KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2022/422

af 14. marts 2022

om fastsættelse af de tekniske specifikationer, foranstaltninger og andre krav til gennemførelsen af det decentrale IT-system, der er omhandlet i Europa-Parlamentets og Rådets forordning (EU) 2020/1783

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) 2020/1783 af 25. november 2020 om samarbejde mellem medlemsstaternes retter om bevisoptagelse på det civil- og handelsretlige område (bevisoptagelse) ([1]), særlig artikel 25, stk. 1, og

ud fra følgende betragtninger:

(1) For at oprette det decentrale IT-system til kommunikation og udveksling af dokumenter med henblik på bevisoptagelse er det nødvendigt at fastsætte og vedtage tekniske specifikationer, foranstaltninger og andre krav til gennemførelsen af dette system.

(2) Der er udviklet værktøjer til digital udveksling af sagsrelaterede oplysninger, som hverken erstatter eller kræver bekostelige ændringer af eksisterende IT-systemer, der allerede er indført i medlemsstaterne. e-CODEX-systemet (e-Justice Communication via On-line Data Exchange) er det hidtil vigtigste af sådanne værktøjer, der er udviklet.

(3) Det decentrale IT-system bør bestå af medlemsstaternes back-end-systemer og interoperable adgangspunkter, hvorigennem de er indbyrdes forbundne. Adgangspunkterne i det decentrale IT-system bør baseres på e-CODEX.

(4) Når det decentrale IT-system er udviklet, vil styringskomitéen sikre dets drift og vedligeholdelse. Styringskomitéen bør nedsættes af Kommissionen i en særskilt retsakt.

(5) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([2]) og afgav udtalelse den 24. januar 2022.

(6) Foranstaltningerne i denne forordning er i overensstemmelse med udtalelse fra Udvalget for Samarbejde mellem Medlemsstaternes Retter om Bevisoptagelse på det Civil- og Handelsretlige område —

VEDTAGET DENNE FORORDNING:

Artikel 1

Tekniske specifikationer for det decentrale IT-system

De tekniske specifikationer, foranstaltninger og andre krav til gennemførelsen af det decentrale IT-system, der er omhandlet i artikel 25 i forordning (EU) 2020/1783, er fastsat i bilaget.

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

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

Artikel 2

Ikrafttræden

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

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

Udfærdiget i Bruxelles, den 14. marts 2022.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand

BILAG

Tekniske specifikationer, foranstaltninger og andre krav til det decentrale IT-system, jf. artikel 1

1. **Indledning**

Udvekslingssystemet til bevisoptagelse (ToE) er et decentralt e-CODEX-baseret IT-system, hvorigennem der kan udveksles dokumenter og meddelelser vedrørende bevisoptagelse mellem de forskellige medlemsstater i overensstemmelse med forordning (EU) 2020/1783. Dette IT-systems decentrale karakter vil muliggøre dataudveksling udelukkende mellem to medlemsstater, uden at nogen af EU-institutionerne inddrages i disse udvekslinger.

2. **Definitioner**

2.1. »HyperText Transport Protocol Secure« (»HTTPS«): krypteret kommunikation og sikre kommunikationskanaler

2.2. »Portal«: referencegennemførelsesløsningen eller den nationale back-end-løsning, der er forbundet med det decentrale IT-system

2.3. »uafviselighed af oprindelse«: foranstaltninger til dokumentation af oplysningernes integritet og oprindelse ved hjælp af metoder som digital certificering, offentlig nøgleinfrastruktur og digital signatur

2.4. »uafviselighed af modtagelse«: den tiltænkte modtagers foranstaltninger til dokumentation af modtagelsen af oplysningerne over for afsender ved hjælp af metoder som digital certificering, offentlig nøgleinfrastruktur og digital signatur

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

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

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

3. **Metoder til elektronisk kommunikation**

ToE-udvekslingssystemet benytter tjenestebaseret elektronisk kommunikation såsom webtjenester eller andre genanvendelige digitaltjenesteinfrastrukturer til udveksling af meddelelser og dokumenter.

Mere specifikt anvendes e-CODEX-infrastrukturen, som består af to vigtige komponenter: Connector-delen og Gateway-delen.

Connector-delen håndterer kommunikationen med referencegennemførelsesløsningen eller de nationale løsninger. Den kan udføre udveksling af meddelelser med Gateway-delen i begge retninger, spore meddelelser og anerkende dem ved hjælp af standarder såsom ETSI-REM-beviser, validere signaturer på forretningsdokumenter, oprette et token med resultatet af valideringen i PDF- og XML-format og oprette en beholder ved hjælp af standarder såsom ASIC-S, hvori en meddelelses forretningsindhold er pakket og signeret.

Gateway-delen sikrer udvekslingen af meddelelser, og den er agnostisk over for meddelelsens indhold. Den kan sende og modtage meddelelser til og fra Connector-delen, validere headeroplysninger, konstatere den korrekte behandlingsmetode, signere og kryptere meddelelser og overføre meddelelser til andre Gateways.

4. **Kommunikationsprotokoller**

ToE-udvekslingssystemet anvender sikre internetprotokoller såsom HTTPS til kommunikation med portalens og det decentrale IT-systems komponenter samt standardkommunikationsprotokoller såsom SOAP til overførsel af strukturerede data og metadata.

e-CODEX giver specifikt en stærk informationssikkerhed ved at udnytte de nyeste autentificeringsmetoder og en kryptografisk protokol med flere lag.

5. **Sikkerhedsstandarder**

De tekniske foranstaltninger, der skal sikre overholdelse af minimumsstandarder for IT-sikkerhed i forbindelse med kommunikation og distribution af oplysninger via ToE-udvekslingssystemet, skal omfatte:

a) foranstaltninger, der sikrer oplysningernes fortrolighed, herunder ved at benytte sikre kanaler (HTTPS)

b) foranstaltninger, der sikrer dataenes integritet under udvekslingen

c) foranstaltninger, der sikrer dataafsenderens og datamodtagerens uafviselighed i ToE-udvekslingssystemet

d) foranstaltninger, der sikrer logning af sikkerhedshændelser i overensstemmelse med anerkendte internationale anbefalinger til IT-sikkerhedsstandarder

e) foranstaltninger, der sikrer autentificering og autorisation af alle registrerede brugere, samt foranstaltninger, der kontrollerer identiteten på de systemer, der er forbundet med ToE-udvekslingssystemet

f) udvikling af ToE-udvekslingssystemet i overensstemmelse med princippet om indbygget databeskyttelse og databeskyttelse gennem indstillinger.

6. **Tjenesternes tilgængelighed**

6.1. Tjenesten skal fungere døgnet rundt alle ugens dage med en teknisk tilgængelighedsgrad på mindst 98 % ekskl. planlagt vedligeholdelse.

6.2. Medlemsstaterne underretter Kommissionen om vedligeholdelsesarbejde som følger:

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

b) 10 arbejdsdage i forvejen for vedligeholdelsesopgaver, der kan gøre systemet utilgængeligt i op til 12 timer

c) 30 arbejdsdage i forvejen for vedligeholdelsesopgaver, der kan gøre systemet utilgængeligt i op til seks dage pr. år.

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

6.4. Hvis medlemsstaterne har afsat et fast ugentligt vedligeholdelsestidspunkt, underretter de Kommissionen om klokkeslæt og ugedag. Uden at det berører forpligtelserne i punkt 6.2, kan medlemsstaterne, hvis deres systemer bliver utilgængelige på disse faste vedligeholdelsestidspunkter, vælge ikke at underrette Kommissionen om det hver gang.

6.5. I tilfælde af uventede tekniske fejl i medlemsstaternes systemer skal medlemsstaterne straks underrette Kommissionen om, at deres system ikke er tilgængeligt, og om muligt angive, hvornår tjenesten forventes genoptaget.

6.6. I tilfælde af uventede fejl i databasen over kompetente myndigheder skal Kommissionen straks underrette medlemsstaterne herom, og om muligt angive, hvornår tjenesten forventes genoptaget.