# KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2022/423

**av den 14 mars 2022**

**om fastställande av tekniska specifikationer, åtgärder och andra krav för införandet av det decentraliserade it-system som avses i Europaparlamentets och rådets förordning (EU) 2020/1784**

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) 2020/1784 av den 25 november 2020 om delgivning i medlemsstaterna av rättegångshandlingar och andra handlingar i mål och ärenden av civil eller kommersiell natur (delgivning av handlingar) ([1]), särskilt artikel 25.1, och

av följande skäl:

(1) För att inrätta det decentraliserade it-systemet är det nödvändigt att fastställa och anta tekniska specifikationer, åtgärder och andra krav för detta.

(2) Det finns verktyg som har utvecklats för digitalt utbyte av ärenderelaterade uppgifter, utan att ersätta eller kräva kostsamma ändringar av de befintliga it-system som redan inrättats i medlemsstaterna. e-Codex (e-Justice Communication via On-line Data Exchange) är det viktigaste verktyget av den här typen som har utvecklats hittills.

(3) Det decentraliserade it-systemet bör bestå av medlemsstaternas back-end-system och interoperabla accesspunkter, genom vilka de är sammankopplade. Accesspunkterna i det decentraliserade it-systemet bör baseras på e-Codex.

(4) När det decentraliserade it-systemet har utvecklats kommer styrkommittén att se till att det fungerar och underhålls. Styrkommittén bör inrättas av kommissionen i en separat akt.

(5) Europeiska datatillsynsmannen, som har hörts i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725 ([2]), avgav ett yttrande den 24 januari 2022.

(6) De åtgärder som föreskrivs i denna förordning är förenliga med yttrandet från kommittén för delgivning i medlemsstaterna av rättegångshandlingar och andra handlingar i mål och ärenden av civil eller kommersiell natur.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

*Artikel 1*

**Tekniska specifikationer för det decentraliserade it-systemet**

De tekniska specifikationer, åtgärder och andra krav för införandet av det decentraliserade it-system som avses i artikel 25 i Europaparlamentets och rådets förordning (EU) 2020/1784 ska vara de som fastställs i bilagan.

([1]) EUT L 405, 2.12.2020, s. 40.

([2]) 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).

*Artikel 2*

**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 14 mars 2022.

*På kommissionens vägnar*
Ursula VON DER LEYEN
*Ordförande*

*BILAGA*

**Tekniska specifikationer, åtgärder och andra krav för det decentraliserade system som avses i artikel 1**

1. **Inledning**

Systemet för utbyte av uppgifter rörande delgivning av handlingar (SoD) är ett e-Codex-baserat decentraliserat it-system som kan utbyta handlingar och uppgifter som rör delgivning av handlingar mellan de olika medlemsstaterna i enlighet med förordning (EU) 2020/1784. Eftersom it-systemet är av decentraliserad karaktär, skulle utbyten av uppgifter enbart mellan två medlemsstater möjliggöras utan att någon av unionens institutioner är inblandade i dessa utbyten.

2. **Definitioner**

2.1 *HyperText Transport Protocol Secure eller https*: krypterad kommunikation och säkra förbindelsekanaler.

2.2 *portal*: referensprogramvarulösning eller nationell back-end-lösning som är kopplad till det decentraliserade it-systemet.

2.3 *non-repudiation of origin (ursprungets oförnekbarhet)*: åtgärder via metoder som digital certifiering, infrastruktur för kryptering av öppna nycklar (PKI) och digitala signaturer som styrker uppgifternas integritet och som utgör ursprungsbevis för dem.

2.4 *non-repudiation of receipt (mottagandets oförnekbarhet)*: åtgärder via metoder som digital certifiering, infrastruktur för kryptering av öppna nycklar (PKI) och digitala signaturer som för avsändaren utgör bevis för att den avsedda mottagaren mottagit uppgifterna.

2.5 *Soap*: i enlighet med standarder fastställda av World Wide Web Consortium, en specifikation för meddelandeprotokoll vid utbyte av strukturerad information då webbtjänster utförs i datanät.

2.6 *webbtjänst*: ett programvarusystem som utarbetats för att hantera driftskompatibel interaktion mellan datorer över ett nätverk. Den har ett gränssnitt som beskrivs i ett maskinläsbart format.

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

3. **Metoder för elektronisk kommunikation**

SoD-systemet ska använda tjänstebaserade metoder för kommunikation, exempelvis webbtjänster eller andra återanvändbara infrastrukturer för digitala tjänster, i syfte att utbyta meddelanden och handlingar.

Närmare bestämt kommer det att använda e-Codex-infrastrukturen, som består av två stora komponenter, Connector-delen och Gateway-delen.

Connector-delen hanterar kommunikationen med referensprogramvarulösningen eller nationella lösningar. Systemet kan behandla utbyte av meddelanden med Gateway-delen i båda riktningarna, spåra meddelanden och kvittera dem med hjälp av standarder som *Etsi-REM Evidence Protocols*, validera signaturer av affärshandlingar, skapa en token som visar resultatet av valideringen i pdf- och xml-format samt skapa en container med hjälp av standarder som ASIC-S, där ett meddelandes affärsinnehåll förpackas och signeras.

Gateway-delen svarar för utbytet av meddelanden och är agnostisk vad gäller meddelandets innehåll. Den kan skicka och ta emot meddelanden till och från Connector-delen, validera information i meddelandets startdel, identifiera korrekt behandlingsmetod, signera och kryptera meddelanden samt överföra meddelanden till andra Gateway-delar.

4. **Kommunikationsprotokoll**

SoD-systemet ska använda säkra internetprotokoll såsom https för kommunikation via portaler och decentraliserade it-systemkomponenter, och standardiserade kommunikationsprotokoll såsom Soap för överföring av strukturerade data och metadata.

e-Codex ger dessutom en stark informationssäkerhet genom att dra nytta av den senaste tekniken för autentisering och flerlagers kryptoprotokoll.

5. **Säkerhetsstandarder**

För kommunikationen och överföringen av information via SoD-systemet ska de tekniska åtgärder som garanterar minimistandarder för it-säkerhet omfatta följande:

a) Åtgärder som garanterar sekretessen för information, bl.a. med hjälp av säkra kanaler (https).

b) Åtgärder som säkerställer att uppgifterna inte kan ändras under själva utbytet.

c) Åtgärder som säkerställer att ursprunget till uppgifter som sänds inom SoD-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.

e) Åtgärder som säkerställer att alla registrerade användare är autentiserade och auktoriserade samt åtgärder för att kontrollera identiteten på system som är kopplade till SoD-systemet.

f) SoD-systemet kommer att utvecklas i enlighet med principen om inbyggt dataskydd och dataskydd som standard.

6. **Tjänsternas tillgänglighet**

6.1 Tjänsterna ska fungera dygnet runt, sju dagar i veckan, med en teknisk tillgänglighetsgrad för systemet på minst 98 % exklusive schemalagt underhåll.

6.2 Medlemsstaterna ska underrätta kommissionen om underhållsarbeten enligt följande:

a) Fem arbetsdagar i förväg om underhållsarbetet gör systemet otillgängligt i upp till fyra timmar.

b) Tio arbetsdagar i förväg om underhållsarbetet gör systemet otillgängligt i upp till tolv timmar.

c) 30 arbetsdagar i förväg om underhållsarbetet gör systemet otillgängligt i upp till sex dagar per år.

6.3 I möjligaste mån ska underhållsarbetet under arbetsdagar planeras äga rum mellan kl. 20.00 och 7.00 centraleuropeisk tid.

6.4 Om medlemsstaterna har avsatt en fast tid för underhållsarbete varje vecka ska kommissionen informeras om tid och veckodag. Utan att det påverkar tillämpningen av skyldigheterna enligt punkt 6.2 kan medlemsstaterna, om deras system blir otillgängliga under sådana fasta tider för underhåll, välja att inte underrätta kommissionen om detta vid varje sådant tillfälle.

6.5 I händelse av oväntade tekniska fel i medlemsstaternas system ska medlemsstaterna utan dröjsmål underrätta kommissionen om att deras system inte är tillgängliga och, om möjligt, när tjänsten förväntas återupptas.

6.6 I händelse av oväntade fel på de behöriga myndigheternas databas ska kommissionen utan dröjsmål informera medlemsstaterna om att databasen inte är tillgänglig och, om möjligt, när tjänsten förväntas återupptas.