PROVÁDĚCÍ ROZHODNUTÍ KOMISE (EU) 2022/483

ze dne 21. března 2022,

kterým se mění prováděcí rozhodnutí (EU) 2021/1073, kterým se stanoví technické specifikace a pravidla k provedení rámce pro důvěryhodnost pro digitální certifikát EU COVID stanoveného nařízením Evropského parlamentu a Rady (EU) 2021/953

(Text s významem pro EHP)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Evropského parlamentu a Rady (EU) 2021/953 ze dne 14. června 2021 o rámci pro vydávání, ověřování a uznávání interoperabilních certifikátů o očkování, o testu a o zotavení v souvislosti s onemocněním COVID-19 (digitální certifikát EU COVID) za účelem usnadnění volného pohybu během pandemie COVID-19 ([1]), a zejména na čl. 9 odst. 1 uvedeného nařízení,

vzhledem k těmto důvodům:

(1) Nařízení (EU) 2021/953 stanoví digitální certifikát EU COVID, který slouží jako doklad o tom, že dané osobě byla podána očkovací látka proti COVID-19, že měla negativní výsledek testu nebo že se z onemocnění zotavila, a to za účelem usnadnění výkonu práva držitelů na volný pohyb během pandemie COVID-19.

(2) Nařízení Evropského parlamentu a Rady (EU) 2021/954 ([2]) stanoví, že členské státy musí pravidla stanovená v nařízení (EU) 2021/953 použít i na státní příslušníky třetích zemí, kteří nespadají do oblasti působnosti uvedeného nařízení, ale kteří mají na jejich území oprávněný pobyt nebo bydliště a kteří mohou v souladu s právem Unie cestovat do jiných členských států.

(3) Doporučení Rady (EU) 2022/290, kterým se mění doporučení Rady (EU) 2020/912 o dočasném omezení cest do EU, jež nejsou nezbytně nutné, a o možném zrušení tohoto omezení ([3]), stanoví, že státní příslušníci třetích zemí, kteří chtějí podniknout cestu ze třetích země do EU, jež není nezbytně nutná, by měli disponovat platným dokladem o očkování nebo o zotavení, jako je například digitální certifikát EU COVID nebo certifikát týkající se onemocnění COVID-19 vydaný třetí zemí, na nějž se vztahuje prováděcí akt přijatý podle čl. 8 odst. 2 nařízení (EU) 2021/953.

(4) Aby digitální certifikát EU COVID fungoval v celé Unii, přijala Komise prováděcí rozhodnutí (EU) 2021/1073 ([4]), kterým se stanoví technické specifikace a pravidla pro vyplňování, bezpečné vydávání a ověřování digitálních certifikátů EU COVID, zajištění ochrany osobních údajů, stanovení společné struktury jedinečného identifikátoru certifikátu a vydávání platného, bezpečného a interoperabilního čárového kódu.

(5) V souladu s článkem 4 nařízení (EU) 2021/953 měly Komise a členské státy zavést a udržovat rámec pro důvěryhodnost digitálního certifikátu EU COVID. Tento rámec pro důvěryhodnost je schopen podporovat dvoustrannou výměnu seznamů zneplatněných certifikátů obsahujících jedinečné identifikátory zneplatněných certifikátů.

([1]) Úř. věst. L 211, 15.6.2021, s. 1.

([2]) Nařízení Evropského parlamentu a Rady (EU) 2021/954 ze dne 14. června 2021 o rámci pro vydávání, ověřování a uznávání interoperabilních certifikátů o očkování, o testu a o zotavení v souvislosti s onemocněním COVID-19 (digitální certifikát EU COVID) ve vztahu ke státním příslušníkům třetích zemí s oprávněným pobytem nebo bydlištěm na území členských států během pandemie COVID-19 (Úř. věst. L 211, 15.6.2021, s. 24).

([3]) Doporučení Rady (EU) 2022/290 ze dne 22. února 2022, kterým se mění doporučení Rady (EU) 2020/912 o dočasném omezení cest do EU, jež nejsou nezbytně nutné, a o možném zrušení tohoto omezení (Úř. věst. L 43, 24.2.2022, s. 79).

([4]) Prováděcí rozhodnutí Komise (EU) 2021/1073 ze dne 28. června 2021, kterým se stanoví technické specifikace a pravidla k provedení rámce pro důvěryhodnost pro digitální certifikát EU COVID stanoveného nařízením Evropského parlamentu a Rady (EU) 2021/953 (Úř. věst. L 230, 30.6.2021, s. 32).

(6) Dne 1. července 2021 byla zprovozněna brána pro digitální certifikát EU COVID (dále jen „brána“), která jako centrální část rámce pro důvěryhodnost umožňuje bezpečnou a důvěryhodnou výměnu veřejných klíčů používaných k ověřování digitálních certifikátů EU COVID mezi členskými státy.

(7) Digitální certifikáty EU COVID se díky svému úspěšnému a rozsáhlému zavedení staly cílem podvodníků, kteří se snaží nalézt způsoby, jak certifikáty podvodně vydávat. Tyto podvodně vydané certifikáty je proto třeba zneplatňovat. Kromě toho mohou členské státy některé digitální certifikáty EU COVID na vnitrostátní úrovni zneplatnit z lékařských důvodů a z důvodu veřejného zdraví, například je-li nějaká šarže podané očkovací látky později shledána vadnou.

(8) Zatímco padělané certifikáty je systém digitálních certifikátů EU COVID schopen ihned odhalit, pravé certifikáty, které jsou vydány protiprávně na základě falešné dokumentace, neoprávněného přístupu nebo s podvodným záměrem, nelze v jiných členských státech odhalit, pokud si členské státy navzájem nevyměňují seznamy zneplatněných certifikátů vytvářené na vnitrostátní úrovni. Totéž platí pro certifikáty, které byly zneplatněny z lékařských důvodů a z důvodu veřejného zdraví. Skutečnost, že ověřovací aplikace členských států nejsou schopny detekovat certifikáty zneplatněné jinými členskými státy, představuje ohrožení veřejného zdraví a podkopává důvěru občanů v systém digitálních certifikátů EU COVID.

(9) Jak je uvedeno v 19. bodě odůvodnění nařízení (EU) 2021/953, z lékařských důvodů a z důvodu veřejného zdraví a v případě podvodně vydaných nebo získaných certifikátů by měly mít členské státy možnost sestavit pro účely uvedeného nařízení seznamy zneplatněných certifikátů a vyměňovat si je s jinými členskými státy, v omezených případech, zejména za účelem zneplatnění certifikátů, které byly vydány chybně, v důsledku podvodu nebo po pozastavení šarže očkovací látky na onemocnění COVID-19, jež byla shledána vadnou. Členské státy by neměly mít možnost zneplatnit certifikáty vydané jinými členskými státy. Vyměňované seznamy zneplatněných certifikátů by neměly obsahovat žádné osobní údaje s výjimkou jedinečných identifikátorů certifikátu. Zejména by neměly obsahovat důvod, proč byl daný certifikát zneplatněn.

(10) Vedle obecného informování o možnosti zneplatnění certifikátů a možných důvodech zneplatnění by příslušný vydávající orgán měl neprodleně informovat držitele zneplatněných certifikátů o zneplatnění jejich certifikátů a o důvodech zneplatnění. V některých případech, zejména v případě digitálních certifikátů EU COVID vydaných v tištěné podobě, však může být nemožné nebo neúměrně náročné držitele vystopovat a informovat o zneplatnění. Členské státy by neměly shromažďovat další osobní údaje, jež nejsou nezbytné pro proces vydávání, jen proto, aby mohly držitele certifikátů informovat, pokud by jejich certifikáty byly zneplatněny.

(11) Je tudíž nezbytné posílit rámec pro důvěryhodnost digitálního certifikátu EU COVID tím, že bude podpořena dvoustranná výměna seznamů zneplatněných certifikátů mezi členskými státy.

(12) Toto rozhodnutí se nevztahuje na dočasné pozastavení platnosti certifikátů ve vnitrostátních situacích, které nespadají do oblasti působnosti nařízení o digitálních certifikátech EU COVID, například na případy, kdy byl držitel certifikátu o očkování pozitivně testován na SARS-CoV-2. Nejsou jím dotčeny zavedené postupy pro kontrolu provozních pravidel týkajících se platnosti certifikátů.

(13) Ačkoliv z technického hlediska jsou proveditelné různé architektury pro výměnu seznamů zneplatněných certifikátů, nejvhodnější je vyměňovat si je prostřednictvím brány, neboť se tím výměna dat omezuje na již zavedený rámec pro důvěryhodnost a ve srovnání s alternativním systémem typu peer-to-peer se minimalizuje jak počet možných bodů selhání, tak počet výměn mezi členskými státy.

(14) Brána pro digitální certifikát EU COVID by tak měla být rozšířena, aby podporovala zabezpečenou výměnu zneplatněných digitálních certifikátů EU COVID pro účely jejich bezpečného ověřování prostřednictvím brány. V tomto ohledu by měla být zavedena vhodná bezpečnostní opatření na ochranu osobních údajů zpracovávaných v bráně. Aby byla zajištěna vysoká úroveň ochrany, měly by členské státy pseudonymizovat atributy certifikátů pomocí nevratné hodnoty hash, která se uvede v seznamech zneplatněných certifikátů. Pro operace zpracování prováděné v rámci brány by se za pseudonymizovaný údaj měl považovat jedinečný identifikátor.

(15) Dále by měla být upravena úloha členských států a Komise, pokud jde o výměnu seznamů zneplatněných certifikátů.

(16) Zpracování osobních údajů držitelů certifikátů, za něž jsou odpovědné členské státy nebo jiné veřejné organizace nebo úřady v členských státech, by mělo být prováděno v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679 ([5]). Zpracování osobních údajů v rámci odpovědnosti Komise pro účely správy a zajištění bezpečnosti brány pro digitální certifikát EU COVID by mělo probíhat v souladu s nařízením Evropského parlamentu a Rady (EU) 2018/1725 ([6]).

(17) Členské státy, zastoupené určenými vnitrostátními orgány nebo úřady, společně stanoví účel a prostředky zpracování osobních údajů prostřednictvím brány pro digitální certifikát EU COVID, a jsou tudíž společnými správci. Článek 26 nařízení (EU) 2016/679 stanoví společným správcům povinnost, aby mezi sebou transparentním ujednáním vymezili své podíly na odpovědnosti za plnění povinností podle uvedeného nařízení. Rovněž stanoví možnost, aby podíly na odpovědnosti vymezilo právo Unie nebo členského státu, které se na správce vztahuje. Ujednání uvedené v článku 26 by mělo být zahrnuto do přílohy III tohoto rozhodnutí.

(18) Nařízení (EU) 2021/953 ukládá Komisi úkol tyto výměny podporovat. Nejvhodnějším způsobem naplnění tohoto mandátu je, aby Komise pro členské státy shromažďovala předané seznamy zneplatněných certifikátů. Komisi by proto měla být přidělena úloha zpracovatele údajů, aby mohla pro členské státy tyto výměny podporovat tím, že usnadní výměny seznamů prostřednictvím brány pro digitální certifikát EU COVID.

(19) Komise, jakožto poskytovatel technických a organizačních řešení pro bránu pro digitální certifikát EU COVID, za členské státy jakožto společné správce zpracovává v rámci brány osobní údaje obsažené v seznamech zneplatněných certifikátů. Působí tedy jako jejich zpracovatel. Podle článku 28 nařízení (EU) 2016/679 a článku 29 nařízení (EU) 2018/1725 se má zpracování zpracovatelem řídit smlouvou nebo právním aktem podle práva Unie nebo členského státu, které zavazují zpracovatele vůči správci a které zpracování vymezují. Je proto třeba stanovit pravidla pro zpracování údajů Komisí jakožto zpracovatelem údajů.

(20) Podpůrná role Komise nezahrnuje zřízení centralizované databáze, jak uvádí 52. bod odůvodnění nařízení (EU) 2021/953. Cílem uvedeného zákazu je zabránit vzniku centralizovaného úložiště všech vydaných digitálních certifikátů EU COVID, což však členským státům nebrání ve výměně seznamů zneplatněných certifikátů, jak výslovně stanoví čl. 4 odst. 2 nařízení (EU) 2021/953.

(21) Při zpracovávání osobních údajů v rámci brány pro digitální certifikát EU COVID je Komise vázána rozhodnutím Komise (EU, Euratom) 2017/46 ([7]).

(22) Ustanovení čl. 3 odst. 10 nařízení (EU) 2021/953 umožňuje Komisi přijmout prováděcí akty, které stanoví, že certifikáty týkající se onemocnění COVID-19, jež byly vydány třetí zemí, s níž Unie a její členské státy uzavřely dohodu o volném pohybu osob, která umožňuje smluvním stranám nediskriminačním způsobem omezit volný pohyb z důvodu veřejného zdraví a jež neobsahuje mechanismus začlenění právních aktů Unie, jsou rovnocenné certifikátům vydávaným v souladu s uvedeným nařízením. Na tomto základě přijala Komise dne 8. července 2021 prováděcí rozhodnutí (EU) 2021/1126 ([8]), kterým se stanoví rovnocennost certifikátů COVID-19 vydaných Švýcarskem.

([5]) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

([6]) 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).

([7]) Další informace o bezpečnostních standardech vztahujících se na všechny informační systémy Evropské komise zveřejňuje Komise na stránkách https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_en.

([8]) Prováděcí rozhodnutí Komise (EU) 2021/1126 ze dne 8. července 2021, kterým se stanoví rovnocennost certifikátů COVID-19 vydaných Švýcarskem a certifikátů vydaných v souladu s nařízením Evropského parlamentu a Rady (EU) 2021/953 (Úř. věst. L 243, 9.7.2021, s. 49).

(23) Ustanovení čl. 8 odst. 2 nařízení (EU) 2021/953 umožňuje Komisi přijmout prováděcí akty, kterými se stanoví, že certifikáty týkající se onemocnění COVID-19, které byly vydány třetí zemí podle norem a technologických systémů, jež jsou interoperabilní s rámcem pro důvěryhodnost pro digitální certifikát EU COVID a jež umožňují ověření pravosti, platnosti a integrity certifikátu, a které obsahují údaje stanovené v příloze uvedeného nařízení, se považují za rovnocenné, pro účely usnadnění výkonu práva jejich držitelů na volný pohyb v Unii, digitálním certifikátům EU COVID. Jak je uvedeno ve 28. bodě odůvodnění nařízení (EU) 2021/953, ustanovení čl. 8 odst. 2 uvedeného nařízení se týká uznávání certifikátů vydaných třetími zeměmi občanům Unie a jejich rodinným příslušníkům. Komise již přijala několik takových prováděcích aktů.

(24) Aby se předešlo mezerám v odhalování zneplatněných certifikátů, na něž se takové prováděcí akty vztahují, mělo by být umožněno, aby i třetí země, jejichž certifikáty týkající se onemocnění COVID-19 se považují za rovnocenné podle čl. 3 odst. 10 a čl. 8 odst. 2 nařízení (EU) 2021/953, mohly bráně pro digitální certifikát EU COVID předávat příslušné seznamy zneplatněných certifikátů.

(25) Někteří státní příslušníci třetích zemí, kteří jsou držiteli zneplatněných certifikátů týkajících se onemocnění COVID-19 vydaných třetí zemí, jejíž certifikáty týkající se onemocnění COVID-19 se podle nařízení (EU) 2021/953 považují za rovnocenné, mohou v okamžiku, kdy dotčená třetí země vygeneruje seznam zneplatněných certifikátů zahrnující jejich certifikáty, spadat mimo oblast působnosti uvedeného nařízení nebo nařízení (EU) 2021/954. Avšak v okamžiku, kdy dotčená třetí země generuje seznam zneplatněných certifikátů, nemůže být známo, zda všichni státní příslušníci třetí země, kteří jsou držiteli zneplatněných certifikátů, spadají do oblasti působnosti některého z uvedených nařízení. Není tudíž proveditelné usilovat o to, aby v okamžiku generování seznamů zneplatněných certifikátů těchto zemí byly vyloučeny osoby, které nespadají do oblasti působnosti žádného z uvedených nařízení, a pokusy o to by vedly k tomu, že by členské státy nebyly schopny odhalit zneplatněné certifikáty v držení státních příslušníků třetích zemí, kteří do Unie cestují poprvé. Avšak i zneplatněné certifikáty těchto státních příslušníků třetích zemí by byly v členských státech ověřeny, když jejich držitelé cestují do Unie a když následně cestují v Unii. Třetí země, jejichž certifikáty se považují za rovnocenné podle nařízení (EU) 2021/953, se neúčastní řízení brány, a nemají tedy postavení společných správců.

(26) Systém digitálních certifikátů EU COVID se navíc ukázal být jediným systémem certifikátů týkajících se onemocnění COVID-19, který funguje v širokém mezinárodním měřítku. V důsledku toho získal digitální certifikát EU COVID rostoucí celosvětový význam a přispěl k řešení pandemie v mezinárodním měřítku tím, že usnadnil bezpečné mezinárodní cestování a podpořil celosvětové oživení. Při přijímání dodatečných prováděcích aktů podle čl. 8 odst. 2 nařízení (EU) 2021/953 se objevily nové potřeby týkající se vyplňování digitálních certifikátů EU COVID. Podle pravidel stanovených v prováděcím rozhodnutí (EU) 2021/1073 je v technickém obsahu certifikátu povinným polem příjmení. Vzhledem k tomu, že v některých třetích zemích existují osoby bez příjmení, za účelem podpory začlenění a interoperability s jinými systémy je nutné tento požadavek změnit. V případech, kdy nelze jméno držitele certifikátu rozdělit na dvě části, by se jméno mělo uvést ve stejném poli (příjmení nebo jméno) digitálního certifikátu EU COVID, v jakém by se uvedlo v cestovním dokladu nebo v průkazu totožnosti daného držitele. Tato změna by rovněž lépe sladila technický obsah certifikátů s aktuálně platnými specifikacemi pro strojově čitelné cestovní doklady vydanými Mezinárodní organizací pro civilní letectví.

(27) Prováděcí rozhodnutí (EU) 2021/1073 by proto mělo být odpovídajícím způsobem změněno.

(28) V souladu s čl. 42 odst. 1 nařízení (EU) 2018/1725 byl konzultován evropský inspektor ochrany údajů, který vydal své stanovisko dne 11. března 2022.

(29) Aby členské státy a Komise měly dostatek času na provedení změn potřebných k umožnění výměny seznamů zneplatněných certifikátů prostřednictvím brány pro digitální certifikát EU COVID, mělo by se toto rozhodnutí začít používat čtyři týdny od vstupu v platnost.

(30) Opatření stanovená tímto rozhodnutím jsou v souladu se stanoviskem výboru zřízeného podle článku 14 nařízení (EU) 2021/953,

PŘIJALA TOTO ROZHODNUTÍ:

Článek 1

Prováděcí rozhodnutí (EU) 2021/1073 se mění takto:

1) vkládají se nové články 5a, 5b a 5c, které znějí:

„Článek 5a

Výměna seznamů zneplatněných certifikátů

1. Rámec pro důvěryhodnost digitálních certifikátů EU COVID umožní výměnu seznamů zneplatněných certifikátů prostřednictvím centrální brány pro digitální certifikát EU COVID (dále jen „brána“) v souladu s technickými specifikacemi uvedenými v příloze I.

2. Pokud členské státy zneplatňují digitální certifikáty EU COVID, mohou seznamy zneplatněných certifikátů předávat bráně.

3. Pokud členské státy předávají seznamy zneplatněných certifikátů, vydávající orgány udržují seznam zneplatněných certifikátů.

4. Dochází-li prostřednictvím brány k výměně osobních údajů, omezuje se jejich zpracování na účely podpory výměny informací o zneplatněných certifikátech. Takové osobní údaje se používají pouze pro účely ověřování stavu zneplatnění digitálních certifikátů EU COVID vydaných v oblasti působnosti nařízení (EU) 2021/953.

5. Informace předávané bráně obsahují tyto údaje v souladu s technickými specifikacemi uvedenými v příloze I:

a) pseudonymizované jedinečné identifikátory zneplatněných certifikátů;

b) datum skončení platnosti předaného seznamu zneplatněných certifikátů.

6. Pokud vydávající orgán zneplatní digitální certifikáty EU COVID, které vydal podle nařízení (EU) 2021/953 nebo nařízení (EU) 2021/954, a hodlá si vyměňovat příslušné informace prostřednictvím brány, předá bráně informace uvedené v odstavci 5 ve formě seznamů zneplatněných certifikátů v zabezpečeném formátu v souladu s technickými specifikacemi uvedenými v příloze I.

7. Vydávající orgány v možném rozsahu poskytnou řešení, pomocí kterého budou v okamžiku zneplatnění držitelé takto zneplatněných certifikátů informováni o stavu zneplatnění svých certifikátů a o důvodu zneplatnění.

8. Brána shromažďuje obdržené seznamy zneplatněných certifikátů. Poskytuje nástroje pro distribuci seznamů členským státům. Seznamy automaticky maže v souladu s datem skončení platnosti, které u každého předaného seznamu uvedl předávající orgán.

9. Určené vnitrostátní orgány nebo úřady členských států, které zpracovávají osobní údaje v bráně, jsou společnými správci zpracovávaných údajů. Příslušné odpovědnosti společných správců jsou rozděleny v souladu s přílohou VI.

10. Zpracovatelem osobních údajů zpracovávaných v rámci brány je Komise. V roli zpracovatele za členské státy Komise zajistí zabezpečení přenosu a uchovávání osobních údajů v rámci brány a plní povinnosti zpracovatele stanovené v příloze VII.

11. Komise a společní správci pravidelně testují, posuzují a hodnotí účinnost technických a organizačních opatření k zajištění bezpečnosti zpracování osobních údajů v rámci brány.

Článek 5b

Předávání seznamů zneplatněných certifikátů třetími zeměmi

Třetí země vydávající certifikáty týkající se onemocnění COVID-19, ve vztahu k nimž Komise přijala prováděcí akt podle čl. 3 odst. 10 nebo čl. 8 odst. 2 nařízení (EU) 2021/953, mohou seznamy zneplatněných certifikátů týkajících se onemocnění COVID-19, na něž se uvedený prováděcí akt vztahuje, předávat ke zpracování Komisí za společné správce v rámci brány uvedené v článku 5a v souladu s technickými specifikacemi uvedenými v příloze I.

Článek 5c

Správa zpracování osobních údajů v centrální bráně pro digitální certifikát EU COVID

1. Rozhodovací proces společných správců řídí pracovní skupina zřízená v rámci výboru uvedeného v článku 14 nařízení (EU) 2021/953.

2. Určené vnitrostátní orgány nebo úřady členských států, které zpracovávají osobní údaje v bráně jako společní správci, jmenují do této skupiny své zástupce.“;

2) příloha I se mění v souladu s přílohou I tohoto rozhodnutí;

3) příloha V se mění v souladu s přílohou II tohoto rozhodnutí;

4) znění přílohy III tohoto rozhodnutí se doplňuje jako nová příloha VI;

5) znění přílohy IV tohoto rozhodnutí se doplňuje jako nová příloha VII.

Článek 2

Toto rozhodnutí vstupuje v platnost třetím dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Použije se po čtyřech týdnech od vstupu v platnost.

V Bruselu dne 21. března 2022.

Za Komisi
předsedkyně
Ursula VON DER LEYEN

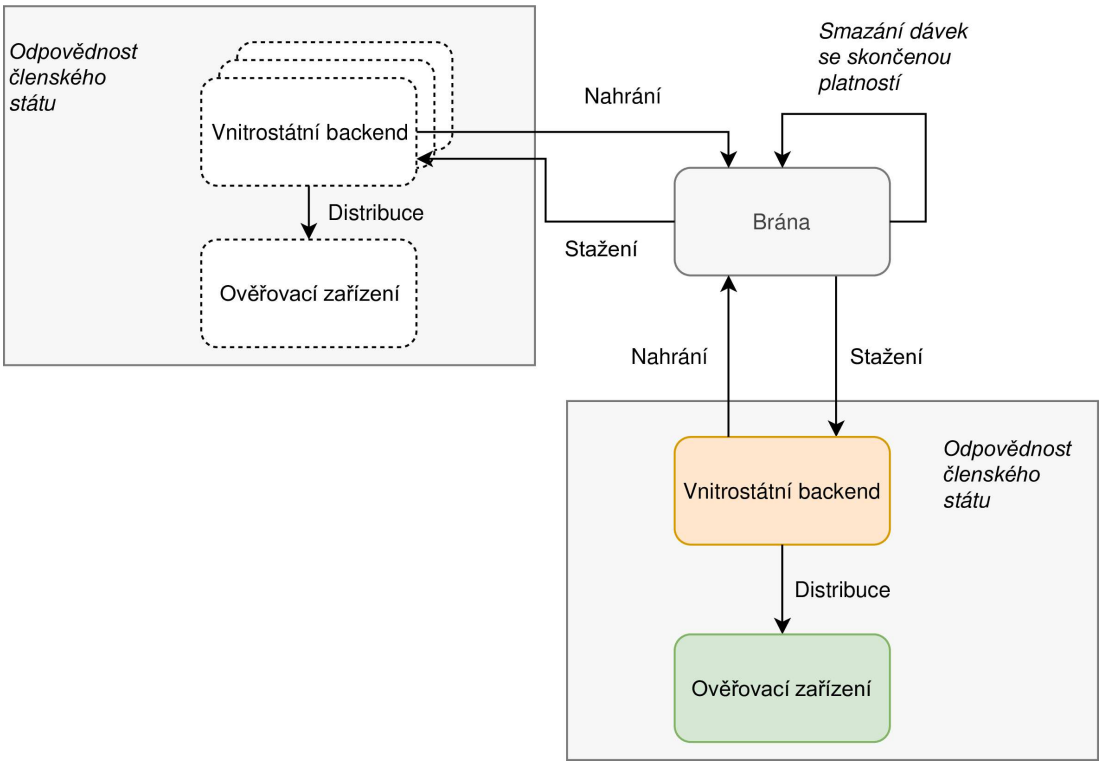
PŘÍLOHA I

V příloze I prováděcího rozhodnutí (EU) 2021/1073 se doplňuje nový oddíl 9, který zní:

„9. **Řešení pro zneplatnění certifikátů**

9.1. **Poskytování seznamu zneplatněných DCC („DRL“)**

Brána poskytuje koncové body a funkce pro uchovávání a správu seznamů zneplatněných certifikátů:



9.2. **Model důvěry**

Veškerá připojení se navazují podle standardního modelu důvěry DCCG s využitím certifikátů NB_{TLS} a NB_{UP} (viz správa certifikátů). Veškeré informace jsou zabaleny a nahrávány ve formě CMS zpráv, aby byla zajištěna integrita.

9.3. **Konstrukce dávek**

9.3.1. *Dávka (Batch)*

Každý seznam zneplatněných certifikátů obsahuje jednu nebo více položek a zabalí se do dávek obsahujících sadu hodnot hash a jejich metadata. Dávka je neměnná (*immutable*) a definuje datum skončení platnosti, které udává, kdy může být dávka smazána. Datum skončení platnosti všech položek v dávce musí být totožné – to znamená, že dávky se musí seskupovat podle data skončení platnosti a podle podepisujícího DSC. Každá dávka obsahuje nejvýše 1 000 položek. Pokud seznam zneplatněných certifikátů obsahuje více než 1 000 položek, vytvoří se více dávek. Každá položka se může vyskytovat nejvýše v jedné dávce. Dávka se zabalí do struktury CMS a podepíše se certifikátem NB_{up} nahrávající země.

9.3.2. *Index dávek (Batch Index)*

Když se vytvoří dávka, brána jí přidělí unikátní ID a dávka se automaticky přidá do indexu. Index dávek je řazen podle data poslední změny ve vzestupném chronologickém pořadí.

9.3.3. *Chování brány*

Brána zpracovává dávky se seznamy zneplatněných certifikátů bez jakýchkoliv změn: nemůže v dávkách žádnou informaci aktualizovat, odstranit ani přidat. Dávky jsou předávány všem schváleným zemím (viz kapitola 9.6).

Brána aktivně sleduje data skončení platnosti dávek a dávky se skončenou platností odstraňuje. Poté, co je dávka smazána, vrací brána pro URL smazané dávky odpověď „HTTP 410 Gone“. Dávka se tedy v indexu dávek objevuje s příznakem „deleted“.

9.4. Typy hodnot hash

Seznam zneplatněných certifikátů obsahuje hodnoty hash, které mohou představovat různé typy/atributy zneplatnění. Tyto typy nebo atributy se uvedou při poskytování seznamů zneplatněných certifikátů. Aktuální typy jsou:

Typ	Atribut	Výpočet hodnot hash
SIGNATURE	DCC Signature	SHA256 of DCC Signature
UCI	UCI (Unique Certificate Identifier)	SHA256 of UCI
COUNTRYCODEUCI	Issuing Country Code + UCI	SHA256 of Issuing CountryCode + UCI

Do dávek se vkládá a k identifikaci zneplatněných DCC slouží pouze prvních 128 bitů hodnot hash vyjádřených jako řetězec v kódování base64 ([1]).

9.4.1. *Typ hodnoty hash: SHA256(DCC Signature)*

V tomto případě se hodnota hash vypočte z bajtů podpisu COSE_SIGN1 z CWT. V případě podpisů RSA se jako vstup použije celý podpis. Vzorec pro certifikáty podepsané algoritmem EC-DSA používá jako vstup hodnotu r:

SHA256(r)

[vyžadováno pro všechny nové implementace]

9.4.2. *Typ hodnoty hash: SHA256(UCI)*

V tomto případě se hodnota hash vypočítá z řetězce UCI v kódování UTF-8 převedeného na pole bajtů (*byte array*).

[zastaralé ([2]), avšak podporováno pro účely zpětné kompatibility]

9.4.3. *Typ hodnoty hash: SHA256(Issuing CountryCode+UCI)*

V tomto případě se vezme kód země vyjádřený jako řetězec v kódování UTF-8 a spojený s identifikátorem UCI vyjádřeným jako řetězec v kódování UTF-8. Výsledek se následně převede na pole bajtů (*byte array*) a použije jako vstup hašovací funkce.

[zastaralé[2], avšak podporováno pro účely zpětné kompatibility]

9.5. Struktura rozhraní API

9.5.1. *API pro poskytování zneplatněných položek*

9.5.1.1. Účel

API dodává položky na seznamech zneplatněných certifikátů ve formě dávek, a to včetně indexu dávek.

9.5.1.2. Koncové body

([1]) Podrobné popisy API naleznete také v oddíle 9.5.1.2.

([2]) Pojmem „zastaralé“ se rozumí, že o této funkci se v nových implementacích neuvažuje, avšak u stávajících implementací bude po přesně vymezené časové období podporována.

9.5.1.2.1. Koncový bod pro stažení seznamu dávek

Koncové body jsou konstruovány jednoduše a vracejí seznam dávek v malém wrapperu poskytujícím metadata. Dávky jsou řazeny podle *data* ve *vzestupném (chronologickém)* pořadí:

/revocation-list

Verb: GET

Content-Type: application/json

Response: JSON Array

```
{
    'more':true|false,
    'batches':
        [{
            'batchId': '{uuid}',
            'country': 'XY',
            'date': '2021-11-01T00:00:00Z'
            'deleted': true | false
        }, ..
        ]
}
```

Poznámka: Výsledek je implicitně omezen na 1 000. Má-li příznak „more" hodnotu „true", odpověď udává, že jsou ke stažení k dispozici další dávky. Pro stažení více položek musí klient nastavit záhlaví If-Modified-Since na datum, které není dřívější než poslední přijatá položka.

V odpovědi je obsaženo pole JSON (*JSON array*) s následující strukturou:

Pole	Definice
more	Příznak typu Boolean, který udává, že jsou k dispozici další dávky
batches	Pole (*array*) se stávajícími dávkami
batchId	https://en.wikipedia.org/wiki/Universally_unique_identifier
country	Kód země dle ISO 3166
date	Datum dle ISO 8601 v UTC. Datum, kdy byla dávka přidána nebo smazána.
deleted	Boolean. Má hodnotu „true", byla-li dávka smazána. Je-li příznak „deleted" nastaven, může být položka po 7 dnech finálně odstraněna z výsledků dotazu.

9.5.1.2.1.1. Kódy odpovědí

Kód	Popis
200	Vše ok.
204	Žádný obsah, pokud záhlaví „If-Modified-Since" nevede k žádné shodě.

Záhlaví požadavku

Záhlaví	Povinné	Popis
If-Modified-Since	Ano	Toto záhlaví obsahuje naposledy stažené datum, aby se získaly pouze nejnovější výsledky. Při prvním volání by mělo být záhlaví nastaveno na '2021-06-01T00:00:00Z'

9.5.1.2.2. Koncový bod pro stažení dávky

Dávky obsahují seznam identifikátorů certifikátů:

/revocation-list/{batchId}

Verb: GET

Accepts: application/cms

Response:CMS with Content

{

'country': 'XY',

'expires': '2022-11-01T00:00:00Z',

'kid':'23S+33f=',

'hashType':'SIGNATURE',

'entries':[{

'hash':'e2e2e2e2e2e2e2e2'

}, ..]

}

Odpověď obsahuje CMS včetně podpisu, který musí odpovídat certifikátu NB_{UP} příslušné země. Všechny položky v poli JSON (*JSON array*) obsahují následující strukturu:

Pole	Povinné	Typ	Definice
expires	Ano	String	Datum, kdy je možné položku odstranit. Datum/čas v UTC dle ISO8601
country	Ano	String	Kód země dle ISO 3166
hashType	Ano	String	Typ hodnoty hash poskytnutých položek (viz Typy hodnot hash)
entries	Ano	JSON Object Array	Viz tabulka Položky
kid	Ano	String	KID certifikátu DSC použitého k podepsání DCC v kódování base64. Není-li KID znám, lze použít řetězec „UNKNOWN_KID“ (bez uvozovek).

Poznámky:

— Dávky se seskupí podle data skončení platnosti a DSC – platnost všech položek skončí ve stejném okamžiku a všechny jsou podepsány stejným klíčem.

— Časem skončení platnosti je datum/čas v UTC, neboť EU-DCC je globální systém a je třeba používat jednoznačný čas.

— Jako datum skončení platnosti trvale zneplatněných DCC se nastaví datum skončení platnosti příslušného DSC použitého k podepsání DCC nebo čas skončení platnosti zneplatněného DCC (a v takovém případě se má za to, že časové údaje ve formátu NumericDate/epoch jsou v časovém pásmu UTC).

— Vnitrostátní backendový systém (NB) odstraní položky ze svého seznamu zneplatněných certifikátů v okamžiku, kdy bude dosaženo datum **skončení platnosti**.

— NB může položky ze svého seznamu zneplatněných certifikátů odstranit v případě, že dojde k zneplatnění **kid** použitého k podepsání DCC.

9.5.1.2.2.1. Položky

Pole	Povinné	Typ	Definice
hash	Ano	String	Prvních 128 bitů hodnoty hash SHA256 jako řetězec v kódování base64

Poznámka: Objekt položek aktuálně obsahuje pouze hodnotu hash, ale pro zajištění kompatibility s budoucími změnami byl namísto pole JSON (*JSON array*) zvolen objekt.

9.5.1.2.2.2. Kódy odpovědí

Kód	Popis
200	Vše ok.
410	Dávka již neexistuje. Dávka může být ve vnitrostátním backendovém systému smazána.

9.5.1.2.2.3. Záhlaví odpovědí

Záhlaví	Popis
ETag	ID dávky.

9.5.1.2.3. Koncový bod pro nahrání dávky

Nahrání se provádí přes stejný koncový bod operací POST:

/revocation-list

Verb: POST

Accepts: application/cms

Request: CMS with Content

ContentType: application/cms

Content:

{

‘country‘: ‘XY‘,

‘expires‘: ‘2022-11-01T00:00:00Z‘,

‘kid‘:‘23S+33f=‘,

‘hashType‘:‘SIGNATURE‘,

‘entries‘:[{

‘hash‘:‘e2e2e2e2e2e2e2e2‘

}, ..]

}

Dávka se podepíše pomocí certifikátu NB_{UP}. Brána ověří, zda byl podpis vytvořen pomocí NB_{UP} pro danou zemi (*country*). Je-li kontrola podpisu neúspěšná, nahrání se nezdaří.

POZNÁMKA: Každá dávka je neměnná (*immutable*) a po nahrání ji již nelze změnit. Je však možné ji smazat. ID každé smazané dávky se uloží a případné nahrání nové dávky se stejným ID se odmítne.

9.5.1.2.4. Koncový bod pro odstranění dávky

Dávku lze odstranit přes stejný koncový bod operací DELETE:

/revocation-list

Verb: DELETE

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

‘batchId‘: ‘...‘

}

nebo, z důvodů kompatibility, přes následující koncový bod operací POST:

/revocation-list/delete

Verb: POST

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

‘batchId‘: ‘...‘

}

9.6. **Ochrana API/obecné nařízení o ochraně osobních údajů (GDPR)**

V tomto oddíle jsou specifikována opatření pro implementaci s ohledem na splnění ustanovení nařízení 2021/953, pokud jde o zpracování osobních údajů.

9.6.1. *Stávající autentizace*

Brána pro autentizaci zemí, které se k ní připojují, v současnosti využívá certifikát NB_{TLS}. Tuto autentizaci lze využít pro určení totožnosti země připojené k bráně. Tato identita může být následně využita pro implementaci řízení přístupu.

9.6.2. *Řízení přístupu*

Aby mohla brána zákonně zpracovávat osobní údaje, zavede mechanismus řízení přístupu.

Brána implementuje seznam řízení přístupu (*Access Control List*) v kombinaci se zabezpečením na základě rolí (*Role Based Security*). V rámci tohoto schématu se vedou dvě tabulky – jedna tabulka popisuje, které role mohou použít které operace na které prostředky, druhá tabulka popisuje, které role jsou přiřazeny kterým uživatelům.

K implementaci kontrolních mechanismů vyžadovaných tímto dokumentem jsou zapotřebí tyto tři role:

RevocationListReader

RevocationUploader

RevocationDeleter

Následující koncové body musí kontrolovat, zda je uživateli přiřazena role RevocationListReader; pokud tomu tak je, je mu umožněn přístup, pokud ne, vrátí se HTTP 403 Forbidden:

GET/revocation-list/

GET/revocation-list/{batchId}

Následující koncové body musí kontrolovat, zda je uživateli přiřazena role RevocationUploader; pokud tomu tak je, je mu umožněn přístup, pokud ne, vrátí se HTTP 403 Forbidden:

POST/revocation-list

Následující koncové body musí kontrolovat, zda je uživateli přiřazena role RevocationDeleter; pokud tomu tak je, je mu umožněn přístup, pokud ne, vrátí se HTTP 403 Forbidden:

DELETE/revocation-list

POST/revocation-list/delete

Brána musí rovněž poskytovat spolehlivou metodu, jak mohou správci spravovat role, které jsou spojeny s uživateli, a to takovým způsobem, aby se snížila možnost lidských chyb a zároveň se předešlo zatěžování správců.“

PŘÍLOHA II

Oddíl 3 přílohy V prováděcího rozhodnutí 2021/1073 se nahrazuje tímto:

„3. ***Společné struktury a všeobecné požadavky***

Digitální certifikát EU COVID se nevydá, pokud kvůli chybějícím informacím nelze správně vyplnit všechna datová pole v souladu s touto specifikací. **Tím není dotčena povinnost členských států vydávat digitální certifikáty EU COVID.**

Informace ve všech polích lze uvádět s použitím celé sady znaků UNICODE 13.0 v kódování UTF-8, pokud není stanoveno výslovné omezení co do souboru hodnot nebo užších souborů znaků.

Společná struktura je tato:

„JSON“:{

„ver“:<informace o verzi>,

„nam“:{

<informace o jméně osoby>

},

„dob“:<datum narození>,

„v“ nebo „t“ nebo „r“:[

{<informace o dávce očkování nebo testu nebo zotavení, jedna položka>}

]

}

Podrobné informace o jednotlivých skupinách a polích jsou uvedeny v dalších oddílech.

Pokud je v pravidlech uvedeno, že se pole má přeskočit, znamená to, že jeho obsah je prázdný a že v obsahu není povoleno uvádět ani název, ani hodnotu pole.

3.1. ***Verze***

Poskytnou se informace o verzi. Verze se vytvářejí podle systému „Semantic Versioning“ (semver: https://semver.org). V produkčním prostředí se musí jednat o jednu z oficiálně zveřejněných verzí (aktuální verze nebo jedna ze starších oficiálně zveřejněných verzí). Pro další podrobnosti viz oddíl Umístění schématu JSON.

ID pole	Název pole	Pokyny
ver	Verze schématu	Musí odpovídat identifikátoru verze schématu použitého k vystavení EUDCC. Příklad: „ver“:“1.3.0“

3.2. ***Jméno a datum narození osoby***

Jméno osoby je celé úřední jméno osoby shodné se jménem uvedeným v cestovních dokladech. Identifikátor struktury je *nam*. Uvede se přesně 1 (jedno) jméno osoby.

ID pole	Název pole	Pokyny
nam/fn	Příjmení	Příjmení držitele. Nemá-li držitel žádná příjmení a má jméno, pole se přeskočí. Ve všech ostatních případech se uvede přesně 1 (jedno) neprázdné pole obsahující všechna příjmení. V případě více příjmení se tato příjmení oddělí mezerou. Kombinovaná jména se spojovníky nebo podobnými znaky však musí zůstat stejná.

		Příklady: „fn“:“Musterfrau-Gößinger“ „fn“:“Musterfrau-Gößinger Müller“
nam/fnt	Standardizované (standardizovaná) příjmení	Příjmení držitele transliterované (transliterovaná) podle stejné konvence jako ve strojově čitelných cestovních dokladech držitele (jako jsou pravidla definovaná v dokumentu ICAO 9303 části 3). Nemá-li držitel žádná příjmení a má jméno, pole se přeskočí. Ve všech ostatních případech se uvede přesně 1 (jedno) neprázdné pole obsahující pouze znaky A–Z a <. Maximální délka: 80 znaků (podle specifikace ICAO 9303). Příklady: „fnt“:“MUSTERFRAU<GOESSINGER“ „fnt“:“MUSTERFRAU<GOESSINGER<MUELLER“
nam/gn	Jméno (jména)	Jméno (jména), např. křestní jméno (jména) držitele. Nemá-li držitel žádné jméno a má příjmení, pole se přeskočí. Ve všech ostatních případech se uvede přesně 1 (jedno) neprázdné pole obsahující všechna jména. V případě více jmen se tato jména oddělí mezerou. Příklad: „gn“:“Isolde Erika“
nam/gnt	Standardizované jméno (standardizovaná jména)	Jméno (jména) držitele transliterované (transliterovaná) podle stejné konvence jako ve strojově čitelných cestovních dokladech držitele (jako jsou pravidla definovaná v dokumentu ICAO 9303 části 3). Nemá-li držitel žádné jméno a má příjmení, pole se přeskočí. Ve všech ostatních případech se uvede přesně 1 (jedno) neprázdné pole obsahující pouze znaky A–Z a <. Maximální délka: 80 znaků. Příklad: „gnt“:“ISOLDE<ERIKA“
dob	Datum narození	Datum narození držitele DCC. Úplné nebo částečné datum bez časového údaje omezené na rozmezí od 1900-01-01 do 2099-12-31. Pokud je známo úplné nebo částečné datum narození, uvede se přesně 1 (jedno) neprázdné pole. Není-li datum narození známo ani částečně, pole se nastaví na prázdný řetězec „”. To by mělo odpovídat informacím uvedeným v cestovních dokladech. Je-li k dispozici údaj o datu narození, použije se jeden z následujících formátů ISO 8601. Jiné možnosti nejsou podporovány. YYYY-MM-DD YYYY-MM YYYY (Ověřovací aplikace může zobrazit chybějící části data narození za použití konvence XX stejně jako u strojově čitelných cestovních dokladů, např. 1990-XX-XX.) Příklady: „dob“:“1979-04-14“ „dob“:“1901-08“ „dob“:“1939“ „dob“:„”

3.3. ***Skupiny údajů specifických pro daný typ certifikátu***

Schéma JSON podporuje tři skupiny údajů, které zahrnují informace specifické pro daný typ certifikátu. Každý EUDCC musí obsahovat přesně 1 (jednu) skupinu. Prázdné skupiny nejsou povoleny.

Identifikátor skupiny	**Název skupiny**	**Údaje**
v	Skupina týkající se očkování	Pokud existuje, musí obsahovat přesně 1 (jeden) údaj popisující přesně 1 (jednu) dávku očkovací látky.
t	Skupina týkající se testu	Pokud existuje, musí obsahovat přesně 1 (jeden) údaj popisující přesně 1 (jeden) výsledek testu.
r	Skupina týkající se zotavení	Pokud existuje, musí obsahovat přesně 1 (jeden) údaj popisující přesně 1 (jedno) potvrzení o zotavení.“

PŘÍLOHA III

„PŘÍLOHA VI

ODPOVĚDNOSTI ČLENSKÝCH STÁTŮ JAKOŽTO SPOLEČNÝCH SPRÁVCŮ, POKUD JDE O BRÁNU PRO DIGITÁLNÍ CERTIFIKÁT EU COVID A VÝMĚNU SEZNAMŮ ZNEPLATNĚNÝCH CERTIFIKÁTŮ EU COVID

ODDÍL 1

Pododdíl 1

Rozdělení odpovědností

1) Společní správci zpracovávají osobní údaje prostřednictvím brány rámce pro důvěryhodnost v souladu s technickými specifikacemi uvedenými v příloze I.

2) Vydávající orgány členských států zůstávají výhradním správcem v souvislosti se shromažďováním, využíváním, sdělováním a veškerým dalším zpracováním informací o zneplatněných certifikátech mimo bránu, včetně postupu vedoucího ke zneplatnění certifikátu.

3) Každý správce odpovídá za zpracování osobních údajů prostřednictvím brány rámce pro důvěryhodnost v souladu s články 5, 24 a 26 obecného nařízení o ochraně osobních údajů.

4) Každý správce zřídí kontaktní místo s dedikovanou e-mailovou schránkou, jež bude sloužit pro komunikaci mezi společnými správci navzájem a mezi společnými správci a zpracovatelem.

5) Rozhodováním o veškerých otázkách vyplývajících z výměny seznamů zneplatněných certifikátů a ze společné správy souvisejícího zpracování osobních údajů a usnadňováním koordinovaného předávání pokynů Komisi jakožto zpracovateli je pověřena pracovní skupina zřízená výborem uvedeným v článku 14 nařízení (EU) 2021/953. Rozhodovací proces společných správců je řízen touto pracovní skupinou a jejím jednacím řádem, který přijme. Základním pravidlem je, že neúčast kteréhokoli společného správce na zasedání této pracovní skupiny, které bylo oznámeno alespoň sedm (7) dní před písemným svoláním, znamená tichý souhlas s výstupy tohoto zasedání pracovní skupiny. Kterýkoli ze společných správců smí svolat zasedání této pracovní skupiny.

6) Pokyny se zpracovateli zasílají prostřednictvím kontaktního místa kteréhokoliv společného správce, a to na základě dohody s ostatními společnými správci a v souladu s rozhodovacím procesem pracovní skupiny popsaným výše v bodě 5. Společný správce, který pokyn předává, by jej měl zpracovateli předat písemně a informovat o tom všechny ostatní společné správce. Je-li záležitost natolik neodkladná, že nelze uspořádat zasedání pracovní skupiny, jak uvádí bod 5 výše, může být pokyn přesto předán, ale pracovní skupina jej může zrušit. Tento pokyn by měl být předán písemně a všichni ostatní společní správci by o tom měli být v době předání pokynu informováni.

7) Zřízení pracovní skupiny podle bodu 5 neupírá žádnému ze společných správců individuální kompetenci učinit ohlášení příslušnému dozorovému úřadu podle článků 33 a 24 obecného nařízení o ochraně osobních údajů. K takovému ohlášení se nevyžaduje souhlas žádného z dalších společných správců.

8) V oblasti působnosti brány rámce pro důvěryhodnost mají k vyměňovaným osobním údajům přístup pouze osoby oprávněné příslušnými vnitrostátními orgány nebo úřady.

9) Každý vydávající orgán vede záznamy o činnostech zpracování spadajících do jeho odpovědnosti. Společná správa může být v záznamech uvedena.

Pododdíl 2

Odpovědnosti a role při vyřizování žádostí subjektů údajů a jejich informování

1) Kromě případů, kdy je to nemožné nebo kdy by s tím bylo spojeno neúměrné úsilí, poskytne každý správce ve své roli vydávajícího orgánu fyzickým osobám, jejichž certifikát(y) zneplatnil (dále jen „subjekty údajů“), informaci o uvedeném zneplatnění a o zpracování jejich osobních údajů v rámci brány pro digitální certifikát EU COVID za účelem podpory výměny seznamů zneplatněných certifikátů v souladu s článkem 14 obecného nařízení o ochraně osobních údajů.

2) Každý správce vystupuje vůči fyzickým osobám, jejichž certifikáty zneplatnil, jako kontaktní místo a vyřizuje žádosti podané subjekty údajů nebo jejich zástupci v rámci výkonu jejich práv v souladu s obecným nařízením o ochraně osobních údajů. Pokud společný správce obdrží od subjektu údajů žádost týkající se certifikátu vydaného jiným společným správcem, oznámí subjektu údajů totožnost a kontaktní údaje odpovědného společného správce. Na žádost jiného společného správce si společní správci poskytují vzájemnou součinnost při vyřizování žádostí subjektů údajů a vzájemně si odpovídají neprodleně, nejpozději však do jednoho měsíce od obdržení žádosti o součinnost. Týká-li se žádost údajů poskytnutých třetí zemí, pak správce, který takovou žádost obdrží, tuto žádost zpracuje a informuje subjekt údajů o totožnosti a kontaktních údajích vydávajícího orgánu v dané třetí zemi.

3) Každý správce údajů zpřístupní subjektům údajů obsah této přílohy včetně ujednání stanovených v bodech 1 a 2.

ODDÍL 2

Řízení bezpečnostních incidentů včetně porušení zabezpečení osobních údajů

1) Společní správci si vzájemně poskytují součinnost při identifikaci a řešení všech bezpečnostních incidentů, včetně porušení zabezpečení osobních údajů, které souvisejí se zpracováním údajů v rámci brány pro digitální certifikát EU COVID.

2) Společní správci se zejména vzájemně informují o:

   a) všech potenciálních nebo skutečných rizicích pro dostupnost, důvěrnost nebo integritu osobních údajů zpracovávaných prostřednictvím brány rámce pro důvěryhodnost;

   b) každém porušení zabezpečení osobních údajů, pravděpodobných důsledcích porušení zabezpečení osobních údajů a posouzení rizika pro práva a svobody fyzických osob, jakož i o všech opatřeních učiněných k vyřešení porušení zabezpečení osobních údajů a zmírnění rizika pro práva a svobody fyzických osob;

   c) každém narušení technických nebo organizačních ochranných opatření, pokud jde o operaci zpracování údajů prostřednictvím brány rámce pro důvěryhodnost.

3) Společní správci oznámí veškerá porušení zabezpečení osobních údajů související s operací zpracování prostřednictvím brány rámce pro důvěryhodnost Komisi, příslušným dozorovým úřadům, a jsou-li povinni tak učinit, také subjektům údajů, a to v souladu s články 33 a 34 obecného nařízení o ochraně osobních údajů nebo po oznámení Komise.

4) Každý vydávající orgán zavede vhodná technická a organizační opatření, která mají za cíl:

   a) zajistit a chránit dostupnost, integritu a důvěrnost společně zpracovávaných osobních údajů;

   b) chránit osobní údaje v jeho držení před jakýmkoliv neoprávněným nebo nezákonným zpracováním, ztrátou, použitím, sdělením, získáním nebo přístupem;

   c) zajistit, aby přístup k osobním údajům nebyl sdělen nebo umožněn nikomu jinému než příjemcům nebo zpracovatelům.

ODDÍL 3

Posouzení vlivu na ochranu osobních údajů

1) Pokud správce ke splnění svých povinností stanovených v článku 35 a 36 nařízení (EU) 2016/679 potřebuje informace od jiného správce, zašle zvláštní žádost do dedikované e-mailové schránky uvedené v oddíle 1 pododdíle 1 bodě 4. Dožádaný správce vynaloží veškeré úsilí, aby tyto informace poskytl.“

PŘÍLOHA IV

„PŘÍLOHA VII

ODPOVĚDNOSTI KOMISE JAKOŽTO ZPRACOVATELE ÚDAJŮ, POKUD JDE O BRÁNU PRO DIGITÁLNÍ CERTIFIKÁT EU COVID A PODPORU VÝMĚNY SEZNAMŮ ZNEPLATNĚNÝCH CERTIFIKÁTŮ EU COVID

Komise:

1) vytvoří a zajistí pro členské státy bezpečnou a spolehlivou komunikační infrastrukturu, která podporuje výměnu seznamů zneplatněných certifikátů předávaných bráně pro digitální certifikát EU COVID;

2) v zájmu plnění svých povinností zpracovatele údajů v souvislosti s bránou rámce pro důvěryhodnost pro členské státy může využít třetí strany jako dílčí zpracovatele; Komise uvědomí společné správce o veškerých zamýšlených změnách týkajících se přidání nebo nahrazení dílčího zpracovatele, což správcům umožňuje proti takovým změnám společně vznést námitku. Komise zajistí, aby se na tyto dílčí zpracovatele vztahovaly stejné povinnosti v oblasti ochrany údajů, jaké jsou stanoveny v tomto rozhodnutí;

3) zpracovává osobní údaje pouze na základě zadokumentovaných pokynů od správců, ledaže to vyžaduje právo Unie nebo členského státu; v takovém případě Komise společné správce informuje o tomto právním požadavku před provedením činnosti zpracování, ledaže by uvedené právo předložení těchto informací zakazovalo z důležitých důvodů veřejného zájmu.

   Zpracování ze strany Komise zahrnuje:

   a) autentizaci vnitrostátních backendových serverů na základě certifikátů vnitrostátních backendových serverů;

   b) příjem údajů uvedených v čl. 5a odst. 3 rozhodnutí nahraných vnitrostátními backendovými servery, a to poskytnutím aplikačního programového rozhraní, které bude nahrávání příslušných údajů vnitrostátním backendovým serverům umožňovat;

   c) ukládání údajů v bráně pro digitální certifikát EU COVID;

   d) zpřístupňování údajů ke stažení vnitrostátními backendovými servery;

   e) mazání údajů k datu skončení jejich platnosti nebo na základě pokynu správce, který tyto údaje předal;

   f) po ukončení poskytování služby vymazání všech zbývajících údajů, pokud právo Unie nebo členského státu nepožaduje uchovávání osobních údajů;

4) přijme všechna nejmodernější organizační, fyzická a logická bezpečnostní opatření pro údržbu brány pro digitální certifikát EU COVID. Za tímto účelem Komise:

   a) určí subjekt odpovědný za řízení zabezpečení na úrovni brány digitálního certifikátu EU COVID, oznámí společným správcům jeho kontaktní údaje a zajistí jeho dostupnost pro reakci na bezpečnostní hrozby;

   b) převezme odpovědnost za zabezpečení brány pro digitální certifikát EU COVID, včetně pravidelného testování, hodnocení a posuzování bezpečnostních opatření;

   c) zajistí, aby se na všechny osoby, kterým je udělen přístup k bráně pro digitální certifikát EU COVID, vztahovala smluvní, profesní nebo zákonná povinnost zachování důvěrnosti;

5) přijme veškerá nezbytná bezpečnostní opatření, aby nedošlo k ohrožení řádného fungování vnitrostátních backendových serverů. Za tímto účelem Komise zavede zvláštní postupy týkající se připojování backendových serverů k bráně pro digitální certifikát EU COVID. To zahrnuje:

   a) postup posouzení rizik s cílem identifikovat a odhadnout potenciální hrozby pro systém;

   b) audit a přezkum s cílem:

      i) zkontrolovat soulad mezi zavedenými bezpečnostními opatřeními a použitelnou bezpečnostní politikou;

      ii) pravidelně kontrolovat integritu systémových souborů, bezpečnostní parametry a udělená oprávnění;

iii) monitorovat případy narušení bezpečnosti a neoprávněného vniknutí;

iv) provést změny, aby se zmírnily stávající nedostatky v zabezpečení;

v) vymezit podmínky, za nichž lze povolit provádění nezávislých auditů, též na žádost správců, a přispět k nim, včetně inspekcí, a přezkumů bezpečnostních opatření, a to za podmínek respektujících Protokol (č. 7) o výsadách a imunitách Evropské unie připojený ke Smlouvě o fungování Evropské unie;

c) změny postupu řízení s cílem zdokumentovat a měřit dopad určité změny před jejím provedením a průběžné informování společných správců o všech změnách, které mohou ovlivnit komunikaci s jejich infrastrukturami nebo jejich zabezpečení;

d) stanovení postupu pro údržbu a opravy, ve kterém budou stanovena pravidla a podmínky, jež musí být dodržovány při případné údržbě nebo opravách zařízení;

e) stanovení postupu pro bezpečnostní incidenty, ve kterém bude definován postup pro hlášení a eskalaci, neprodlené informování dotčených správců, neprodlené informování správců, aby mohli dále informovat příslušné vnitrostátní dozorové orgány pro ochranu údajů o jakémkoliv porušení zabezpečení osobních údajů, a definování disciplinárního postupu pro řešení porušení zabezpečení;

6) přijme nejmodernější fyzická nebo logická bezpečnostní opatření pro zařízení, kde je umístěno zařízení brány pro digitální certifikát EU COVID, a opatření pro kontrolu logického přístupu k datům a zabezpečení. Za tímto účelem Komise:

a) vynucuje fyzickou bezpečnost s cílem vytvořit rozlišená bezpečnostní pásma a umožnit odhalování případů narušení;

b) kontroluje přístup do zařízení a vede registr návštěvníků pro účely sledování;

c) zajistí, aby externí osoby, jimž byl udělen přístup do prostor, byly doprovázeny řádně pověřenými pracovníky;

d) zajistí, aby zařízení nebylo možné přidat, nahradit nebo odstranit bez předchozího povolení určených odpovědných orgánů;

e) kontroluje přístup z vnitrostátních backendových serverů do brány rámce pro důvěryhodnost a opačně;

f) zajistí, aby osoby, které přistupují k bráně pro digitální certifikát EU COVID, byly identifikovány a autentizovány;

g) přezkoumá oprávnění související s přístupem k bráně pro digitální certifikát EU COVID v případě narušení bezpečnosti s dopadem na tuto infrastrukturu;

h) zajistí zachování integrity informací přenášených prostřednictvím brány pro digitální certifikát EU COVID;

i) zavede technická a organizační bezpečnostní opatření, která zabrání neoprávněnému přístupu k osobním údajům;

j) podle potřeby zajistí implementaci opatření směřujících k zablokování neoprávněného přístupu k bráně pro digitální certifikát EU COVID z domény vydávajících orgánů (např. blokaci podle lokality/IP adresy);

7) podnikne kroky k ochraně své domény, včetně přerušení připojení, v případě závažného odchýlení od zásad a koncepcí v oblasti kvality nebo bezpečnosti;

8) spravuje plán řízení rizik v oblasti své působnosti;

9) monitoruje – v reálném čase – výkonnost všech složek služby v rámci svých služeb brány rámce pro důvěryhodnost, vypracovává pravidelné statistiky a vede záznamy;

10) poskytuje nepřetržitou podporu v angličtině pro všechny služby brány rámce pro důvěryhodnost prostřednictvím telefonu, e-mailu nebo webového portálu a přijímá hovory od oprávněných volajících, jimiž jsou: koordinátoři brány pro digitální certifikát EU COVID a jejich příslušné asistenční služby, projektoví pracovníci a pověřené osoby Komise;

11) pomáhá společným správcům formou vhodných technických a organizačních opatření, pokud je to možné v souladu s článkem 12 nařízení (EU) 2018/1725, při plnění povinnosti správců reagovat na žádosti o výkon práv subjektu údajů, jak jsou stanovena v kapitole III obecného nařízení o ochraně osobních údajů;

12) podporuje společné správce poskytováním informací o bráně pro digitální certifikát EU COVID za účelem plnění povinností podle článků 32, 33, 34, 35 a 36 obecného nařízení o ochraně osobních údajů;

13) zajišťuje, aby údaje zpracovávané v rámci brány pro digitální certifikát EU COVID byly nečitelné pro všechny osoby, které nejsou oprávněny k nim přistupovat;

14) přijme veškerá příslušná opatření, která zabrání tomu, aby obsluha brány pro digitální certifikát EU COVID měla neoprávněný přístup k předávaným údajům;

15) přijme opatření k usnadnění interoperability a komunikace mezi určenými správci brány pro digitální certifikát EU COVID;

16) vede záznamy o činnostech zpracování prováděných za společné správce v souladu s čl. 31 odst. 2 nařízení (EU) 2018/1725.“