Publicatieblad
van de Europese Unie

NL
L-serie

2025/2447

5.12.2025

UITVOERINGSVERORDENING (EU) 2025/2447 VAN DE COMMISSIE

van 4 december 2025

tot vaststelling van de regels voor de toepassing van Verordening (EU) 2018/1727 van het Europees Parlement en de Raad, wat betreft de technische specificaties, maatregelen en andere vereisten voor de instelling en het gebruik van het gedecentraliseerde IT-systeem voor de beveiligde verwerking en verstrekking van informatie

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) 2018/1727 van het Europees Parlement en de Raad van 14 november 2018 betreffende het Agentschap van de Europese Unie voor justitiële samenwerking in strafzaken (Eurojust), en tot vervanging en intrekking van Besluit 2002/187/JBZ van de Raad ([1]), en met name artikel 22 bis, lid 3, en artikel 22 ter, lid 1, punten a), b) c) en d),

Overwegende hetgeen volgt:

(1) Verordening (EU) 2018/1727 voorziet in het kader voor de nieuwe digitale interne infrastructuur van Eurojust en in de instelling van een gedecentraliseerd beveiligd digitaal communicatiesysteem tussen de bevoegde nationale autoriteiten van de lidstaten en Eurojust.

(2) De beveiligde digitale communicatie moet worden uitgevoerd via het gedecentraliseerde IT-systeem. Voor het instellen van het gedecentraliseerde IT-systeem moeten technische specificaties ter bepaling van de communicatiemethoden en de communicatieprotocollen, technische maatregelen ter waarborging van minimumnormen voor informatiebeveiliging en beveiliging en minimumbeschikbaarheidsdoelstellingen voor de implementatie van dat systeem worden vastgesteld.

(3) Overeenkomstig artikel 22 bis, lid 1, van Verordening (EU) 2018/1727 moet het gedecentraliseerde IT-systeem bestaan uit de IT-systemen van de lidstaten en van Eurojust en interoperabele e-Codex-toegangspunten die die IT-systemen met elkaar verbinden. In de technische specificaties en andere vereisten voor het gedecentraliseerde IT-systeem die in deze verordening zijn vastgesteld, moet dat kader in acht worden genomen.

(4) De toegangspunten van het gedecentraliseerde IT-systeem moeten zijn gebaseerd op geautoriseerde e-Codex-toegangspunten zoals gedefinieerd in artikel 3, punt 3), van Verordening (EU) 2022/850 van het Europees Parlement en de Raad ([2]).

(5) Het gedecentraliseerde IT-systeem wordt geïmplementeerd binnen een groter op e-Codex gebaseerd gedecentraliseerd IT-systeem, Judex (Justice Digital Exchange System). Daartoe moet worden gezorgd voor een doeltreffende uitwisseling van informatie over horizontale ontwikkelingen.

(6) Overeenkomstig artikel 22 bis, lid 4, van Verordening (EU) 2018/1727 kunnen de lidstaten en Eurojust ervoor kiezen om de door de Commissie ontwikkelde referentie-implementatiesoftware te gebruiken als hun back-endsysteem, in plaats van een nationaal IT-systeem. Om de interoperabiliteit te waarborgen, moeten zowel de nationale IT-systemen als de referentie-implementatiesoftware aan dezelfde technische specificaties en vereisten voldoen.

(7) Gegevens met betrekking tot strafbare feiten van terroristische aard en ernstige georganiseerde criminaliteit moeten op gestructureerde wijze worden doorgegeven om de kwaliteit en relevantie van de informatie te verbeteren en ervoor te zorgen dat de informatie efficiënter kan worden geïntegreerd in het casemanagementsysteem van Eurojust en beter kan worden vergeleken met informatie die reeds in dat systeem is opgeslagen. Voor vingerafdrukgegevens en foto's die aan Eurojust kunnen worden doorgegeven met het oog op de identificatie van personen tegen wie een strafprocedure in verband met strafbare feiten van terroristische aard loopt, moeten het formaat en de technische normen voor de doorgifte worden vastgesteld.

([1]) PB L 295 van 21.11.2018, blz. 138, ELI: http://data.europa.eu/eli/reg/2018/1727/oj.

([2]) Verordening (EU) 2022/850 van het Europees Parlement en de Raad van 30 mei 2022 betreffende een geautomatiseerd systeem voor de grensoverschrijdende elektronische gegevensuitwisseling op het gebied van justitiële samenwerking in civiele en strafzaken (e-Codex), en tot wijziging van Verordening (EU) 2018/1726 (PB L 150 van 1.6.2022, blz. 1, ELI: http://data.europa.eu/eli/reg/2022/850/oj).

(8) Eurojust vergemakkelijkt en ondersteunt de indiening en tenuitvoerlegging van verzoeken om justitiële samenwerking, waaronder de verzoeken en besluiten die zijn gebaseerd op instrumenten waarmee uitvoering wordt gegeven aan het beginsel van wederzijdse erkenning. De nationale bevoegde autoriteiten moeten Eurojust via het gedecentraliseerde IT-systeem om bijstand en coördinatie kunnen verzoeken.

(9) Om efficiëntie en consistentie te waarborgen, is het belangrijk dat de op grond van Verordening (EU) 2018/1727 vast te stellen technische specificaties verenigbaar zijn met de technische specificaties die zijn vastgesteld op grond van de Verordeningen (EU) 2023/2844 ([3]), (EU) 2023/1543 ([4]) en (EU) 2024/3011 ([5]) van het Europees Parlement en de Raad, evenals met toekomstige digitaliseringsmaatregelen die relevant zijn voor de taak van Eurojust om de nationale bevoegde autoriteiten te ondersteunen.

(10) Alle andere communicatie tussen Eurojust en de bevoegde nationale autoriteiten, zoals de verstrekking van informatie over de resultaten van de verwerking van informatie, met inbegrip van het bestaan van verbanden met zaken die reeds overeenkomstig artikel 22 van Verordening (EU) 2018/1727 in het casemanagementsysteem zijn opgeslagen wanneer Eurojust op eigen initiatief handelt, of van informatie die aan Eurojust is doorgegeven met het oog op het bewaren, analyseren en opslaan van bewijsmateriaal met betrekking tot genocide, misdaden tegen de menselijkheid, oorlogsmisdaden en daarmee verband houdende strafbare feiten overeenkomstig artikel 4, lid 1, punt j), van die verordening, moet ook via het gedecentraliseerde IT-systeem mogelijk worden gemaakt.

(11) Om ervoor te zorgen dat de operationele behoeften van Eurojust in deze verordening naar behoren in aanmerking worden genomen, is Eurojust geraadpleegd overeenkomstig artikel 22 bis, lid 3, van Verordening (EU) 2018/1727.

(12) Overeenkomstig artikel 4 van Protocol nr. 21 betreffende de positie van het Verenigd Koninkrijk en Ierland ten aanzien van de ruimte van vrijheid, veiligheid en recht, gehecht aan het Verdrag betreffende de Europese Unie en het Verdrag betreffende de werking van de Europese Unie, heeft Ierland, bij brief van 9 september 2019, kennisgegeven van zijn wens Verordening (EU) 2018/1727 te aanvaarden en erdoor gebonden te zijn. Deze deelname is bevestigd bij Besluit (EU) 2019/2006 van de Commissie ([6]). Verordening (EU) 2018/1727 is gewijzigd bij Verordening (EU) 2023/2131 van het Europees Parlement en de Raad ([7]) om beveiligde digitale communicatiekanalen tussen Eurojust en de bevoegde nationale autoriteiten mogelijk te maken en vormt de rechtsgrondslag voor deze verordening. Aangezien Ierland geen kennis heeft gegeven van zijn wens deel te nemen aan de vaststelling en toepassing van Verordening (EU) 2023/2131 en geen kennis heeft gegeven van zijn wens deze verordening te aanvaarden en erdoor gebonden te zijn, is Ierland, overeenkomstig de artikelen 1 en 2 en artikel 4 bis, lid 1, van Protocol nr. 21, niet gebonden door Verordening (EU) 2023/2131 of onderworpen aan de toepassing ervan. Bijgevolg neemt Ierland niet deel aan de vaststelling van deze verordening.

(13) Overeenkomstig de artikelen 1 en 2 van Protocol nr. 22 betreffende de positie van Denemarken, gehecht aan het Verdrag betreffende de Europese Unie en het Verdrag betreffende de werking van de Europese Unie, heeft Denemarken niet deelgenomen aan de vaststelling van Verordening (EU) 2018/1727. Deze verordening is derhalve niet bindend voor, noch van toepassing in Denemarken.

([3]) Verordening (EU) 2023/2844 van het Europees Parlement en de Raad van 13 december 2023 betreffende de digitalisering van de justitiële samenwerking en de toegang tot de rechter in grensoverschrijdende burgerlijke, handels- en strafzaken, en tot wijziging van bepaalde handelingen op het gebied van justitiële samenwerking (PB L, 2023/2844, 27.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2844/oj).

([4]) Verordening (EU) 2023/1543 van het Europees Parlement en de Raad van 12 juli 2023 betreffende het Europees verstrekkingsbevel en het Europees bewaringsbevel voor elektronisch bewijsmateriaal in strafzaken en de tenuitvoerlegging van vrijheidsstraffen als gevolg van een strafprocedure (PB L 191 van 28.7.2023, blz. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

([5]) Verordening (EU) 2024/3011 van het Europees Parlement en de Raad van 27 november 2024 betreffende de overdracht van strafvervolging (PB L, 2024/3011, 18.12.2024, ELI: http://data.europa.eu/eli/reg/2024/3011/oj).

([6]) Besluit (EU) 2019/2006 van de Commissie van 29 november 2019 betreffende de deelneming van Ierland aan Verordening (EU) 2018/1727 van het Europees Parlement en de Raad betreffende het Agentschap van de Europese Unie voor justitiële samenwerking in strafzaken (Eurojust) (PB L 310 van 2.12.2019, blz. 59, ELI: http://data.europa.eu/eli/dec/2019/2006/oj).

([7]) Verordening (EU) 2023/2131 van het Europees Parlement en de Raad van 4 oktober 2023 tot wijziging van Verordening (EU) 2018/1727 van het Europees Parlement en de Raad en van Besluit 2005/671/JBZ van de Raad, wat de uitwisseling van digitale informatie in terrorismezaken betreft (PB L, 2023/2131, 11.10.2023, ELI: http://data.europa.eu/eli/reg/2023/2131/oj).

(14) De Europese Toezichthouder voor gegevensbescherming is geraadpleegd overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ([8]) en heeft op 21 oktober 2025 een advies uitgebracht.

(15) De in deze verordening vervatte maatregelen zijn in overeenstemming met het advies van het bij artikel 22 quater van Verordening (EU) 2018/1727 ingestelde comité,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

Technische specificaties van het gedecentraliseerde IT-systeem

De technische specificaties, maatregelen en doelstellingen van het gedecentraliseerde IT-systeem bedoeld in artikel 22 ter, lid 1, punten a), b), c) en d), van Verordening (EU) 2018/1727 zijn die welke zijn opgenomen in bijlage I bij deze verordening.

Artikel 2

Digitale procesnormen

De digitale procesnormen die van toepassing zijn op de elektronische communicatie via het in artikel 22 bis, lid 3, van Verordening (EU) 2018/1727 bedoelde gedecentraliseerde IT-systeem, zijn die welke zijn opgenomen in bijlage II bij deze verordening.

Artikel 3

Technische specificaties voor de doorgifte van vingerafdrukken en foto's

De technische specificaties en het formaat voor de doorgifte van vingerafdrukken en foto's bedoeld in artikel 22 bis, lid 3, van Verordening (EU) 2018/1727 zijn die welke zijn opgenomen in bijlage III bij deze verordening.

Artikel 4

Inwerkingtreding

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in de lidstaten overeenkomstig de Verdragen.

Gedaan te Brussel, 4 december 2025.

Voor de Commissie
De voorzitter
Ursula VON DER LEYEN

([8]) Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

BIJLAGE I

TECHNISCHE SPECIFICATIES, MAATREGELEN EN DOELSTELLINGEN VAN HET GEDECENTRALISEERDE IT-SYSTEEM

1. **Inleiding en reikwijdte**

Deze bijlage bevat de technische specificaties, maatregelen en doelstellingen van het gedecentraliseerde IT-systeem voor de uitwisseling van informatie uit hoofde van Verordening (EU) 2018/1727.

Het gedecentraliseerde karakter van het IT-systeem maakt de rechtstreekse en beveiligde uitwisseling van gegevens tussen de bevoegde nationale autoriteiten en Eurojust mogelijk.

2. **Definities**

Voor de toepassing van deze bijlage wordt verstaan onder:

2.1. "HyperText Transfer Protocol Secure" of "HTTPS": versleutelde kanalen voor communicatie en beveiligde verbinding;

2.2. "onweerlegbaarheid van de herkomst": de maatregelen die het bewijs van de integriteit en van de herkomst van de gegevens leveren via methoden zoals digitale certificering, publiekesleutelinfrastructuur, elektronische handtekeningen en elektronische zegels;

2.3. "onweerlegbaarheid van de ontvangst": de maatregelen die aan de verzender van de gegevens het bewijs van ontvangst door de beoogde ontvanger leveren via methoden zoals digitale certificering, publiekesleutelinfrastructuur, elektronische handtekeningen en elektronische zegels;

2.4. "SOAP" (Simple Object Access Protocol): een met de normen van het World Wide Web Consortium overeenstemmende specificatie van een berichtenprotocol voor de uitwisseling van gestructureerde informatie bij de implementatie van webdiensten in computernetwerken;

2.5. "REST" (Representational State Transfer): een voor het ontwerp van netwerktoepassingen gebruikt type architectuur op basis van een stateless client/server-communicatiemodel dat gebruikmaakt van standaardmethoden voor het uitvoeren van acties op doorgaans in gestructureerde formaten weergegeven bronnen;

2.6. "webdienst": een softwaresysteem ontworpen voor de ondersteuning van interoperabele machine-tot-machine netwerkinteractie dat een in een machinaal verwerkbaar formaat beschreven interface heeft;

2.7. "gegevensuitwisseling": de uitwisseling van berichten en stukken via het gedecentraliseerde IT-systeem;

2.8. "e-Codex": het e-Codex-systeem zoals gedefinieerd in artikel 3, punt 1), van Verordening (EU) 2022/850;

2.9. "EU e-Justice Core Vocabularies": de EU e-Justice Core Vocabularies zoals gedefinieerd in punt 4) van de bijlage bij Verordening (EU) 2022/850;

2.10. "ebMS": de in het kader van OASIS ontwikkelde ebXML-berichtendienst die de beveiligde, betrouwbare en interoperabele uitwisseling van elektronische bedrijfsdocumenten die SOAP gebruiken, mogelijk maakt, en daarmee de integratie tussen bedrijven onderling in verschillende systemen ondersteunt;

2.11. "AS4": Applicability Statement 4, een OASIS-norm die ebMS 3.0 profileert; beveiligd en interoperabel berichtenverkeer tussen bedrijven onderling wordt vereenvoudigd door gebruik te maken van open standaarden zoals SOAP en WS-beveiliging;

2.12. “hersteltijddoelstelling”: de maximaal toegestane tijd om na een incident de dienstverlening te hervatten;

2.13. “herstelpuntdoelstelling”: het maximaal aanvaardbare gegevensverlies bij een defect.

3. **Methoden voor elektronische communicatie**

3.1. Het gedecentraliseerde IT-systeem maakt voor het uitwisselen van berichten en stukken gebruik van op diensten gebaseerde methoden voor elektronische communicatie, zoals webdiensten of andere herbruikbare onderdelen en softwareoplossingen.

3.2. Specifiek behelst het gedecentraliseerde IT-systeem communicatie via e-Codex-toegangspunten, zoals bepaald in artikel 5, lid 2, van Verordening (EU) 2022/850. Om een doeltreffende en interoperabele grensoverschrijdende gegevensuitwisseling te waarborgen, ondersteunt het gedecentraliseerde IT-systeem derhalve communicatie via het e-Codex-systeem.

4. **Communicatieprotocollen**

4.1. Het gedecentraliseerde IT-systeem maakt gebruik van beveiligde internetprotocollen voor:

a) communicatie binnen het gedecentraliseerde IT-systeem tussen bevoegde autoriteiten en Eurojust;

b) communicatie met de databank van de bevoegde autoriteiten/rechtbanken als bedoeld in punt 7.1.

4.2. Voor de definitie en de doorgifte van gestructureerde gegevens en metagegevens worden de onderdelen van het gedecentraliseerde IT-systeem gebaseerd op uitgebreide en algemeen aanvaarde industrienormen en -protocollen, zoals SOAP en REST.

4.3. Voor de Transport Protocols en Messaging Protocols wordt het gedecentraliseerde IT-systeem gebaseerd op protocollen die op grond van beveiligingsnormen werken, zoals:

a) AS4 Profile voor grensoverschrijdende uitwisseling van gegevens, dat beveiligd, betrouwbaar, versleuteld en onweerlegbaar berichtenverkeer waarborgt;

b) HTTPS/RESTful API’s voor communicatie op basis van JSON- en XML-formaten;

c) SOAP voor interacties met hoge betrouwbaarheid waarin WS-beveiliging voor authenticatie en versleuteling is geïntegreerd.

4.4. Met het oog op een naadloze en interoperabele uitwisseling van gegevens voldoen de door het gedecentraliseerde IT-systeem gebruikte communicatieprotocollen aan de relevante interoperabiliteitsnormen.

4.5. In voorkomend geval maken de XML-schema’s gebruik van relevante normen of vocabularia die nodig zijn voor de correcte validatie van de in dit schema gedefinieerde elementen en typen. Die normen of vocabularia kunnen zijn:

a) EU e-Justice Core Vocabulary;

b) Unqualified Data Types;

c) een codelijst voor de European Union Language Codes.

4.6. Voor de beveiligings- en authenticatieprotocollen wordt het gedecentraliseerde IT-systeem op op normen gebaseerde protocollen gegrond, zoals:

a) TLS (Transport Layer Security) voor versleutelde en geauthentiseerde communicatie via netwerken, dat wederzijdse authenticatie via X.509-certificaten ondersteunt;

b) OAuth/OpenID Connect (OIDC) voor beveiligde authenticatie en autorisatie;

c) PKI (publiekesleutelinfrastructuur) en digitale handtekeningen voor beveiligde uitwisseling van sleutels en verificatie van de integriteit van berichten, waarbij door betrouwbare certificatieautoriteiten afgegeven digitale certificaten (X.509) worden gebruikt.

5. **Doelstellingen inzake informatiebeveiliging en relevante technische maatregelen**

5.1. Voor de informatie-uitwisseling via het gedecentraliseerde IT-systeem worden onder meer de volgende technische maatregelen toegepast om minimumnormen voor IT-beveiliging te waarborgen:

a) maatregelen om de vertrouwelijkheid van de informatie te waarborgen, waaronder het gebruik van beveiligde communicatiekanalen;

b) maatregelen om de integriteit van gegevens in rust en in transit te waarborgen;

c) maatregelen ter waarborging van de onweerlegbaarheid van de herkomst van de verzender van de informatie in het gedecentraliseerde IT-systeem en de onweerlegbaarheid van de ontvangst van informatie;

d) maatregelen die waarborgen dat beveiligingsincidenten worden vastgelegd in een logbestand overeenkomstig erkende internationale aanbevelingen voor normen voor IT-beveiliging ([1]);

e) maatregelen voor gebruikersauthenticatie en -autorisatie en maatregelen ter verificatie van de identiteit van de met het gedecentraliseerde IT-systeem verbonden systemen.

5.2. De onderdelen van het gedecentraliseerde IT-systeem waarborgen beveiligde communicatie en doorgifte van gegevens door gebruik te maken van versleuteling, publiekesleutelinfrastructuur met digitale certificaten voor authenticatie en beveiligde sleuteluitwisseling, en beveiligde berichtenprotocollen zoals AS4 (ebMS), RESTful API's en SOAP om de vertrouwelijkheid en integriteit van berichten te beschermen.

5.3. Wanneer TLS wordt gebruikt in de context van het gedecentraliseerde IT-systeem, wordt de meest recente stabiele versie van het protocol gebruikt, of, bij gebreke daarvan, een versie zonder bekende beveiligingskwestbaarheden. Alleen sleutellengten die een adequaat niveau van cryptografische beveiliging garanderen, zijn toegestaan, en het gebruik van coderingssuites waarvan bekend is dat zij onveilig of verouderd zijn, is niet toegestaan.

5.4. Voor zover mogelijk worden digitale PKI-certificaten die voor de werking van het gedecentraliseerde IT-systeem worden gebruikt, afgegeven door certificatieautoriteiten die overeenkomstig Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad ([2]) zijn erkend als gekwalificeerde verleners van vertrouwensdiensten. Er worden maatregelen genomen om ervoor te zorgen dat dergelijke certificaten uitsluitend worden gebruikt voor de beoogde doeleinden, op het vereiste betrouwbaarheidsniveau en in overeenstemming met de toepasselijke vereisten van Verordening (EU) nr. 910/2014.

5.5. De onderdelen van het gedecentraliseerde IT-systeem worden ontwikkeld in overeenstemming met het beginsel van gegevensbescherming door ontwerp en door standaardinstellingen, en er worden passende administratieve, organisatorische en technische maatregelen genomen om een hoog niveau van cyberbeveiliging te waarborgen.

5.6. De Commissie ontwerpt, ontwikkelt en onderhoudt de referentie-implementatiesoftware overeenkomstig de voorschriften en beginselen inzake gegevensbescherming van Verordening (EU) 2018/1725. De door de Commissie verstrekte referentie-implementatiesoftware stelt de lidstaten in staat te voldoen aan hun verplichtingen uit hoofde van Verordening (EU) 2016/679 van het Europees Parlement en de Raad ([3]) en Richtlijn (EU) 2016/680, naargelang het geval.

([1]) Onverminderd de vastlegging in een logbestand voor beveiligingsdoeleinden, maken de logmechanismen die door de onderdelen van het gedecentraliseerde IT-systeem worden gebruikt, voor zover passend, naleving mogelijk van de vereisten van artikel 88 van Verordening (EU) 2018/1725, en indien van toepassing, van artikel 25 van Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (PB L 119 van 4.5.2016, blz. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

([2]) Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (PB L 257 van 28.8.2014, blz. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([3]) Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

5.7. Lidstaten die een ander nationaal back-endsysteem gebruiken dan de referentie-implementatiesoftware, treffen de nodige maatregelen om te waarborgen dat hun nationale back-endsysteem voldoet aan de vereisten van Verordening (EU) 2016/679 en Richtlijn (EU) 2016/680, naargelang het geval.

5.8. Eurojust treft de nodige maatregelen om te waarborgen dat zijn back-endsysteem, of een instantie van de referentie-implementatiesoftware die het uitrolt, voldoet aan de vereisten van de Verordeningen (EU) 2018/1725 en (EU) 2018/1727.

5.9. De lidstaten en Eurojust brengen robuuste mechanismen voor dreigingsdetectie en incidentrespons tot stand om tijdige identificatie, beperking en herstel van veiligheidsincidenten te waarborgen, in overeenstemming met hun relevante beleidsmaatregelen, voor de onder hun verantwoordelijkheid vallende IT-systemen die deel uitmaken van het gedecentraliseerde IT-systeem.

6. **Minimumbeschikbaarheidsdoelstellingen**

6.1. Eurojust en de lidstaten waarborgen dat de onderdelen van het gedecentraliseerde IT-systeem die onder hun verantwoordelijkheid vallen, 24 uur per dag en zeven dagen per week beschikbaar zijn, waarbij de nagestreefde technische beschikbaarheidsgraad ervan ten minste 98 % op jaarbasis moet bedragen, gepland onderhoud buiten beschouwing gelaten.

6.2. De Commissie waarborgt dat de databank van rechtbanken 24 uur per dag en zeven dagen per week beschikbaar is, waarbij de nagestreefde technische beschikbaarheidsgraad ervan ten minste 99 % op jaarbasis moet bedragen, gepland onderhoud buiten beschouwing gelaten.

6.3. Voor zover mogelijk moeten tijdens werkdagen de onderhoudswerkzaamheden worden gepland tussen 20.00 uur en 7.00 uur Midden-Europese tijd.

6.4. De lidstaten stellen de Commissie, Eurojust en de andere lidstaten als volgt in kennis van onderhoudswerkzaamheden:

a) onderhoudswerkzaamheden waardoor het systeem maximaal vier uur buiten werking kan zijn: vijf werkdagen van tevoren;

b) onderhoudswerkzaamheden waardoor het systeem tussen vier en twaalf uur buiten werking kan zijn: tien werkdagen van tevoren;

c) onderhoudswerkzaamheden waardoor het systeem meer dan twaalf uur buiten werking kan zijn: dertig werkdagen van tevoren.

6.5. Wanneer lidstaten vaste en regelmatige onderhoudsperioden hebben, stellen zij de Commissie, Eurojust en de andere lidstaten in kennis van het tijdstip en de dag(en) waarop dergelijke vaste en regelmatige perioden zijn gepland. In afwijking van de in eerste zin bedoelde verplichtingen kunnen de lidstaten, ingeval onderdelen van het gedecentraliseerde IT-systeem die onder de verantwoordelijkheid van de lidstaten vallen tijdens een dergelijke vaste en regelmatige periode niet beschikbaar zijn, ervoor kiezen de Commissie niet telkens in kennis te stellen.

6.6. Bij een onverwacht technisch defect aan een onderdeel van het gedecentraliseerde IT-systeem dat onder de verantwoordelijkheid van de lidstaten valt, stellen zij de Commissie en de andere lidstaten onverwijld in kennis van dat defect en, indien bekend, van de verwachte hersteltijd.

6.7. Eurojust stelt de Commissie en de lidstaten als volgt in kennis van onderhoudsactiviteiten:

a) onderhoudswerkzaamheden waardoor het systeem maximaal vier uur buiten werking kan zijn: vijf werkdagen van tevoren;

b) onderhoudswerkzaamheden waardoor het systeem tussen vier en twaalf uur buiten werking kan zijn: tien werkdagen van tevoren;

c) onderhoudswerkzaamheden waardoor het systeem meer dan twaalf uur buiten werking kan zijn: dertig werkdagen van tevoren.

6.8. Wanneer Eurojust vaste en regelmatige onderhoudsperioden heeft, stelt Eurojust de Commissie en de lidstaten in kennis van het tijdstip en de dag(en) waarop dergelijke vaste en regelmatige perioden zijn gepland. In afwijking van de in eerste zin bedoelde verplichtingen kan Eurojust, ingeval onderdelen van het gedecentraliseerde IT-systeem die onder de verantwoordelijkheid van Eurojust vallen tijdens een dergelijke vaste en regelmatige periode niet beschikbaar zijn, ervoor kiezen de Commissie niet telkens in kennis te stellen.

6.9. Bij een onverwacht technisch defect aan een onderdeel van het gedecentraliseerde IT-systeem dat onder de verantwoordelijkheid van Eurojust valt, stelt Eurojust de Commissie en de lidstaten onverwijld in kennis van dat defect en, indien bekend, van de verwachte hersteltijd.

6.10. Bij een onverwacht technisch defect van de databank van bevoegde autoriteiten/rechtbanken stelt de Commissie Eurojust en de lidstaten onverwijld in kennis van de onbeschikbaarheid ervan en, indien bekend, van de verwachte hersteltijd.

6.11. Bij een storing aan de dienstverlening zorgen de lidstaten en Eurojust er in overeenstemming met de hersteltijd-doelstelling en de herstelpuntdoelstelling voor dat de dienst snel wordt hersteld en dat zo min mogelijk gegevens verloren gaan.

6.12. De lidstaten en Eurojust treffen passende maatregelen om bovengenoemde beschikbaarheidsdoelstellingen te verwezenlijken en brengen procedures voor een doeltreffende incidentrespons tot stand.

7. **Databank van bevoegde autoriteiten/rechtbanken**

7.1. Overeenkomstig artikel 22 bis van Verordening (EU) 2018/1727 maakt het gedecentraliseerde IT-systeem elektronische communicatie tussen de bevoegde nationale autoriteiten en Eurojust mogelijk. Gezien de verplichtingen inzake uitwisseling van informatie tussen de bevoegde nationale autoriteiten en Eurojust uit hoofde van de artikelen 21, 21 bis en 22, maar ook de rol van Eurojust bij het faciliteren en ondersteunen van de indiening en tenuitvoerlegging van verzoeken om wederzijdse rechtshulp of wederzijdse erkenning overeenkomstig artikel 8, lid 1, van Verordening (EU) 2018/1727, moeten de betrokken bevoegde autoriteiten duidelijk identificeerbaar zijn wanneer zij het gedecentraliseerde IT-systeem gebruiken. Daarom is het van essentieel belang om voor het gedecentraliseerde IT-systeem een gezaghebbende databank van informatie over die autoriteiten op te zetten.

7.2. De databank van bevoegde autoriteiten/rechtbanken bevat de volgende informatie in een gestructureerd formaat:

a) voor de toepassing van artikel 8, leden 1, 3 en 4, artikel 21, artikel 21 bis en artikel 22 van Verordening (EU) 2018/1727, informatie over de bevoegde nationale autoriteiten, met inbegrip van nationale correspondenten als bedoeld in artikel 20 van die verordening en nationale leden overeenkomstig artikel 7 ([4]) van die verordening;

b) in voorkomend geval, de informatie die nodig is om de geografische of inhoudelijke werkgebieden van de bevoegde autoriteiten te bepalen, of andere relevante criteria die nodig zijn om hun bevoegdheid vast te stellen;

c) de informatie die nodig is voor de correcte technische routebepaling van berichten binnen het gedecentraliseerde IT-systeem.

7.3. De Commissie is verantwoordelijk voor de ontwikkeling, het onderhoud, het beheer en de ondersteuning van de databank van bevoegde autoriteiten/rechtbanken.

7.4. De databank van bevoegde autoriteiten/rechtbanken stelt de lidstaten en Eurojust in staat de informatie in de databank bij te werken, en de bevoegde nationale autoriteiten en nationale leden die deelnemen aan het gedecentraliseerde IT-systeem om programmatisch toegang te krijgen tot de informatie in de databank en deze op te vragen.

7.5. Toegang tot de databank van bevoegde autoriteiten/rechtbanken is mogelijk via een gemeenschappelijk communicatieprotocol, ongeacht of de bevoegde autoriteiten die op het gedecentraliseerde IT-systeem zijn aangesloten, een nationaal back-endsysteem gebruiken dan wel de referentie-implementatiesoftware uitrollen.

7.6. De lidstaten zorgen ervoor dat de in punt 7.2 bedoelde informatie over hun bevoegde autoriteiten in de databank van bevoegde autoriteiten/rechtbanken volledig en nauwkeurig is en actueel blijft.

([4]) Dit laat de delegatie van bevoegdheden van het nationale lid aan zijn plaatsvervanger, andere personeelsleden van het nationale bureau of bevoegd personeel van Eurojust onverlet.

BIJLAGE II

DIGITALE PROCESNORMEN

In artikel 3, punt 9), van Verordening (EU) 2022/850 worden digitale procesnormen gedefinieerd als de technische specificaties voor bedrijfsprocesmodellen en gegevensschema's, waarin de elektronische structuur van de via het e-Codex-systeem uitgewisselde gegevens wordt gedefinieerd.

Deze bijlage bevat de technische specificaties voor de bedrijfsprocesmodellen en de technische specificaties voor de gegevensschema's.

1. **Technische specificaties voor de bedrijfsprocesmodellen uit hoofde van Verordening (EU) 2018/1727**

De technische specificaties voor bedrijfsprocesmodellen worden uiteengezet in de punten 1.1 tot en met 1.5. Deze specificaties bestrijken de belangrijkste aspecten die nodig zijn om elektronische communicatie voor de toepassing van Verordening (EU) 2018/1727 via het gedecentraliseerde IT-systeem mogelijk te maken.

Het gedecentraliseerde IT-systeem maakt alleen uitwisseling van informatie tussen de bevoegde nationale autoriteiten van een lidstaat en het nationale lid van die lidstaat mogelijk.

1.1. *Uitwisseling van informatie in verband met het Europees gerechtelijk register voor terrorismebestrijding (CTR) — artikel 21 bis van Verordening (EU) 2018/1727*

1.1.1. Model voor het doorgeven van CTR-gegevens:

De bevoegde nationale autoriteit stuurt gegevens over terrorismeprocedures voor het CTR door aan het nationale lid.

1.1.2. Model voor het ontvangen van CTR-gegevens:

Het nationale lid ontvangt de CTR-gegevens.

1.1.3. Model voor een verzoek om toestemming:

Het nationale lid verzoekt zijn bevoegde nationale autoriteit om toestemming.

1.1.4. Model voor het ontvangen van een verzoek om toestemming:

De bevoegde nationale autoriteit ontvangt het verzoek om toestemming.

1.1.5. Model voor het versturen van een antwoord op het verzoek om toestemming:

De bevoegde nationale autoriteit verstuurt een antwoord op het verzoek om toestemming.

1.1.6. Model voor het ontvangen van het antwoord op het verzoek om toestemming:

Het nationale lid ontvangt het antwoord op het verzoek om toestemming.

1.1.7. Model voor informatie over verbanden:

Het nationale lid informeert de bevoegde nationale autoriteit over een verband met een andere zaak.

1.1.8. Model voor het bijwerken van CTR-gegevens:

De bevoegde nationale autoriteit stuurt bij te werken of te wissen gegevens door aan haar nationale lid.

1.1.9. Model voor het ontvangen van bijgewerkte CTR-gegevens:

Het nationale lid ontvangt de CTR-gegevens die moeten worden bijgewerkt of gewist.

1.2. *Uitwisseling van informatie in verband met ernstige criminaliteit — artikel 21 van Verordening (EU) 2018/1727*

1.2.1. Model voor het doorgeven van gegevens over ernstige grensoverschrijdende criminaliteit:

De bevoegde nationale autoriteit stuurt gegevens over ernstige grensoverschrijdende criminaliteit door aan Eurojust.

1.2.2. Model voor het ontvangen van gegevens over ernstige grensoverschrijdende criminaliteit:

Het nationale lid ontvangt de gegevens over ernstige grensoverschrijdende criminaliteit.

1.2.3. Model voor een verzoek om toestemming:

Het nationale lid verzoekt zijn bevoegde nationale autoriteit om toestemming.

1.2.4. Model voor het ontvangen van een verzoek om toestemming:

De bevoegde nationale autoriteit ontvangt het verzoek om toestemming.

1.2.5. Model voor het versturen van een antwoord op het verzoek om toestemming:

De bevoegde nationale autoriteit verstuurt een antwoord op het verzoek om toestemming.

1.2.6. Model voor het ontvangen van het antwoord op het verzoek om toestemming:

Het nationale lid ontvangt het antwoord op het verzoek om toestemming.

1.2.7. Model voor informatie over verbanden:

Het nationale lid informeert de bevoegde nationale autoriteit over een verband met een andere zaak.

1.2.8. Model voor het bijwerken van gegevens over ernstige grensoverschrijdende criminaliteit:

De bevoegde nationale autoriteit stuurt bij te werken of te wissen gegevens door aan haar nationale lid.

1.2.9. Model voor het ontvangen van bijgewerkte gegevens over ernstige grensoverschrijdende criminaliteit:

Het nationale lid ontvangt de gegevens over ernstige grensoverschrijdende criminaliteit die moeten worden bijgewerkt of gewist.

1.3. *Uitwisseling van algemene informatie*

1.3.1. Model voor het versturen van informatie:

Het nationale lid verstuurt informatie aan de bevoegde nationale autoriteit of vice versa.

1.3.2. Model voor het ontvangen van informatie:

De bevoegde nationale autoriteit of het nationale lid ontvangt de informatie.

1.3.3. Model voor het versturen van een antwoord op de informatie:

De bevoegde nationale autoriteit verstuurt een antwoord op de van het nationale lid ontvangen informatie of vice versa.

1.3.4. Model voor het ontvangen van het antwoord:

Het nationale lid ontvangt het antwoord van de bevoegde nationale autoriteit.

1.3.5. Model voor het versturen van informatie:

De bevoegde nationale autoriteit verstuurt informatie aan het nationale lid.

1.3.6. Model voor het ontvangen van informatie:

Het nationale lid ontvangt de informatie.

1.3.7. Model voor het versturen van een antwoord op de informatie:

Het nationale lid verstuurt een antwoord op de van de bevoegde nationale autoriteit ontvangen informatie.

1.3.8. Model voor het ontvangen van het antwoord:

De bevoegde nationale autoriteit ontvangt het antwoord van het nationale lid.

1.4. *Faciliterende en ondersteunende rol — Artikel 8, lid 1, van Verordening (EU) 2018/1727*

Opmerking: Indien de in punt 1.5 beschreven modellen voor het faciliteren of ondersteunen van de indiening en tenuitvoerlegging van verzoeken voorzien in de uitwisseling van wettelijk vereiste formulieren die zijn vastgesteld bij rechtshandelingen van de Unie op het gebied van justitiële samenwerking in strafzaken, maken de modellen, indien beschikbaar, gebruik van de relevante gestructureerde gegevensweergaven en XML-schema's die voor die handelingen zijn ontwikkeld, bijvoorbeeld die welke zijn vastgesteld met het oog op de uitvoering van Verordening (EU) 2023/2844 of andere relevante instrumenten.

1.5. *Model voor het faciliteren of ondersteunen van verzoeken*

1.5.1. Model voor doorgeven van een verzoek om facilitering of ondersteuning:

De bevoegde nationale autoriteit stuurt een verzoek om facilitering of ondersteuning door aan haar respectieve nationale lid:

1.5.2. Model voor het ontvangen van een verzoek om facilitering of ondersteuning:

Het nationale lid ontvangt het verzoek om facilitering of ondersteuning en stuurt het buiten Judex door aan het nationale lid van de aangezochte lidstaat.

1.5.3. Model voor het doorsturen van een verzoek om facilitering of ondersteuning aan de bevoegde nationale autoriteit:

Het nationale lid van de aangezochte lidstaat stuurt het verzoek door aan zijn respectieve bevoegde nationale autoriteit.

1.5.4. Model voor het ontvangen van een verzoek om facilitering of ondersteuning:

De bevoegde nationale autoriteit ontvangt het verzoek om facilitering of ondersteuning.

1.5.5. Model voor het versturen van een antwoord op het verzoek om facilitering of ondersteuning:

De bevoegde nationale autoriteit verstuurt een antwoord op of informatie betreffende het verzoek aan het nationale lid van de aangezochte lidstaat.

1.5.6. Model voor het ontvangen van het antwoord op het verzoek om facilitering of ondersteuning:

Het nationale lid ontvangt het antwoord op of informatie betreffende het verzoek om facilitering of ondersteuning en deelt dat antwoord/die informatie buiten Judex met het nationale lid van de verzoekende lidstaat.

1.5.7. Model voor het beantwoorden van het verzoek om facilitering of ondersteuning:

Het nationale lid van de verzoekende lidstaat beantwoordt of deelt de informatie betreffende het verzoek om facilitering of ondersteuning van de bevoegde nationale autoriteit.

1.5.8. Model voor het ontvangen van het antwoord:

De bevoegde nationale autoriteit ontvangt het antwoord op of informatie betreffende het verzoek om facilitering of ondersteuning.

2. **Technische specificaties voor gegevensschema's**

De technische specificaties die moeten dienen als basis voor de ontwikkeling van XML-schemadefinities (XSD's) voor de digitalisering van Verordening (EU) 2018/1727 worden uiteengezet in de punten 2.1 en 2.2 van deze bijlage. Deze specificaties bestrijken de belangrijkste elementen en andere informatie om een alomvattende beschrijving te geven voor de productie van deze schema's.

De beschrijving is bedoeld om algemeen te zijn, zodat de geproduceerde XSD's kunnen worden gewijzigd en uitgebreid zonder dat er significante wijzigingen van deze specificaties nodig zijn.

De specificaties zijn van toepassing op de wettelijk voorgeschreven vorm van de schema's in de bijlage bij Verordening (EU) 2018/1727, vooraf gedefinieerde berichten of alle vrijetekstberichten die worden gebruikt in uitwisselingen uit hoofde van die verordening.

2.1. *Algemene overwegingen*

Op alle te verstrekken schema's zijn de volgende bepalingen van toepassing:

2.1.1. Versiebeheer

Er wordt een versieattribuut opgenomen dat het versiebeheer van het schema faciliteert en waarmee het schema in toekomstige versies kan worden bijgewerkt volgens de bedrijfsmatige vereisten. Het versieattribuut geeft aan of de nieuwe versie achterwaarts compatibel is bij de invoering van nieuwe functionaliteiten of verfijningen.

2.1.2. Schemadeclaratie en metagegevens

— In voorkomend geval maakt het schema gebruik van relevante normen of vocabularia, zoals vereist door e-Codex voor het tot stand brengen van interoperabiliteit, die nodig zijn voor de correcte validatie van de in dit schema gedefinieerde elementen en typen. Hieronder kan worden begrepen:

  — EU e-Justice Core Vocabulary ;

  — Unqualified Data Types;

  — een codelijst voor de European Union Language Codes.

— In voorkomend geval kunnen in het schema ook relevante ETSI-normen worden geïntegreerd om de definities ervan te gebruiken.

2.1.3. Annotaties en documentatie

— **Annotaties**: elk element in het schema gaat doorgaans vergezeld van annotaties. De annotaties bieden informatie in een voor mensen leesbaar formaat over het element en definiëren vaak het doel of gebruik ervan op een duidelijke en beknopte manier.

2.1.4. Gebruik en aanpasbaarheid

Het schema volgt de regels van de punten a) tot en met d):

a) **modulaire structuur**: elke sectie wordt ontworpen met een specifieke functionaliteit en kan onafhankelijk worden hergebruikt of aangepast. Hierdoor kan het schema eenvoudig worden aangepast aan verschillende gebruiksgevallen;

b) **uitbreidbaarheid**: het schema wordt zodanig ontworpen dat het de opneming van nieuwe elementen of attributen ondersteunt als in de toekomst aanvullende informatie nodig is. Dit wordt bereikt door gebruik te maken van optionele elementen en sequenties die kunnen worden uitgebreid zonder bestaande implementaties te verstoren;

c) **aanpasbare structuur**: het schema wordt zodanig ontworpen dat er indien nodig elementen of gegevenstypen kunnen worden toegevoegd of gewijzigd. De structuur van het schema kan worden aangepast aan wijzigingen in de vereisten zonder dat er een ingrijpend herontwerp nodig is;

d) **optionele elementen**: elementen in een schema kunnen worden gemarkeerd als optioneel, dat wil zeggen dat zij kunnen worden opgenomen of weggelaten naargelang van specifieke omstandigheden.

Het schema wordt zodanig ontworpen dat het verzamelen van gestructureerde gegevens voor specifieke verzoeken wordt ondersteund.

2.1.5. Wijzigingen

Het ontwerp van het schema wordt gekenmerkt door flexibiliteit, modulariteit en gemakkelijke aanpassing. Complexe typen en optionele elementen worden op zodanige wijze in het ontwerp geïntegreerd dat het diverse scenario's kan accommoderen en toch gemakkelijk kan worden gewijzigd en uitgebreid.

2.2. *Uitwisseling van gestructureerde gegevens*

In de in punten 2.2.1 en 2.2.2 bedoelde gestructureerde gegevens worden verstrekt overeenkomstig artikel 22 bis, lid 3, van Verordening (EU) 2018/1727. Het schema moet het ook mogelijk maken om in toekomstige actualiseringen te verwijderen gegevensreeksen aan te geven.

2.2.1. Gegevens van het Europees gerechtelijk register voor terrorismebestrijding

De volgende technische specificaties voor het gegevensschema vormen een gestructureerd kader voor het maken van het schema in XML-formaat.

a) Top-level-sectie

Deze top-level-sectie komt overeen met de informatie in bijlage III bij Verordening (EU) 2018/1727 voor het Europees gerechtelijk register voor terrorismebestrijding (CTR).

b) Structuur van het bericht

De structuur van de CTR-gegevens wordt gevormd door een reeks elementen en omvat ten minste het volgende:

i) informatie ter identificatie van natuurlijke personen:

— achternaam (familienaam),

— voornamen,

— eventuele aliassen,

— geboortedatum,

— geboorteplaats (plaats en land),

— nationaliteit(en),

— identificatiedocument (type en documentnummer),

— geslacht,

— verblijfplaats;

ii) informatie ter identificatie van rechtspersonen:

— firmanaam,

— rechtsvorm,

— plaats van het hoofdkantoor;

iii) informatie ter identificatie van zowel natuurlijke personen als rechtspersonen:

— telefoonnummers,

— e-mailadressen,

— nadere gegevens van rekeningen bij banken of andere financiële instellingen,

— stand van zaken in de procedure;

iv) informatie over het strafbare feit:

— informatie over rechtspersonen die betrokken zijn bij de voorbereiding of het plegen van een strafbaar feit van terroristische aard,

— wettelijke omschrijving van het strafbare feit volgens nationaal recht,

— toepasselijke vorm van ernstige criminaliteit uit de lijst van bijlage I,

— eventuele banden met een terroristische groepering,

— soort terrorisme, zoals jihadistisch, separatistisch, links of rechts,

— beknopte samenvatting van de zaak;

v) informatie over de nationale procedure:

— stand van zaken in de procedure,

— bevoegd openbaar ministerie,

— zaaknummer,

— datum waarop de formele gerechtelijke procedure is ingeleid,

— verband met andere relevante zaken;

vi) veld voor aanvullende informatie (vrije tekst);

vii) code voor voorafgaande toestemming.

2.2.2. Overeenkomstig artikel 21 van Verordening (EU) 2018/1727 doorgegeven gegevens

a) Artikel 21, lid 4, van Verordening (EU) 2018/1727, instellen van gemeenschappelijke onderzoeksteams (GOT's)

i) Top-level-sectie

Deze top-level-sectie komt overeen met de in artikel 21, lid 4, van Verordening (EU) 2018/1727 bedoelde informatie over het instellen van gemeenschappelijke onderzoeksteams.

ii) Structuur van het bericht

De structuur van de gegevens wordt gevormd door een reeks elementen en omvat ten minste het volgende:

— Nationale justitiële autoriteit die is belast met de strafprocedure

— Nationaal referentienummer van de strafprocedure

— Stand van zaken in de strafprocedure

— Onderzochte strafbare feiten

— Andere bij de zaak betrokken landen

— Wordt de zaak al door Eurojust ondersteund?

— Zo ja, wat is de zaak-ID van Eurojust?

— Zo neen, is dit een verzoek om ondersteuning?

— Wordt de zaak ondersteund door Europol?

— Zo ja, operationele taskforce (“OTF”) en/of applicatie voor veilige informatie-uitwisseling (“Siena”)?

— GOT-overeenkomst:

— Betrokken landen

— Partijen bij de GOT-overeenkomst (nationale autoriteiten die zijn belast met het onderzoek)

— Nationaal referentienummer van de strafprocedure waarvoor het GOT is ingesteld

— Datum van ondertekening

— Duur

— Onderzochte strafbare feiten

— Beknopte samenvatting van de zaak

— Hoofdverdachten in de strafprocedures waarvoor het GOT is ingesteld (voornamen, achternaam, geboortedatum en -plaats en eventuele andere relevante en noodzakelijke categorieën gegevens als bedoeld in bijlage II)

— Resultaten van het werk van het GOT:

— Moeilijkheden/vertragingen bij:

— het instellen van het GOT

— het opvragen/delen van bewijsmateriaal binnen het GOT

— het overeenkomen over/uitvoeren van een gemeenschappelijke vervolgingsstrategie

— Ontvankelijkheid/niet-ontvankelijkheid/beoordeling van GOT-bewijs in nationale procedures

— Uitkomst van gerechtelijke procedures (succesvolle/mislukte vervolgingen en veroordelingen/vrijspraken)

iii) Code voor voorafgaande toestemming

b) Artikel 21, lid 5, van Verordening (EU) 2018/1727, ernstige complexe zaken

i) Top-level-sectie

Deze top-level-sectie komt overeen met de in artikel 21, lid 5, van de Eurojust-verordening bedoelde informatie over ernstige complexe zaken.

ii) Structuur van het bericht

De structuur van de gegevens wordt gevormd door een reeks elementen en omvat ten minste het volgende:

— Nationale justitiële autoriteit die is belast met de strafprocedure

— Nationaal referentienummer van de strafprocedure

— Stand van zaken in de strafprocedure

— Onderzochte strafbare feiten

— Andere bij de zaak betrokken landen

— Wordt de zaak al door Eurojust ondersteund?

— Zo ja, wat is de zaak-ID van Eurojust?

— Zo neen, is dit een verzoek om ondersteuning?

— Wordt de zaak ondersteund door Europol?

— Zo ja, operationele taskforce en/of Siena?

— Toepasselijke vorm van ernstige criminaliteit

— Betrokkenheid van een georganiseerd crimineel netwerk

— Maffia-achtig

— Transnationaal georganiseerd crimineel netwerk

— Repercussies op EU-niveau

— Hoofdverdachten in de strafprocedure (voornamen, achternaam, geboortedatum en -plaats en eventuele andere relevante en noodzakelijke categorieën gegevens als bedoeld in bijlage II)

— Beknopte samenvatting van de zaak

— Andere betrokken landen

— Landen waarmee al samenwerking is gestart

— Betrokken bevoegde autoriteiten in een ander land

— Gebruikte instrumenten voor justitiële samenwerking

— Aantal verstuurde/ontvangen verzoeken

— Bestaan van onderling samenhangende onderzoeken

— Landen waarmee de samenwerking moet worden geactiveerd/mogelijk getroffen landen

— Soort samenwerking die nodig is (zoals uitlevering, bewijsverkrijging, andere samenwerking)

— Bestaan van onderling samenhangende onderzoeken

iii) Code voor voorafgaande toestemming

c) Artikel 21, lid 6, punt a), van Verordening (EU) 2018/1727, jurisdictiegeschillen

i) Top-level-sectie

Deze top-level-sectie komt overeen met de in artikel 21, lid 6, punt a), van Verordening (EU) 2018/1727 bedoelde informatie: jurisdictiegeschillen.

ii) Structuur van het bericht

De structuur van de gegevens wordt gevormd door een reeks elementen en omvat ten minste het volgende:

— Nationale justitiële autoriteit die is belast met de strafprocedure

— Nationaal referentienummer van de strafprocedure

— Stand van zaken in de strafrechtelijke procedure (bv. onderzoek, vervolging, proces)

— Onderzochte strafbare feiten

— Andere bij de zaak betrokken landen

— Wordt de zaak al door Eurojust ondersteund?

— Zo ja, wat is de zaak-ID van Eurojust?

— Zo neen, is dit een verzoek om ondersteuning?

— Wordt de zaak ondersteund door Europol?

— Zo ja, operationele taskforce en/of Siena?

— Andere betrokken landen

— Bevoegde nationale autoriteiten in het andere land, indien bekend

— Nationaal referentienummer van de strafprocedure in het andere land

— Fase van de procedure in het andere land, indien bekend

— Positief of negatief jurisdictiegeschil

— Feitelijk of potentieel jurisdictiegeschil

— Reeds ondernomen coördinatieactiviteiten (bv. raadplegingen overeenkomstig Kaderbesluit 2009/948/JBZ van de Raad ([1]))

— Beknopte samenvatting van de zaak

— Belangrijkste gewone verdachten (voornamen, achternaam, geboortedatum en -plaats en eventuele andere relevante en noodzakelijke categorieën gegevens als bedoeld in bijlage II)

iii) Code voor voorafgaande toestemming

d) Artikel 21, lid 6, punt b), gecontroleerde afleveringen

i) Top-level-sectie

Deze top-level-sectie komt overeen met de in artikel 21, lid 6, punt b), van Verordening (EU) 2018/1727 bedoelde informatie: gecontroleerde afleveringen.

ii) Structuur van het bericht

De structuur van de gegevens wordt gevormd door een reeks elementen en omvat ten minste het volgende:

— Nationale justitiële autoriteit die is belast met de strafprocedure

— Nationaal referentienummer van de strafprocedure

— Stand van zaken in de strafrechtelijke procedure (bv. onderzoek, vervolging, proces)

— Onderzochte strafbare feiten

— Andere bij de zaak betrokken landen

— Wordt de zaak al door Eurojust ondersteund?

— Zo ja, wat is de zaak-ID van Eurojust?

— Zo neen, is dit een verzoek om ondersteuning?

— Wordt de zaak ondersteund door Europol?

— Zo ja, operationele taskforce en/of Siena?

— Andere betrokken landen

— Land van herkomst/doorvoer/bestemming

— Bevoegde nationale autoriteiten in andere landen

— Bestaan van onderling samenhangende onderzoeken in andere landen

([1]) Kaderbesluit 2009/948/JBZ van de Raad van 30 november 2009 over het voorkomen en beslechten van geschillen over de uitoefening van rechtsmacht bij strafprocedures (PB L 328 van 15.12.2009, blz. 42, ELI: http://data.europa.eu/eli/dec_framw/2009/948/oj).

— Type geleverde goederen (bv. drugs en type/geld/wapens/sigaretten/andere)

— Status van de gecontroleerde aflevering (bv. gepland, lopend, voltooid)

— Resultaat van de gecontroleerde aflevering, indien reeds uitgevoerd

— Gebruikte instrumenten voor justitiële samenwerking

— Belangrijkste gewone verdachten (voornamen, achternaam, geboortedatum en -plaats en eventuele andere relevante en noodzakelijke categorieën gegevens als bedoeld in bijlage II)

iii) Code voor voorafgaande toestemming

e) Artikel 21, lid 6, punt c), van Verordening (EU) 2018/1727, herhaalde problemen met instrumenten voor justitiële samenwerking

i) Top-level-sectie

Deze top-level-sectie komt overeen met de in artikel 21, lid 6, punt c), van Verordening (EU) 2018/1727 bedoelde informatie: herhaalde problemen met instrumenten voor justitiële samenwerking.

ii) Structuur van het bericht

De structuur van de gegevens wordt gevormd door een reeks elementen en omvat ten minste het volgende:

— Nationale justitiële autoriteit die is belast met de strafprocedure

— Nationaal referentienummer van de strafprocedure

— Stand van zaken in de strafrechtelijke procedure (bv. onderzoek, vervolging, proces)

— Onderzochte strafbare feiten

— Andere bij de zaak betrokken landen

— Wordt de zaak al door Eurojust ondersteund?

— Zo ja, wat is de zaak-ID van Eurojust?

— Zo neen, is dit een verzoek om ondersteuning?

— Wordt de zaak ondersteund door Europol?

— Zo ja, operationele taskforce en/of Siena?

— Andere betrokken landen

— Bevoegde nationale autoriteiten, indien bekend

— Optredend als indienende of tenuitvoerleggende autoriteit

— Betrokken instrument voor justitiële samenwerking (bv. EAB, EOB, bevriezing, confiscatie)

— Specifiek verzoek in kwestie (d.w.z. welke onderzoeksmaatregel, welk type bevriezing, EAB met het oog op de tenuitvoerlegging van een straf of ter fine van vervolging)

— Weigering of herhaalde problemen

— In geval van weigering, welke specifieke grond wordt dan ingeroepen?

— Korte beschrijving van het probleem

— Andere nationale autoriteiten die hetzelfde probleem ondervinden, indien van toepassing

iii) Code voor voorafgaande toestemming

2.3. *Codes voor voorafgaande toestemming*

Wanneer via Judex gegevens met Eurojust worden gedeeld, geven de bevoegde nationale autoriteiten door middel van codes voor voorafgaande toestemming te kennen hoe de verdere toegang tot en verwerking en doorgifte van gegevens moeten verlopen nadat een verband is vastgesteld. De codes voor voorafgaande toestemming geven aan of en in hoeverre informatie met betrekking tot het verband mag worden gedeeld met andere bevoegde nationale autoriteiten, andere organen en instanties van de Unie, derde landen of internationale organisaties.

2.4. *Vooraf gedefinieerde berichten*

Vooraf gedefinieerde berichten zijn weergaven van uitwisselingen die zijn vastgesteld bij Verordening (EU) 2018/1727, maar waarvoor geen specifieke vorm in de rechtshandeling is opgenomen. De typen en aantallen ervan worden bepaald tijdens de bedrijfs- en de technische analyse.

De XLM-schemadefinities (XSD) voor vooraf gedefinieerde berichten worden zodanig ontworpen dat de consistentie, structuur en naleving van de bedrijfsbehoeften worden gewaarborgd.

Op deze schema's is het onderstaande van toepassing.

a) De top-level-sectie in dit schema krijgt een naam op basis van het specifieke berichttype dat wordt gedefinieerd.

b) De velden die nodig zijn voor het specifieke berichttype worden binnen deze structuur toegevoegd en gedefinieerd, zodat een correcte weergave van de gegevenselementen wordt gewaarborgd.

2.5. *Vrijetekstberichten*

Vrijetekstberichten zijn weergaven van uitwisselingen die ongestructureerde of gedeeltelijk gestructureerde inhoud mogelijk maken, waardoor flexibiliteit wordt geboden met inachtneming van de regelgevings- en bedrijfsvereisten. De XSD voor vrijetekstberichten wordt zodanig ontworpen dat consistentie en het juiste formaat worden gewaarborgd.

Op deze schema's is het onderstaande van toepassing.

a) De top-level-sectie in dit schema krijgt een naam op basis van het specifieke vrijetekstberichttype dat wordt gedefinieerd.

b) In het schema wordt de noodzakelijke structuur voor het vrijetekstbericht gedefinieerd, terwijl het, indien nodig, mogelijk blijft de elementen te ordenen.

c) De velden die nodig zijn voor het specifieke berichttype worden binnen deze structuur toegevoegd en gedefinieerd, zodat een correcte weergave van de gegevenselementen wordt gewaarborgd.

BIJLAGE III

TECHNISCHE SPECIFICATIES VOOR VINGERAFDRUKKEN EN FOTO'S

Berichten die via het gedecentraliseerde IT-systeem worden uitgewisseld, kunnen vergezeld gaan van bijlagen, waaronder bestanden van het nationaal instituut voor normen en technologie (National Institute of Standards and Technology, "NIST") met vingerafdrukken en foto's, in overeenstemming met de technische specificaties in de punten 1 en 2.

1. **Vingerafdrukken**

De vingerafdrukken die met Eurojust kunnen worden gedeeld met het oog op de betrouwbare identificatie van personen tegen wie een strafprocedure inzake strafbare feiten van terroristische aard loopt, moeten voldoen aan de volgende voorwaarden:

a) de vingerafdrukken worden in één bestand met digitale vingerafdrukbeelden (het NIST-vingerafdrukbestand) aangeleverd en ingediend overeenkomstig de norm ANSI/NIST-ITL 1-2011 Update 2015 (of een recentere versie);

b) het NIST-vingerafdrukbestand bevat maximaal tien individuele vingerafdrukken: de vingerafdrukken zijn gerold, vlak of beide;

c) alle vingerafdrukken zijn voorzien van een label;

d) de vingerafdrukken zijn verkregen met behulp van live-scanapparatuur of inkt op papier, op voorwaarde dat met inkt op papier verkregen vingerafdrukken zijn gescand met de vereiste resolutie en dezelfde kwaliteit;

e) in het NIST-bestand met vingerafdrukken kan aanvullende informatie worden opgenomen, zoals de voorwaarden voor vingerafdrukregistratie en de methode voor het verkrijgen van individuele vingerafdrukbeelden;

f) de vingerafdrukken hebben een nominale resolutie van 500 of 1 000 ppi ([1]) (met een aanvaardbare afwijking van ± 10 ppi) met 256 grijstinten;

g) het te gebruiken compressiealgoritme voor vingerafdrukken moet voldoen aan de aanbevelingen van het NIST. Vingerafdrukgegevens met een resolutie van 500 ppi worden gecomprimeerd aan de hand van het WSQ-algoritme (ISO/IEC 19794-5:2005). Vingerafdrukgegevens met een resolutie van 1 000 ppi worden gecomprimeerd aan de hand van de beeldcompressienorm en het coderingssysteem JPEG 2000 (ISO/IEC 15444-1). De beoogde compressieverhouding is 15:1.

2. **Foto's**

De foto's die met Eurojust kunnen worden gedeeld met het oog op de betrouwbare identificatie van personen tegen wie een strafprocedure inzake strafbare feiten van terroristische aard loopt, moeten voldoen aan de volgende voorwaarden:

a) in een fotobestand (het NIST-fotobestand) wordt slechts één gezichtsopname verstrekt. Deze opname wordt ingediend overeenkomstig de norm ANSI/NIST-ITL 1-2011 Update 2015, of een recentere versie;

b) de foto's zijn in grijstinten, kleur of nabij-infrarood;

c) de kwaliteit van de foto's is gebaseerd op de beeldvereisten van ISO/IEC 19794-5:2011 Frontal image type, of een recentere versie;

d) in het NIST-fotobestand kan aanvullende informatie worden opgenomen, waaronder de datum waarop de foto is gemaakt;

([1]) Pixels per inch.

e) de foto's in portretmodus hebben een resolutie van ten minste 600 pixels bij 800 pixels en een maximale resolutie van 1 200 pixels bij 1 600 pixels;

f) het gezicht neemt een ruimte in beslag op de foto die een minimum waarborgt van 120 pixels tussen de middelpunten van de ogen;

g) het te gebruiken compressiealgoritme voor foto's moet voldoen aan de aanbevelingen van het NIST. Foto's worden slechts één keer gecomprimeerd aan de hand van de beeldcompressienorm en het coderingssysteem JPG (ISO/IEC 10918) of JPEG 2000 (ISO/IEC 15444), met een maximaal toegestane beeldcompressieverhouding van 20:1.