

II

(Nelegislativní akty)

ROZHODNUTÍ

PROVÁDĚCÍ ROZHODNUTÍ KOMISE (EU) 2020/1023

ze dne 15. července 2020,

kterým se mění prováděcí rozhodnutí (EU) 2019/1765, pokud jde o přeshraniční výměnu údajů mezi vnitrostátními mobilními aplikacemi pro vysledování kontaktů a varování s ohledem na boj proti pandemii COVID-19

(Text s významem pro EHP)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na směrnici Evropského parlamentu a Rady 2011/24/EU ze dne 9. března 2011 o uplatňování práv pacientů v přeshraniční zdravotní péči ⁽¹⁾, a zejména na čl. 14 odst. 3 uvedené směrnice,

vzhledem k těmto důvodům:

- (1) Podle článku 14 směrnice 2011/24/EU má Unie podporovat a usnadňovat spolupráci a výměnu informací mezi členskými státy, které působí v rámci dobrovolné sítě spojující vnitrostátní orgány odpovědné za elektronické zdravotnictví, jež určily členské státy (dále jen „sít pro elektronické zdravotnictví“).
- (2) Prováděcí rozhodnutí Komise (EU) 2019/1765 ⁽²⁾ stanoví pravidla pro zřízení, řízení a fungování sítě vnitrostátních orgánů odpovědných za elektronické zdravotnictví. Podle článku 4 uvedeného rozhodnutí je síti pro elektronické zdravotnictví svěřen úkol usnadňovat větší interoperabilitu vnitrostátních systémů informačních a komunikačních technologií a přeshraniční přenositelnost elektronických zdravotních údajů v oblasti přeshraniční zdravotní péče.
- (3) Vzhledem ke krizi v oblasti veřejného zdraví způsobené pandemií COVID-19 vyvinulo několik členských států mobilní aplikace, které podporují vysledování kontaktů a umožňují upozorňovat uživatele těchto aplikací, aby přijali vhodná opatření, jako je testování nebo samoizolace, jestliže byli potenciálně vystaveni viru, protože se nacházeli v blízkosti jiného uživatele těchto aplikací, který nahlásil pozitivní diagnózu. Tyto aplikace využívají technologii Bluetooth ke zjištění blízkosti mezi zařízeními. Protože byla omezení cestování mezi členskými státy od června 2020 zrušena, mělo by být dosaženo větší interoperability vnitrostátních systémů informačních a komunikačních technologií mezi členskými státy v síti pro elektronické zdravotnictví zavedením digitální infrastruktury umožňující interoperabilitu mezi vnitrostátními mobilními aplikacemi, které podporují vysledování kontaktů a varování.

⁽¹⁾ Úř. věst. L 88, 4.4.2011, s. 45.

⁽²⁾ Prováděcí rozhodnutí Komise (EU) 2019/1765 ze dne 22. října 2019, kterým se stanoví pravidla pro zřízení, řízení a fungování sítě vnitrostátních orgánů odpovědných za elektronické zdravotnictví a zrušuje prováděcí rozhodnutí 2011/890/EU (Úř. věst. L 270, 24.10.2019, s. 83).

- (4) Komise podporuje členské státy, pokud jde o výše uvedené mobilní aplikace. Komise dne 8. dubna 2020 přijala doporučení o společné sadě nástrojů Unie pro využití technologií a dat k boji proti krizi COVID-19 a ukončování souvisejících mimořádných opatření, zejména pokud jde o mobilní aplikace a využívání anonymizovaných dat o mobilitě (dále jen „doporučení Komise“) ⁽³⁾. Členské státy v síti pro elektronické zdravotnictví přijaly za podpory Komise společnou sadu nástrojů EU pro členské státy pro mobilní aplikace na podporu vysledování kontaktů ⁽⁴⁾, jakož i pokyny pro interoperabilitu pro schválené mobilní aplikace pro vysledování kontaktů v EU ⁽⁵⁾. Tato sada nástrojů vysvětluje vnitrostátní požadavky na vnitrostátní mobilní aplikace pro vysledování kontaktů a varování, a zejména skutečnost, že by měly být dobrovolné, schválené příslušným vnitrostátním zdravotnickým orgánem, měly by zachovávat soukromí a měly by být odstraněny, jakmile již nebudou potřebné. Po nejnovějším vývoji krize COVID-19 vydaly Komise ⁽⁶⁾ a Evropský sbor pro ochranu údajů ⁽⁷⁾ pokyny k mobilním aplikacím a nástrojům pro vysledování kontaktů v souvislosti s ochranou osobních údajů. Návrh mobilních aplikací členských států a digitální infrastruktury umožňující jejich interoperabilitu vychází ze společné sady nástrojů EU, výše uvedených pokynů a technických specifikací dohodnutých v rámci sítě pro elektronické zdravotnictví.
- (5) Aby se usnadnila interoperabilita vnitrostátních mobilních aplikací pro vysledování kontaktů a varování, vyvinuly členské státy účastníci se sítě pro elektronické zdravotnictví, které se rozhodly dobrovolně rozšířit svou spolupráci v této oblasti, za podpory Komise digitální infrastrukturu, a to jako nástroj IT pro výměnu údajů. Tato digitální infrastruktura se nazývá „federační brána“.
- (6) V tomto rozhodnutí jsou uvedena ustanovení o roli zúčastněných členských států a Komise při fungování federační brány pro přeshraniční interoperabilitu vnitrostátních mobilních aplikací pro vysledování kontaktů a varování.
- (7) Zpracování osobních údajů uživatelů mobilních aplikací pro vysledování kontaktů a varování, 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 ⁽⁸⁾ („obecné nařízení o ochraně osobních údajů“) a směrnicí Evropského parlamentu a Rady 2002/58/ES ⁽⁹⁾. Zpracování osobních údajů, za něž je odpovědná Komise, pro účely řízení a zajištění bezpečnosti federační brány by mělo být prováděno v souladu s nařízením Evropského parlamentu a Rady (EU) 2018/1725 ⁽¹⁰⁾.
- (8) Federační brána by měla sestávat ze zabezpečené IT infrastruktury zajišťující společné rozhraní, kde si mohou určené vnitrostátní orgány nebo úřady vyměňovat minimální soubory údajů týkající se kontaktů s osobami infikovanými virem SARS-CoV-2, aby informovaly ostatní o jejich potenciálním vystavení této nákaze a podpořily účinnou spolupráci mezi členskými státy ve zdravotní péči usnadněním výměny příslušných informací.
- (9) Toto rozhodnutí by proto mělo stanovit způsoby přeshraniční výměny údajů mezi určenými vnitrostátními orgány nebo úřady prostřednictvím federační brány v rámci EU.

⁽³⁾ Doporučení Komise (EU) 2020/518 ze dne 8. dubna 2020 o společné sadě nástrojů Unie pro využití technologií a dat k boji proti krizi COVID-19 a ukončování souvisejících mimořádných opatření, zejména pokud jde o mobilní aplikace a využívání anonymizovaných dat o mobilitě (Úř. věst. L 114, 14.4.2020, s. 7).

⁽⁴⁾ https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

⁽⁵⁾ https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf

⁽⁶⁾ Sdělení Komise Pokyny k aplikacím podporujícím boj proti pandemii COVID-19 ve vztahu k ochraně údajů (Úř. věst. C 124 I, 17.4.2020, s. 1).

⁽⁷⁾ Pokyny 04/2020 k používání lokalizačních údajů a nástrojů k vysledování kontaktů v souvislosti s rozšířením onemocnění COVID-19 a prohlášení EDPB ze dne 16. června 2020 o dopadu interoperability aplikací pro vysledování kontaktů na ochranu osobních údajů, obojí k dispozici na <https://edpb.europa.eu>

⁽⁸⁾ 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).

⁽⁹⁾ Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích) (Úř. věst. L 201, 31.7.2002, s. 37).

⁽¹⁰⁾ 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).

- (10) Zúčastněné členské státy, zastoupené určenými vnitrostátními orgány nebo úřady, společně stanoví účel a prostředky zpracování osobních údajů prostřednictvím federální brány, a jsou tudíž společnými správci těchto údajů. Článek 26 obecného nařízení o ochraně osobních údajů stanoví povinnost společných správců operací zpracování osobních údajů určit transparentním způsobem své podíly na odpovědnosti za plnění povinností podle tohoto nařízení. Rovněž stanoví možnost, aby jejich podíl na odpovědnosti vymezilo právo Unie nebo členského státu, které se na správce vztahuje. Každý ze správců by měl zajistit, aby měl na vnitrostátní úrovni právní základ pro zpracování ve federální bráně.
- (11) Komise jako poskytovatel technických a organizačních řešení pro federální bránu zpracovává pseudonymizované osobní údaje jménem zúčastněných členských států ve federální bráně jako společných správců, a je tedy zpracovatelem. Podle článku 28 obecného nařízení o ochraně osobních údajů a článku 29 nařízení (EU) 2018/1725 se zpracování zpracovatelem řídí smlouvou nebo právním aktem podle práva Unie nebo členského státu, které zavazují zpracovatele vůči správci a které zpracování vymezují. Toto rozhodnutí stanoví pravidla pro zpracovávání údajů ze strany Komise jako zpracovatele.
- (12) Při zpracování osobních údajů v rámci federální brány je Komise vázána rozhodnutím Komise (EU, Euratom) 2017/46 ⁽¹⁾.
- (13) Vzhledem k tomu, že účely, pro které správci zpracovávají osobní údaje ve vnitrostátních mobilních aplikacích pro vysledování kontaktů a varování, nutně nevyžadují identifikaci subjektu údajů, nemusí mít správce vždy možnost zajistit uplatnění práv subjektů údajů. Práva podle článků 15 až 20 obecného nařízení o ochraně osobních údajů se proto nemusí uplatnit, když jsou splněny podmínky podle článku 11 uvedeného nařízení.
- (14) Stávající přílohu prováděcího rozhodnutí (EU) 2019/1765 je vzhledem k přidání dvou nových příloh nutno přechýšlovat.
- (15) Prováděcí rozhodnutí (EU) 2019/1765 by proto mělo být odpovídajícím způsobem změněno.
- (16) Vzhledem k naléhavosti situace vyvolané pandemií COVID-19 by toto rozhodnutí mělo platit od prvního dne po vyhlášení v Úředním věstníku Evropské unie.
- (17) V souladu s čl. 42 odst. 1 nařízení (EU) 2018/1725 byl konzultován evropský inspektor ochrany údajů, který vydal stanovisko dne 9. července 2020.
- (18) Opatření stanovená tímto rozhodnutím jsou v souladu se stanoviskem výboru zřízeného podle článku 16 směrnice 2011/24/EU,

PŘIJALA TOTO ROZHODNUTÍ:

Článek 1

Prováděcí rozhodnutí (EU) 2019/1765 se mění takto:

1) V čl. 2 odst. 1 se doplňují písmena g), h), i), j), k), l), m), n) a o), která znějí:

- „g) „uživatelé aplikace“ osoba vlastníci inteligentní zařízení, která si stáhla a má spuštěnou schválenou mobilní aplikaci pro vysledování kontaktů a varování;
- h) „vysledování kontaktů“ opatření provedená pro vysledování osob, které byly vystaveny zdroji vážné přeshraniční zdravotní hrozby ve smyslu čl. 3 písm. c) rozhodnutí Evropského parlamentu a Rady č. 1082/2013/EU (*);

⁽¹⁾ Rozhodnutí Komise (EU, Euratom) 2017/46 ze dne 10. ledna 2017 o bezpečnosti komunikačních a informačních systémů v Evropské komisi (Úř. věst. L 6, 11.1.2017, s. 40). Komise zveřejňuje další informace o bezpečnostních standardech vztahujících se na všechny informační systémy Evropské komise na https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_cs

- i) „vnitrostátní mobilní aplikací pro vysledování kontaktů a varování“ softwarová aplikace schválená na vnitrostátní úrovni, která běží na inteligentních zařízeních, zejména chytrých telefonech, které jsou obvykle navrženy k rozsáhlé a cílené interakci s webovými zdroji, která zpracovává data o vzájemném přiblížení a další kontextuální informace shromážděné pomocí mnoha senzorů nalézajících se v inteligentních zařízeních za účelem vysledování kontaktů s osobami nakaženými virem SARS-CoV-2 a varování osob, které mohly být viru SARS-CoV-2 vystaveny. Tyto mobilní aplikace jsou schopny zjistit přítomnost jiných zařízení používajících Bluetooth a vyměňovat si informace s backendovými servery s využitím internetu;
- j) „federální branou“ síťová brána provozovaná Komisí prostřednictvím zabezpečeného IT nástroje, která přijímá, ukládá a zpřístupňuje minimální soubory osobních údajů mezi backendovými servery členských států za účelem zajištění interoperability vnitrostátních mobilních aplikací pro vysledování kontaktů a varování;
- k) „klíčem“ jedinečný dočasný identifikátor uživatelů aplikace, kteří hlásí, že byli nakaženi virem SARS-CoV-2 nebo mohli být viru SARS-CoV-2 vystaveni;
- l) „ověřením nákazy“ metoda použitá pro potvrzení nákazy virem SARS-CoV-2, zejména zda šlo o vlastní hlášení uživatele aplikace nebo zda byla nákaza potvrzena vnitrostátním zdravotnickým orgánem nebo laboratorním testem;
- m) „zeměmi zájmu“ členský stát nebo členské státy, v nichž uživatel aplikace pobýval v průběhu 14 dní před datem odeslání klíčů a v nichž si stáhl schválenou vnitrostátní mobilní aplikaci pro vysledování kontaktů a varování, anebo do nichž cestoval;
- n) „zemí původu klíčů“ členský stát, kde se nachází backendový server, který odeslal klíče do federální brány;
- o) „údaji z protokolů“ automatické záznamy aktivity v souvislosti s výměnou údajů a přístupem k údajům zpracovaným prostřednictvím federální brány, které uvádějí zejména druh činnosti zpracování, datum a čas činnosti zpracování a identifikátor osoby zpracovávající údaje.

(*) Rozhodnutí Evropského parlamentu a Rady č. 1082/2013/EU ze dne 22. října 2013 o vážných přeshraničních zdravotních hrozbách a o zrušení rozhodnutí č. 2119/98/ES (Úř. věst. L 293, 5.11.2013, s. 1).“

2) V čl. 4 odst. 1 se doplňuje nové písmeno h), které zní:

„h) poskytovat členským státům pokyny ohledně přeshraniční výměny osobních údajů přes federální bránu mezi vnitrostátními mobilními aplikacemi pro vysledování kontaktů a varování.“

3) V čl. 6 odst. 1 se doplňují písmena f) a g), která znějí:

„f) vyvíjí, zavádí a zachovává vhodná technická a organizační opatření související s bezpečností přenosu a hostováním osobních údajů ve federální bráně za účelem zajištění interoperability vnitrostátních mobilních aplikací pro vysledování kontaktů a varování;

g) podporuje síť pro elektronické zdravotnictví při schvalování technického a organizačního souladu vnitrostátních orgánů s požadavky na přeshraniční výměnu osobních údajů ve federální bráně tím, že poskytuje a provádí nezbytné testy a audity. Auditorům Komise mohou být nápomocni odborníci z členských států.“

4) Článek 7 se mění takto:

a) název se nahrazuje tímto: „Ochrana osobních údajů zpracovávaných prostřednictvím infrastruktury digitálních služeb pro elektronické zdravotnictví“;

b) v odstavci 2 se slovo „příloha“ nahrazuje slovy „příloha I“.

- 5) Vkládá se nový článek 7a, který zní:

„Článek 7a

Přeshraniční výměna údajů mezi vnitrostátními mobilními aplikacemi pro vysledování a varování přes federační bránu

1. Pokud se osobní údaje vyměňují přes federační bránu, zpracování se omezí na účely usnadnění interoperability vnitrostátních mobilních aplikací pro vysledování kontaktů a varování v rámci federační brány a kontinuitu vysledování kontaktů v přeshraničním kontextu.
 2. Osobní údaje uvedené v odstavci 3 se přenášejí do federační brány v pseudonymizovaném formátu.
 3. Pseudonymizované osobní údaje vyměňované přes federační bránu a zpracovávané ve federační bráně zahrnují pouze tyto informace:
 - a) klíče přenášené vnitrostátními mobilními aplikacemi pro vysledování kontaktů a varování do 14 dnů před datem odeslání klíčů;
 - b) údaje z protokolů související s klíči v souladu s protokolem technických specifikací používaným v zemi původu klíčů;
 - c) ověření náказы;
 - d) země zájmu a zemi původu klíčů.
 4. Určené vnitrostátní orgány nebo úřady zpracovávající osobní údaje ve federační bráně jsou společnými správci údajů zpracovávaných ve federační bráně. Příslušné odpovědnosti společných správců jsou rozděleny v souladu s přílohou II. Každý členský stát, který má zájem o účast v přeshraniční výměně údajů mezi vnitrostátními mobilními aplikacemi pro vysledování kontaktů a varování, uvědomí předem Komisi o svém záměru a uvede vnitrostátní orgán nebo úřad, který určil jako odpovědného správce.
 5. Komise je zpracovatelem osobních údajů zpracovávaných v rámci federační brány. Jako zpracovatel zajistí Komise bezpečnost zpracování, včetně přenosu a hostování osobních údajů, ve federační bráně a plní povinnosti zpracovatele stanovené v příloze III.
 6. Komise a vnitrostátní orgány s oprávněním k přístupu do federační brány pravidelně testují, posuzují a hodnotí účinnost technických a organizačních opatření pro zajištění bezpečnosti zpracování osobních údajů ve federační bráně.
 7. Aniž je dotčeno rozhodnutí společných správců ukončit zpracování ve federační bráně, provoz federační brány se deaktivuje nejpozději 14 dnů poté, co všechny připojené vnitrostátní mobilní aplikace pro vysledování kontaktů a varování přestanou zasílat klíče přes federační bránu.“
- 6) Dosavadní příloha se označuje jako příloha I.
- 7) Doplnuje se příloha II a III ve znění uvedeném v příloze tohoto rozhodnutí.

Článek 2

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

V Bruselu dne 15. července 2020.

Za Komisi
Ursula VON DER LEYEN
předsedkyně

PŘÍLOHA

V prováděcím rozhodnutí (EU) 2019/1765 se doplňují přílohy II a III, které znějí:

„PŘÍLOHA II

**POVINNOSTI ZÚČASTNĚNÝCH ČLENSKÝCH STÁTŮ JAKO SPOLEČNÝCH SPRÁVCŮ FEDERAČNÍ BRÁNY
PRO ÚČELY PŘESHRANIČNÍHO ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ MEZI VNITROSTÁTNÍMI MOBILNÍMI
APLIKACEMI PRO VYSLEDOVÁNÍ KONTAKTŮ A VAROVÁNÍ**

ODDÍL 1

Pododdíl 1

Rozdělení povinností

- 1) Společní správci zpracovávají osobní údaje přes federační bránu v souladu s technickými specifikacemi stanovenými síti pro elektronické zdravotnictví ⁽¹⁾.
- 2) Každý správce je odpovědný za zpracování osobních údajů ve federační bráně v souladu s obecným nařízením o ochraně osobních údajů a směrnici 2002/58/ES.
- 3) Každý správce zřídí kontaktní místo s funkční e-mailovou schránkou, které bude sloužit pro komunikaci mezi společnými správci a mezi společnými správci a zpracovatelem.
- 4) Dočasná podskupina zřízená síti pro elektronické zdravotnictví podle čl. 5 odst. 4 bude mít za úkol zkoumat veškeré záležitosti vyplývající z interoperability vnitrostátních mobilních aplikací pro vysledování kontaktů a varování a ze společného správcovství souvisejícího zpracování osobních údajů a zprostředkovávat zaslání koordinovaných pokynů Komisi jako zpracovateli. Vedle jiných záležitostí mohou správci v rámci dočasné podskupiny pracovat na společném přístupu k uchovávání údajů v jejich vnitrostátních backendových serverech, s přihlédnutím k době uchovávání údajů stanovené pro federační bránu.
- 5) Pokyny zpracovateli zasílá kterékoli z kontaktních míst společných správců po dohodě s ostatními společnými správci v podskupině uvedené výše.
- 6) Přístup k osobním údajům uživatelů vyměňovaným ve federační bráně mohou mít pouze osoby pověřené určenými vnitrostátními orgány nebo úřady.
- 7) Každý určený vnitrostátní orgán nebo úřad přestává být společným správcem od data zrušení své účasti ve federační bráně. Zůstane však odpovědným za zpracování ve federační bráně, k němuž došlo před tímto zrušením.

Pododdíl 2

Povinnosti a role při vyřizování žádostí a informování subjektů údajů

- 1) Každý správce poskytne uživatelům své vnitrostátní mobilní aplikace pro vysledování kontaktů a varování („subjektům údajů“) informace o zpracování jejich osobních údajů ve federační bráně pro účely přeshraniční interoperability vnitrostátních mobilních aplikací pro vysledování kontaktů a varování v souladu s články 13 a 14 obecného nařízení o ochraně osobních údajů.
- 2) Každý správce funguje jako kontaktní místo pro uživatele své vnitrostátní mobilní aplikace pro vysledování kontaktů a varování a zpracovává žádosti týkající se výkonu práv subjektů údajů, které tyto uživatelé nebo jejich zástupci předložili, v souladu s obecným nařízením o ochraně osobních údajů. Každý správce určí zvláštní kontaktní místo vyhrazené pro žádosti obdržené od subjektů údajů. Jestliže společný správce obdrží žádost od subjektu údajů, která nespadá do jeho odpovědnosti, neprodleně ji předá odpovědnému společnému správci. Společní správci si na požádání poskytují vzájemnou součinnost při vyřizování žádostí subjektů údajů a vzájemně si odpovídají neprodleně, nejpozději však do 15 dní od obdržení žádosti o součinnost.

⁽¹⁾ Zejména specifikace interoperability pro přeshraniční přenosové řetězce mezi schválenými aplikacemi ze dne 16. června 2020, k dispozici na: https://ec.europa.eu/health/ehealth/key_documents_cs#anchor0

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

ODDÍL 2

Řízení bezpečnostních incidentů, včetně porušení ochrany osobních údajů

- 1) Společní správci si vzájemně poskytují součinnost při identifikaci a řešení všech bezpečnostních incidentů, včetně porušení ochrany osobních údajů, které souvisejí se zpracováním ve federační bráně.
- 2) Společní správci se zejména vzájemně informují o:
 - a) všech potenciálních nebo skutečných rizicích pro dostupnost, důvěrnost anebo integritu osobních údajů zpracovávaných ve federační bráně;
 - b) všech bezpečnostních incidentech, které souvisejí s operací zpracování ve federační bráně;
 - c) každém porušení ochrany osobních údajů, pravděpodobných důsledcích porušení ochrany osobních údajů a hodnocení rizika pro práva a svobody fyzických osob a o všech opatřeních učiněných k vyřešení porušení ochrany osobních údajů a zmírnění rizika pro práva a svobody fyzických osob;
 - d) každém narušení technických anebo organizačních ochranných opatření u operace zpracování ve federační bráně.
- 3) Společní správci informují o každém porušení ochrany osobních údajů v souvislosti s operací zpracování ve federační bráně Komisi, příslušné dozorové úřady a případně subjekty údajů, pokud je to požadováno, v souladu s článkem 33 a 34 nařízení (EU) 2016/679 nebo po oznámení Komise.

ODDÍL 3

Posouzení vlivu na ochranu osobních údajů

Jestliže správce potřebuje informace od jiného správce, aby splnil své povinnosti uvedené v člancích 35 a 36 obecného nařízení o ochraně osobních údajů, zašle konkrétní žádost do funkční e-mailové schránky uvedené v oddíle 1 pododdíle 1 bodě 3. Dožádaný správce vynaloží veškeré úsilí, aby tyto informace poskytl.

PŘÍLOHA III

POVINNOSTI KOMISE JAKO ZPRACOVATELE ÚDAJŮ FEDERAČNÍ BRÁNY PRO ÚČELY PŘESHRAŇNÍHO ZPRACOVÁNÍ MEZI VNITROSTÁTNÍMI MOBILNÍMI APLIKACEMI PRO VYSLEDOVÁNÍ KONTAKTŮ A VAROVÁNÍ

Komise:

- 1) Vytváří a zajišťuje bezpečnou a spolehlivou komunikační infrastrukturu, která propojuje vnitrostátní mobilní aplikace pro vysledování a varování členských států účastnících se federační brány. Za účelem splnění svých povinností jako zpracovatele údajů federační brány může Komise využívat služeb třetích stran jako dílčích zpracovatelů; Komise informuje společné správce o všech zamýšlených změnách týkajících se přijetí dalších dílčích zpracovatelů nebo jejich nahrazení, a poskytne tak správčům příležitost vyslovit vůči těmto změnám společně námitky, jak je uvedeno v příloze II oddílu 1 pododdílu 1 bodě 4. Komise zajistí, aby se na tyto dílčí zpracovatele vztahovaly stejné povinnosti v oblasti ochrany údajů, jaké jsou stanoveny v tomto rozhodnutí.
- 2) Zpracovává osobní údaje pouze na základě zadokumentovaných pokynů od správců, ledaže to vyžaduje právo Unie nebo členského státu; v takovém případě Komise správce informuje o tomto právním požadavku před zpracováním, ledaže by toto právo předložení těchto informací zakazovalo z důležitých důvodů veřejného zájmu.
- 3) Zpracování Komisí zahrnuje:
 - a) ověření vnitrostátních backendových serverů podle certifikátů vnitrostátních backendových serverů;
 - b) přijetí údajů uvedených v čl. 7a odst. 3 prováděcího rozhodnutí zaslaných vnitrostátními backendovými servery poskytnutím aplikačního programovacího rozhraní, které vnitrostátním backendovým serverům umožňuje zasílat příslušné údaje;
 - c) uložení těchto údajů ve federační bráně po jejich přijetí od vnitrostátních backendových serverů;
 - d) zpřístupnění údajů vnitrostátním backendovým serverům ke stažení;
 - e) vymazání údajů, jakmile si je stáhly všechny účastníci se backendové servery, nebo 14 dnů po jejich přijetí, podle toho, co nastane dříve;
 - f) po ukončení poskytování služby vymazání všech zbývajících údajů, pokud právo Unie nebo členského státu nepožaduje uložení osobních údajů.

Zpracovatel přijme nezbytná opatření k zachování integrity zpracovávaných údajů.

- 4) Přijme veškerá nejmodernější organizační, fyzická a logická bezpečnostní opatření pro údržbu federační brány. Za tímto účelem Komise:
 - a) určí subjekt odpovědný za řízení bezpečnosti na úrovni federační brány, sdělí správčům údajů jeho kontaktní údaje a zajistí jeho dostupnost pro reakci na bezpečnostní hrozby;
 - b) nese odpovědnost za bezpečnost federační brány;
 - c) zajistí, aby se na všechny osoby, kterým je udělen přístup do federační brány, vztahovala smluvní, profesionální nebo zákonná povinnost zachování důvěrnosti.
- 5) Přijme veškerá nezbytná bezpečnostní opatření, aby nedošlo k ohrožení řádného fungování vnitrostátních backendových serverů. Za tímto účelem zavede Komise zvláštní postupy týkající se připojení backendových serverů k federační bráně. To zahrnuje:
 - a) postup posuzování rizik za účelem určení a odhadu možných hrozeb pro systém;
 - b) audit a přezkum s cílem:
 - i. zkontrolovat soulad mezi zaváděnými bezpečnostními opatřeními a příslušnou bezpečnostní politikou;
 - ii. pravidelně kontrolovat integritu souborů systémů, bezpečnostní parametry a udělená oprávnění;
 - iii. monitorovat případy narušení bezpečnosti a neoprávněného vniknutí;
 - iv. provést změny, aby se zmírnily stávající nedostatky v zabezpečení;
 - v. povolit, a to i na žádost správců, provádění nezávislých auditů včetně inspekci a přezkumů bezpečnostních opatření a příspěk k němu, a to za podmínek, které jsou v souladu s Protokolem (č. 7) o výsadách a imunitách Evropské unie připojeným ke Smlouvě o fungování Evropské unie ⁽²⁾;

⁽²⁾ Protokol (č. 7) o výsadách a imunitách Evropské unie (Úř. věst. C 326, 26.10.2012, s. 266).

- c) změnu kontrolního postupu, pokud jde o dokumentaci a měření dopadu změny před jejím provedením, a informování správců o všech změnách, které mohou ovlivnit komunikaci s infrastrukturami anebo bezpečnost těchto infrastruktur;
 - d) stanovení postupu údržby a oprav za účelem stanovení pravidel a podmínek, jež je třeba dodržet, pokud by se měla provést údržba anebo oprava zařízení;
 - e) stanovení postupu pro bezpečnostní incidenty s cílem definovat postupy hlášení a eskalace, neprodleně informovat správce a evropského inspektora ochrany údajů o jakémkoli narušení bezpečnosti osobních údajů a stanovit disciplinární postup pro řešení narušení bezpečnosti.
 - 6) Přijme nejmodernější fyzická anebo logická bezpečnostní opatření pro zařízení, v nichž se nachází vybavení federační brány, a pro kontroly přístupu k logickým údajům a zabezpečení. Za tímto účelem Komise:
 - a) prosazuje fyzickou bezpečnost s cílem vytvořit rozlišená bezpečnostní pásma a umožnit odhalování případů porušení předpisů;
 - b) kontroluje přístup do zařízení a vede registr návštěvníků pro účely monitorování;
 - 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 a do vnitrostátních backendových serverů do federační brány;
 - f) zajistí, aby jednotlivci, kteří mají přístup k federační bráně, byli identifikováni a ověřeni;
 - g) přezkoumá přístupová práva související s přístupem do federační brány v případě narušení bezpečnosti, které má dopad na tuto infrastrukturu;
 - h) zachovává integritu informací předávaných přes federační bránu;
 - i) zavede technická a organizační bezpečnostní opatření, která zabrání neoprávněnému přístupu k osobním údajům;
 - j) v případě potřeby provede opatření s cílem zabránit neoprávněnému přístupu do federační brány z domény vnitrostátních orgánů (tj.: zablokuje určení polohy/IP adresu).
 - 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) Sleduje – v reálném čase – výkonnost všech složek služby v rámci svých služeb federační brány, vypracovává pravidelné statistiky a vede záznamy.
 - 10) Poskytuje nepřetržitou podporu všem službám federační brány v angličtině prostřednictvím telefonu, e-mailu nebo webového portálu a přijímá volání od oprávněných volajících, jimiž jsou: koordinátoři federační brány a jejich příslušné asistenční služby, projektoví referenti a osoby určené Komisí.
 - 11) Pomáhá správcům prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, 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 správce poskytováním informací o federační bráně za účelem plnění povinností podle článků 32, 35 a 36 obecného nařízení o ochraně osobních údajů.
 - 13) Zajišťuje, aby údaje zpracovávané ve federační bráně byly nesrozumitelné všem osobám, které nemají oprávnění přístupu k těmto údajům.
 - 14) Přijme veškerá příslušná opatření, která zabrání tomu, aby provozovatelé federační brány měli neoprávněný přístup k předávaným údajům.
 - 15) Přijme opatření s cílem usnadnit interoperabilitu a komunikaci mezi určenými správci federační brány.
 - 16) Vede záznamy o činnostech zpracování prováděných za správce podle čl. 31 odst. 2 nařízení (EU) 2018/1725.“
-