim besedilom so primeri izmenjav, ki omogočajo nestrukturirano ali delno strukturirano vsebino, s čimer omogočajo prožnost, hkrati pa še vedno izpolnjujejo regulativne in poslovne zahteve. XSD za sporočila s poljubnim besedilom je zasnovana tako, da se zagotovita doslednost in ustrezno oblikovanje.

Za te sheme velja naslednje:

(a) najvišja raven sheme se imenuje v skladu s posebno vrsto sporočila, ki se opredeljuje;

(b) shema opredeljuje potrebno strukturo za sporočilo s poljubnim besedilom, hkrati pa omogoča ustrezno razvrščanje elementov, kot je potrebno;

(c) v tej strukturi se dodajo in opredelijo polja, potrebna za določeno vrsto sporočila s prostim besedilom, da se zagotovi ustrezna predstavitev podatkovnih elementov.

PRILOGA III

TEHNIČNE SPECIFIKACIJE ZA PRSTNE ODTISE IN FOTOGRAFIJE

Sporočilom, izmenjanim prek decentraliziranega sistema IT, se lahko v skladu s tehničnimi specifikacijami iz točk 1 in 2 priložijo priloge, vključno z datotekami ameriškega nacionalnega inštituta za standarde in tehnologijo (NIST), ki vsebujejo prstne odtise in fotografije.

1. **Prstni odtisi**

Prstni odtisi, ki se lahko pošljejo Eurojustu za namene zanesljive identifikacije posameznikov, ki so v kazenskem postopku v zvezi s terorističnimi kaznivimi dejanji, izpolnjujejo naslednje pogoje:

(a) podatki o prstnih odtisih se zagotovijo v eni datoteki, ki vsebuje digitalne podobe prstnih odtisov (datoteka NIST s prstnimi odtisi), in se predložijo v skladu s standardom ANSI/NIST-ITL 1-2011, posodobljenim leta 2015 (ali novejšo različico);

(b) datoteka NIST s prstnimi odtisi zajema do deset posameznih prstnih odtisov: in sicer povaljane ali ploske prstne odtise ali oboje;

(c) vsi prstni odtisi so označeni;

(d) prstni odtisi so pridobljeni z elektronskim skeniranjem v živo ali s črnilom na papirju, če se prstni odtisi, pridobljeni s črnilom na papirju, skenirajo v zahtevani ločljivosti in enake kakovosti;

(e) datoteka NIST s prstnimi odtisi omogoča vključitev dopolnilnih informacij, kot so pogoji evidentiranja prstnih odtisov in metoda pridobitve posameznih podob prstnih odtisov;

(f) prstni odtisi imajo nominalno ločljivost 500 ali 1 000 ppi ([1]) (ob sprejemljivem odstopanju +/– 10 ppi) z 256 ravnmi sivine;

(g) kompresijski algoritem za kompresiranje prstnih odtisov, ki se uporabi, upošteva priporočila NIST. Podatki o prstnih odtisih z ločljivostjo 500 ppi se kompresirajo z uporabo algoritma WSQ (ISO/IEC 19794-5:2005). Podatki o prstnih odtisih z ločljivostjo 1 000 ppi se kompresirajo z uporabo standarda kompresije podobe in sistema označevanja JPEG 2000 (ISO/IEC 15444-1). Ciljno kompresijsko razmerje je 15 : 1.

2. **Fotografije**

Fotografije, ki se lahko pošljejo Eurojustu za namene zanesljive identifikacije posameznikov, ki so v kazenskem postopku v zvezi s terorističnimi kaznivimi dejanji, izpolnjujejo naslednje pogoje:

(a) datoteka s fotografijo vsebuje samo eno podobo obraza (datoteka NIST s fotografijo), ki se predloži v skladu s standardom ANSI/NIST-ITL 1-2011, posodobljenim leta 2015, ali novejšo dostopno različico;

(b) fotografije so bodisi črno-bele, barvne ali posnete v bližnje infrardečem območju;

(c) kakovost fotografij temelji na zahtevah glede frontalne podobe v skladu s standardom ISO/IEC 19794-5:2011 ali katero koli novejšo dostopno različico;

(d) datoteka NIST s fotografijo omogoča vključitev dopolnilnih informacij, vključno z datumom posnetja slike;

([1]) Slikovne pike na palec.

(e) fotografije v pokončni usmerjenosti imajo ločljivost najmanj 600 slikovnih pik × 800 slikovnih pik in največ 1 200 slikovnih pik × 1 600 slikovnih pik;

(f) obraz zaseda dovolj prostora na fotografiji, da se zagotovi, da je med središčema obeh očes najmanj 120 slikovnih pik;

(g) kompresijski algoritem za kompresiranje fotografij, ki se uporabi, upošteva priporočila NIST. Fotografije se kompresirajo samo enkrat s standardom kompresije podobe in sistemom označevanja JPG (ISO/IEC 10918) ali JPEG 2000 (ISO/IEC 15444), pri čemer je največje dovoljeno kompresijsko razmerje 20 : 1.