UITVOERINGSVERORDENING (EU) 2022/423 VAN DE COMMISSIE

van 14 maart 2022

tot vaststelling van de technische specificaties, maatregelen en andere vereisten voor de implementatie van het gedecentraliseerde IT-systeem bedoeld in Verordening (EU) 2020/1784 van het Europees Parlement en de Raad

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) 2020/1784 van het Europees Parlement en de Raad van 25 november 2020 inzake de betekening en de kennisgeving in de lidstaten van gerechtelijke en buitengerechtelijke stukken in burgerlijke of in handelszaken (de betekening en de kennisgeving van stukken) ([1]), en met name artikel 25, lid 1,

Overwegende hetgeen volgt:

(1) Met het oog op de invoering van het gedecentraliseerde IT-systeem moeten technische specificaties, maatregelen en andere vereisten voor de implementatie van dat systeem worden vastgesteld.

(2) Voor de digitale uitwisseling van zaakgerelateerde gegevens zijn instrumenten ontwikkeld die geen vervanging van de bestaande, in de lidstaten reeds gebruikte IT-systemen nodig maken en geen dure aanpassingen vergen. Het e-Codex-systeem (e-Justice Communication via Online Data Exchange) is het belangrijkste instrument van dit type dat tot dusver is ontwikkeld.

(3) Het gedecentraliseerde IT-systeem moet bestaan uit de back-endsystemen van de lidstaten en interoperabele toegangspunten waardoor deze onderling verbonden zijn. De toegangspunten van het gedecentraliseerde IT-systeem moeten worden gebaseerd op e-Codex.

(4) Zodra het gedecentraliseerde IT-systeem is ontwikkeld, zorgt de stuurgroep voor de exploitatie en het onderhoud ervan. De stuurgroep moet door de Commissie bij een afzonderlijke handeling worden ingesteld.

(5) De Europese Toezichthouder voor gegevensbescherming is geraadpleegd overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ([2]) en heeft op 24 januari 2022 advies uitgebracht.

(6) De maatregelen waarin deze verordening voorziet, zijn in overeenstemming met het advies van het Comité inzake de betekening en de kennisgeving in de lidstaten van gerechtelijke en buitengerechtelijke stukken in burgerlijke of in handelszaken,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

Technische specificaties van het gedecentraliseerde IT-systeem

De technische specificaties, maatregelen en andere vereisten voor de implementatie van het gedecentraliseerde IT-systeem bedoeld in artikel 25 van Verordening (EU) 2020/1784 zijn in de bijlage opgenomen.

([1]) PB L 405 van 2.12.2020, blz. 40.

([2]) 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).

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, 14 maart 2022.

Voor de Commissie
De voorzitter
Ursula VON DER LEYEN

BIJLAGE

Technische specificaties, maatregelen en andere vereisten betreffende het in artikel 1 bedoelde gedecentraliseerde IT-systeem

1. **Inleiding**

Het uitwisselingssysteem voor de betekening en de kennisgeving van stukken is een op e-Codex gebaseerd gedecentraliseerd IT-systeem dat zorgt voor de uitwisseling tussen de verschillende lidstaten, uit hoofde van Verordening (EU) 2020/1784, van stukken en berichten in verband met de betekening en de kennisgeving van stukken. Het gedecentraliseerde karakter van het IT-systeem zou alleen gegevensuitwisseling tussen één lidstaat en een andere mogelijk maken, zonder dat een van de instellingen van de Unie bij die uitwisseling betrokken is.

2. **Definities**

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

2.2. "portaal": de referentie-implementatieoplossing of de nationale back-endoplossing die verbonden is met het gedecentraliseerde IT-systeem;

2.3. "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 (Public Key Infrastructure — PKI) en digitale handtekeningen;

2.4. "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 (Public Key Infrastructure — PKI) en digitale handtekeningen;

2.5. "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;

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

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

3. **Methoden voor elektronische communicatie**

Voor de uitwisseling van berichten en stukken moet het uitwisselingssysteem voor de betekening en de kennisgeving van stukken gebruikmaken van op diensten gebaseerde methoden voor elektronische communicatie, zoals webdiensten of andere herbruikbare digitalediensteninfrastructuren.

Meer bepaald zal gebruik worden gemaakt van de e-Codexinfrastructuur, die uit twee belangrijke componenten bestaat, namelijk de connector en de gateway.

De connector is verantwoordelijk voor de communicatie met de referentie-implementatieoplossing of de nationale implementaties. De connector kan de uitwisseling van berichten met de gateway in beide richtingen verwerken, berichten traceren en bevestigen met behulp van normen zoals ETSI-REM Evidences, handtekeningen van bedrijfsstukken valideren, een token creëren dat het resultaat van de validering in PDF- en XML-formaat bevat en een container aanmaken met behulp van normen zoals ASIC-S, waarin de zakelijke inhoud van een bericht is verpakt en ondertekend.

De gateway zorgt voor de uitwisseling van berichten, zonder de inhoud van de berichten te hoeven kennen. De gateway kan berichten naar en van de connector verzenden en ontvangen, headerinformatie valideren, de correcte verwerkingsmodus identificeren, berichten ondertekenen en versleutelen en berichten doorgeven naar andere gateways.

4. **Communicatieprotocollen**

Het uitwisselingssysteem voor de betekening en de kennisgeving van stukken maakt gebruik van beveiligde internetprotocollen, zoals HTTPS, voor de communicatie tussen de componenten van het portaal en van het gedecentraliseerde IT-systeem, en de standaardcommunicatieprotocollen, zoals SOAP, voor de transmissie van gestructureerde gegevens en metagegevens.

E-Codex biedt met name krachtige informatiebeveiliging door gebruik te maken van geavanceerde authenticatie en meerlagige cryptografische protocollen.

5. **Beveiligingsnormen**

Voor de communicatie en de verspreiding van informatie via het uitwisselingssysteem voor de betekening en de kennisgeving van stukken 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 kanalen (HTTPS);

b) maatregelen om de integriteit van de gegevens tijdens de uitwisseling ervan te waarborgen;

c) maatregelen ter waarborging van de onweerlegbaarheid van de herkomst van de verzender van de informatie in het uitwisselingssysteem voor de betekening en de kennisgeving van stukken en de onweerlegbaarheid van de ontvangst van informatie;

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

e) maatregelen voor de authenticatie en autorisatie van alle geregistreerde gebruikers en maatregelen ter verificatie van de identiteit van de met het uitwisselingssysteem voor de betekening en de kennisgeving van stukken verbonden systemen;

f) ontwikkeling van het uitwisselingssysteem voor de betekening en de kennisgeving van stukken in overeenstemming met het beginsel van gegevensbescherming door ontwerp en door standaardinstellingen.

6. **Beschikbaarheid van diensten**

6.1. De diensten moeten 24 uur per dag en zeven dagen per week beschikbaar zijn en de technische beschikbaarheidsgraad van het systeem moet ten minste 98 % bedragen, gepland onderhoud buiten beschouwing gelaten.

6.2. De lidstaten moeten de Commissie in kennis stellen van onderhoudsactiviteiten met de volgende termijnen:

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

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

c) onderhoudswerkzaamheden waardoor het systeem maximaal zes dagen per jaar buiten werking kan zijn: 30 werkdagen van tevoren.

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

6.4. De lidstaten die vaste wekelijkse onderhoudsperioden hanteren, moeten de Commissie meedelen voor welke dag en welk tijdstip die vaste wekelijkse onderhoudsperioden gepland zijn. Onverminderd de in 6.2, aangegeven verplichtingen hoeven lidstaten, als hun systemen gedurende een dergelijke vaste periode niet beschikbaar zijn, die niet-beschikbaarheid niet elke keer aan de Commissie te melden.

6.5. Bij een onverwachte technische storing van de systemen van een lidstaat meldt die lidstaat de Commissie onverwijld dat zijn systemen niet beschikbaar zijn en geeft hij zo mogelijk aan wanneer de dienstverlening zal worden hervat.

6.6. Bij een onverwachte technische storing van de databank van bevoegde instanties meldt de Commissie de lidstaten onverwijld dat het systeem niet beschikbaar is en geeft zij zo mogelijk aan wanneer de dienstverlening zal worden hervat.