2025/2447

5.12.2025

KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2025/2447

af 4. december 2025

om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) 2018/1727 for så vidt angår de tekniske specifikationer, foranstaltninger og andre krav til oprettelse og brug af det decentrale IT-system til sikker behandling og kommunikation af oplysninger

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) 2018/1727 af 14. november 2018 om Den Europæiske Unions Agentur for Strafferetligt Samarbejde (Eurojust) og om erstatning og ophævelse af Rådets afgørelse 2002/187/JHA ([1]), særlig artikel 22a, stk. 3, og artikel 22b, stk. 1, litra a), b), c) og d), og

ud fra følgende betragtninger:

(1) Forordning (EU) 2018/1727 fastlægger rammen for Eurojusts nye digitale interne infrastruktur og oprettelsen af et decentraliseret sikkert digitalt kommunikationssystem mellem medlemsstaternes kompetente nationale myndigheder og Eurojust.

(2) Den sikre digitale kommunikation skal foregå gennem det decentrale IT-system. For at oprette det decentrale IT-system er det nødvendigt at fastsætte tekniske specifikationer, der definerer kommunikationsmetoder og kommunikationsprotokoller, tekniske foranstaltninger, der sikrer minimumsstandarder for informationssikkerhed og anden sikkerhed samt minimumsmål for tilgængelighed for gennemførelsen af dette system.

(3) I overensstemmelse med artikel 22a, stk. 1, i forordning (EU) 2018/1727 bør det decentrale IT-system bestå af medlemsstaternes og Eurojusts IT-systemer og interoperable e-CODEX-adgangspunkter, hvorigennem disse IT-systemer er forbundne. De tekniske specifikationer og andre krav til det decentrale IT-system, der er fastsat i denne forordning, bør tage hensyn til denne ramme.

(4) Adgangspunkterne i det decentrale IT-system bør være baseret på autoriserede e-CODEX-adgangspunkter som defineret i artikel 3, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2022/850 ([2]).

(5) Det decentrale IT-system gennemføres inden for rammerne af et større e-CODEX-baseret decentralt IT-system, der benævnes det digitale udvekslingssystem (JUDEX). Det er derfor nødvendigt at sikre en effektiv udveksling af oplysninger angående den horisontale udvikling.

(6) I overensstemmelse med artikel 22a, stk. 4, i forordning (EU) 2018/1727 kan medlemsstaterne og Eurojust vælge at anvende den referencegennemførelsessoftware, der er udviklet af Kommissionen, som deres back-end-system i stedet for et nationalt IT-system. For at sikre interoperabilitet bør både de nationale IT-systemer og referencegennemførelsessoftwaren være underlagt de samme tekniske specifikationer og krav.

(7) Data vedrørende terrorhandlinger og grov organiseret kriminalitet bør fremsendes på en struktureret måde for at forbedre oplysningernes kvalitet og relevans samt for at sikre, at oplysningerne kan integreres mere effektivt i Eurojusts sagsforvaltningssystem og bedre krydstjekkes med oplysninger, der allerede er lagret i dette system. For fingeraftryksoplysninger og fotografier, der kan fremsendes til Eurojust med henblik på at identificere personer, der er genstand for straffesager i forbindelse med terrorhandlinger, bør formatet og de tekniske standarder for videregivelsen defineres.

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

([2]) Europa-Parlamentets og Rådets forordning (EU) 2022/850 af 30. maj 2022 om et IT-system til grænseoverskridende elektronisk udveksling af oplysninger på området civil- og strafferetligt samarbejde (e-CODEX-systemet) og om ændring af forordning (EU) 2018/1726 (EUT L 150 af 1.6.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/850/oj).

(8) Eurojust fremmer og støtter udstedelsen og fuldbyrdelsen af anmodninger om retligt samarbejde, herunder anmodninger og afgørelser baseret på instrumenter, der gennemfører princippet om gensidig anerkendelse. De nationale kompetente myndigheder bør kunne søge bistand og hjælp til koordinering hos Eurojust gennem det decentrale IT-system.

(9) For at sikre effektivitet og sammenhæng er det vigtigt, at de tekniske specifikationer, der skal fastsættes i henhold til forordning (EU) 2018/1727, er forenelige med de tekniske specifikationer, der er fastsat i henhold til Europa-Parlamentets og Rådets forordning (EU) 2023/2844 ([3]), (EU) 2023/1543 ([4]) og (EU) 2024/3011 ([5]), samt med fremtidige digitaliseringsforanstaltninger, der er relevante for Eurojusts mandat til at støtte de nationale kompetente myndigheder.

(10) Al anden kommunikation mellem Eurojust og de kompetente nationale myndigheder, såsom meddelelse af oplysninger om resultaterne af behandlingen af oplysninger, herunder eksistensen af forbindelser til sager, der allerede er lagret i sagsforvaltningssystemet i overensstemmelse med artikel 22 i forordning (EU) 2018/1727, når Eurojust handler på eget initiativ, eller af oplysninger, der fremsendes til Eurojust med henblik på opbevaring, analyse og lagring af bevismateriale vedrørende folkedrab, forbrydelser mod menneskeheden, krigsforbrydelser og tilknyttede strafbare handlinger i overensstemmelse med nævnte forordnings artikel 4, stk. 1, litra j), bør også muliggøres gennem det decentrale IT-system.

(11) For at sikre, at denne forordning tager hensyn til Eurojusts operationelle behov, er Eurojust blevet hørt i overensstemmelse med artikel 22a, stk. 3, i forordning (EU) 2018/1727.

(12) I medfør af artikel 4 i protokol nr. 21 om Det Forenede Kongeriges og Irlands stilling for så vidt angår området med frihed, sikkerhed og retfærdighed, der er knyttet som bilag til traktaten om Den Europæiske Union og til traktaten om Den Europæiske Unions funktionsmåde, har Irland ved brev af 9. september 2019 meddelt, at det ønsker at acceptere og blive bundet af forordning (EU) 2018/1727. Irlands deltagelse blev bekræftet ved Kommissionens afgørelse (EU) 2019/2006 ([6]). Europa-Parlamentets og Rådets forordning (EU) 2023/2131 ([7]) ændrede forordning (EU) 2018/1727 for at gøre det muligt at etablere sikre digitale kommunikationskanaler mellem Eurojust og de kompetente nationale myndigheder og udgør retsgrundlaget for nærværende forordning. Under omstændigheder, hvor Irland ikke har meddelt, at det ønsker at deltage i vedtagelsen og anvendelsen af forordning (EU) 2023/2131, og ikke har meddelt, at det ønsker at acceptere og være bundet af nævnte forordning, er Irland i henhold til artikel 1 og 2 og artikel 4a, stk. 1, i protokol nr. 21 ikke bundet af forordning (EU) 2023/2131 og denne finder ikke anvendelse i Irland. Irland deltager derfor ikke i vedtagelsen af denne forordning.

(13) I medfør af artikel 1 og 2 i protokol nr. 22 om Danmarks stilling, der er knyttet som bilag til traktaten om Den Europæiske Union og til traktaten om Den Europæiske Unions funktionsmåde, deltog Danmark ikke i vedtagelsen af forordning (EU) 2018/1727. Denne forordning er derfor ikke bindende for og finder ikke anvendelse i Danmark.

([3]) Europa-Parlamentets og Rådets forordning (EU) 2023/2844 af 13. december 2023 om digitalisering af retligt samarbejde og adgang til domstolsprøvelse i grænseoverskridende civil-, handels- og strafferetlige sager og om ændring af visse retsakter inden for retligt samarbejde (EUT L, 2023/2844, 27.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2844/oj).

([4]) Europa-Parlamentets og Rådets forordning (EU) 2023/1543 af 12. juli 2023 om europæiske editionskendelser og europæiske sikringskendelser om elektronisk bevismateriale i straffesager og om fuldbyrdelse af frihedsstraffe idømt som led i en straffesag (EUT L 191 af 28.7.2023, s. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

([5]) Europa-Parlamentets og Rådets direktiv 2024/3011/EU af 27. november 2024 om den europæiske efterforskningskendelse i straffesager (EUT L, 2024/3011, 18.12.2024, ELI: http://data.europa.eu/eli/reg/2024/3011/oj).

([6]) Kommissionens afgørelse (EU) 2019/2006 af 29. november 2019 om Irlands deltagelse i Europa-Parlamentets og Rådets forordning (EU) 2018/1727 om Den Europæiske Unions Agentur for Strafferetligt Samarbejde (Eurojust) (EUT L 310 af 2.12.2019, s. 59, ELI: http://data.europa.eu/eli/dec/2019/2006/oj).

([7]) Europa-Parlamentets og Rådets forordning (EU) 2023/2131 af 4. oktober 2023 om ændring af Europa-Parlamentets og Rådets forordning (EU) 2018/1727 og Rådets afgørelse 2005/671/RIA for så vidt angår digital informationsudveksling i terrorsager (EUT L, 2023/2131, 11.10.2023, ELI: http://data.europa.eu/eli/reg/2023/2131/oj).

(14) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([8]) og afgav udtalelse den 21. oktober 2025.

(15) Foranstaltningerne i denne forordning er i overensstemmelse med udtalelse fra det udvalg, der er nedsat ved artikel 22c i forordning (EU) 2018/1727 —

VEDTAGET DENNE FORORDNING:

Artikel 1

Tekniske specifikationer for det decentrale IT-system

De tekniske specifikationer, foranstaltninger og mål for det decentrale IT-system, der er omhandlet i artikel 22b, stk. 1, litra a), b), c) og d), i forordning (EU) 2018/1727, er fastsat i bilag I til nærværende forordning.

Artikel 2

Digitale proceduremæssige standarder

De digitale proceduremæssige standarder, der finder anvendelse på elektronisk kommunikation via det decentrale IT-system, der er omhandlet i artikel 22a, stk. 3, i forordning (EU) 2018/1727, er fastsat i bilag II til nærværende forordning.

Artikel 3

Tekniske specifikationer for fremsendelse af fingeraftryk og fotografier

De tekniske specifikationer og formatet for fremsendelse af fingeraftryk og fotografier, jf. artikel 22a, stk. 3, i forordning (EU) 2018/1727, er fastsat i bilag III til nærværende forordning.

Artikel 4

Ikrafttræden

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i medlemsstaterne i overensstemmelse med traktaterne.

Udfærdiget i Bruxelles, den 4. december 2025.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand

([8]) Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

BILAG I

TEKNISKE SPECIFIKATIONER, FORANSTALTNINGER OG MÅL FOR DET DECENTRALE IT-SYSTEM

1. **Indledning og anvendelsesområde**

I dette bilag fastsættes de tekniske specifikationer, foranstaltninger og mål i forbindelse med det decentrale IT-system, der anvendes til den i forordning (EU) 2018/1727 omhandlede udveksling af oplysninger

IT-systemets decentraliserede karakter gør det muligt at udveksle data direkte og sikkert mellem kompetente nationale myndigheder og Eurojust.

2. **Definitioner**

I dette bilag forstås ved:

2.1. »Hypertext Transfer Protocol Secure« (»HTTPS«): krypteret kommunikation og sikre kommunikationskanaler

2.2. »uafviselighed af oprindelse«: foranstaltninger til dokumentation af oplysningernes integritet og oprindelse ved hjælp af metoder som digital certificering, offentlig nøgleinfrastruktur, elektroniske signaturer og elektroniske segl

2.3. »uafviselighed af modtagelse«: foranstaltninger til dokumentation over for ophavsmanden af den tiltænkte modtagers modtagelse af oplysningerne ved hjælp af metoder som digital certificering, offentlig nøgleinfrastruktur, elektroniske signaturer og elektroniske segl

2.4. »SOAP« (»Simple Object Access Protocol«): i overensstemmelse med standarderne fra World Wide Web Consortium, specifikation af en meddelelsesoverførende protokol til udveksling af strukturerede oplysninger i forbindelse med implementeringen af webtjenester i computernetværk

2.5. »REST« (»Representational State Transfer«): en arkitektonisk stil til udformning af netværksbaserede applikationer, der bygger på en stateless klient-server-kommunikationsmodel som anvender standardmetoder til at udføre operationer vedrørende ressourcer, som typisk er repræsenteret i strukturerede formater

2.6. »webtjeneste«: et softwaresystem, der er udformet med henblik på at støtte indbyrdes kompatibel interaktion mellem maskiner over et netværk, og som har et interface, der er beskrevet i et format, som kan behandles maskinelt

2.7. »dataudveksling« udveksling af meddelelser og dokumenter gennem det decentrale IT-system

2.8. »e-CODEX«: det e-CODEX system, der er defineret i artikel 3, nr. 1), i forordning (EU) 2022/850

2.9. »EU's centrale glossarer for e-justice«: EU's centrale glossarer for e-justice som defineret i punkt 4 i bilaget til forordning (EU) 2022/850

2.10. »ebMS«: ebXML Messaging Service, en meddelelsesoverførende protokol, der er udviklet inden for rammerne af OASIS og muliggør sikker, pålidelig og interoperabel udveksling af elektroniske forretningsdokumenter ved hjælp af SOAP Protokollen støtter integration mellem virksomheder på tværs af forskellige systemer.

2.11. »AS4«: Applicability Statement 4, en OASIS-standard, som anvendes til profilering af ebMS 3.0; den forenkler sikker og interoperabel kommunikation mellem virksomheder ved hjælp af åbne standarder såsom SOAP og WS-Security

2.12. »Recovery Time Objective« (»RTO«): den maksimalt acceptable tid for genoprettelse af en tjeneste efter en hændelse

2.13. »Recovery Point Objective« (»RPO«): den maksimalt acceptable mængde datatab i tilfælde af nedbrud.

3. **Metoder til elektronisk kommunikation**

3.1. Det decentrale IT-system benytter tjenestebaseret elektronisk kommunikation såsom webtjenester eller andre genanvendelige komponenter og softwareløsninger til udveksling af meddelelser og dokumenter.

3.2. Specifikt skal det decentrale IT-system omfatte kommunikation gennem e-CODEX-adgangspunkter, jf. artikel 5, stk. 2, i forordning (EU) 2022/850. For at sikre effektiv og interoperabel grænseoverskridende dataudveksling understøtter det decentrale IT-system derfor kommunikation via e-CODEX-systemet.

4. **Kommunikationsprotokoller**

4.1. Det decentrale IT-system anvender sikre internetprotokoller til:

a) kommunikation inden for det decentrale IT-system mellem kompetente myndigheder og Eurojust

b) kommunikation med den kompetente myndighed/domstolsdatabasen, jf. punkt 7.1.

4.2. Med henblik på definition og fremsendelse af strukturerede data og metadata baseres komponenterne i det decentrale IT-system på omfattende og bredt accepterede industristandarder og -protokoller såsom SOAP og REST.

4.3. For så vidt angår transportprotokoller og meddelelsesoverførende protokoller skal det decentrale IT-system være baseret på sikre standardbaserede protokoller såsom:

a) en AS4-profil til grænseoverskridende dataudveksling, der sikrer sikker og pålidelig meddelelsesoverførsel med kryptering og uafviselighed

b) HTTPS/RESTful API'er til kommunikation med understøttelse af JSON- og XML-formater

c) SOAP til interaktioner med høj pålidelighed, der integrerer WS-Security til autentificering og kryptering.

4.4. Med henblik på gnidningsløs og interoperabel dataudveksling skal de kommunikationsprotokoller, der anvendes af det decentrale IT-system, overholde relevante interoperabilitetsstandarder.

4.5. Hvis det er relevant, skal XML-skemaerne gøre brug af relevante standarder eller glossarer, som er nødvendige for korrekt validering af de elementer og typer, der er defineret i dette skema. Disse standarder eller glossarer kan omfatte:

a) EU's centrale glossar for e-justice

b) Unqualified Data Types

c) en kodeliste for Den Europæiske Unions sprogkoder.

4.6. For så vidt angår sikkerheds- og autentificeringsprotokoller skal det decentrale IT-system være baseret på standardbaserede protokoller såsom:

a) TLS (Transport Layer Security) til krypteret og autentificeret kommunikation via netværk, der understøtter gensidig autentificering via X.509-digitale certifikater

b) OAuth/OpenID Connect (OIDC) med henblik på sikker autentificering og godkendelse

c) PKI (offentlig nøgleinfrastruktur) og digitale signaturer til sikker nøgleudveksling og verificering af meddelelsers integritet ved hjælp af digitale certifikater (X.509) udstedt af betroede certificeringsmyndigheder.

5. **Informationssikkerhedsmål og relevante tekniske foranstaltninger**

5.1. De tekniske foranstaltninger, der skal sikre overholdelse af minimumsstandarder for IT-sikkerhed i forbindelse med udveksling af oplysninger via det decentrale IT-system, skal omfatte:

a) foranstaltninger, der sikrer oplysningernes fortrolighed, herunder ved at benytte sikre kommunikationskanaler

b) foranstaltninger til sikring af integriteten af data i hvile og i transit

c) foranstaltninger, der sikrer uafviseligheden af oprindelsen hos afsenderen af information og uafviseligheden af modtagelsen af information i det decentrale IT-system

d) foranstaltninger, der sikrer logning af sikkerhedshændelser i overensstemmelse med anerkendte internationale anbefalinger med hensyn til IT-sikkerhedsstandarder ([1])

e) foranstaltninger, der sikrer brugerautentificering og -autorisation af alle registrerede brugere, samt foranstaltninger til kontrol af identiteten af de systemer, der er forbundet med det decentrale IT-system.

5.2. Komponenterne i det decentrale IT-system skal sikre sikker kommunikation og dataoverførsel ved at anvende kryptering, offentlig nøgleinfrastruktur med digitale certifikater til autentificering og sikker nøgleudveksling samt sikre meddelelsesoverførende protokoller såsom AS4 (ebMS), RESTful API'er og SOAP for at bevare meddelelsernes fortrolighed og integritet.

5.3. Hvis der anvendes TLS i forbindelse med det decentrale IT-system, anvendes den seneste stabile version af protokollen eller, hvis dette ikke er muligt, en version uden kendte sikkerhedsmæssige sårbarheder. Kun nøglelængder, der sikrer et tilstrækkeligt niveau af kryptografisk sikkerhed, er tilladt, og der må ikke anvendes cipher suiter, der vides at være usikre eller forældede.

5.4. Digitale PKI-certifikater, der anvendes med henblik på drift af det decentrale IT-system, udstedes så vidt muligt af certificeringsmyndigheder, der er anerkendt som kvalificerede tillidstjenesteudbydere i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 ([2]). Der skal gennemføres foranstaltninger for at sikre, at sådanne certifikater udelukkende anvendes til de tilsigtede formål, med den nødvendige grad af tillid og i overensstemmelse med de gældende krav i forordning (EU) nr. 910/2014.

5.5. Komponenterne i det decentrale IT-system udvikles i overensstemmelse med princippet om databeskyttelse gennem design og gennem standardindstillinger, og der gennemføres passende administrative, organisatoriske og tekniske foranstaltninger for at sikre et højt cybersikkerhedsniveau.

5.6. Kommissionen udformer, udvikler og vedligeholder referencegennemførelsessoftwaren i overensstemmelse med de databeskyttelseskrav og -principper, der er fastsat i forordning (EU) 2018/1725. Den referencegennemførelsessoftware, som Kommissionen stiller til rådighed, skal gøre det muligt for medlemsstaterne at opfylde deres forpligtelser i henhold til henholdsvis Europa-Parlamentets og Rådets forordning (EU) 2016/679 ([3]) og direktiv (EU) 2016/680, alt efter hvad der er relevant.

([1]) Uden at det berører logning til sikkerhedsformål, skal de logningsmekanismer, der anvendes af komponenterne i det decentrale IT-system, i givet fald gøre det muligt at sikre overholdelse af kravene i artikel 88 i forordning (EU) 2018/1725 og, hvor det er relevant, artikel 25 i Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA (EUT L 119 af 4.5.2016, s. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

([2]) Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF (EUT L 257 af 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([3]) Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

5.7. Medlemsstater, der anvender et nationalt back-end-system, der adskiller sig fra referencegennemførelsessoftwaren, gennemfører de nødvendige foranstaltninger for at sikre, at deres nationale back-end-system opfylder kravene i forordning (EU) 2016/679 og direktiv (EU) 2016/680, alt efter hvad der er relevant.

5.8. Eurojust gennemfører de nødvendige foranstaltninger for at sikre, at dets back-end-system eller et eksempel på den referencegennemførelsessoftware, det anvender, opfylder kravene i forordning (EU) 2018/1725 og (EU) 2018/1727.

5.9. Medlemsstaterne og Eurojust etablerer robuste mekanismer til opdagelse af trusler og reaktion på hændelser for at sikre rettidig identifikation, afbødning og genopretning efter sikkerhedshændelser i overensstemmelse med deres relevante politikker for de IT-systemer under deres ansvar, der udgør en del af det decentrale IT-system.

6. **Minimumsmål for tilgængelighed**

6.1. Eurojust og medlemsstaterne sikrer, at komponenterne i det decentrale IT-system, som de er ansvarlige for, er tilgængelige i 24 timer i døgnet 7 dage om ugen med et mål for den tekniske tilgængelighed på mindst 98 % på årsbasis, eksklusive planlagt vedligeholdelse.

6.2. Kommissionen sikrer, at domstolsdatabasen er tilgængelig i 24 timer i døgnet 7 dage om ugen med et mål for den tekniske tilgængelighed på over 99 % på årsbasis, eksklusive planlagt vedligeholdelse.

6.3. På arbejdsdage skal vedligeholdelsesopgaver så vidt muligt planlægges mellem kl. 20.00 og kl. 7.00 CET.

6.4. Medlemsstaterne underretter Kommissionen, Eurojust og de øvrige medlemsstater om vedligeholdelsesaktiviteter som følger:

a) 5 arbejdsdage i forvejen for vedligeholdelsesopgaver, der kan gøre systemet utilgængeligt i op til 4 timer

b) 10 arbejdsdage i forvejen for vedligeholdelsesopgaver, der kan gøre systemet utilgængeligt i mellem 4 og 12 timer

c) 30 arbejdsdage i forvejen for vedligeholdelsesopgaver, der kan gøre systemet utilgængeligt i mere end 12 timer.

6.5. Hvis medlemsstaterne har faste regelmæssige vedligeholdelsesvinduer, underretter de Kommissionen, Eurojust og de andre medlemsstater om tidspunkterne og dagene for sådanne faste regelmæssige vinduer. Uanset de forpligtelser, der er fastsat i punkt 1, kan medlemsstaterne, hvis komponenter i det decentrale IT-system under medlemsstaternes ansvar bliver utilgængelige under et sådant fast regelmæssigt vindue, vælge ikke at underrette Kommissionen hver gang.

6.6. I tilfælde af en uventet teknisk fejl i en komponent i det decentrale IT-system, som medlemsstaterne har ansvaret for, underretter medlemsstaterne straks Kommissionen og de øvrige medlemsstater om fejlen og, hvis den kendes, om den forventede tidsramme for genopretning.

6.7. Eurojust underretter Kommissionen og medlemsstaterne om vedligeholdelsesaktiviteter som følger:

a) 5 arbejdsdage i forvejen for vedligeholdelsesopgaver, der kan gøre systemet utilgængeligt i op til 4 timer

b) 10 arbejdsdage i forvejen for vedligeholdelsesopgaver, der kan gøre systemet utilgængeligt i mellem 4 og 12 timer

c) 30 arbejdsdage i forvejen for vedligeholdelsesopgaver, der kan gøre systemet utilgængeligt i mere end 12 timer.

6.8. Hvis Eurojust har faste regelmæssige vedligeholdelsesvinduer, underretter Eurojust Kommissionen og medlemsstaterne om tidspunkterne og dagene for sådanne faste regelmæssige vinduer. Uanset de forpligtelser, der er fastsat i punkt 1, kan Eurojust, hvis komponenter i det decentrale IT-system under Eurojusts ansvar bliver utilgængelige under et sådant fast regelmæssigt vindue, vælge ikke at underrette Kommissionen hver gang.

6.9. I tilfælde af en uventet teknisk fejl i en komponent i det decentrale IT-system, som Eurojust har ansvaret for, underretter Eurojust straks Kommissionen og medlemsstaterne om fejlen og, hvis den kendes, om den forventede tidsramme for genopretning.

6.10. I tilfælde af en uventet teknisk fejl hos den kompetente myndighed/domstolsdatabasen, underretter Kommissionen straks Eurojust og medlemsstaterne om fejlen og, hvis den kendes, om den forventede tidsramme for genopretning.

6.11. I tilfælde af en afbrydelse af tjenesten sikrer medlemsstaterne og Eurojust, at tjenesten hurtigt genoprettes, og at datatabet er minimalt i overensstemmelse med målet om RTO og RPO.

6.12. Medlemsstaterne og Eurojust gennemfører passende foranstaltninger for at nå de mål for tilgængelighed, der er fastlagt ovenfor, og fastlægger procedurer for effektiv reaktion på hændelser.

7. **De kompetente myndigheder/domstolsdatabasen (CDB)**

7.1. I henhold til artikel 22a i forordning (EU) 2018/1727 skal det decentrale IT-system muliggøre elektronisk kommunikation mellem de kompetente nationale myndigheder og Eurojust. I betragtning af forpligtelserne til at udveksle oplysninger mellem kompetente nationale myndigheder og Eurojust i henhold til artikel 21, 21a og 22, men også Eurojusts rolle med hensyn til at fremme og støtte fremsættelsen eller efterkommelsen af alle anmodninger om gensidig retlig bistand eller gensidig anerkendelse i overensstemmelse med artikel 8, stk. 1, i forordning (EU) 2018/1727, skal de involverede kompetente myndigheder klart kunne identificeres, når de anvender det decentrale IT-system. Det er derfor afgørende at oprette en autoritativ database over disse myndigheders oplysninger, som kan anvendes af det decentrale IT-system.

7.2. CDB skal indeholde følgende oplysninger i et struktureret format:

a) med henblik på artikel 8, stk. 1, 3 og 4, artikel 21, artikel 21a og artikel 22 i forordning (EU) 2018/1727 oplysninger om de kompetente nationale myndigheder, herunder nationale korrespondenter, jf. artikel 20 i nævnte forordning, samt nationale medlemmer i overensstemmelse med artikel 7 ([4]) i nævnte forordning

b) hvis det er relevant, oplysninger, der er nødvendige for at fastlægge de geografiske eller materielle områder for de kompetente myndigheders kompetence, eller andre relevante kriterier, der er nødvendige for at fastslå deres kompetence

c) oplysninger, der er nødvendige for den korrekte tekniske overførsel af meddelelser i det decentrale IT-system.

7.3. Kommissionen er ansvarlig for udvikling, vedligeholdelse, drift og systemsupport af og til CDB.

7.4. CDB giver medlemsstaterne og Eurojust mulighed for at ajourføre oplysningerne i CDB og gør det muligt for de kompetente nationale myndigheder og nationale medlemmer, der deltager i det decentrale IT-system, programmatisk at tilgå og hente oplysninger i CDB.

7.5. Der skal være mulighed for adgang til CDB via en fælles kommunikationsprotokol, uanset om de kompetente myndigheder, der er tilsluttet det decentrale IT-system, driver et nationalt back-end-system eller gennemfører en indførelse af referencegennemførelsessoftwaren

7.6. Medlemsstaterne sikrer, at oplysningerne om deres kompetente myndigheder i CDB, jf. punkt 7.2, er fuldstændige, nøjagtige og ajourførte.

([4]) Dette berører ikke delegationen af beføjelser fra det nationale medlem til dennes stedfortræder, andet personale ved det nationale kontor eller bemyndiget Eurojustpersonale.

BILAG II

DIGITALE PROCEDUREMÆSSIGE STANDARDER

I artikel 3, stk. 9, i forordning (EU) 2022/850 defineres digitale proceduremæssige standarder som de tekniske specifikationer for forretningsprocesmodeller og dataskemaer, der fastsætter den elektroniske struktur af de oplysninger, der udveksles via e-CODEX-systemet.

I dette bilag fastsættes de tekniske specifikationer for forretningsprocesmodeller og de tekniske specifikationer for dataskemaer.

1. **Tekniske specifikationer for forretningsprocesmodeller i henhold til forordning (EU) 2018/1727**

De tekniske specifikationer for forretningsprocesmodeller er fastsat i punkt 1.1-1.5. De definerer de centrale aspekter, der er nødvendige for at muliggøre elektronisk kommunikation i henhold til forordning (EU) 2018/1727 gennem det decentrale IT-system.

Det decentrale IT-system tillader kun udveksling af oplysninger mellem en medlemsstats kompetente nationale myndigheder og det nationale medlem fra den pågældende medlemsstat.

1.1. *Udveksling af oplysninger vedrørende det europæiske retlige terrorbekæmpelsesregister (CTR) jf. artikel 21a i forordning (EU) 2018/1727*

1.1.1. Model for fremsendelse af CTR-data:

Den kompetente nationale myndighed fremsender data om terrorsager for CTR til det nationale medlem.

1.1.2. Model for modtagelse af CTR-data:

Det nationale medlem modtager CTR-dataene.

1.1.3. Model for anmodning om samtykke:

Det nationale medlem anmoder om samtykke fra sin kompetente nationale myndighed.

1.1.4. Model for modtagelse af anmodning om samtykke:

Den kompetente nationale myndighed modtager anmodningen om samtykke.

1.1.5. Model for afsendelse af svar på anmodning om samtykke:

Den kompetente nationale myndighed sender et svar på anmodningen om samtykke.

1.1.6. Model for modtagelse af svar på anmodning om samtykke:

Det nationale medlem modtager svaret på anmodningen om samtykke.

1.1.7. Model for underretning om forbindelse:

Det nationale medlem underretter den kompetente nationale myndighed om forbindelsen til en anden sag.

1.1.8. Model for ajourføring af CTR-data:

Den kompetente nationale myndighed fremsender data, der skal ajourføres eller slettes, til sit respektive nationale medlem.

1.1.9. Model for modtagelse af ajourførte CTR-data:

Det nationale medlem modtager de CTR-data, der skal ajourføres eller slettes.

1.2. *Udveksling af oplysninger vedrørende grov kriminalitet jf. artikel 21 i forordning (EU) 2018/1727*

1.2.1. Model for fremsendelse af data vedrørende grov grænseoverskridende kriminalitet:

Den nationale kompetente myndighed fremsender data om grov grænseoverskridende kriminalitet til Eurojust.

1.2.2. Model for modtagelse af data vedrørende grov grænseoverskridende kriminalitet:

Det nationale medlem modtager data om grov grænseoverskridende kriminalitet.

1.2.3. Model for anmodning om samtykke:

Det nationale medlem anmoder om samtykke fra sin nationale kompetente myndighed.

1.2.4. Model for modtagelse af anmodning om samtykke:

Den kompetente nationale myndighed modtager anmodningen om samtykke.

1.2.5. Model for afsendelse af svar på anmodning om samtykke:

Den kompetente nationale myndighed sender et svar på anmodningen om samtykke.

1.2.6. Model for modtagelse af svar på anmodning om samtykke:

Det nationale medlem modtager svaret på anmodningen om samtykke.

1.2.7. Model for underretning om forbindelse:

Det nationale medlem underretter den kompetente nationale myndighed om forbindelsen til en anden sag.

1.2.8. Model for ajourføring af data vedrørende grov grænseoverskridende kriminalitet:

Den kompetente nationale myndighed fremsender data, der skal ajourføres eller slettes, til sit respektive nationale medlem.

1.2.9. Model for modtagelse af ajourførte data vedrørende grov grænseoverskridende kriminalitet:

Det nationale medlem modtager de oplysninger om grov grænseoverskridende kriminalitet, der skal ajourføres eller slettes.

1.3. *Udveksling af generelle oplysninger*

1.3.1. Model for afsendelse af oplysninger:

Det nationale medlem sender oplysninger til den kompetente nationale myndighed eller omvendt.

1.3.2. Model for modtagelse af oplysninger:

Den kompetente nationale myndighed eller det nationale medlem modtager oplysningerne.

1.3.3. Model for svar angående oplysninger:

Den kompetente nationale myndighed afgiver svar angående de oplysninger, der er modtaget fra det nationale medlem eller omvendt.

1.3.4. Model for modtagelse af svar:

Det nationale medlem modtager svaret fra den kompetente nationale myndighed.

1.3.5. Model for afsendelse af oplysninger:

Den kompetente nationale myndighed sender oplysninger til det nationale medlem.

1.3.6. Model for modtagelse af oplysninger:

Det nationale medlem modtager oplysningerne.

1.3.7. Model for svar angående oplysninger:

Det nationale medlem besvarer de oplysninger, der er modtaget fra den kompetente nationale myndighed.

1.3.8. Model for modtagelse af svar:

Den kompetente nationale myndighed modtager svaret fra det nationale medlem.

1.4. *Fremmende og støttende roller, jf. artikel 8, stk. 1, i forordning (EU) 2018/1727*

Bemærk: Hvis modellerne for fremme og støtte, der er beskrevet i punkt 1.5, omfatter udveksling af en lovbestemt udformning, der er fastsat ved EU-retsakter inden for retligt samarbejde i straffesager, skal modellerne, hvis sådanne foreligger, anvende de relevante strukturerede datapræsentationer og XML-skemaer, der er udviklet til disse retsakter, f.eks. dem, der er oprettet med henblik på gennemførelsesforordning (EU) 2023/2844 eller andre relevante instrumenter.

1.5. *Model for anmodning om fremme eller støtte*

1.5.1. Model for fremsendelse af anmodning om fremme eller støtte:

Den nationale kompetente myndighed fremsender en anmodning om fremme eller støtte til sit respektive nationale medlem.

1.5.2. Model for modtagelse af anmodning om fremme eller støtte:

Det nationale medlem modtager anmodningen om fremme eller støtte og videresender den til det nationale medlem af den anmodede medlemsstat uden for JUDEX.

1.5.3. Model for videresendelse af anmodning om fremme eller støtte til den kompetente nationale myndighed:

Det nationale medlem fra den anmodede medlemsstat sender anmodningen til sin respektive kompetente nationale myndighed.

1.5.4. Model for modtagelse af anmodning om fremme eller støtte:

Den kompetente nationale myndighed modtager anmodningen om fremme eller støtte.

1.5.5. Model for afsendelse af svar på anmodning om fremme eller støtte:

Den kompetente nationale myndighed sender et svar på eller oplysninger vedrørende anmodningen til det nationale medlem fra den anmodede medlemsstat.

1.5.6. Model for modtagelse af svar på anmodning om fremme eller støtte:

Det nationale medlem modtager svar på eller oplysninger om anmodningen om fremme eller støtte fra den kompetente nationale myndighed og deler dette eller disse med det nationale medlem i den anmodende medlemsstat uden for JUDEX.

1.5.7. Model for besvarelse af anmodning om fremme eller støtte:

Det nationale medlem fra den anmodende medlemsstat besvarer eller deler oplysningerne vedrørende anmodningen om fremme eller støtte fra den kompetente nationale myndighed.

1.5.8. Model for modtagelse af svar:

Den kompetente nationale myndighed modtager svaret eller oplysningerne vedrørende anmodningen om fremme eller støtte.

2. **Tekniske specifikationer for dataskemaer**

De tekniske specifikationer, der skal danne grundlag for udviklingen af XML Schema Definitions (XSD'er) med henblik på digitalisering af forordning (EU) 2018/1727, er fastsat i punkt 2.1 og 2.2 i dette bilag. Disse specifikationer definerer nøglekomponenterne og alle andre oplysninger med henblik på at give en omfattende beskrivelse af udarbejdelsen af disse skemaer.

Beskrivelsen skal være generisk, således at de producerede XSD'er kan ændres og udvides, uden at der kræves væsentlige ændringer af disse specifikationer.

Specifikationerne finder anvendelse på skemaernes lovbestemte udformning, jf. bilag til forordning (EU) 2018/1727, og alle foruddefinerede meddelelser eller eventuelle fritekstmeddelelser, der anvendes i udvekslinger i henhold til nævnte forordning.

2.1. *Generelle betragtninger*

For alle skemaer gælder følgende bestemmelser:

2.1.1. Versionering

Der skal inkluderes en versionsattribut, der fremmer forvaltningen af skemaerne og gør det muligt at ajourføre skemaet i fremtidige iterationer i overensstemmelse med gældende forretningskrav. Versionsattributten skal angive, om den nye version er bagudkompatibel, når der indføres nye funktioner eller forbedringer.

2.1.2. Skematisk erklæring og metadata

— Hvis det er relevant, skal skemaet gøre brug af relevante standarder eller glossarer, for at e-CODEX kan sikre interoperabilitet, som er nødvendige for en korrekt validering af de elementer og typer, der er defineret i det pågældende skema. Dette kunne f.eks. omfatte:

  — EU's centrale glossar for e-justice

  — Unqualified Data Types

  — en kodeliste for Den Europæiske Unions sprogkoder.

— Hvor det er relevant, kan skemaer også omfatte relevante ETSI-standarder for at gøre brug af deres definitioner.

2.1.3. Anmærkninger og dokumentation

— **Anmærkninger**: Hvert element i skemaet skal typisk ledsages af anmærkninger. Anmærkningerne giver menneskeligt læsbare oplysninger om elementet og definerer ofte dets formål eller anvendelse på en klar og koncis måde.

2.1.4. Anvendelse og muligheder for tilpasning

Skemaet skal følge reglerne i punkt a) til d):

a) **Modulopbygget struktur**: hvert afsnit skal konstrueres med en specifik funktionalitet og kan genbruges eller tilpasses uafhængigt. Dette skal gøre skemaet let at tilpasse til forskellige anvendelsestilfælde.

b) **Mulighed for udvidelse**: skemaet skal udformes med henblik på at understøtte medtagelsen af nye elementer eller attributter, hvis der er behov for yderligere oplysninger i fremtiden. Dette skal opnås ved at anvende valgfrie elementer og sekvenser, der kan udvides uden at afvige fra eksisterende implementeringer.

c) **Justerbar struktur**: skemaet skal udformes på en måde, der giver mulighed for om nødvendigt at tilføje eller ændre elementer eller datatyper. Skemaets struktur skal tage højde for ændringer i kravene, uden at der er behov for større ændringer af skemaets udformning.

d) **Valgfri elementer**: elementer i et skema kan markeres som valgfrie, dvs. de kan medtages eller udelades på grundlag af særlige omstændigheder.

Skemaet skal være udformet til at støtte indsamlingen af strukturerede data til specifikke anmodninger.

2.1.5. Ændringer

Skemaets udformning skal være kendetegnet ved fleksibilitet, modulopbygning og mulighed for let tilpasning. Komplekse typer og valgfrie elementer skal indarbejdes i designet på en sådan måde, at det kan håndtere forskellige scenarier, samtidig med at det forbliver let at ændre og udvide.

2.2. *Udveksling af strukturerede data*

De strukturerede data, der er omhandlet i punkt 2.2.1 og 2.2.2, leveres i overensstemmelse med artikel 22a, stk. 3, i forordning (EU) 2018/1727. Skemaet skal også gøre det muligt at markere datasæt, der skal slettes i fremtidige ajourføringer.

2.2.1. Data fra det europæiske retlige terrorbekæmpelsesregister

Følgende tekniske specifikationer for dataskemaet fastlægger en struktureret ramme for oprettelse af skemaet i XML-format.

a) Afsnit på højeste niveau

Dette afsnit på højeste niveau svarer til oplysningerne i bilag III til forordning (EU) 2018/1727, oplysninger til det europæiske retlige terrorbekæmpelsesregister (CTR).

b) Meddelelsens opbygning

CTR-datastrukturen skal bestå af en sekvens af elementer og som minimum omfatte følgende:

i) Oplysninger til identifikation af fysiske personer:

— efternavn (familienavn)

— fornavne

— eventuelle kaldenavne

— fødselsdato

— fødested (by og land)

— nationalitet eller nationaliteter

— identifikationsdokument (type og dokumentnummer)

— køn

— bopæl

ii) Oplysninger til identifikation af juridiske personer:

— firmanavn

— retlig form

— hovedkontorets adresse

iii) Oplysninger til identifikation af både fysiske og juridiske personer:

— telefonnumre

— e-mailadresser

— oplysninger om konti i banker eller andre finansieringsinstitutter

— status i sagen

iv) Oplysninger om lovovertrædelsen:

— oplysninger om juridiske personer, der medvirker til at forberede eller begå en terrorhandling

— juridisk betegnelse for lovovertrædelsen i henhold til national ret

— den relevante form for grov kriminalitet fra listen i bilag I

— eventuel tilknytning til en terrorgruppe

— terrorismens art, såsom jihadisme, separatisme, venstre- eller højreterrorisme

— et kort resumé af sagen

v) Oplysninger om nationale retssager:

— status for sådanne sager

— den ansvarlige offentlige anklagemyndighed

— sagsnummer

— dato for indledning af formel retssag

— forbindelser til andre relevante sager

vi) Felt til yderligere oplysninger (fritekst)

vii) Kode for forudgående tilladelse.

2.2.2. Oplysninger fremsendt i overensstemmelse med artikel 21 i forordning (EU) 2018/1727

a) Artikel 21, stk. 4, i forordning (EU) 2018/1727 om oprettelse af fælles efterforskningshold (»JIT'er«)

i) Afsnit på højeste niveau
Dette afsnit på højeste niveau svarer til de oplysninger, der er fastsat i artikel 21, stk. 4, i forordning (EU) 2018/1727 om oprettelse af JIT'er.

ii) Meddelelsens opbygning
Datastrukturen skal bestå af en sekvens af elementer og som minimum omfatte følgende:

— national retlig myndighed med ansvar for straffesagen

— det nationale referencenummer for straffesagen

— status for straffesagen

— efterforskede strafbare handlinger

— andre lande, der er involveret i sagen

— modtages der allerede støtte til sagen fra Eurojust?

— hvis ja, Eurojusts sags-ID?

— hvis nej, er der så tale om en anmodning om støtte?

— modtages der støtte til sagen fra Europol?

— hvis ja, drejer det sig om operationel taskforce (»OHF«) og/eller netværksprogram til sikker informationsudveksling (»SIENA«)?

— JIT-aftale:

— deltagende lande

— JIT-parter (nationale myndigheder med ansvar for efterforskningen)

— nationalt referencenummer for de straffesager, der varetages af JIT'et

— dato for undertegnelse

— varighed

— efterforskede strafbare handlinger

— et kort resumé af sagen

— hovedmistænkte i den straffesag, der varetages af JIT'et (fornavn, efternavn, fødselsdato og fødested og eventuelt andre relevante og nødvendige datakategorier jf. bilag II)

— resultater af JIT'ernes arbejde:

— vanskeligheder/forsinkelser i forbindelse med:

— oprettelse af JIT'et

— anmodning om/deling af bevismateriale inden for JIT'et

— opnåelse af enighed om/gennemførelse af en fælles retsforfølgningsstrategi

— antagelighed/uantagelighed/vurdering af JIT-bevismateriale i nationale procedurer

— resultat af retssager (vellykket/mislykket retsforfølgning og domfældelse/frifindelse)

iii) Kode for forudgående tilladelse

b) Artikel 21, stk. 5, i forordning (EU) 2018/1727, grove komplekse sager

i) Afsnit på højeste niveau

Dette afsnit på højeste niveau svarer til de oplysninger, der er fastsat i Eurojustforordningens artikel 21, stk. 5, grove komplekse sager

ii) Meddelelsens opbygning

Datastrukturen skal bestå af en sekvens af elementer og som minimum omfatte følgende:

— national retlig myndighed med ansvar for straffesagen

— det nationale referencenummer for straffesagen

— status for straffesagen

— efterforskede strafbare handlinger

— andre lande, der er involveret i sagen

— modtages der allerede støtte til sagen fra Eurojust?

— hvis ja, Eurojusts sags-ID?

— hvis nej, er der så tale om en anmodning om støtte?

— modtages der støtte til sagen fra Europol?

— hvis ja, drejer det sig om operationel taskforce og/eller SIENA?

— den omhandlede form for grov kriminalitet

— involvering af et netværk for organiseret kriminalitet

— mafia

— grænseoverskridende netværk for organiseret kriminalitet

— konsekvenser på EU-plan

— hovedmistænkte i straffesagen (fornavn, efternavn, fødselsdato og fødested og eventuelt andre relevante og nødvendige datakategorier jf. bilag II)

— et kort resumé af sagen

— andre involverede lande

— lande, med hvilke der allerede er indledt et samarbejde

— kompetente myndigheder, der er involveret i et andet land

— anvendte instrumenter til retligt samarbejde

— antal afsendte/modtagne anmodninger

— findes der indbyrdes forbundne undersøgelser?

— lande, med hvilke der planlægges samarbejde/lande, der kan blive berørt

— den type samarbejde, der er behov for (f.eks. udlevering, indsamling af bevismateriale eller andet samarbejde)

— findes der indbyrdes forbundne undersøgelser?

iii) Kode for forudgående tilladelse

c) Artikel 21, stk. 6, litra a), i forordning (EU) 2018/1727, kompetencekonflikter

i) Afsnit på højeste niveau

Dette afsnit på højeste niveau svarer til de oplysninger, der er fastsat i artikel 21, stk. 6, litra a), i forordning (EU) 2018/1727, konflikt om stedlig kompetence.

ii) Meddelelsens opbygning

Datastrukturen skal bestå af en sekvens af elementer og som minimum omfatte følgende:

— national retlig myndighed med ansvar for straffesagen

— det nationale referencenummer for straffesagen

— status for straffesagen (f.eks. efterforskning, retsforfølgning eller retssag)

— efterforskede strafbare handlinger

— andre lande, der er involveret i sagen

— modtages der allerede støtte til sagen fra Eurojust?

— hvis ja, Eurojusts sags-ID?

— hvis nej, er der så tale om en anmodning om støtte?

— modtages der støtte til sagen fra Europol?

— hvis ja, drejer det sig om operationel taskforce og/eller SIENA?

— andre involverede lande

— kompetente nationale myndigheder i det andet land, hvis de kendes

— nationalt referencenummer for straffesager i det andet land

— sagens fase i det andet land, hvis kendt

— positiv eller negativ kompetencekonflikt

— faktisk eller potentiel kompetencekonflikt

— allerede gennemførte koordineringsaktiviteter (f.eks. høringer i henhold til Rådets rammeafgørelse 2009/948/JHA ([1]))

— et kort resumé af sagen

— fælles hovedmistænkte (fornavn, efternavn, fødselsdato og fødested og eventuelt andre relevante og nødvendige datakategorier jf. bilag II)

iii) Kode for forudgående tilladelse

d) Artikel 21, stk. 6, litra b), kontrollerede leverancer

i) Afsnit på højeste niveau

Dette afsnit på højeste niveau svarer til de oplysninger, der er fastsat i artikel 21, stk. 6, litra b), i forordning (EU) 2018/1727: kontrollerede leverancer.

ii) Meddelelsens opbygning

Datastrukturen skal bestå af en sekvens af elementer og som minimum omfatte følgende:

— national retlig myndighed med ansvar for straffesagen

— det nationale referencenummer for straffesagen

— status for straffesagen (f.eks. efterforskning, retsforfølgning eller retssag)

— efterforskede strafbare handlinger

— andre lande, der er involveret i sagen

— modtages der allerede støtte til sagen fra Eurojust?

— hvis ja, Eurojusts sags-ID?

— hvis nej, er der så tale om en anmodning om støtte?

— modtages der støtte til sagen fra Europol?

— hvis ja, drejer det sig om operationel taskforce og/eller SIENA?

— andre involverede lande

— oprindelsesland/transitland/endeligt bestemmelsessted

— kompetente nationale myndigheder i andre lande

— eksistensen af forbunden efterforskning i andre lande

([1]) Rådets rammeafgørelse 2009/948/RIA af 30. november 2009 om forebyggelse og bilæggelse af konflikter om udøvelse af jurisdiktion i straffesager (EUT L 328 af 15.12.2009, s. 42, ELI: http://data.europa.eu/eli/dec_framw/2009/948/oj).

— type af leverede varer (f.eks. narkotika og type/penge/våben/cigaretter/andet)

— status for den kontrollerede leverance (f.eks. planlagt, igangværende, afsluttet)

— resultat af den kontrollerede leverance, hvis den allerede er gennemført

— anvendt instrument til retligt samarbejde

— fælles hovedmistænkte (fornavn, efternavn, fødselsdato og fødested og eventuelt andre relevante og nødvendige datakategorier jf. bilag II)

iii) Kode for forudgående tilladelse

e) Artikel 21, stk. 6, litra c), i forordning (EU) 2018/1727, gentagne vanskeligheder baseret på instrumenterne for retligt samarbejde

i) Afsnit på højeste niveau

Dette afsnit på højeste niveau svarer til de oplysninger, der er fastsat i artikel 21, stk. 6, litra c), i forordning (EU) 2018/1727: gentagne vanskeligheder baseret på instrumenter til retligt samarbejde.

ii) Meddelelsens opbygning

Datastrukturen skal bestå af en sekvens af elementer og som minimum omfatte følgende:

— national retlig myndighed med ansvar for straffesagen

— det nationale referencenummer for straffesagen

— status for straffesagen (f.eks. efterforskning, retsforfølgning eller retssag)

— efterforskede strafbare handlinger

— andre lande, der er involveret i sagen

— modtages der allerede støtte til sagen fra Eurojust?

— hvis ja, Eurojusts sags-ID?

— hvis nej, er der så tale om en anmodning om støtte?

— modtages der støtte til sagen fra Europol?

— hvis ja, drejer det sig om operationel taskforce og/eller SIENA?

— andre involverede lande

— kompetente nationale myndigheder, hvis de kendes

— der fungerer som udstedelses- eller fuldbyrdelsesmyndighed

— det involverede retlige samarbejdsinstrument (f.eks. den europæiske arrestordre, den europæiske efterforskningskendelse, indefrysning eller konfiskation)

— specifik berørt anmodning (dvs. hvilken efterforskningsforanstaltning, hvilken type indefrysning, europæisk arrestordre med henblik på fuldbyrdelse af straf eller retsforfølgning)

— afslag eller gentagne vanskeligheder

— i tilfælde af afslag, hvilken specifik grund anføres da?

— kort beskrivelse af forholdene

— eventuelle andre nationale myndigheder, der er berørt af samme forhold

iii) kode for forudgående tilladelse

2.3. *Koder for forudgående tilladelser*

Når de kompetente nationale myndigheder udveksler data med Eurojust via JUDEX, angiver de, når der er fundet en forbindelse, via koder for forudgående tilladelser, hvordan den videre behandling, adgang og overførsel af oplysninger skal forløbe. Koderne for forudgående tilladelse angiver, om og i hvilket omfang oplysninger vedrørende forbindelsen kan deles med andre kompetente nationale myndigheder, andre EU-agenturer og -organer, tredjelande eller internationale organisationer.

2.4. *Foruddefinerede meddelelser*

Foruddefinerede meddelelser er udtryk for udvekslinger, der er oprettet jf. forordning (EU) 2018/1727, men for hvilke forordningen ikke indeholder nogen specifik formular. Deres type og antal bestemmes i forbindelse med den forretningsmæssige og tekniske analyse.

XML Schema Definitions (XSD'er) for foruddefinerede meddelelser skal udformes med henblik på at sikre sammenhæng, struktur og overholdelse af forretningsmæssige behov.

For disse skemaer gælder følgende:

a) skemaets afsnit på højeste niveau skal angives i overensstemmelse med den specifikke meddelelsestype, der defineres

b) de nødvendige felter, der kræves for den specifikke meddelelsestype, skal tilføjes og defineres inden for denne struktur, så der sikres en korrekt repræsentation af dataelementerne.

2.5. *Fritekstmeddelelser*

Fritekstmeddelelser er udtryk for udvekslinger, der giver mulighed for ustruktureret eller delvist struktureret indhold, hvilket muliggør fleksibilitet, samtidig med at man fortsat overholder de lovgivningsmæssige og forretningsmæssige krav. XSD'en for fritekstmeddelelser skal udformes på en sådan måde, at der sikres sammenhæng og korrekt formatering.

For disse skemaer gælder følgende:

a) skemaets afsnit på højeste niveau skal angives i overensstemmelse med den specifikke fritekstmeddelelsestype, der defineres.

b) skemaet skal definere den nødvendige struktur for fritekstmeddelelsen, samtidig med at der gives mulighed for at tilpasse elementernes placering efter behov.

c) de nødvendige felter, der kræves for den specifikke fritekstmeddelelsestype, skal tilføjes og defineres inden for denne struktur, så der sikres en korrekt repræsentation af dataelementerne.

BILAG III

TEKNISKE SPECIFIKATIONER FOR FINGERAFTRYK OG FOTOGRAFIER

Meddelelser, der udveksles via det decentrale IT-system, kan ledsages af bilag, herunder filer fra National Institute of Standards and Technology (»NIST«), der indeholder fingeraftryk og fotografier, i overensstemmelse med de tekniske specifikationer i punkt 1 og 2.

1. **Fingeraftryk**

Fingeraftryk, der kan deles med Eurojust med henblik på pålidelig identifikation af personer, der er genstand for straffesager i forbindelse med terrorhandlinger, skal opfylde følgende betingelser:

a) fingeraftrykkene samles i én fil, der skal indeholde digitale fingeraftryksbilleder (en NIST-fingeraftryksfil), og indgives i overensstemmelse med standarden ANSI/NIST-ITL 1-2011 Update 2015 (eller nyere version)

b) NIST-fingeraftryksfilen består af op til ti individuelle fingeraftryk: enten rullede eller flade fingeraftryk eller begge dele

c) alle fingeraftryk er mærket

d) fingeraftrykkene er indsamlet ved direkte scanning eller med blæk på papir, forudsat at de fingeraftryk, der optages med blæk på papir, er blevet scannet i den krævede opløsning og i samme kvalitet

e) NIST-fingeraftryksfilen gør det muligt at medtage supplerende oplysninger såsom betingelserne for registrering af fingeraftryk og den metode, der er anvendt til at erhverve individuelle fingeraftryksbilleder

f) fingeraftrykkene har en nominel opløsning på enten 500 eller 1 000 ppi ([1]) (med en acceptabel afvigelse på +/– 10 ppi) med 256 gråtoneniveauer

g) den algoritme, der anvendes til komprimering af fingeraftryksbilleder, skal følge anbefalingerne fra National Institute of Standards and Technology (»NIST«). Fingeraftryksoplysninger med en opløsning på 500 ppi komprimeres ved hjælp af WSQ-algoritmen (ISO/IEC 19794-5:2005). Fingeraftryksoplysninger med en opløsning på 1 000 ppi komprimeres ved hjælp af JPEG 2000-billedkomprimeringsstandarden (ISO/IEC 15444-1) og -kodningssystemet. Målkomprimeringsforholdet er 15:1.

2. **Fotografier**

Fotografier, der kan deles med Eurojust med henblik på pålidelig identifikation af personer, der er genstand for straffesager i forbindelse med terrorhandlinger, skal opfylde følgende betingelser:

a) der indsendes kun ét ansigtsbillede i en fotofil (en NIST-fotofil), og det indsendes i overensstemmelse med standarden ANSI/NIST-ITL 1-2011 Update 2015 eller en nyere tilgængelig version

b) fotografierne er enten gråskala, farve eller nær infrarød

c) kvaliteten af fotografierne er baseret på billedkravene til frontalbilleder i henhold til ISO/IEC 19794-5:2011 eller en nyere tilgængelig version

d) NIST-fotofilen gør det muligt at medtage supplerende oplysninger, herunder den dato, hvor billedet blev taget

([1]) Pixel pr. tomme.

e) fotografierne i portrættilstand har en opløsning på mindst 600 pixels × 800 pixels og en maksimal opløsning på 1 200 pixels × 1 600 pixels

f) ansigtet optager tilstrækkelig plads på fotografiet til at sikre, at der er mindst 120 pixel mellem midten af hvert øje.

g) den anvendte fotokompressionsalgoritme følger anbefalingerne fra National Institute of Standards and Technology (»NIST«). Fotografier komprimeres kun én gang med JPG (ISO/IEC 10918) eller JPEG 2000 (ISO/IEC 15444) -billedkompressionsstandard og -kodningssystem ved et maksimalt tilladt billedkompressionsforhold på 20:1.