

**PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2022/423****ze dne 14. března 2022,****kterým se stanoví technické specifikace, opatření a další požadavky pro zavedení decentralizovaného informačního systému uvedené v nařízení Evropského parlamentu a Rady (EU) 2020/1784**

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Evropského parlamentu a Rady (EU) 2020/1784 ze dne 25. listopadu 2020 o doručování soudních a mimosoudních písemností ve věcech občanských a obchodních v členských státech (doručování písemností) <sup>(1)</sup>, a zejména na čl. 25 odst. 1 uvedeného nařízení,

vzhledem k těmto důvodům:

- (1) Za účelem zřízení decentralizovaného informačního systému je nezbytné definovat a přijmout technické specifikace, opatření a další požadavky pro zavedení tohoto systému.
- (2) Jsou k dispozici nástroje, které byly vyvinuty pro digitální výměnu údajů souvisejících s případy, aniž by byly nahrazovány informační systémy již zavedené v členských státech nebo vyžadovány jejich nákladné úpravy. Hlavním nástrojem tohoto druhu, který byl dosud vyvinut, je systém komunikace v oblasti e-justice prostřednictvím výměny informací on-line (e-CODEX).
- (3) Decentralizovaný informační systém by měl být tvořen koncovými systémy členských států a interoperabilními přístupovými body, jejichž prostřednictvím jsou tyto systémy propojeny. Základem přístupových bodů decentralizovaného informačního systému by měl být systém e-CODEX.
- (4) Po dokončení vývoje decentralizovaného informačního systému bude jeho provoz a údržbu zajišťovat řídicí výbor. Řídicí výbor by měla zřídit Komise samostatným aktem.
- (5) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 <sup>(2)</sup> byl konzultován evropský inspektor ochrany údajů a ten vydal stanovisko dne 24. ledna 2022.
- (6) Opatření stanovená tímto nařízením jsou v souladu se stanoviskem Výboru pro doručování soudních a mimosoudních písemností ve věcech občanských a obchodních v členských státech,

PŘIJALA TOTO NAŘÍZENÍ:

*Článek 1***Technické specifikace decentralizovaného informačního systému**

Technické specifikace, opatření a další požadavky pro zavedení decentralizovaného informačního systému uvedené v článku 25 nařízení (EU) 2020/1784 jsou uvedeny stanoveny v příloze.

<sup>(1)</sup> Úř. věst. L 405, 2.12.2020, s. 40.<sup>(2)</sup> Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Úř. věst. L 295, 21.11.2018, s. 39).

*Článek 2***Vstup v platnost**

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Toto nařízení je závazné v celém rozsahu a přímo použitelné v členských státech v souladu se Smlouvami.

V Bruselu dne 14. března 2022.

*Za Komisi*  
*předsedkyně*  
Ursula VON DER LEYEN

---

## PŘÍLOHA

**Technické specifikace, opatření a další požadavky decentralizovaného informačního systému uvedené v článku 1****1. Úvod**

Systém pro doručování písemností je decentralizovaný informační systém založený na systému e-CODEX, který může zajišťovat výměnu dokumentů a údajů týkajících se doručování mezi různými členskými státy v souladu s nařízením (EU) 2020/1784. Decentralizovaná povaha tohoto informačního systému by umožňovala výměny údajů výhradně mezi dvěma členskými státy bez zapojení jakéhokoli orgánu Unie do těchto výměn.

**2. Definice**

- 2.1. Protokolem „HyperText Transport Protocol Secure“ nebo „HTTPS“ se rozumí šifrovaná komunikace a zabezpečené kanály propojení;
- 2.2. „portálem“ se rozumí referenční implementační řešení nebo národní koncový systém připojený k decentralizovanému informačnímu systému;
- 2.3. „nepopíratelností původu“ se rozumí opatření poskytující důkaz o integritě a důkaz o původu údajů prostřednictvím metod, jako jsou elektronická certifikace, infrastruktura veřejných klíčů a digitální podpisy;
- 2.4. „nepopíratelností přijetí“ se rozumí opatření poskytující původci údajů důkaz o přijetí údajů zamýšleným příjemcem prostřednictvím metod, jako jsou elektronická certifikace, infrastruktura veřejných klíčů a digitální podpisy;
- 2.5. protokolem „SOAP“ (Simple Object Access Protocol) se rozumí, podle norem konsorcia W3C, specifikace komunikačního protokolu pro výměnu strukturovaných informací při zavádění webových služeb v počítačových sítích;
- 2.6. „webovou službou“ se rozumí softwarový systém určený k podpoře interoperabilní interakce mezi počítači prostřednictvím počítačové sítě; má rozhraní popsané ve strojově zpracovatelném formátu;
- 2.7. „výměnou údajů“ se rozumí výměna zpráv a dokumentů prostřednictvím decentralizovaného informačního systému.

**3. Způsoby komunikace elektronickými prostředky**

Systém pro doručování písemností využívá pro výměnu zpráv a dokumentů způsoby elektronické komunikace založené na službách, jako jsou webové služby nebo jiné opakovaně použitelné infrastruktury digitálních služeb.

Konkrétně bude využívat infrastrukturu systému e-CODEX, která se skládá ze dvou hlavních složek: konektoru a brány.

Konektor zajišťuje komunikaci s referenčním implementačním řešením a s národními implementačními řešeními. Může provádět výměnu zpráv s bránou v obou směrech, sledovat zprávy a potvrzovat jejich přijetí standardním způsobem, například pomocí důkazů v rámci doporučeného elektronické doručování definovaných Evropským ústavem pro telekomunikační normy (ETSI), ověřovat podpisy obchodních dokumentů, vytvořit token, který obsahuje výsledek validace ve formátu PDF a XML, a vytvořit kontejner za použití standardů, jako je ASiC-S, kde je obchodní obsah zprávy opatřen pečeti a podepsán.

Brána je odpovědná za výměnu zpráv bez ohledu na jejich obsah. Může odesílat zprávy do konektoru a přijímat je z něj, validovat informace uvedené v záhlaví, rozpoznat správný režim zpracování, podepisovat a šifrovat zprávy a předávat zprávy dalším bránám.

#### 4. Komunikační protokoly

Systém pro doručování písemností používá zabezpečené internetové protokoly, jako například HTTPS, pro komunikaci mezi portálem a decentralizovanými složkami informačního systému a standardní komunikační protokoly, jako například SOAP, pro přenos strukturovaných dat a metadat.

Systém e-CODEX konkrétně zajišťuje vysokou bezpečnost informací tím, že využívá nejmodernější autentizaci a vícevrstvý šifrovací protokol.

#### 5. Bezpečnostní standardy

Pro komunikaci a šíření informací prostřednictvím systému pro doručování písemností musí technická opatření zajišťující minimální bezpečnostní standardy informačních technologií zahrnovat:

- a) opatření k zajištění důvěrnosti informací, a to i prostřednictvím používání zabezpečených kanálů (HTTPS);
- b) opatření k zajištění integrity údajů při výměně;
- c) opatření k zajištění nepopiratelnosti původu odesílatele informací v rámci systému pro doručování písemností a nepopiratelnosti přijetí informací;
- d) opatření k zajištění protokolování bezpečnostních událostí v souladu s uznávanými mezinárodními doporučeními pro bezpečnostní standardy informačních technologií;
- e) opatření k zajištění ověření a autorizace všech registrovaných uživatelů a opatření k ověření totožnosti systémů připojených k systému pro doručování písemností;
- f) systém pro doručování písemností musí být vyvinut v souladu se zásadou záměrné a standardní ochrany údajů.

#### 6. Dostupnost služeb

- 6.1. Časový rámec služeb musí být 24 hodin/7 dnů v týdnu, s mírou dostupnosti systému nejméně 98 %, s výjimkou plánované údržby.
- 6.2. Členské státy oznámí Komisi činnosti údržby takto:
  - a) 5 pracovních dnů předem v případě údržby, která může způsobit nedostupnost o délce až 4 hodin;
  - b) 10 pracovních dnů předem v případě údržby, která může způsobit nedostupnost o délce až 12 hodin;
  - c) 30 pracovních dnů předem v případě údržby, která může způsobit nedostupnost o délce až 6 dnů ročně.
- 6.3. Pokud je to možné, operace údržby během pracovních dnů musí být plánovány na dobu mezi 20:00–7:00 SEČ.
- 6.4. Pokud členské státy stanovily pravidelné týdenní termíny údržby, sdělí Komisi den v týdnu a dobu, kdy se takové pravidelné termíny údržby plánují. Aniž jsou dotčeny povinnosti uvedené v bodě 6.2, pokud systémy členských států přestanou být k dispozici během takového pravidelného termínu, nemusí členské státy Komisi každý jednotlivý případ oznamovat.

- 6.5. V případě neočekávaného technického selhání systémů členských států informují členské státy Komisi neprodleně o nedostupnosti svého systému a o termínu předpokládaného obnovení služby, je-li znám.
- 6.6. V případě neočekávaného selhání databáze příslušných orgánů informuje Komise členské státy neprodleně o nedostupnosti služby a o termínu jejího předpokládaného obnovení, je-li znám.
-