



2025/1550

29.7.2025

UITVOERINGSVERORDENING (EU) 2025/1550 VAN DE COMMISSIE

van 28 juli 2025

tot vaststelling van de technische specificaties en andere vereisten voor het gedecentraliseerde IT-systeem bedoeld in Verordening (EU) 2023/1543 van het Europees Parlement en de Raad

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) 2023/1543 van het Europees Parlement en de Raad van 12 juli 2023 betreffende het Europees verstrekingsbevel en het Europees bewaringsbevel voor elektronisch bewijsmateriaal in strafzaken en de tenuitvoerlegging van vrijheidsstraffen als gevolg van een strafprocedure ⁽¹⁾, en met name artikel 25, lid 1, punten a), b), c) en d),

Overwegende hetgeen volgt:

- (1) Met het oog op de invoering van het gedecentraliseerde IT-systeem bedoeld in Verordening (EU) 2023/1543 moeten technische specificaties, maatregelen en doelstellingen voor de implementatie van dat systeem worden vastgesteld.
- (2) Overeenkomstig Verordening (EU) 2023/1543 moet het gedecentraliseerde IT-systeem bestaan uit de IT-systemen van de lidstaten en de agentschappen en organen van de Unie en interoperabele e-Codex-toegangspunten die die IT-systemen met elkaar verbinden. Dienovereenkomstig moeten de technische specificaties en de andere vereisten van het gedecentraliseerde IT-systeem dit kader weerspiegelen.
- (3) Overeenkomstig Verordening (EU) 2023/1543 moeten de toegangspunten van het gedecentraliseerde IT-systeem gebaseerd zijn op geautoriseerde e-Codex-toegangspunten zoals gedefinieerd in artikel 3, lid 3, van Verordening (EU) 2022/850 van het Europees Parlement en de Raad ⁽²⁾.
- (4) De lidstaten kunnen desgewenst gebruikmaken van de door de Commissie ontwikkelde referentie-implementatie-software in plaats van een nationaal IT-systeem als back-endsysteem. Om de interoperabiliteit te waarborgen, moeten zowel de nationale IT-systemen als de referentie-implementatiesoftware aan dezelfde technische specificaties en vereisten van deze verordening voldoen.
- (5) Om potentiële technische problemen met de capaciteit en de betrouwbaarheid van het gedecentraliseerde IT-systeem te beperken, moet een drempelwaarde voor de hoeveelheid via het systeem doorgegeven elektronisch bewijsmateriaal worden vastgesteld. Na de opstart van het systeem moet op de frequentie van doorgiften en de hoeveelheid ervan worden toegezien en de drempelwaarde moet, zo nodig, worden aangepast om de efficiëntie van het systeem te maximaliseren.
- (6) Om de interoperabiliteit en de efficiëntie van het gedecentraliseerde IT-systeem te versterken, moet het gebruik van passende ETSI-normen bindend zijn. Toekomstige ontwikkelingen moeten in het oog worden gehouden en, waar nodig, moeten aanvullende ETSI-normen worden overwogen.
- (7) Ierland is gebonden door Verordening (EU) 2023/1543 en neemt derhalve deel aan de vaststelling van deze verordening.
- (8) 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, is deze verordening niet bindend voor, noch van toepassing op Denemarken.

⁽¹⁾ PB L 191 van 28.7.2023, blz. 118, ELI: <http://data.europa.eu/eli/reg/2023/1543/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>).

- (9) De Europese Toezichthouder voor gegevensbescherming is geraadpleegd overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ⁽³⁾ en heeft op 25 juni 2025 een advies uitgebracht.
- (10) De in deze verordening vervatte maatregelen zijn in overeenstemming met het advies van het bij artikel 26 van Verordening (EU) 2023/1543 ingestelde comité,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

Technische specificaties van het gedecentraliseerde IT-systeem

De technische specificaties en de vereisten, de maatregelen en de doelstellingen van het gedecentraliseerde IT-systeem bedoeld in artikel 25, lid 1, van Verordening (EU) 2023/1543 voor communicatie in de zin van artikel 19 van die verordening worden in de bijlage bij deze verordening vastgesteld.

Artikel 2

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, 28 juli 2025.

Voor de Commissie

De voorzitter

Ursula VON DER LEYEN

⁽³⁾ 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

TECHNISCHE SPECIFICATIES VAN HET GEDECENTRALISEERDE IT-SYSTEEM

(als bedoeld in artikel 1)

1. Inleiding en reikwijdte

Deze bijlage bevat de technische specificaties, de maatregelen en de doelstellingen van het gedecentraliseerde IT-systeem voor de procedures uit hoofde van Verordening (EU) 2023/1543.

Overeenkomstig Verordening (EU) 2023/1543, en met name artikel 19 daarvan, moet het gedecentraliseerde IT-systeem schriftelijke communicatie tussen de bevoegde autoriteiten en de aangewezen vestigingen of de wettelijke vertegenwoordigers, tussen de bevoegde autoriteiten onderling, evenals tussen de bevoegde autoriteiten en de bevoegde agentschappen of organen van de Unie mogelijk maken.

2. Definities

- 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, publieke-sleutelinfrastructuur en 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, publieke-sleutelinfrastructuur, en elektronische handtekeningen en elektronische zegels;
- 2.4. “SOAP”: 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. Representational State Transfer (“REST”): 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, formulieren, stukken en bewijsmateriaal via het gedecentraliseerde IT-systeem;
- 2.8. “API”: een applicatieprogramma-interface op basis van een gemeenschappelijke norm voor gegevensuitwisseling waarmee dienstaanbieders die gebruikmaken van op maat gemaakte IT-oplossingen voor de uitwisseling van informatie en gegevens in verband met verzoeken om elektronisch bewijsmateriaal, via geautomatiseerde middelen tot de gedecentraliseerde IT-systemen toegang krijgen;
- 2.9. “webgebaseerde interface”: een via HTTPS op het internet beschikbare gebruikersinterface waarmee dienstaanbieders, zonder dat zij hun eigen specifieke infrastructuur hoeven op te zetten, handmatig toegang kunnen krijgen tot het gedecentraliseerde IT-systeem met het oog op beveiligde communicatie met de autoriteiten en de uitwisseling van informatie en gegevens in verband met verzoeken om elektronisch bewijsmateriaal;
- 2.10. “ETSI-normen”: door het Europees Instituut voor telecommunicatienormen (ETSI) ontwikkelde technische specificaties en normen die de interoperabiliteit, beveiliging en efficiëntie in informatie- en communicatietechnologieën waarborgen. Deze bieden kaders, protocollen en beste praktijken voor een breed scala aan technologieën, met inbegrip van mobiele netwerken, radiocommunicatie, cyberbeveiliging en internetinfrastructuur;

- 2.11. “hashwaarde”: een door een cryptografische hashfunctie gegenereerde uitvoer met vaste lengte bij toepassing op een invoer van willekeurige lengte. Een cryptografische hashfunctie is ontworpen om tegemoet te komen aan fundamentele beveiligingseigenschappen, met inbegrip van bestendigheid tegen het vinden van een invers en een tweede invers beeld en botsingsbestendigheid, om de bestendigheid ervan tegen inversie en tegen aanvallen via botsingen te waarborgen;
- 2.12. “e-Codex-systeem”: het e-Codex-systeem zoals gedefinieerd in artikel 3, lid 1, van Verordening (EU) 2022/850;
- 2.13. “EU e-Justice Core Vocabularies”: de EU e-Justice Core Vocabularies zoals gedefinieerd in punt 4 van de bijlage bij Verordening (EU) 2022/850;
- 2.14. “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;
- 2.15. “AS4”: Applicability Statement 4, een OASIS-norm die ebMS 3.0 profileert; het vereenvoudigt beveiligd en interoperabel berichtenverkeer tussen bedrijven onderling door gebruik te maken van open standaarden zoals SOAP en WS-beveiliging;
- 2.16. Hersteltijd doelstelling: de maximaal toegestane tijd om na een incident de dienstverlening te hervatten;
- 2.17. “Herstelpunt doelstelling”: het maximaal aanvaardbare gegevensverlies bij een defect.

3. Methoden voor elektronische communicatie

- 3.1. Met het oog op de schriftelijke communicatie tussen de bevoegde autoriteiten van de lidstaten, tussen de bevoegde autoriteiten en de aangewezen vestigingen of wettelijke vertegenwoordigers van dienstverleners, evenals tussen de bevoegde autoriteiten en de agentschappen en organen van de Unie gebruikt het gedecentraliseerde IT-systeem op diensten gebaseerde methoden voor elektronische communicatie zoals webdiensten of andere herbruikbare onderdelen en softwareoplossingen voor gegevensuitwisseling. Het omvat met name communicatie via de e-Codex-toegangspunten zoals bepaald in artikel 5, lid 2, van Verordening (EU) 2022/850. Om doeltreffende en interoperabele grensoverschrijdende uitwisseling van gegevens te waarborgen, ondersteunt het gedecentraliseerde IT-systeem communicatie via het e-Codex-systeem.
- 3.2. Gezien de verwachte grote hoeveelheid elektronisch bewijsmateriaal die naar aanleiding van een Europees verstrekingsbevel via het gedecentraliseerde IT-systeem moet worden verzonden, zoals uiteengezet in artikel 19, leden 1 en 4, van Verordening (EU) 2023/1543, wat tot technische capaciteitsbeperkingen met mogelijk negatieve gevolgen voor het gedecentraliseerde IT-systeem kan leiden, wordt elektronisch bewijsmateriaal via dit systeem verzonden zolang het niet groter is dan 25 megabytes (25 600 kilobytes). De doorgifte van elektronisch bewijsmateriaal dat groter is, vindt plaats overeenkomstig artikel 19, lid 5 van die verordening.
- 3.3. Gezien artikel 19, lid 6, van Verordening (EU) 2023/1543, geldt, als een doorgifte met in dat lid bedoelde alternatieve middelen plaatsvindt omdat het onmogelijk is om het gedecentraliseerde IT-systeem vanwege een van de in artikel 19, lid 5, van die verordening genoemde redenen te gebruiken, het volgende:
 - 3.3.1. als de doorgifte schriftelijke communicatie, met inbegrip van de uitwisseling van formulieren, tussen bevoegde autoriteiten en dienstverleners in de zin van artikel 19, lid 1, van Verordening (EU) 2023/1543 betreft, registreert de verzender de doorgifte in zijn nationaal IT-systeem dat onderdeel van het gedecentraliseerde IT-systeem is. De geregistreerde informatie moet minimaal een zaak- of dossiernummer, de datum en het tijdstip van doorgifte, de afzender en de ontvanger, de naam van het bestand en de omvang ervan bevatten.
 - 3.3.2. als de doorgifte schriftelijke communicatie, met inbegrip van de uitwisseling van formulieren, tussen bevoegde autoriteiten onderling, evenals schriftelijke communicatie met bevoegde agentschappen en organen van de Unie in de zin van artikel 19, lid 4, van Verordening (EU) 2023/1543 betreft, registreert de verzender de doorgifte in het gedecentraliseerde IT-systeem, met name in zijn nationale IT-systeem of, in voorkomend geval, in de IT-systemen van het bevoegde agentschap of orgaan van de Unie. De geregistreerde informatie moet minimaal een zaak- of dossiernummer, de datum en het tijdstip van doorgifte, de afzender en de ontvanger, de naam van het bestand en de omvang ervan bevatten.

3.3.3. als het elektronisch bewijsmateriaal op grond van een Europees verstrekingsbevel met alternatieve communicatiemiddelen tussen de dienstverleners en de bevoegde autoriteiten in de uitvaardigende staat ⁽¹⁾ is doorgegeven, of als het elektronische bewijsmateriaal met alternatieve middelen is doorgegeven van de tenuitvoerleggingsautoriteit naar de bevoegde autoriteiten in de uitvaardigende staat krachtens de in artikel 16, lid 9, van Verordening (EU) 2023/1543 bedoelde handhavingprocedure:

- a) registreert de verzender de volgende informatie als onderdeel van een manifest en geeft die informatie door aan de autoriteit waarnaar het elektronische bewijsmateriaal is verzonden of waaraan het beschikbaar is gesteld:
 - 1) informatie over de verzender en de ontvanger;
 - 2) metagegevens die het verstrekte elektronische bewijsmateriaal aan een bepaald of bepaalde Europese verstrekings- of bewaringsbevelen koppelen;
 - 3) de datum en het tijdstip van de doorgifte of het moment waarop het elektronische bewijsmateriaal aan de ontvanger ter beschikking is gesteld;
 - 4) informatie over de wijze van doorgifte (bv. een registratie van een beveiligde link waarlangs het elektronische bewijsmateriaal ter beschikking was gesteld, bewijs van ontvangst of levering van postdiensten enz. ⁽²⁾);
 - 5) de volledige bestandsnaam of -namen van het elektronische bewijsmateriaal dat is doorgegeven of anderszins aan de beoogde ontvanger in de uitvaardigende staat ter beschikking is gesteld;
 - 6) de omvang van het elektronische bewijsmateriaal dat is doorgegeven of anderszins aan de beoogde ontvanger in de uitvaardigende staat ter beschikking is gesteld;
 - 7) ten minste één hashwaarde van de doorgegeven of anderszins ter beschikking gestelde gegevens en een vermelding van de gebruikte hashalgoritmen. De hashalgoritmen die voor de berekening van de hashwaarde(n) worden gebruikt, zijn cryptografisch sterk, algemeen gebruikt en niet aan openbaar gemaakte zwaktes zoals botsingen onderhevig (bv. SHA-512, SHA3-512, BLAKE2 of RIPEMD-160, maar mogelijk sterkere algoritmes, afhankelijk van technologische ontwikkelingen);
- b) vermeldt de verzender in voorkomend geval als onderdeel van het in bovenstaand punt a) bedoelde manifest de datum en het tijdstip tot wanneer het elektronische bewijsmateriaal ter beschikking blijft. Deze termijn moet redelijk zijn voor de bevoegde autoriteit in de uitvaardigende staat om het elektronische bewijsmateriaal op te vragen, en niet minder dan 10 kalenderdagen en niet meer dan 45 kalenderdagen bedragen vanaf het moment waarop het elektronische bewijsmateriaal ter beschikking is gesteld. Op verzoek van de bevoegde autoriteit van de uitvaardigende staat kan de door de verzender aangegeven termijn in een specifieke zaak worden verlengd;
- c) kan voor de zaak relevante aanvullende informatie of opmerkingen registreren en doorgeven aan de autoriteit waarnaar het elektronische bewijsmateriaal werd doorgegeven of waaraan het ter beschikking werd gesteld, als onderdeel van het in bovenstaand punt a) bedoeld manifest.

3.4. Gezien artikel 28 van Verordening (EU) 2023/1543 worden via de referentie-implementatiesoftware de in lid 2) van dat artikel bedoelde statistieken in gestructureerde (bv. XML) en ongestructureerde (bv. PDF) dataformaten programmatisch verzameld, doorgegeven of anderszins ter beschikking gesteld. Overeenkomstig artikel 28, lid 3, van Verordening (EU) 2023/1543 kunnen, indien technisch uitgerust, de door de lidstaten beheerde nationale portalen ⁽³⁾ deze statistieken ook via een geautomatiseerd proces aan de Commissie doorgeven of verstrekken. De Commissie vaardigt richtsnoeren uit over de gegevensstructuur en de methode om deze statistieken te verzamelen en erover te communiceren.

⁽¹⁾ Met het oog op meer duidelijkheid moeten verwijzingen naar bevoegde nationale autoriteiten mutatis mutandis ook worden opgevat als verwijzingen naar de nationale leden van Eurojust, de Europese aanklagers en de gedelegeerde Europese aanklagers, voor zover zij gemachtigd zijn om dezelfde functies overeenkomstig het EU-recht en het nationaal recht te vervullen.

⁽²⁾ Er zij aan herinnerd dat overeenkomstig artikel 19, lid 5, doorgifte met alternatieve communicatiemiddelen snel, veilig en betrouwbaar moet zijn, wat het voor de ontvanger mogelijk maakt de echtheid van de informatie vast te stellen.

⁽³⁾ "Nationale portalen" moeten worden opgevat als nationale "IT-systemen" die deel uitmaken van het in artikel 3, lid 21, van Verordening (EU) 2023/1543 bedoelde gedecentraliseerde IT-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,
 - b) communicatie binnen het gedecentraliseerde IT-systeem tussen bevoegde autoriteiten en agentschappen en organen van de Unie,
 - c) communicatie tussen bevoegde autoriteiten en dienstverleners via een API en de webinterface, en
 - d) communicatie met de Databank van rechtbanken.
- 4.2. Voor de definitie en de doorgifte van gestructureerde gegevens en metagegevens worden de onderdelen van het gedecentraliseerde IT-systeem op uitgebreide en algemeen aanvaarde industriestandaarden en -protocollen, zoals SOAP en REST, gebaseerd, met name die waarnaar Europese normalisatieorganisaties, zoals ETSI, verwijzen.
- 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-Security 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 voor elektronisch bewijsmateriaal gebruik van relevante normen of vocabularia die nodig zijn voor de correcte validatie van de in dit schema gedefinieerde elementen en typen. Hieronder vallen:
- a) EU e-Justice Core Vocabulary;
 - b) Unqualified Data Types;
 - c) Een codelijst voor European Union Language Codes.
- In voorkomend geval kunnen in de XML-schema's ook relevante ETSI-normen worden geïntegreerd om de definities ervan te gebruiken.
- 4.6. De Commissie bepaalt de specificaties voor de gemeenschappelijke API die als methode om toegang te krijgen tot het gedecentraliseerde IT-systeem door de tenuitvoerleggingsstaten aan dienstverleners ter beschikking wordt gesteld. Voor zover mogelijk en redelijk is deze API gebaseerd op ETSI TS 104 144 ("interfacedefinitie voor Verordening (EU) 2023/1543 voor nationale autoriteiten en dienstverleners").
- 4.7. 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) Publiekessleutelinfrastructuur 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 (berichten, formulieren, stukken en elektronisch bewijsmateriaal) 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 om de beschikbaarheid te waarborgen door permanente toegang tot diensten en gegevens te waarborgen en verstoringen als gevolg van cyberaanvallen of defecten te voorkomen;
 - e) maatregelen die waarborgen dat beveiligingsincidenten in een logbestand worden vastgelegd overeenkomstig erkende internationale aanbevelingen voor normen voor IT-beveiliging;
 - f) 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 APIs en SOAP om de vertrouwelijkheid en integriteit van berichten te beschermen.
- 5.3. De onderdelen van het gedecentraliseerde IT-systeem worden in overeenstemming met het beginsel van gegevensbescherming door ontwerp en door standaardinstellingen ontwikkeld, en er worden passende administratieve, organisatorische en technische maatregelen getroffen om een hoog niveau van cyberbeveiliging te waarborgen.
- 5.4. 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 respectievelijk Verordening (EU) 2016/679 van het Europees Parlement en de Raad ⁽⁴⁾ en Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad ⁽⁵⁾, naargelang het geval.
- 5.5. Lidstaten die een ander nationaal IT-systeem gebruiken dan de referentie-implementatiesoftware, treffen de nodige maatregelen om te waarborgen dat het aan de vereisten van Verordening (EU) 2016/679 en Richtlijn (EU) 2016/680 voldoet, naargelang het geval.
- 5.6. Gezien hun deelname aan het gedecentraliseerde IT-systeem treffen Eurojust en het Europees Openbaar Ministerie de nodige maatregelen om te waarborgen dat hun respectieve IT-systemen aan de vereisten van Verordening (EU) 2018/1725 en hun oprichtingshandelingen voldoen.
- 5.7. De lidstaten, Eurojust en het Europees Openbaar Ministerie 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 een onderdeel vormen van het gedecentraliseerde IT-systeem.

6. **Versleuteling van het elektronisch bewijsmateriaal ⁽⁶⁾**

- 6.1. Onverminderd de beveiligingsmaatregelen van het gedecentraliseerde IT-systeem kunnen bevoegde autoriteiten bij de uitvaardiging van een Europees verstekkingsbevel aanvullend een specifiek digitaal X.509-certificaat voor de asymmetrische versleuteling van elektronisch bewijsmateriaal verstrekken.

⁽⁴⁾ 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).

⁽⁵⁾ 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).

⁽⁶⁾ Voor alle duidelijkheid: de term "elektronisch bewijsmateriaal" is beperkt tot de definitie van artikel 3, lid 8, van Verordening (EU) 2023/1543.

- 6.2. Voor de uitvaardiging, het beheer, de verificatie en alle daarmee verband houdende aspecten van de in punt 6.1 bedoelde certificaten, samen met de bijbehorende publiekesleutelinfrastructuur (PKI), ligt de volledige verantwoordelijkheid bij de uitvaardigende staat.
- 6.3. Onverminderd de toekomstige technologische ontwikkelingen, ondersteunen de digitale certificaten op industriële normen gebaseerde encryptiealgoritmen zoals RSA (Rivest-Shamir-Adleman) of ECDH (Elliptic Curve Diffie-Hellman) voor ECC (Elliptic Curve Cryptography).
- 6.4. Digitale certificaten beschikken over de passende “keyUsage”-extensie, zoals “keyEncipherment” of “dataEncipherment” voor op RSA gebaseerde certificaten, en “keyAgreement” voor op ECC gebaseerd certificaten. Certificaten worden in het PEM- (Privacy-Enhanced Mail) of het DER-formaat (Distinguished Encoding Rules) ter beschikking gesteld.
- 6.5. Wanneer de uitvaardigende autoriteit een digitaal X.509-certificaat heeft verstrekt, en wanneer een dienstaanbieder het overgelegde elektronisch bewijsmateriaal op grond van een Europees verstrekingsbevel verzendt, versleutelt de verstrekker voorafgaand aan de doorgifte van die gegevens via het gedecentraliseerde IT-systeem het elektronische bewijsmateriaal met behulp van het respectieve door de uitvaardigende staat verstrekte digitale X.509-certificaat.
- 6.6. Wanneer de uitvaardigende autoriteit een digitaal X.509-certificaat heeft verstrekt, maar wanneer de doorgifte van het versleutelde elektronisch bewijsmateriaal om technische of andere gerechtvaardigde redenen niet mogelijk is, en onverminderd het bepaalde in artikel 19, lid 5, van Verordening (EU) 2023/1543, kan de dienstaanbieder de gegevens zonder versleuteling van de inhoud doorgeven. In dergelijke gevallen verstrekt de dienstaanbieder een met redenen omklede toelichting aan de uitvaardigende autoriteit.

7. Minimumbeschikbaarheidsdoelstellingen

- 7.1. De lidstaten, Eurojust en het Europees Openbaar Ministerie 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 en de technische beschikbaarheidsgraad ervan moet ten minste 98 % bedragen, gepland onderhoud buiten beschouwing gelaten.
- 7.2. De Commissie waarborgt dat de Databank van rechtbanken 24 uur per dag en zeven dagen per week beschikbaar is en de technische beschikbaarheidsgraad van het systeem moet ten minste 99 % bedragen, gepland onderhoud buiten beschouwing gelaten.
- 7.3. Voor zover mogelijk moeten tijdens werkdagen de onderhoudswerkzaamheden worden gepland tussen 20.00 uur en 7.00 uur Midden-Europese tijd.
- 7.4. De lidstaten, Eurojust en het Europees Openbaar Ministerie stellen de Commissie en de andere lidstaten als volgt in kennis van de 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.
- 7.5. Wanneer de lidstaten, Eurojust of het Europees Openbaar Ministerie vaste en regelmatige onderhoudsperioden hebben, stellen zij de Commissie en de deelnemers aan het gedecentraliseerde IT-systeem in kennis van het tijdstip en de dag(en) waarop dergelijke vaste en regelmatige perioden zijn gepland. Niettegenstaande de in punt 7.4 bedoelde verplichtingen kunnen de lidstaten, ingeval onderdelen van het gedecentraliseerde IT-systeem die onder de verantwoordelijkheid van de lidstaten, Eurojust of het Europees Openbaar Ministerie vallen, tijdens een dergelijke vaste en regelmatige periode niet beschikbaar zijn, ervoor kiezen de Commissie niet telkens in kennis te stellen.

- 7.6. Bij een onverwacht technisch defect aan de onderdelen van het gedecentraliseerde IT-systeem die onder de verantwoordelijkheid van de lidstaten, Eurojust of het Europees Openbaar Ministerie vallen, stellen zij de Commissie en de deelnemers aan het gedecentraliseerde IT-systeem onverwijld in kennis van dit defect en, indien bekend, van de verwachte hersteltermijn.
- 7.7. Wanneer onderhoudsactiviteiten of een onverwacht technisch defect van de onderdelen in het gedecentraliseerde IT-systeem die onder de verantwoordelijkheid van een lidstaat vallen, de beschikbaarheid van de API en/of de webinterface voor de dienstverleners in het gedrang brengen, maakt de betrokken lidstaat deze informatie onverwijld op een website beschikbaar en/of deelt hij deze onverwijld mee aan de dienstverleners op zijn grondgebied.
- 7.8. Bij een onverwacht technisch defect van de Databank van rechtbanken deelt de Commissie de lidstaten, Eurojust en het Europees Openbaar Ministerie onverwijld de onbeschikbaarheid ervan en, indien bekend, de verwachte hersteltermijn mee.
- 7.9. Bij een storing aan de dienstverlening waarborgen de lidstaten, Eurojust en het Europees Openbaar Ministerie in overeenstemming met de herstellijd-doelstelling en de herstelpunt-doelstelling dat de dienst snel wordt hersteld en dat de gegevens zo min mogelijk verloren gaan.
- 7.10. De lidstaten, Eurojust en het Europees Openbaar Ministerie treffen passende maatregelen om de bovengenoemde beschikbaarheidsdoelstellingen te verwezenlijken en brengen procedures voor een doeltreffende incidentrespons tot stand.

8. Bevoegde autoriteiten/Databank van rechtbanken

- 8.1. Gezien artikel 19 van Verordening (EU) 2023/1543 is het met het oog op de werking van het gedecentraliseerde IT-systeem van essentieel belang een gezaghebbende databank over de dienstverleners en de bevoegde autoriteiten op te zetten.
- 8.2. De gezaghebbende databank van de bevoegde autoriteiten bevat de volgende informatie in een gestructureerd formaat:
- voor de toepassing van artikel 19 van Verordening (EU) 2023/1543, overeenkomstig artikel 31, lid 1, punten a), b) en c), van die verordening ter kennis gebrachte informatie over de bevoegde autoriteiten, ook wat betreft:
 - de nationale leden van Eurojust, samen met een indicatie of zij overeenkomstig het nationale recht bevoegd zijn Europese verstrekingsbevelen en Europese bewaringsbevelen uit te vaardigen in de zin van artikel 8, leden 3 en 4, van Verordening (EU) 2018/1727 van het Europees Parlement en de Raad ⁽⁷⁾;
 - de gedelegeerd Europese aanklagers en de Europese aanklagers, ingeval de lidstaten overeenkomstig artikel 105, lid 3, van Verordening (EU) 2017/1939 ⁽⁸⁾ van de Raad, kennis hebben gegeven van het feit dat deze autoriteiten de bevoegde uitvaardigende autoriteit zijn in de zin van Verordening (EU) 2023/1543;
 - in voorkomend geval, de informatie die nodig is om de geografische gebieden van de bevoegdheid van de autoriteiten te bepalen, of andere relevante criteria die nodig zijn om hun bevoegdheid vast te stellen;
 - de informatie die nodig is voor de correcte werking van en de technische routebepaling van de berichten over de uitwisselingen van gegevens in het gedecentraliseerde IT-systeem.

8.2.1. De in punt 8.2., c), bedoelde informatie omvat het volgende:

- de informatie over de lidstaat waar de aangewezen vestiging van de dienstverlener is opgericht of waar zijn wettelijke vertegenwoordiger verblijft:
 - lidstaat;
 - centrale autoriteit;

⁽⁷⁾ 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 (PB L 295 van 21.11.2018, blz. 138).

⁽⁸⁾ Verordening (EU) 2017/1939 van de Raad van 12 oktober 2017 betreffende nauwere samenwerking bij de instelling van het Europees Openbaar Ministerie ("EOM") (PB L 283 van 31.10.2017, blz. 1).

- b) informatie over de dienstaanbieder:
 - 1) naam;
 - 2) adres/zetel;
 - 3) registratienummer;
 - 4) rechtsvorm;
 - 5) telefoonnummer;
 - 6) e-mail;
- c) informatie over de aangewezen vestiging/de wettelijke vertegenwoordiger:
 - 1) soort entiteit (aangewezen vestiging/wettelijke vertegenwoordiger);
 - 2) naam;
 - 3) adres/zetel;
 - 4) telefoonnummer;
 - 5) e-mail;
 - 6) contactpersoon/entiteit voor algemene kwesties;
 - 7) door de dienstaanbieder/aangewezen vestiging/wettelijke vertegenwoordiger aanvaarde officiële taal of talen;
 - 8) de in artikel 2, lid 1, van Richtlijn (EU) 2023/1544 van het Europees Parlement en de Raad ^(*) bedoelde diensten aangeboden in de Unie;
 - 9) soort rechtsinstrumenten van de EU waarvoor de aangewezen vestiging/wettelijke vertegenwoordiger is aangewezen (wanneer de lidstaten niet aan alle relevante rechtsinstrumenten van de EU deelnemen);
 - 10) territoriaal toepassingsgebied van de aanwijzing/benoeming;
- d) authenticatie van de informatie:
 - 1) naam van de gemachtigde vertegenwoordiger;
 - 2) functie;
 - 3) adres;
 - 4) telefoonnummer;
 - 5) e-mail;
 - 6) datum.

8.2.2. Indien beschikbaar bevat de in punt 8.2., c), bedoelde informatie het volgende:

- a) informatie over de dienstaanbieder:
 - 1) contactpersoon voor vragen over de kennisgevingen (indien verschillend van de ondertekenaar);
 - 2) website;
- b) soorten beschikbare gegevens:
 - 1) voor elke betrokken dienst:
 - soorten beschikbare gegevens;
 - categorie van de gegevens;
 - identificatoren;
 - periode waarin gegevens beschikbaar zijn;

^(*) Richtlijn (EU) 2023/1544 van het Europees Parlement en de Raad van 12 juli 2023 tot vaststelling van geharmoniseerde regels inzake de aanwijzing van aangewezen vestigingen en de aanstelling van wettelijke vertegenwoordigers ten behoeve van de vergaring van elektronisch bewijsmateriaal in strafprocedure (PB L 191 van 28.7.2023, blz. 181, ELI: <http://data.europa.eu/eli/dir/2023/1544/oj>).

- 2) aanvullende informatie over de gegevens;
- 3) aanvullende informatie over de dienst (bv. onderaannemingsrelaties);
- c) informatie over de aangewezen vestiging/de wettelijke vertegenwoordiger:
 - 1) andere dienstaanbieders waarvoor deze aangewezen vestiging of wettelijke vertegenwoordiger is aangewezen;
 - 2) contactgegevens voor technische bijstand;
 - 3) contactgegevens bij noodgevallen;
- d) technische informatie:
 - 1) naam van het contactpunt voor technische ondersteuning;
 - 2) telefoonnummer van het technische ondersteuning;
 - 3) telefoonnummer van het contactpunt voor technische ondersteuning;
 - 4) API-URL voor het dynamisch opvragen van informatie over de soorten data;
 - 5) soort verbinding met het nationale IT-systeem:
 - webinterface;
 - API;
 - Push API-URL.

8.3. Met het oog op de operationele noden van het gedecentraliseerde IT-systeem:

- a) is de Commissie verantwoordelijk voor de ontwikkeling, het onderhoud, het beheer en de ondersteuning van de gezaghebbende databank;
- b) maakt de Commissie toegang tot de gezaghebbende databank mogelijk via een API die aan de bevoegde autoriteiten, Eurojust en het Europees Openbaar Ministerie ter beschikking wordt gesteld met het oog op hun deelname aan het gedecentraliseerde IT-systeem;
- c) waarborgen de lidstaten dat de in punt 8.2, a) en b), bedoelde informatie over hun bevoegde autoriteiten in de gezaghebbende databank volledig en nauwkeurig is, en bijgewerkt blijft;
- d) stelt de gezaghebbende databank de lidstaten in staat de informatie in die databank over hun dienstaanbieders te verstrekken en bij te werken, en stelt de autoriteiten die aan het gedecentraliseerde IT-systeem deelnemen, in staat zich programmatische toegang tot die informatie te verschaffen en die informatie op te vragen;
- e) waarborgen de lidstaten en de dienstaanbieders dat de in punt 8.2, c), bedoelde informatie in de gezaghebbende databank volledig en nauwkeurig is, en bijgewerkt blijft.
