Europeiska unionens
officiella tidning

SV
L-serien

2025/2447

5.12.2025

KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2025/2447

av den 4 december 2025

om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2018/1727 vad gäller tekniska specifikationer, åtgärder och andra krav för inrättande och användning av det decentraliserade it-systemet för säker behandling och överföring av information

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) 2018/1727 av den 14 november 2018 om Europeiska unionens byrå för straffrättsligt samarbete (Eurojust), och om ersättning och upphävande av rådets beslut 2002/187/RIF ([1]), särskilt artiklarna 22a.3 samt 22b.1 a, b, c och d, och

av följande skäl:

(1) I förordning (EU) 2018/1727 fastställs en ram för Eurojusts nya digitala interna infrastruktur och inrättandet av ett decentraliserat säkert digitalt system för kommunikation mellan medlemsstaternas behöriga nationella myndigheter och Eurojust.

(2) Säker digital kommunikation kommer att ske via det decentraliserade it-systemet. För att inrätta det decentraliserade it-systemet behövs tekniska specifikationer som fastställer metoderna för kommunikation och kommunikationsprotokoll, tekniska åtgärder som säkerställer minimistandarder för informationssäkerhet och annan säkerhet samt minimimål för tillgänglighet för genomförandet av it-systemet.

(3) I enlighet med artikel 22a.1 i förordning (EU) 2018/1727 ska det decentraliserade it-systemet bestå av medlemsstaternas och Eurojusts it-system, och interoperabla e-Codex-åtkomstpunkter som dessa it-system är sammankopplade genom. Denna ram bör beaktas i de tekniska specifikationerna och i övriga krav avseende det decentraliserade it-systemet som fastställs i denna förordning.

(4) Åtkomstpunkterna i det decentraliserade it-systemet baseras på auktoriserade e-Codex-åtkomstpunkter enligt definitionen i artikel 3.3 i Europaparlamentets och rådets förordning (EU) 2022/850 ([2]).

(5) Det decentraliserade it-systemet genomförs inom ett större e-Codex-baserat decentraliserat it-system som kallas Judex (Justice Digital Exchange System). Det är därför nödvändigt att säkerställa ett effektivt informationsutbyte om den horisontella utvecklingen.

(6) I enlighet med artikel 22a.4 i förordning (EU) 2018/1727 kan medlemsstaterna och Eurojust välja att i stället för ett nationellt it-system använda den referensgenomförandeprogramvara som kommissionen har utvecklat som sitt back-end-system. För att säkerställa interoperabilitet bör både nationella it-system och referensgenomförandeprogramvaran omfattas av samma tekniska specifikationer och krav.

(7) Uppgifter som rör terroristbrott och grov organiserad brottslighet bör överföras på ett strukturerat sätt för att förbättra informationens kvalitet och relevans samt för att säkerställa att informationen kan integreras mer effektivt i Eurojusts ärendehanteringssystem och kontrolleras bättre mot information som redan finns lagrad i systemet. Format och tekniska standarder för överföring bör fastställas för uppgifter om fingeravtryck och fotografier som kan överföras till Eurojust i syfte att identifiera personer som är föremål för straffrättsliga förfaranden med anknytning till terroristbrott.

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

([2]) Europaparlamentets och rådets förordning (EU) 2022/850 av den 30 maj 2022 om ett datoriserat system för gränsöverskridande elektroniskt utbyte av uppgifter på området civil- och straffrättsligt samarbete (e-Codex-systemet) och om ändring av förordning (EU) 2018/1726 (EUT L 150, 1.6.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/850/oj).

(8) Eurojust underlättar och stödjer utfärdandet och verkställandet av ansökningar om rättslig hjälp, inklusive ansökningar och beslut som bygger på instrument som ger verkan åt principen om ömsesidigt erkännande. Nationella behöriga myndigheter bör kunna be om hjälp och samordning från Eurojust genom det decentraliserade it-systemet.

(9) För att säkerställa effektivitet och samstämmighet är det viktigt att de tekniska specifikationer som fastställs enligt förordning (EU) 2018/1727 är förenliga med de tekniska specifikationer som fastställs i Europaparlamentets och rådets förordningar (EU) 2023/2844 ([3]), (EU) 2023/1543 ([4]) och (EU) 2024/3011 ([5]) samt med framtida digitaliseringsåtgärder som är relevanta för Eurojusts mandat att stödja nationella behöriga myndigheter.

(10) Annan kommunikation mellan Eurojust och de behöriga nationella myndigheterna som också bör möjliggöras genom det decentraliserade it-systemet är t.ex. överföring av information om resultaten av informationsbehandlingen, inbegripet förekomsten av kopplingar till ärenden som redan finns lagrade i ärendehanteringssystemet i enlighet med artikel 22 i förordning (EU) 2018/1727, när Eurojust agerar på eget initiativ, eller överföring av information till Eurojust i syfte att bevara, analysera och lagra bevis som rör folkmord, brott mot mänskligheten, krigsförbrytelser och brott som hör samman med sådan brottslighet i enlighet med artikel 4.1 j i den förordningen.

(11) För att säkerställa att Eurojusts operativa behov beaktas i denna förordning har samråd hållits med Eurojust i enlighet med artikel 22a.3 i förordning (EU) 2018/1727.

(12) I enlighet med artikel 4 i protokoll nr 21 om Förenade kungarikets och Irlands ställning med avseende på området med frihet, säkerhet och rättvisa, fogat till fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt, har Irland genom en skrivelse av den 9 september 2019 meddelat sin önskan att godta och vara bundet av förordning (EU) 2018/1727. Detta deltagande bekräftas genom kommissionens beslut (EU) 2019/2006 ([6]). Förordning (EU) 2018/1727 ändrades genom Europaparlamentets och rådets förordning (EU) 2023/2131 ([7]) för att möjliggöra inrättandet av säkra digitala kommunikationskanaler mellan Eurojust och de behöriga nationella myndigheterna och utgör den rättsliga grunden för den här förordningen. I fall där Irland inte har meddelat sin önskan att delta i antagandet och tillämpningen av förordning (EU) 2023/2131 och inte har meddelat sin önskan att godta och vara bundet av den förordningen, är förordning (EU) 2023/2131, i enlighet med artiklarna 1, 2 och 4a.1 i protokoll nr 21, inte bindande för eller tillämplig på Irland. Irland deltar därför inte i antagandet av den här förordningen.

(13) I enlighet med artiklarna 1 och 2 i protokoll nr 22 om Danmarks ställning, fogat till fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt, deltog Danmark inte i antagandet av förordning (EU) 2018/1727. Den här förordningen är därför inte bindande för eller tillämplig på Danmark.

([3]) Europaparlamentets och rådets förordning (EU) 2023/2844 av den 13 december 2023 om digitalisering av rättsligt samarbete och tillgång till rättslig prövning i gränsöverskridande frågor på privaträttens och straffrättens område och om ändring av vissa rättsakter inom området för rättsligt samarbete (EUT L, 2023/2844, 27.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2844/oj).

([4]) Europaparlamentets och rådets förordning (EU) 2023/1543 av den 12 juli 2023 om europeiska utlämnandeorder och europeiska bevarandeorder för elektroniska bevis i straffrättsliga förfaranden och för verkställighet av fängelsestraff eller annan frihetsberövande åtgärd till följd av straffrättsliga förfaranden (EUT L 191, 28.7.2023, s. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

([5]) Europaparlamentets och rådets förordning (EU) 2024/3011 av den 27 november 2024 om överföring av straffrättsliga förfaranden (EUT L, 2024/3011, 18.12.2024, ELI: http://data.europa.eu/eli/reg/2024/3011/oj).

([6]) Kommissionens beslut (EU) 2019/2006 av den 29 november 2019 om Irlands deltagande i Europaparlamentets och rådets förordning (EU) 2018/1727 om Europeiska unionens byrå för straffrättsligt samarbete (Eurojust) (EUT L 310, 2.12.2019, s. 59, ELI: http://data.europa.eu/eli/dec/2019/2006/oj).

([7]) Europaparlamentets och rådets förordning (EU) 2023/2131 av den 4 oktober 2023 om ändring av Europaparlamentets och rådets förordning (EU) 2018/1727 och rådets beslut 2005/671/RIF vad gäller digitalt informationsutbyte i terrorismärenden (EUT L, 2023/2131, 11.10.2023, ELI: http://data.europa.eu/eli/reg/2023/2131/oj).

(14) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725 ([8]) och avgav ett yttrande den 21 oktober 2025.

(15) De åtgärder som föreskrivs i denna förordning är förenliga med yttrandet från den kommitté som inrättats genom artikel 22c i förordning (EU) 2018/1727.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Tekniska specifikationer för det decentraliserade it-systemet

De tekniska specifikationer, åtgärder och mål för det decentraliserade it-system som avses i artikel 22b.1 a, b, c och d i förordning (EU) 2018/1727 ska vara de som anges i bilaga I till den här förordningen.

Artikel 2

Standarder för digitala förfaranden

De standarder för digitala förfaranden som är tillämpliga på elektronisk kommunikation via det decentraliserade it-system som avses i artikel 22a.3 i förordning (EU) 2018/1727 ska vara de som anges i bilaga II till den här förordningen.

Artikel 3

Tekniska specifikationer för överföring av fingeravtryck och fotografier

De tekniska specifikationer och det format för överföring av fingeravtryck och fotografier som avses i artikel 22a.3 i förordning (EU) 2018/1727 ska vara de som anges i bilaga III till den här förordningen.

Artikel 4

Ikraftträdande

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Denna förordning är till alla delar bindande och direkt tillämplig i medlemsstaterna i enlighet med fördragen.

Utfärdad i Bryssel den 4 december 2025.

På kommissionens vägnar
Ursula VON DER LEYEN
Ordförande

([8]) Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

BILAGA I

TEKNISKA SPECIFIKATIONER, ÅTGÄRDER OCH MÅL FÖR DET DECENTRALISERADE IT-SYSTEMET

1. Inledning och omfattning

I denna bilaga fastställs de tekniska specifikationerna, åtgärderna och målen för det decentraliserade it-systemet för utbyte av information enligt förordning (EU) 2018/1727.

It-systemets decentraliserade karaktär gör det möjligt att på ett direkt och säkert sätt utbyta uppgifter mellan behöriga nationella myndigheter och Eurojust.

2. Definitioner

I denna bilaga gäller följande definitioner:

2.1 *Hypetext Transfer Protocol Secure* (*HTTPS*): krypterad kommunikation och säkra förbindelsekanaler.

2.2 *ursprungets ofrånkomlighet*: åtgärder via sådana metoder som digital certifiering, infrastruktur för kryptering av öppna nycklar och elektroniska signaturer och elektroniska stämplar som styrker uppgifternas integritet och som utgör ursprungsbevis för dem.

2.3 *mottagandets ofrånkomlighet*: åtgärder via sådana metoder som digital certifiering, infrastruktur för kryptering av öppna nycklar, elektroniska signaturer och elektroniska stämplar som för avsändaren utgör bevis för att den avsedda mottagaren mottagit uppgifterna.

2.4 *SOAP* (*Simple Object Access Protocol*): i enlighet med standarder fastställda av World Wide Web Consortium, en specifikation för meddelandeprotokoll vid utbyte av strukturerad information då webbtjänster utförs i datanät.

2.5 *REST* (*Representational State Transfer*): en arkitektonisk stil för utformning av nätverksbaserade applikationer, som bygger på en modell för client-server-kommunikation (stateless) som använder standardmetoder för att utföra operationer med avseende på resurser, vilka i normalfallet är representerade i strukturerade format.

2.6 *webbtjänst*: ett programvarusystem som utarbetats för att hantera interoperabel interaktion maskin-till-maskin över ett nätverk och vars gränssnitt beskrivs i ett maskinläsbart format.

2.7 *utbyte av uppgifter*: utbyte av meddelanden och handlingar genom det decentraliserade it-systemet.

2.8 *e-Codex*: det e-Codex-system som definieras i artikel 3.1 i förordning (EU) 2022/850.

2.9 *EU:s basvokabulär för e-juridik*: EU:s grundläggande terminologi för e-juridik enligt definitionen i punkt 4 i bilagan till förordning (EU) 2022/850.

2.10 *ebMS* (*ebXML Message Service*): ett meddelandeprotokoll som utvecklats inom ramen för OASIS och som möjliggör ett säkert, tillförlitligt och interoperabelt utbyte av elektroniska affärshandlingar med hjälp av SOAP. Det stöder integration mellan företag via olika system.

2.11 *AS4* (*Applicability Statement* 4): en OASIS-standard för profilering av ebMS 3.0 som underlättar säker och interoperabel kommunikation mellan företag genom att använda öppna standarder såsom SOAP och WS-Security.

2.12 *RTO* (*Recovery Time Objective*): maximal godtagbar tid för återupprättande av en tjänst efter en incident.

2.13 *RPO* (*Recovery Point Objective*): den högsta godtagbara mängden förlorade data i händelse av fel.

3. **Metoder för elektronisk kommunikation**

3.1 Det decentraliserade it-systemet ska använda tjänstebaserade metoder för kommunikation, exempelvis webbtjänster eller andra återanvändbara komponenter och programvarulösningar, i syfte att utbyta meddelanden och handlingar.

3.2 Det decentraliserade it-systemet ska särskilt inbegripa kommunikation via e-Codex-åtkomstpunkter, i enlighet med artikel 5.2 i förordning (EU) 2022/850. För att säkerställa ett effektivt och interoperabelt gränsöverskridande utbyte av uppgifter ska det decentraliserade it-systemet därför stödja kommunikationen via e-Codex-systemet.

4. **Kommunikationsprotokoll**

4.1 Det decentraliserade it-systemet ska använda säkra internetprotokoll för

a) kommunikation inom det decentraliserade it-systemet mellan behöriga myndigheter och Eurojust,

b) kommunikation med behöriga myndigheter/domstolsdatabasen enligt punkt 7.1.

4.2 Vad gäller definition och överföring av strukturerade uppgifter och metadata ska komponenterna i det decentraliserade it-systemet baseras på omfattande och allmänt godtagna branschstandarder och branschprotokoll, såsom SOAP och REST.

4.3 Vad gäller transport- och meddelandeprotokoll ska det decentraliserade it-systemet grunda sig på säkra standardbaserade protokoll såsom

a) AS4-profilen för gränsöverskridande utbyte av uppgifter som säkerställer säker och tillförlitlig meddelandehantering med kryptering och oavvislighet,

b) HTTPS/RESTful API:er för kommunikation till stöd för JSON- och XML-format,

c) SOAP för interaktion med hög tillförlitlighet, med WS-säkerhet för autentisering och kryptering.

4.4 För ett smidigt och interoperabelt utbyte av uppgifter ska de kommunikationsprotokoll som används av det decentraliserade it-systemet uppfylla relevanta interoperabilitetsstandarder.

4.5 I tillämpliga fall ska XML-schemana använda relevanta standarder eller vokabulärer som är nödvändiga för en korrekt validering av de element och typer som definieras i schemat. Dessa standarder eller vokabulärer kan omfatta

a) EU:s basvokabulär för e-juridik,

b) UDT (Unqualified Data Types),

c) en kodlista för Europeiska unionens språkkoder.

4.6 Vad gäller säkerhets- och autenticeringsprotokollen ska det decentraliserade it-systemet grunda sig på säkra standardbaserade protokoll såsom

a) TLS (Transport Layer Security) för krypterad och autentiserad kommunikation via nätverk, som stöder ömsesidig autentisering via digitala X.509-certifikat,

b) OAuth/OpenID Connect (OIDC) för säker autentisering och auktorisation,

c) PKI (infrastruktur för kryptering med öppen nyckel) och digitala signaturer för säkert utbyte av nycklar och kontroll av meddelandeintegritet med användning av digitala certifikat (X.509) som utfärdats av betrodda certifieringsmyndigheter.

5. **Informationssäkerhetsmål och relevanta tekniska åtgärder**

5.1 De tekniska åtgärder som ska säkerställa efterlevnad av minimistandarder för it-säkerhet i samband med utbyte av information via det decentraliserade it-systemet ska omfatta följande:

a) Åtgärder som säkerställer sekretessen för information, bl.a. med hjälp av säkra kommunikationskanaler.

b) Åtgärder som säkerställer uppgifters integritet i vila och under överföring.

c) Åtgärder som säkerställer att ursprunget till uppgifter som översänds inom det decentraliserade it-systemet oavvisligen kan spåras till avsändaren och att mottagande av uppgifter oavvisligen kan påvisas.

d) Åtgärder som säkerställer att säkerhetsrelaterade händelser loggas i enlighet med erkända internationella rekommendationer angående it-säkerhetsstandarder ([1]).

e) Åtgärder som säkerställer autentisering och auktorisering av användare samt åtgärder för att kontrollera identiteten på system som är kopplade till det decentraliserade it-systemet.

5.2 Komponenterna i det decentraliserade it-systemet ska säkerställa säker kommunikation och överföring av uppgifter, genom användning av kryptering, infrastruktur för öppna nycklar med digitala certifikat för autentisering och säkert utbyte av nycklar, och säkra meddelandeprotokoll såsom AS4 (ebMS), RESTful API:er och SOAP för att upprätthålla meddelandesekretess och integritet.

5.3 Om TLS används inom ramen för det decentraliserade it-systemet ska den senaste stabila versionen av protokollet användas eller, om detta inte är möjligt, en version utan kända säkerhetsbrister. Endast nyckellängder som säkerställer en lämplig nivå av kryptografisk säkerhet ska tillåtas, och chiffersviter som är kända för att vara osäkra eller ogiltiga får inte användas.

5.4 I möjligaste mån ska digitala PKI-certifikat som används för driften av det decentraliserade it-systemet utfärdas av certifieringsmyndigheter som erkänns som kvalificerade tillhandahållare av betrodda tjänster i enlighet med Europaparlamentets och rådets förordning (EU) nr 910/2014 ([2]). Åtgärder ska vidtas för att säkerställa att sådana certifikat endast används för sina avsedda ändamål, på den nivå av förtroende som krävs och i överensstämmelse med de tillämpliga kraven i förordning (EU) nr 910/2014.

5.5 Komponenterna i det decentraliserade it-systemet ska utvecklas i enlighet med principen om inbyggt dataskydd och dataskydd som standard, och lämpliga administrativa, organisatoriska och tekniska åtgärder ska genomföras för att säkerställa en hög cybersäkerhetsnivå.

5.6 Kommissionen ska utforma, utveckla och underhålla referensgenomförandeprogramvaran i enlighet med de krav och principer för dataskydd som fastställs i förordning (EU) 2018/1725. Den referensgenomförandeprogramvara som tillhandahålls av kommissionen ska göra det möjligt för medlemsstaterna att fullgöra sina skyldigheter i enlighet med Europaparlamentets och rådets förordning (EU) 2016/679 ([3]) respektive direktiv (EU) 2016/680, beroende på vad som är tillämpligt.

([1]) Utan att det påverkar loggningen av säkerhetsskäl ska de loggningsmekanismer som används av komponenterna i det decentraliserade it-systemet, beroende på vad som är lämpligt, göra det möjligt att säkerställa efterlevnad av kraven i artikel 88 i förordning (EU) 2018/1725 och, i tillämpliga fall, artikel 25 i Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 4.5.2016, s. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

([2]) Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (EUT L 257, 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([3]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

5.7 Medlemsstater som använder ett annat back-end-system än referensprogramvaran ska vidta nödvändiga åtgärder för att säkerställa att deras nationella back-end-system uppfyller kraven i förordning (EU) 2016/679 och direktiv (EU) 2016/680, beroende på vad som är tillämpligt.

5.8 Eurojust ska genomföra de åtgärder som krävs för att säkerställa att dess back-end-system, eller ett exempel på den referensgenomförandeprogramvara som används, uppfyller kraven i förordningarna (EU) 2018/1725 och (EU) 2018/1727.

5.9 Medlemsstaterna och Eurojust ska inrätta robusta mekanismer för upptäckt av hot och incidenthantering för att säkerställa snabb identifiering, begränsning och återhämtning från säkerhetsincidenter, i enlighet med sina relevanta policyer, för de it-system under deras ansvar som ingår i det decentraliserade it-systemet.

6. **Minimimål för tillgänglighet**

6.1 Eurojust och medlemsstaterna ska säkerställa att komponenterna i det decentraliserade it-system som de ansvarar för är tillgängliga dygnet runt, sju dagar i veckan, med ett mål för teknisk tillgänglighetsgrad på minst 98 % på årsbasis, exklusive planerat underhåll.

6.2 Kommissionen ska säkerställa att domstolsdatabasen är tillgänglig dygnet runt, sju dagar i veckan, med ett mål för teknisk tillgänglighetsgrad på minst 99 % på årsbasis, exklusive planerat underhåll.

6.3 I möjligaste mån ska underhållsarbetet under arbetsdagar planeras så att det äger rum mellan kl. 20.00 och 07.00 centraleuropeisk tid.

6.4 Medlemsstaterna ska underrätta kommissionen, Eurojust och övriga medlemsstater om underhållsarbeten enligt följande:

a) 5 arbetsdagar i förväg om underhållsarbetet gör systemet otillgängligt i upp till 4 timmar.

b) 10 arbetsdagar i förväg om underhållsarbetet gör systemet otillgängligt i 4 till 12 timmar.

c) 30 arbetsdagar i förväg om underhållsarbetet gör systemet otillgängligt i mer än 12 timmar.

6.5 Om medlemsstaterna har fastställda perioder för regelbundet underhåll ska de informera kommissionen, Eurojust och övriga medlemsstater om de tidpunkter och dagar då sådant fastställt regelbundet underhåll planeras. Om komponenter i det decentraliserade it-systemet som faller under medlemsstaternas ansvar blir otillgängliga under sådant fastställt regelbundet underhåll får medlemsstaterna, genom undantag från de skyldigheter som anges i punkt 1, välja att inte anmäla detta till kommissionen vid varje tillfälle.

6.6 Vid oväntade tekniska fel i en komponent i det decentraliserade it-systemet som faller under medlemsstaternas ansvar ska de utan dröjsmål informera kommissionen och övriga medlemsstater om detta fel och om möjligt ange den förutsedda tidsramen för återställande.

6.7 Eurojust ska underrätta kommissionen och medlemsstaterna om underhållsverksamhet enligt följande:

a) 5 arbetsdagar i förväg om underhållsarbetet gör systemet otillgängligt i upp till 4 timmar.

b) 10 arbetsdagar i förväg om underhållsarbetet gör systemet otillgängligt i 4 till 12 timmar.

c) 30 arbetsdagar i förväg om underhållsarbetet gör systemet otillgängligt i mer än 12 timmar.

6.8 Om Eurojust har fastställda perioder för regelbundet underhåll ska Eurojust informera kommissionen och medlemsstaterna om tidpunkter och dagar när sådant fastställt regelbundet underhåll planeras. Om komponenter i det decentraliserade it-systemet som faller under Eurojusts ansvar blir otillgängliga under sådant fastställt regelbundet underhåll får Eurojust, genom undantag från de skyldigheter som anges i punkt 1, välja att inte anmäla detta till kommissionen vid varje tillfälle.

6.9 Vid oväntade tekniska fel i en komponent i det decentraliserade it-systemet som faller under Eurojusts ansvar ska Eurojust utan dröjsmål informera kommissionen och medlemsstaterna om detta fel och om möjligt ange den förutsedda tidsramen för återställande.

6.10 Vid oväntade tekniska fel i behöriga myndigheter/domstolsdatabasen ska kommissionen utan dröjsmål informera Eurojust och medlemsstaterna om den bristande tillgängligheten och om möjligt ange den förutsedda tidsramen för återställande.

6.11 I händelse av driftsstörningar ska medlemsstaterna och Eurojust säkerställa ett snabbt återställande och sörja för minsta möjliga dataförlust, i enlighet med RTO och RPO.

6.12 Medlemsstaterna och Eurojust ska vidta lämpliga åtgärder för att uppnå de tillgänglighetsmål som anges ovan och fastställa förfaranden för effektiv hantering av incidenter.

7. **Behöriga myndigheter/domstolsdatabasen (CDB)**

7.1 Enligt artikel 22a i förordning (EU) 2018/1727 ska det decentraliserade it-systemet möjliggöra elektronisk kommunikation mellan de behöriga nationella myndigheterna och Eurojust. Med tanke på att de behöriga nationella myndigheterna och Eurojust är skyldiga att utbyta information mellan sig enligt artiklarna 21, 21a och 22 i förordning (EU) 2018/1727, men också givet Eurojusts roll när det gäller att underlätta och stödja utfärdande och verkställande av ansökningar om ömsesidig rättslig hjälp eller ömsesidigt erkännande i enlighet med artikel 8.1 i samma förordning, måste de berörda behöriga myndigheterna vara tydligt identifierbara när de använder det decentraliserade it-systemet. Det är därför nödvändigt att upprätta en officiell databas för det decentraliserade it-systemet med information avseende dessa myndigheter.

7.2 CDB ska innehålla följande information i ett strukturerat format:

a) Vid tillämpning av artikel 8.1, 8.3, 8.4, artiklarna 21–21a och artikel 22 i förordning (EU) 2018/1727, information om de behöriga nationella myndigheterna, inbegripet nationella kontaktpersoner enligt artikel 20, samt nationella medlemmar i enlighet med artikel 7 ([4]) i den förordningen.

b) I förekommande fall, information som är nödvändig för att fastställa de geografiska områden eller sakområden som omfattas av de behöriga myndigheternas behörighet eller andra relevanta kriterier som krävs för att fastställa deras behörighet.

c) Information som är nödvändig för en korrekt teknisk överföring av meddelanden inom det decentraliserade it-systemet.

7.3 Kommissionen ska ansvara för utveckling, underhåll, drift av och stöd till CDB.

7.4 CDB ska göra det möjligt för medlemsstaterna och Eurojust att uppdatera informationen i databasen och för behöriga nationella myndigheter och nationella medlemmar som deltar i det decentraliserade it-systemet att programmatiskt få tillgång till och hämta information därifrån.

7.5 Åtkomst till CDB ska möjliggöras via ett gemensamt kommunikationsprotokoll, oavsett om de behöriga myndigheter som är anslutna till det decentraliserade it-systemet använder ett nationellt back-end-system eller en referensgenomförandeprogramvara.

7.6 Medlemsstaterna ska säkerställa att informationen om deras behöriga myndigheter i CDB är fullständig, korrekt och aktuell i enlighet med punkt 7.2.

([4]) Detta påverkar inte delegeringen av befogenheter från den nationella medlemmen till biträdande nationella medlemmar, annan personal vid den nationella enheten eller behörig Eurojustpersonal.

BILAGA II

STANDARDER FÖR DIGITALA FÖRFARANDEN

I artikel 3.9 i förordning (EU) 2022/850 definieras standardena för digitala förfaranden som de tekniska specifikationer för verksamhetsmodeller och datascheman som anger den elektroniska strukturen för de uppgifter som utbyts genom e-Codex-systemet.

I denna bilaga anges de tekniska specifikationerna för verksamhetsmodeller och de tekniska specifikationerna för datascheman.

1. **Tekniska specifikationer för verksamhetsmodellerna enligt förordning (EU) 2018/1727**

De tekniska specifikationerna för verksamhetsmodeller anges i punkterna 1.1–1.5. Där fastställs de viktigaste aspekterna som är nödvändiga för att möjliggöra elektronisk kommunikation genom det decentraliserade it-systemet vid tillämpningen av förordning (EU) 2018/1727.

Det decentraliserade it-systemet ska endast möjliggöra informationsutbyte mellan de behöriga nationella myndigheterna i en medlemsstat och den nationella medlemmen från den medlemsstaten.

1.1 *Utbyte av information om det europeiska rättsliga terrorismbekämpningsregistret (CTR), artikel 21a i förordning (EU) 2018/1727*

1.1.1 Modell för överföring av CTR-uppgifter:

Den behöriga nationella myndigheten överför CTR-uppgifter om terrorismärenden till den nationella medlemmen.

1.1.2 Modell för mottagande av CTR-uppgifter:

Den nationella medlemmen tar emot CTR-uppgifterna.

1.1.3 Modell för begäran om samtycke:

Den nationella medlemmen begär att dess behöriga nationella myndighet ger sitt samtycke.

1.1.4 Modell för mottagande av begäran om samtycke:

Den behöriga nationella myndigheten tar emot begäran om samtycke.

1.1.5 Modell för avsändande av svar på begäran om samtycke:

Den behöriga nationella myndigheten skickar ett svar på begäran om samtycke.

1.1.6 Modell för mottagande av svar på begäran om samtycke:

Den nationella medlemmen tar emot svaret på begäran om samtycke.

1.1.7 Modell för underrättande om koppling:

Den nationella medlemmen underrättar den behöriga nationella myndigheten om en koppling till ett annat ärende.

1.1.8 Modell för uppdatering av CTR-uppgifter:

Den behöriga nationella myndigheten överför uppgifter som behöver uppdateras eller raderas till sin respektive nationella medlem.

1.1.9 Modell för mottagande av uppdaterade CTR-uppgifter:

Den nationella medlemmen tar emot de CTR-uppgifter som behöver uppdateras eller raderas.

1.2 *Utbyte av information om grov brottslighet, artikel 21 i förordning (EU) 2018/1727*

1.2.1 Modell för överföring av uppgifter om grov gränsöverskridande brottslighet:

Den behöriga nationella myndigheten överför uppgifter om grov gränsöverskridande brottslighet till Eurojust.

1.2.2 Modell för mottagande av uppgifter om grov gränsöverskridande brottslighet:

Den nationella medlemmen tar emot uppgifterna om grov gränsöverskridande brottslighet.

1.2.3 Modell för begäran om samtycke:

Den nationella medlemmen begär att dess behöriga nationella myndighet ger sitt samtycke.

1.2.4 Modell för mottagande av begäran om samtycke:

Den behöriga nationella myndigheten tar emot begäran om samtycke.

1.2.5 Modell för avsändande av svar på begäran om samtycke:

Den behöriga nationella myndigheten skickar ett svar på begäran om samtycke.

1.2.6 Modell för mottagande av svar på begäran om samtycke:

Den nationella medlemmen tar emot svaret på begäran om samtycke.

1.2.7 Modell för underrättande om koppling:

Den nationella medlemmen underrättar den behöriga nationella myndigheten om en koppling till ett annat ärende.

1.2.8 Modell för uppdatering av uppgifter om grov gränsöverskridande brottslighet:

Den behöriga nationella myndigheten överför uppgifter som behöver uppdateras eller raderas till sin respektive nationella medlem.

1.2.9 Modell för mottagande av uppdaterade uppgifter om grov gränsöverskridande brottslighet:

Den nationella medlemmen tar emot de uppgifter om grov gränsöverskridande brottslighet som behöver uppdateras eller raderas.

1.3 *Utbyte av allmän information*

1.3.1 Modell för avsändande av information:

Den nationella medlemmen skickar information till den behöriga nationella myndigheten eller vice versa.

1.3.2 Modell för mottagande av information:

Den behöriga nationella myndigheten eller den nationella medlemmen tar emot informationen.

1.3.3 Modell för besvarande av information:

Den behöriga nationella myndigheten besvarar informationen från den nationella medlemmen eller vice versa.

1.3.4 Modell för mottagande av svar:

Den nationella medlemmen tar emot svaret från den behöriga nationella myndigheten.

1.3.5 Modell för avsändande av information:

Den behöriga nationella myndigheten skickar information till den nationella medlemmen.

1.3.6 Modell för mottagande av information:

Den nationella medlemmen tar emot informationen.

1.3.7 Modell för besvarande av information:

Den nationella medlemmen svarar på informationen från den behöriga nationella myndigheten.

1.3.8 Modell för mottagande av svar:

Den behöriga nationella myndigheten tar emot svaret från den nationella medlemmen.

1.4 *Underlättande och stödjande roll, artikel 8.1 i förordning (EU) 2018/1727*

Anm.: Om de modeller för underlättande och stöd som beskrivs under punkt 1.5 inbegriper utbyte av lagstadgad utformning som fastställts genom unionsrättsakter på området straffrättsligt samarbete ska modellerna, i förekommande fall, använda de relevanta strukturerade datarepresentationer och XML-scheman som utarbetats för dessa rättsakter, till exempel de som fastställts för tillämpningen av genomförandeförordning (EU) 2023/2844 eller andra relevanta instrument.

1.5 *Modell för begäran om underlättande eller stöd*

1.5.1 Modell för begäran om överföring eller stöd:

Den nationella behöriga myndigheten överför en begäran om underlättande eller stöd till sin respektive nationella medlem.

1.5.2 Modell för mottagande av begäran om underlättande eller stöd:

Den nationella medlemmen tar emot begäran om underlättande eller stöd och vidarebefordrar den till den tillfrågade medlemsstatens nationella medlem utanför Judex.

1.5.3 Modell för vidarebefordran av begäran om underlättande eller stöd till behörig nationell myndighet:

Den tillfrågade medlemsstatens nationella medlem skickar begäran till sin respektive behöriga nationella myndighet.

1.5.4 Modell för mottagande av begäran om underlättande eller stöd:

Den behöriga nationella myndigheten tar emot begäran om underlättande eller stöd.

1.5.5 Modell för avsändande av svar på begäran om underlättande eller stöd:

Den behöriga nationella myndigheten skickar ett svar på eller information om begäran till den nationella medlemmen i den tillfrågade medlemsstaten.

1.5.6 Modell för mottagande av svar på begäran om underlättande eller stöd:

Den nationella medlemmen tar emot svaret på eller information om begäran om underlättande eller stöd från den behöriga nationella myndigheten och delar detta med till den begärande medlemsstatens nationella medlem utanför Judex.

1.5.7 Modell för besvarande av begäran om underlättande eller stöd:

Den nationella medlemmen i den begärande medlemsstaten besvarar eller delar informationen om begäran om underlättande eller stöd från den behöriga nationella myndigheten.

1.5.8 Modell för mottagande av svar:

Den behöriga nationella myndigheten tar emot svaret på eller information om underlättande eller stöd.

2. Tekniska specifikationer för datascheman

De tekniska specifikationer som ska ligga till grund för utvecklingen av XML-schemadefinitioner (XSD) för digitaliseringen av förordning (EU) 2018/1727 anges i punkterna 2.1 och 2.2 i denna bilaga. I dessa specifikationer definieras huvudsakliga komponenter och annan information som ska ge en heltäckande beskrivning av hur dessa scheman skapas.

Beskrivningen är avsedd att vara generisk vilket gör det möjligt att modifiera och utvidga de XSD som skapats utan att göra några betydande ändringar i dessa specifikationer.

Specifikationerna ska gälla den lagstadgade utformningen av de scheman som bifogas förordning (EU) 2018/1727 samt i förväg fastställda meddelanden eller fritextmeddelanden som används vid utbyten enligt den förordningen.

2.1 *Allmänna överväganden*

För alla scheman gäller följande bestämmelser:

2.1.1 Versioner

Ett version-attribut ska inkluderas för att underlätta hanteringen av schemaversioner och göra det möjligt att uppdatera dem framledes i enlighet med verksamhetskraven. Det ska framgå av version-attributet om den nya versionen är bakåtkompatibel vid införande av nya funktioner eller förbättringar.

2.1.2 Schemadeklaration och metadata

— I tillämpliga fall ska schemat använda de relevanta standarder eller vokabulärer som krävs av e-Codex för att skapa interoperabilitet, och som är nödvändiga för en korrekt validering av de element och typer som definieras i detta schema. Det kan bland annat röra sig om följande:

  — EU:s basvokabulär för e-juridik.

  — UDT (Unqualified Data Types).

  — En kodlista för Europeiska unionens språkkoder.

— I tillämpliga fall kan schemat även innehålla relevanta Etsi-standarder för användning av definitionerna.

2.1.3 Kommentarer och dokumentation

— **Kommentarer**: Varje element i schemat ska normalt åtföljas av kommentarer. Kommentarerna innehåller människoläsbar information om elementet, ofta med en tydlig och kortfattad definition av dess syfte eller användning.

2.1.4 Användning och anpassningsbarhet

Schemat ska följa reglerna i leden a–d:

a) **Modulär struktur**: varje avsnitt ska vara utformat för en särskild funktion och kan återanvändas eller anpassas oberoende av andra sektioner. Detta ska göra det enkelt att anpassa schemat för olika användningsfall.

b) **Utvidgningsbarhet**: schemat ska utformas för att stödja inkludering av nya element eller attribut om ytterligare information behövs framledes. Detta ska uppnås med hjälp av valfria element och sekvenser som kan utvidgas utan att befintliga genomföranden bryts.

c) **Anpassningsbar struktur**: schemat ska utformas så att det blir möjligt att vid behov lägga till eller ändra på element eller datatyper. Schemats struktur ska möjliggöra ändringar i kraven utan att några större omarbetningar måste göras.

d) **Valfria element**: element inom ett schema kan markeras som valfria, dvs. de kan inkluderas eller utelämnas beroende på vilka specifika omständigheter som råder.

Schemat ska utformas för att stödja insamlingen av strukturerade uppgifter för särskilda begäranden.

2.1.5 Modifieringar

Schemat ska kännetecknas av flexibilitet, modularitet och anpassningsbarhet. Komplexa typer och valfria element ska införlivas i utformningen så att den anpassas till olika scenarier och samtidigt förblir enkel att modifiera och utvidga.

2.2 *Utbyte av strukturerade uppgifter*

De strukturerade uppgifter som avses i punkterna 2.2.1 och 2.2.2 ska tillhandahållas i enlighet med artikel 22a.3 i förordning (EU) 2018/1727. Schemat ska också göra det möjligt att ange vilka dataset som ska raderas vid framtida uppdateringar.

2.2.1 Uppgifter i det europeiska rättsliga terrorismbekämpningsregistret

I följande tekniska specifikationer för dataschemat fastställs en strukturerad ram för att skapa schemat i XML-format.

a) Överordnat avsnitt

Detta överordnade avsnitt motsvarar informationen i bilaga III till förordning (EU) 2018/1727 avseende det europeiska rättsliga terrorismbekämpningsregistret (CTR).

b) Meddelandets struktur

CTR-uppgifternas struktur ska bestå av en sekvens av element och minst omfatta följande:

i) Information för att identifiera fysiska personer:

— Efternamn (familjenamn).

— Förnamn.

— Eventuella alias.

— Födelsedatum.

— Födelseort (ort och land).

— Medborgarskap.

— Identitetshandling (typ och handlingens nummer).

— Kön.

— Bostadsort.

ii) Information för att identifiera juridiska personer:

— Företagsnamn.

— Juridisk form.

— Huvudkontor.

iii) Information för att identifiera både fysiska och juridiska personer:

— Telefonnummer.

— E-postadresser.

— Uppgifter om konton hos banker eller andra finansinstitut.

— Status för förfarandena.

iv) Information om brottet:

— Information om juridiska personer som deltar i förberedelsen eller utförandet av ett terroristbrott.

— Brottsrubricering enligt nationell rätt.

— Tillämplig form av allvarlig brottslighet från den förteckning som avses i bilaga I.

— Eventuell anknytning till en terroristgrupp.

— Typ av terrorism, t.ex. jihadistisk, separatistisk, vänsterextrem eller högerextrem.

— Kort sammanfattning av ärendet.

v) Information om de nationella förfarandena:

— Status för sådana förfaranden.

— Ansvarig åklagarmyndighet.

— Ärendenummer.

— Datum då formella rättsliga förfaranden inleddes.

— Kopplingar till andra relevanta ärenden.

vi) Ytterligare information (fritext)

vii) Kod för förhandstillstånd

2.2.2 Uppgifter som har överförts i enlighet med artikel 21 i förordning (EU) 2018/1727

a) Artikel 21.4 i förordning (EU) 2018/1727 om inrättande av gemensamma utredningsgrupper

i) Överordnat avsnitt
Detta överordnade avsnitt motsvarar informationen i artikel 21.4 i förordning (EU) 2018/1727, information om inrättande av gemensamma utredningsgrupper.

ii) Meddelandets struktur
Uppgifternas struktur ska bestå av en sekvens av element och minst omfatta följande:

— Nationell rättslig myndighet med ansvar för det straffrättsliga förfarandet.

— Nationellt referensnummer för det straffrättsliga förfarandet.

— Status för de straffrättsliga förfarandena.

— Utredda brott.

— Andra länder som berörs i ärendet.

— Får ärendet redan stöd av Eurojust?

— Om ja; ange ärende-id.

— Om nej; ange om detta är en begäran om stöd.

— Får ärendet stöd av Europol?

— Om ja; ange operativ specialgrupp och/eller nätapplikation för säkert informationsutbyte (Siena).

— Avtal om en gemensam utredningsgrupp.

— Länder som berörs.

— Parter i den gemensamma utredningsgruppen (nationella myndigheter med ansvar för utredningarna).

— Nationellt referensnummer för de straffrättsliga förfaranden som hanteras av den gemensamma utredningsgruppen.

— Datum för undertecknande.

— Varaktighet.

— Utredda brott.

— Kort sammanfattning av ärendet.

— Huvudmisstänkta i de straffrättsliga förfaranden som hanteras av den gemensamma utredningsgruppen (förnamn, efternamn, födelsedatum och födelseort samt andra eventuella relevanta och nödvändiga uppgiftskategorier enligt bilaga II).

— Resultat av de gemensamma utredningsgruppernas arbete:

— Svårigheter/förseningar i fråga om att

— inrätta den gemensamma utredningsgruppen,

— begära/dela bevis inom den gemensamma utredningsgruppen,

— enas om/genomföra en gemensam strategi för lagföring.

— Tillåtlighet/otillåtlighet/utvärdering av bevis från gemensamma utredningsgrupper i nationella förfaranden.

— Resultat av rättsliga förfaranden (framgångsrika/icke framgångsrika åtal och fällande domar/frikännanden).

iii) Kod för förhandstillstånd

b) Artikel 21.5 i förordning (EU) 2018/1727, allvarliga komplexa ärenden

i) Överordnat avsnitt
Detta överordnade avsnitt motsvarar informationen i artikel 21.5 i Eurojustförordningen, dvs. om allvarliga komplexa fall.

ii) Meddelandets struktur
Uppgifternas struktur ska bestå av en sekvens av element och minst omfatta följande:

— Nationell rättslig myndighet med ansvar för det straffrättsliga förfarandet.

— Nationellt referensnummer för det straffrättsliga förfarandet.

— Status för de straffrättsliga förfarandena.

— Utredda brott.

— Andra länder som berörs i ärendet.

— Får ärendet redan stöd av Eurojust?

— Om ja; ange ärende-id.

— Om nej; ange om detta är en begäran om stöd.

— Får ärendet stöd av Europol?

— Om ja, ange operativ specialgrupp och/eller Siena.

— Tillämplig form av grov brottslighet.

— Inblandning av en brottsorganisation.

— Maffiatyp.

— Transnationell brottsorganisation.

— Återverkningar på EU-nivå.

— Huvudmisstänkta i de straffrättsliga förfarandena (förnamn, efternamn, födelsedatum och födelseort samt andra eventuella relevanta och nödvändiga uppgiftskategorier enligt bilaga II).

— Kort sammanfattning av ärendet.

— Andra länder som berörs.

— Länder med vilka samarbete redan har inletts.

— Behöriga myndigheter som berörs i ett annat land.

— Instrument för rättsligt samarbete som använts.

— Antal mottagna/skickade begäranden.

— Förekomst av utredningar med inbördes kopplingar.

— Länder med vilka samarbete ska påbörjas/länder som eventuellt berörs.

— Typ av samarbete som behövs (t.ex. utlämning, insamling av bevis, annat samarbete).

— Förekomst av utredningar med inbördes kopplingar.

iii) Kod för förhandstillstånd

c) Artikel 21.6 a i förordning (EU) 2018/1727, behörighetskonflikter

i) Överordnat avsnitt

Detta överordnade avsnitt motsvarar informationen i artikel 21.6 a i förordning (EU) 2018/1727, dvs. om behörighetskonflikter.

ii) Meddelandets struktur

Uppgifternas struktur ska bestå av en sekvens av element och minst omfatta följande:

— Nationell rättslig myndighet med ansvar för det straffrättsliga förfarandet.

— Nationellt referensnummer för det straffrättsliga förfarandet.

— Status för de straffrättsliga förfarandena (t.ex. utredning, åtal, rättegång).

— Utredda brott.

— Andra länder som berörs i ärendet.

— Får ärendet redan stöd av Eurojust?

— Om ja; ange ärende-id.

— Om nej; ange om detta är en begäran om stöd.

— Får ärendet stöd av Europol?

— Om ja, ange operativ specialgrupp och/eller Siena.

— Andra länder som berörs.

— Behöriga nationella myndigheter i det andra landet, om sådan information finns tillgänglig.

— Nationellt referensnummer för straffrättsliga förfaranden i annat land.

— Skede för förfarandena i annat land, om sådan information finns tillgänglig.

— Positiv eller negativ konflikt.

— Faktisk eller potentiell konflikt.

— Redan genomförd samordningsverksamhet (t.ex. samråd enligt rådets rambeslut 2009/948/RIF ([1])).

— Kort sammanfattning av ärendet.

— Gemensamma huvudmisstänkta (förnamn, efternamn, födelsedatum och födelseort samt andra eventuella relevanta och nödvändiga uppgiftstyper enligt bilaga II).

iii) Kod för förhandstillstånd

d) Artikel 21.6 b, kontrollerade leveranser

i) Överordnat avsnitt
Detta överordnade avsnitt motsvarar informationen i artikel 21.6 b i förordning (EU) 2018/1727: kontrollerade leveranser.

ii) Meddelandets struktur
Uppgifterna ska struktureras som en sekvens av element och minst omfatta följande:

— Nationell rättslig myndighet med ansvar för det straffrättsliga förfarandet.

— Nationellt referensnummer för det straffrättsliga förfarandet.

— Status för de straffrättsliga förfarandena (t.ex. utredning, åtal, rättegång).

— Utredda brott.

— Andra länder som berörs i ärendet.

— Får ärendet redan stöd av Eurojust?

— Om ja; ange ärende-id.

— Om nej; ange om detta är en begäran om stöd.

— Får ärendet stöd av Europol?

— Om ja, ange operativ specialgrupp och/eller Siena.

— Andra länder som berörs.

— Ursprungsland/transitland/slutdestination.

— Behöriga nationella myndigheter i andra länder.

— Förekomst av utredningar med inbördes kopplingar i andra länder.

([1]) Rådets rambeslut 2009/948/RIF av den 30 november 2009 om förebyggande och lösning av tvister om utövande av jurisdiktion i straffrättsliga förfaranden (EUT L 328, 15.12.2009, s. 42, ELI: http://data.europa.eu/eli/dec_framw/2009/948/oj).

— Typ av levererad vara (t.ex. narkotika och typ av narkotika/pengar/vapen/cigaretter/annat).

— Status för den kontrollerade leveransen (t.ex. planerad, pågående, slutförd).

— Resultat av den kontrollerade leveransen, om den redan har genomförts.

— Instrument för rättsligt samarbete som använts.

— Gemensamma huvudmisstänkta (förnamn, efternamn, födelsedatum och födelseort samt andra eventuella relevanta och nödvändiga uppgiftstyper enligt bilaga II).

iii) Kod för förhandstillstånd

e) Artikel 21.6 c i förordning (EU) 2018/1727, upprepade svårigheter avseende instrument för rättsligt samarbete

i) Överordnat avsnitt

Detta överordnade avsnitt motsvarar informationen i artikel 21.6 c i förordning (EU) 2018/1727: upprepade svårigheter avseende instrument för rättsligt samarbete.

ii) Meddelandets struktur

Uppgifternas struktur ska bestå av en sekvens av element och minst omfatta följande:

— Nationell rättslig myndighet med ansvar för det straffrättsliga förfarandet.

— Nationellt referensnummer för det straffrättsliga förfarandet.

— Status för de straffrättsliga förfarandena (t.ex. utredning, åtal, rättegång).

— Utredda brott.

— Andra länder som berörs i ärendet.

— Får ärendet redan stöd av Eurojust?

— Om ja; ange ärende-id.

— Om nej; ange om detta är en begäran om stöd.

— Får ärendet stöd av Europol?

— Om ja, ange operativ specialgrupp och/eller Siena.

— Andra länder som berörs.

— Behöriga nationella myndigheter, om sådan information finns tillgänglig.

— Utfärdande eller verkställande myndighet.

— Aktuellt instrument för rättsligt samarbete (t.ex. europeisk arresteringsorder, europeisk utredningsorder, frysning och förverkande).

— Ansökan som berörs specifikt (dvs. vilken utredningsåtgärd, vilken typ av frysning, europeisk arresteringsorder för verkställighet av ett straff eller lagföring).

— Avslag eller upprepade svårigheter.

— Vid avslag, ange vilket särskilt skäl som har åberopats.

— Kort beskrivning av svårigheten.

— Andra eventuella nationella myndigheter med samma svårighet.

iii) Kod för förhandstillstånd

2.3 *Kod för förhandstillstånd*

Efter att en koppling har identifierats ska de behöriga nationella myndigheterna ange vidare hantering, åtkomst och överföring av uppgifter med hjälp av koder för förhandstillstånd när de delar uppgifter med Eurojust via Judex. Det ska framgå av koderna för förhandstillstånd om och i vilken utsträckning information om kopplingen får delas med andra behöriga nationella myndigheter, andra unionsbyråer och unionsorgan, tredjeländer eller internationella organisationer.

2.4 *I förväg fastställda meddelanden*

I förväg fastställda meddelanden är representationer av de utbyten som fastställts genom förordning (EU) 2018/1727, men för vilka förordningen inte fastställer någon specifik form. Deras typ och antal fastställs under verksamhetsanalysen och den tekniska analysen.

XLM-schemadefinitionerna (XSD) för i förväg fastställda meddelanden ska utformas för att säkerställa enhetlighet, struktur och överensstämmelse med verksamhetens behov.

För dessa scheman gäller följande:

a) Det överordnade avsnittet i detta schema ska anges i enlighet med den specifika meddelandetyp som fastställs.

b) De fält som krävs för den specifika meddelandetypen ska läggas till och fastställas inom denna struktur för att säkerställa en korrekt representation av dataelementen.

2.5 *Fritextmeddelanden*

Fritextmeddelanden är representationer av utbyten som kan ha ostrukturerat eller delvis strukturerat innehåll, vilket möjliggör flexibilitet samtidigt som regel- och verksamhetskrav uppfylls. XSD för fritextmeddelanden ska utformas så att enhetlighet och korrekt formatering säkerställs.

För dessa scheman gäller följande:

a) Det överordnade avsnittet i schemat ska anges i enlighet med den specifika typ av fritextmeddelande som fastställs.

b) Schemat ska fastställa vilken struktur som krävs för fritextmeddelandet och samtidigt göra det möjligt att anpassa elementens placering efter behov.

c) De nödvändiga fälten för den specifika typen av fritextmeddelande ska läggas till och fastställas inom ramen för denna struktur för att säkerställa en korrekt representation av dataelementen.

BILAGA III

TEKNISKA SPECIFIKATIONER FÖR FINGERAVTRYCK OCH FOTOGRAFIER

Meddelanden som utbyts genom det decentraliserade it-systemet kan åtföljas av bilagor, bland annat så kallade NIST-filer (National Institute of Standards and Technology) med fingeravtryck och fotografier, i enlighet med de tekniska specifikationer som anges i punkterna 1 och 2.

1. **Fingeravtryck**

De fingeravtryck som får delas med Eurojust i syfte att på ett tillförlitligt sätt identifiera personer som är föremål för straffrättsliga förfaranden med anknytning till terroristbrott ska uppfylla följande villkor:

a) Fingeravtrycken tillhandahålls i en fil som innehåller digitala fingeravtrycksbilder (NIST-filen med fingeravtryck) och lämnas in i enlighet med 2015 års uppdatering av standarden ANSI/NIST-ITL 1-2011 (eller nyare version).

b) NIST-filen med fingeravtryck består av upp till tio individuella fingeravtryck: rullade, platta eller båda.

c) Alla fingeravtryck har en märkning.

d) Fingeravtrycken tas genom direkt skanning eller med bläck på papper, förutsatt att fingeravtrycken på papper har skannats med erforderlig upplösning och med samma kvalitet.

e) NIST-filen med fingeravtryck gör det möjligt att inkludera kompletterande information, såsom villkoren för registrering av fingeravtryck och vilken metod som använts för att förvärva enskilda fingeravtrycksbilder.

f) Fingeravtrycken har en nominell upplösning på antingen 500 eller 1 000 ppi ([1]) (med en godtagbar avvikelse på ±10 ppi) med 256 grå nivåer.

g) Den algoritm som används för att komprimera fingeravtrycken följer rekommendationerna från National Institute of Standards and Technology (NIST). Uppgifter om fingeravtryck med en upplösning på 500 ppi komprimeras med WSQ-algoritmen (ISO/IEC 19794-5:2005). Uppgifter om fingeravtryck med en upplösning på 1 000 ppi komprimeras med JPEG 2000 bildkomprimeringsstandard (ISO/IEC 15444-1) och kodningssystem. Målkomprimeringsförhållandet är 15:1.

2. **Fotografier**

De fotografier som får delas med Eurojust i syfte att på ett tillförlitligt sätt identifiera personer som är föremål för straffrättsliga förfaranden med anknytning till terroristbrott ska uppfylla följande villkor:

a) Endast en ansiktsbild tillhandahålls i en fotofil (NIST-fotofilen) och lämnas in i enlighet med 2015 års uppdatering av standarden ANSI/NIST-ITL 1-2011, eller en tillgänglig nyare version.

b) Fotografierna är antingen i gråskala, färg eller nära infrarött.

c) Kvaliteten på fotografierna baseras på bildkraven i ISO/IEC 19794-5:2011 Frontal image type, eller en tillgänglig nyare version.

d) NIST-fotofilen gör det möjligt att inkludera kompletterande information, såsom datum då bilden togs.

([1]) Pixlar per tum.

e) Fotografierna i stående format har en upplösning på minst 600 × 800 pixlar och högst 1 200 × 1 600 pixlar.

f) Ansiktet upptar ett utrymme inom fotografiet som säkerställer minst 120 pixlar mellan mittpunkten i vardera ögat.

g) Den algoritm som används för att komprimera fotografierna följer rekommendationerna från National Institute of Standards and Technology (NIST). Fotografier komprimeras endast en gång med JPG- (ISO/IEC 10918) eller JPEG 2000 (ISO/IEC 15444) bildkompressionsstandard och kodningssystem, och det största tillåtna bildkompressionsförhållandet ska vara på 20:1.