RÈGLEMENT D'EXÉCUTION (UE) 2022/423 DE LA COMMISSION

du 14 mars 2022

établissant les spécifications, mesures et autres exigences techniques pour la mise en œuvre du système informatique décentralisé visées dans le règlement (UE) 2020/1784 du Parlement européen et du Conseil

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) 2020/1784 du Parlement européen et du Conseil du 25 novembre 2020 relatif à la signification et à la notification dans les États membres des actes judiciaires et extrajudiciaires en matière civile ou commerciale (signification ou notification des actes) ([1]), et notamment son article 25, paragraphe 1,

considérant ce qui suit:

(1) Aux fins de la mise en place du système informatique décentralisé, il convient de définir et d'adopter des spécifications, mesures et autres exigences techniques pour la mise en œuvre de ce système.

(2) Certains outils ont été mis au point pour permettre l'échange numérique de données relatives aux affaires, sans remplacer les systèmes informatiques existants déjà mis en place dans les États membres ni nécessiter de modifications coûteuses de ces systèmes. Le système e-CODEX («e-Justice Communication via On-line Data Exchange») est le principal outil de ce type à avoir été créé à ce jour.

(3) Le système informatique décentralisé devrait comprendre les systèmes dorsaux des États membres et les points d'accès interopérables, par lesquels ils sont interconnectés. Les points d'accès du système informatique décentralisé devraient être basés sur e-CODEX.

(4) Une fois que le système informatique décentralisé aura été mis au point, le comité directeur en assurera le fonctionnement et la maintenance. Le comité directeur devrait être établi par la Commission dans un acte distinct.

(5) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil ([2]) et a rendu un avis le 24 janvier 2022.

(6) Les mesures prévues au présent règlement sont conformes à l'avis du comité relatif à la signification et la notification dans les États membres des actes judiciaires et extrajudiciaires en matière civile et commerciale,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Spécifications techniques du système informatique décentralisé

Les spécifications, mesures et autres exigences techniques pour la mise en œuvre du système informatique décentralisé visées à l'article 25 du règlement (UE) 2020/1784 sont énoncées à l'annexe.

([1]) JO L 405 du 2.12.2020, p. 40.

([2]) Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

Article 2

Entrée en vigueur

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans les États membres conformément aux traités.

Fait à Bruxelles, le 14 mars 2022.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE

Spécifications, mesures et autres exigences techniques du système informatique décentralisé visées à l'article 1er

1. **Introduction**

Le système d'échange dans le cadre de la signification ou notification des actes est un système informatique décentralisé basé sur e-CODEX qui peut procéder à des échanges de documents et de données relatifs à l'obtention des preuves entre les différents États membres conformément au règlement (UE) 2020/1784. Par son caractère décentralisé, ce système informatique permettrait les échanges de données exclusivement d'un État membre à l'autre, sans que l'une ou l'autre des institutions de l'Union intervienne dans ces échanges.

2. **Définitions**

2.1. On entend par «HyperText Transport Protocol Secure» ou «HTTPS»: les canaux de communication cryptée et de connexion sécurisée;

2.2. «portail»: la solution de référence pour la mise en œuvre du système ou le système dorsal national connecté au système informatique décentralisé;

2.3. «non-répudiation de l'origine»: les mesures apportant la preuve de l'intégrité et la preuve de l'origine des données grâce à des méthodes telles que la certification numérique, l'infrastructure à clé publique et les signatures numériques;

2.4. «non-répudiation de la réception»: les mesures apportant à l'émetteur la preuve de la réception des données par le destinataire prévu des données grâce à des méthodes telles que la certification numérique, l'infrastructure à clé publique et les signatures numériques;

2.5. «Simple Object Access Protocol (SOAP)»: selon les normes du World Wide Web Consortium, une spécification de protocole de messagerie pour l'échange d'informations structurées dans la mise en œuvre de services web dans les réseaux informatiques;

2.6. «service web»: un logiciel destiné à assurer une interaction interopérable machine-machine sur un réseau; il dispose d'une interface décrite sous un format pouvant être traité par machine;

2.7. «échange de données», l'échange de messages et de documents par l'intermédiaire du système informatique décentralisé.

3. **Méthodes de communication par voie électronique**

Aux fins de l'échange de messages et de documents, le système d'échange dans le cadre de la signification ou notification des actes utilise des méthodes de communication fondées sur des services telles que des services web ou d'autres infrastructures de services numériques réutilisables.

Plus précisément, il utilisera l'infrastructure e-CODEX, qui est composée de deux éléments principaux, le connecteur et la passerelle.

Le connecteur gère le traitement de la communication avec la solution de mise en œuvre de référence ou les mises en œuvre nationales. Il peut traiter les échanges de messages avec la passerelle dans les deux sens, suivre les messages et les reconnaître en utilisant des normes telles que les preuves ETSI-REM, valider les signatures des documents professionnels, créer un jeton contenant les résultats de la validation en format PDF et XML et créer un conteneur utilisant des normes telles que ASIC-S où le contenu professionnel d'un message est comprimé sous forme de paquet et signé.

La passerelle est responsable de l'échange de messages et est neutre quant au contenu du message. Elle peut envoyer et recevoir des messages à destination et en provenance du connecteur, valider les informations d'en-tête, déterminer le mode de traitement correct, signer et crypter les messages et transférer des messages vers d'autres passerelles.

4. **Protocoles de communication**

Le système d'échange dans le cadre de la signification ou notification des actes utilise des protocoles internet sécurisés, tels que HTTPS pour la communication des éléments du portail et du système informatique décentralisé, ainsi que les protocoles de communication standard, tels que SOAP, pour la transmission de données et métadonnées structurées.

En particulier, e-CODEX garantit un niveau élevé de sécurité de l'information en tirant parti de l'authentification de pointe et du protocole cryptographique multicouches.

5. **Normes de sécurité**

En ce qui concerne la communication et la diffusion d'informations au moyen du système d'échange dans le cadre de la signification ou notification des actes, les mesures techniques permettant d'assurer le respect des normes minimales de sécurité informatique sont notamment les suivantes:

a) mesures visant à garantir la confidentialité des informations, y compris par le recours à des canaux sécurisés (HTTPS);

b) mesures visant à garantir l'intégrité des données lors de leur échange;

c) mesures visant à garantir la non-répudiation de l'origine de l'émetteur des informations au sein du système d'échange d'informations dans le cadre de la signification ou notification des actes et la non-répudiation de la réception des informations;

d) mesures visant à garantir la journalisation des événements liés à la sécurité conformément aux recommandations internationales reconnues en matière de normes de sécurité informatique;

e) mesures visant à garantir l'authentification et l'autorisation de tout utilisateur inscrit et mesures visant à vérifier l'identité des systèmes connectés au système d'échange dans le cadre de la signification ou notification des actes;

f) le système d'échange dans le cadre de la signification ou notification des actes sera développé conformément au principe de la protection des données dès la conception et par défaut.

6. **Disponibilité des services**

6.1. Le service fonctionne 24 heures sur 24, 7 jours sur 7, avec un taux de disponibilité technique du système d'au moins 98 % hors maintenance programmée.

6.2. Les États membres notifient à la Commission les opérations de maintenance dans les délais suivants:

a) 5 jours ouvrables à l'avance en cas d'opérations de maintenance pouvant entraîner jusqu'à 4 heures d'indisponibilité;

b) 10 jours ouvrables à l'avance en cas d'opérations de maintenance pouvant entraîner jusqu'à 12 heures d'indisponibilité;

c) 30 jours ouvrables à l'avance en cas d'opérations de maintenance, dont il peut résulter jusqu'à 6 jours d'indisponibilité par an.

6.3. Dans la mesure du possible, pendant les jours ouvrables, les opérations de maintenance doivent être planifiées entre 20 h 00 et 7 h 00 HEC.

6.4. Lorsqu'un État membre a fixé des créneaux hebdomadaires de maintenance, il notifie à la Commission le jour de la semaine et les heures prévus pour ces créneaux. Sans préjudice des obligations visées au point 6.2, si le système d'un État membre est indisponible dans l'un de ces créneaux fixes, celui-ci n'est pas tenu de le notifier chaque fois à la Commission.

6.5. En cas de défaillance technique imprévue du système d'un État membre, celui-ci notifie immédiatement à la Commission l'indisponibilité de son système et le délai prévisible de rétablissement du service, s'il est connu.

6.6. En cas de défaillance imprévue de la base de données des autorités compétentes, la Commission notifie immédiatement aux États membres l'indisponibilité de la base de données et le délai prévisible de rétablissement du service, s'il est connu.