II

(Nelegislatívne akty)

ROZHODNUTIA

VYKONÁVACIE ROZHODNUTIE KOMISIE (EÚ) 2020/1023

z 15. júla 2020,

ktorým sa mení vykonávacie rozhodnutie (EÚ) 2019/1765, pokiaľ ide o cezhraničnú výmenu údajov medzi vnútroštátnymi mobilnými aplikáciami na vyhľadávanie kontaktov a varovanie v súvislosti s bojom proti pandémii COVID-19

(Text s významom pre EHP)

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na smernicu Európskeho parlamentu a Rady 2011/24/EÚ z 9. marca 2011 o uplatňovaní práv pacientov pri cezhraničnej zdravotnej starostlivosti ([1]), a najmä na jej článok 14 ods. 3,

keďže:

(1) V článku 14 smernice 2011/24/EÚ bola Únia poverená tým, aby podporovala a uľahčovala spoluprácu a výmenu informácií medzi členskými štátmi, ktoré spolupracujú v rámci dobrovoľnej siete spájajúcej členskými štátmi určené vnútroštátne orgány zodpovedné za elektronické zdravotníctvo (ďalej len „sieť elektronického zdravotníctva“).

(2) Vykonávacím rozhodnutím Komisie (EÚ) 2019/1765 ([2]) sa stanovujú pravidlá pre zriadenie, riadenie a fungovanie siete vnútroštátnych orgánov zodpovedných za elektronické zdravotníctvo. Článkom 4 uvedeného rozhodnutia sa sieť elektronického zdravotníctva poveruje úlohou umožniť väčšiu interoperabilitu vnútroštátnych systémov informačných a komunikačných technológií a cezhraničnú prenosnosť elektronických údajov týkajúcich sa zdravia pri cezhraničnej zdravotnej starostlivosti.

(3) V súvislosti s krízou v oblasti verejného zdravia spôsobenou pandémiou COVID-19 vytvorili viaceré členské štáty mobilné aplikácie, ktoré podporujú vyhľadávanie kontaktov a ich používateľom umožňujú dostávať upozornenia, aby prijali vhodné opatrenia, napríklad testovanie alebo samoizoláciu, ak boli potenciálne vystavení vírusu v blízkosti iného používateľa takýchto aplikácií, u ktorého bola táto diagnóza zistená Tieto aplikácie využívajú na detekciu blízkosti medzi zariadeniami technológiu Bluetooth. Keďže obmedzenia cestovania medzi členskými štátmi sa od júna 2020 uvoľňujú, mala by sa v rámci siete elektronického zdravotníctva dosiahnuť medzi členskými štátmi väčšia interoperabilita ich systémov informačných a komunikačných technológií, a to zavedením digitálnej infraštruktúry umožňujúcej interoperabilitu medzi vnútroštátnymi mobilnými aplikáciami podporujúcimi vyhľadávanie kontaktov a varovanie.

([1]) Ú. v. EÚ L 88, 4.4.2011, s. 45.

([2]) Vykonávacie rozhodnutie Komisie (EÚ) 2019/1765 z 22. októbra 2019, ktorým sa stanovujú pravidlá pre zriadenie, riadenie a fungovanie siete vnútroštátnych orgánov zodpovedných za elektronické zdravotníctvo a ktorým sa zrušuje vykonávacie rozhodnutie 2011/890/EÚ (Ú. v. EÚ L 270, 24.10.2019, s. 83).

(4) Komisia v súvislosti s uvedenými mobilnými aplikáciami členské štáty podporuje. Dňa 8. apríla 2020 prijala Odporúčanie o spoločnom súbore nástrojov Únie na využívanie technológií a údajov na boj proti kríze spôsobenej ochorením COVID-19 a jej prekonanie, najmä pokiaľ ide o mobilné aplikácie a využívanie anonymizovaných údajov o mobilite (ďalej len „odporúčanie“) ([3]). Členské štáty v sieti elektronického zdravotníctva prijali s podporou Komisie spoločný súbor nástrojov EÚ pre členské štáty týkajúci sa mobilných aplikácií na podporu vyhľadávania kontaktov ([4]), ako aj usmernenia pre interoperabilitu týkajúce sa schválených mobilných aplikácií na vyhľadávanie kontaktov v EÚ ([5]). V súbore nástrojov sa vysvetľujú vnútroštátne požiadavky na mobilné aplikácie na vyhľadávanie kontaktov a varovanie, najmä to, že by mali byť dobrovoľné, schválené príslušným vnútroštátnym zdravotníckym orgánom, mali by rešpektovať súkromie a byť odstránené hneď, ako prestanú byť potrebné. V nadväznosti na najnovší vývoj krízy spôsobenej ochorením COVID-19 vydali Komisia ([6]) a Európsky výbor pre ochranu údajov ([7]) usmernenia týkajúce sa mobilných aplikácií a nástrojov na vyhľadávanie kontaktov v súvislosti s ochranou údajov. Návrh mobilných aplikácií členských štátov a digitálnej infraštruktúry, ktorá umožní ich interoperabilitu, vychádza zo spoločného súboru nástrojov EÚ, z vyššie uvedených usmernení a technických špecifikácií, na ktorých sa dohodla sieť elektronického zdravotníctva.

(5) V záujme uľahčenia interoperability vnútroštátnych mobilných aplikácií na vyhľadávanie kontaktov a varovanie sa vytvorila digitálna infraštruktúra vo forme IT nástroja na výmenu údajov, o čo sa s podporou Komisie zaslúžili tie členské štáty zapojené do siete elektronického zdravotníctva, ktoré sa rozhodli prehĺbiť svoju spoluprácu v tejto oblasti na dobrovoľnom základe. Táto digitálna infraštruktúra sa označuje ako „federačná brána“ (z angl. „federation gateway“).

(6) Týmto rozhodnutím sa stanovujú ustanovenia o úlohe zapojených členských štátov a Komisie pri fungovaní federačnej brány pre cezhraničnú interoperabilitu vnútroštátnych mobilných aplikácií na vyhľadávanie kontaktov a varovanie.

(7) Spracovanie osobných údajov používateľov mobilných aplikácií na vyhľadávanie kontaktov a varovanie, za ktoré sú zodpovedné členské štáty alebo iné verejné organizácie alebo subjekty v členských štátoch, by sa malo vykonávať v súlade s nariadením Európskeho parlamentu a Rady (EÚ) 2016/679 ([8]) (všeobecným nariadením o ochrane údajov) a smernicou Európskeho parlamentu a Rady 2002/58/ES ([9]). Spracovanie osobných údajov na účely riadenia a zaistenia bezpečnosti federačnej brány, za ktoré je zodpovedná Komisia, by malo byť v súlade s nariadením Európskeho parlamentu a Rady (EÚ) 2018/1725 ([10]).

(8) Zriadenie federačnej brány by malo pozostávať zo zabezpečenej IT infraštruktúry poskytujúcej spoločné rozhranie, v rámci ktorého si určené vnútroštátne orgány resp. verejné subjekty môžu vymieňať minimálny súbor údajov, pokiaľ ide o kontakty s osobami nakazenými vírusom spôsobujúcim ochorenie COVID-19. Cieľom systému je informovať ostatných o možnom vystavení tejto nákaze a podporovať účinnú spoluprácu medzi členskými štátmi v oblasti zdravotnej starostlivosti prostredníctvom uľahčenia výmeny relevantných informácií.

(9) Týmto rozhodnutím by sa preto mali stanoviť spôsoby cezhraničnej výmeny údajov medzi určenými vnútroštátnymi orgánmi resp. verejnými subjektmi v rámci EÚ prostredníctvom federačnej brány.

([3]) Odporúčanie Komisie (EÚ) 2020/518 z 8. apríla 2020 o spoločnom súbore nástrojov Únie na využívanie technológií a údajov na boj proti kríze spôsobenej ochorením COVID-19 a jej prekonanie, najmä pokiaľ ide o mobilné aplikácie a využívanie anonymizovaných údajov o mobilite (Ú. v. EÚ 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]) Oznámenie Komisie – Usmernenie týkajúce sa aplikácií podporujúcich boj proti pandémii COVID-19 v súvislosti s ochranou údajov (Ú. v. EÚ C 124I, 17.4.2020, s. 1).

([7]) Usmernenia 4/2020 týkajúce sa lokalizačných údajov a nástrojov na vyhľadávanie kontaktov v kontexte pandémie COVID-19 a vyhlásenie EDPB zo 16. júna 2020 o vplyve interoperability aplikácií určených na vyhľadávanie kontaktov na ochranu osobných údajov, obidve dostupné na adrese: https://edpb.europa.eu.

([8]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1).

([9]) Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 31.7.2002, s. 37).

([10]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (Ú. v. EÚ L 295, 21.11.2018, s. 39).

(10) Členské štáty, ktoré sú zastúpené určenými vnútroštátnymi orgánmi alebo verejnými subjektmi, spoločne stanovia cieľ a spôsob spracúvania osobných údajov prostredníctvom federačnej brány, a preto sú spoločnými prevádzkovateľmi týchto údajov. V článku 26 všeobecného nariadenia o ochrane údajov sa stanovuje povinnosť spoločných prevádzkovateľov operácií spracúvania osobných údajov transparentne určiť ich príslušné zodpovednosti za plnenie povinností podľa uvedeného nariadenia. Zároveň sa v ňom uvádza, že ich zodpovednosť môže byť daná právom Únie alebo členského štátu, ktorému spoloční prevádzkovatelia podliehajú. Každý z prevádzkovateľov by mal zabezpečiť, aby mal na vnútroštátnej úrovni právny základ na spracúvanie údajov vo federačnej bráne.

(11) Komisia ako poskytovateľ technických a organizačných riešení federačnej brány spracúva pseudonymizované osobné údaje v mene členských štátov vo federačnej bráne ako spoločných prevádzkovateľov, a preto je sprostredkovateľom. V súlade s článkom 28 všeobecného nariadenia o ochrane údajov a článkom 29 nariadenia (EÚ) 2018/1725 sa spracúvanie sprostredkovateľom riadi zmluvou alebo iným právnym aktom podľa práva Únie alebo práva členského štátu, ktoré zaväzujú sprostredkovateľa voči prevádzkovateľovi a ktorými sa špecifikuje spracúvanie. Týmto rozhodnutím sa stanovujú pravidlá spracúvania, ktoré vykonáva Komisia ako sprostredkovateľ.

(12) Pri spracúvaní osobných údajov v rámci federačnej brány je Komisia viazaná svojím rozhodnutím (EÚ, Euratom) 2017/46 ([11]).

(13) Vzhľadom na to, že účely, na ktoré prevádzkovatelia spracúvajú osobné údaje vo vnútroštátnych mobilných aplikáciách na vyhľadávanie kontaktov a varovanie, si nemusia vyžadovať identifikáciu dotknutej osoby, prevádzkovatelia nemusia byť vždy schopní zabezpečiť uplatňovanie práv dotknutých osôb. Práva uvedené v článkoch 15 až 20 všeobecného nariadenia o ochrane údajov sa preto nemusia uplatňovať, ak sú splnené podmienky článku 11 uvedeného nariadenia.

(14) Súčasná príloha k vykonávaciemu rozhodnutiu (EÚ) 2019/1765 sa musí prečíslovať v dôsledku pridania dvoch nových príloh.

(15) Vykonávacie rozhodnutie (EÚ) 2019/1765 by sa preto malo zodpovedajúcim spôsobom zmeniť.

(16) Vzhľadom na naliehavosť situácie vyvolanej pandémiou COVID-19 by sa malo toto rozhodnutie začať uplatňovať dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie*.

(17) V súlade s článkom 42 ods. 1 nariadenia (EÚ) 2018/1725 sa uskutočnili konzultácie s európskym dozorným úradníkom pre ochranu údajov, ktorý vydal 9. júla 2020 stanovisko.

(18) Opatrenia stanovené v tomto rozhodnutí sú v súlade so stanoviskom výboru zriadeného v zmysle článku 16 smernice 2011/24/EÚ,

PRIJALA TOTO ROZHODNUTIE:

Článok 1

Vykonávacie rozhodnutie (EÚ) 2019/1765 sa mení takto:

1. V článku 2 ods. 1 sa vkladajú tieto písmená g), h), i), j), k), l), m), n) a o):

„g) „používateľ aplikácie“ je osoba vlastniaca inteligentné zariadenie, ktorá si stiahla a používa schválené mobilné aplikácie na vyhľadávanie kontaktov a varovanie;

h) „vyhľadávanie kontaktov“ sú opatrenia vykonávané s cieľom vystopovať osoby, ktoré boli vystavené pôsobeniu zdroja závažného cezhraničného ohrozenia zdravia v zmysle článku 3 písm. c) rozhodnutia Európskeho parlamentu a Rady č. 1082/2013/EÚ (*);

([11]) Rozhodnutie Komisie (EÚ, Euratom) 2017/46 z 10. januára 2017 o bezpečnosti komunikačných a informačných systémov v Európskej komisii (Ú. v. EÚ L 6, 11.1.2017, s. 40). Komisia uverejňuje ďalšie informácie o bezpečnostných normách, ktoré sa týkajú všetkých informačných systémoch, na adrese https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_en.

i) „mobilná aplikácia na vyhľadávanie kontaktov a varovanie“ je softvérová aplikácia schválená na vnútroštátnej úrovni, ktorá funguje na inteligentných zariadeniach, najmä smartfónoch, je určená na rozsiahlu a cielenú interakciu s webovými zdrojmi a spracúva údaje z bezprostrednej blízkosti a ďalšie kontextové informácie zhromaždené mnohými snímačmi, ktoré sa nachádzajú v inteligentných zariadeniach, na účely vyhľadávania kontaktov s osobami nakazenými vírusom spôsobujúcim ochorenie COVID-19 a varovania osôb, ktoré by mohli byť tomuto vírusu vystavené. Tieto mobilné aplikácie dokážu pomocou systému Bluetooth zistiť prítomnosť iných zariadení a vymieňať si informácie so zálohovými servermi pomocou internetu;

j) „federačná brána“ je sieťová brána prevádzkovaná Komisiou prostredníctvom zabezpečeného IT nástroja, ktorá prijíma, uchováva a sprístupňuje minimálny súbor osobných údajov medzi zálohovými servermi členských štátov na účely zabezpečenia interoperability vnútroštátnych mobilných aplikácií na sledovanie kontaktov a varovanie;

k) „kľúč“ je jedinečný efemérny identifikátor vzťahujúci sa na používateľov aplikácie, ktorí nahlasujú, že boli infikovaní vírusom spôsobujúcim ochorenie COVID-19 alebo mohli byť tomuto vírusu vystavení;

l) „overovanie infekcie“ je metóda, ktorá sa používa na potvrdenie prítomnosti infekcie vírusom spôsobujúcim ochorenie COVID-19, konkrétne, či ju oznámil samotný používateľ aplikácie, alebo je výsledkom potvrdenia vnútroštátneho zdravotníckeho orgánu alebo laboratórneho testu;

m) „krajiny záujmu“ sú členský štát alebo členské štáty, v ktorých sa používateľ aplikácie zdržiaval počas 14 dní pred dátumom nahratia kľúčov a kde si stiahol schválenú vnútroštátnu mobilnú aplikáciu na vyhľadávanie kontaktov a varovanie a/alebo kam cestoval;

n) „krajina pôvodu kľúčov“ je členský štát, v ktorom sa nachádza zálohový server, ktorý nahral kľúče do federačnej brány;

o) „údaje z protokolov“ sú automatické záznamy o činnosti v súvislosti s výmenou údajov a prístupom k týmto údajom spracúvaným prostredníctvom federačnej brány, ktoré uvádzajú najmä druh spracovateľskej činnosti, dátum a čas spracovania a identifikátor osoby, ktorá údaje spracúva.

_____

(*) Rozhodnutie Európskeho parlamentu a Rady č. 1082/2013/EÚ z 22. októbra 2013 o závažných cezhraničných ohrozeniach zdravia, ktorým sa zrušuje rozhodnutie č. 2119/98/ES (Ú. v. EÚ L 293, 5.11.2013, s. 1).“

2. V článku 4 ods. 1 sa vkladá toto písmeno h):

„h) poskytovať členským štátom usmernenia týkajúce sa cezhraničnej výmeny osobných údajov prostredníctvom federačnej brány medzi mobilnými aplikáciami na vyhľadávanie kontaktov a varovanie.“

3. V článku 6 ods. 1 sa vkladajú tieto písmená f) a g):

„f) vyvíja, zavádza a zachováva primerané technické a organizačné opatrenia týkajúce sa bezpečnosti prenosu a ukladania osobných údajov vo federačnej bráne na účely zabezpečenia interoperability vnútroštátnych mobilných aplikácií na sledovanie kontaktov a varovanie;

g) pomáha sieti elektronického zdravotníctva pri overovaní technického a organizačného súladu vnútroštátnych orgánov s požiadavkami na cezhraničnú výmenu osobných údajov vo federačnej bráne tým, že stanovuje a vykonáva potrebné testy a audity. Audítorom Komisie môžu pomáhať experti z členských štátov.“

4. Článok 7 sa mení takto:

a) Názov sa nahrádza názvom „Ochrana osobných údajov spracúvaných prostredníctvom infraštruktúry digitálnych služieb elektronického zdravotníctva“;

b) v odseku 2 sa slovo „prílohe“ nahrádza slovom „prílohe I“.“

5. Vkladá sa tento článok 7a:

„*Článok 7a*

Cezhraničná výmena údajov medzi mobilnými aplikáciami na vyhľadávanie kontaktov a varovanie prostredníctvom federačnej brány

1. Ak sa osobné údaje vymieňajú prostredníctvom federačnej brány, spracúvanie sa obmedzuje na účely uľahčenia interoperability vnútroštátnych mobilných aplikácií na vyhľadávanie kontaktov a varovanie v rámci federačnej brány a kontinuity vyhľadávania kontaktov v cezhraničnom kontexte.

2. Osobné údaje uvedené v odseku 3 sa do federačnej brány prenášajú v pseudonymizovanom formáte.

3. Pseudonymizované osobné údaje, ktoré sa vymieňajú a spracúvajú vo federačnej bráne, zahŕňajú len tieto informácie:

a) kľúče prenesené vnútroštátnymi mobilnými aplikáciami na vyhľadávanie kontaktov a varovanie maximálne 14 dní pred dátumom nahratia kľúčov;

b) údaje z protokolov súvisiace s kľúčmi v súlade s protokolom o technických špecifikáciách, ktorý sa používa v krajine pôvodu kľúčov;

c) overovanie infekcie;

d) krajiny záujmu a krajina pôvodu kľúčov.

4. Určené vnútroštátne orgány alebo iné verejné subjekty spracúvajúce osobné údaje vo federačnej bráne sú spoločnými prevádzkovateľmi údajov spracúvaných vo federačnej bráne. Príslušné zodpovednosti spoločných prevádzkovateľov sa prideľujú v súlade s prílohou II. Každý členský štát, ktorý má záujem zapojiť sa do cezhraničnej výmeny údajov medzi vnútroštátnymi mobilnými aplikáciami na vyhľadávanie kontaktov a varovanie, musí Komisiu ešte predtým, ako sa zapojí, o tomto úmysle informovať a nahlásiť vnútroštátny orgán alebo iný verejný subjekt, ktorý bol určený ako zodpovedný prevádzkovateľ.

5. Sprostredkovateľom osobných údajov spracúvaných vo federačnej bráne je Komisia. Komisia ako sprostredkovateľ zaisťuje bezpečnosť prenosu a ukladania osobných údajov vo federačnej bráne a dodržiava povinnosti sprostredkovateľa stanovené v prílohe III.

6. Komisia a vnútroštátne orgány, ktoré majú oprávnenie na prístup do federačnej brány, pravidelne testujú, posudzujú a hodnotia účinnosť technických a organizačných opatrení na zaistenie bezpečnosti spracúvania osobných údajov vo federačnej bráne.

7. Bez toho, aby bolo dotknuté rozhodnutie spoločných prevádzkovateľov ukončiť spracúvanie údajov vo federačnej bráne, prevádzka federačnej brány sa deaktivuje najneskôr 14 dní po tom, ako všetky pripojené vnútroštátne mobilné aplikácie na vyhľadávanie kontaktov a varovanie prestanú prenášať kľúče prostredníctvom federačnej brány.“

6. Príloha sa stáva prílohou I.

7. Dopĺňajú sa prílohy II a III, ktorých texty sa uvádzajú v prílohe k tomuto rozhodnutiu.

Článok 2

Toto rozhodnutie nadobúda účinnosť dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie*.

V Bruseli 15. júla 2020

Za Komisiu
predsedníčka
Ursula VON DER LEYEN

PRÍLOHA

K vykonávaciemu rozhodnutiu 2019/1765 sa dopĺňajú tieto prílohy II a III:

„PRÍLOHA II

POVINNOSTI ZÚČASTNENÝCH ČLENSKÝCH ŠTÁTOV AKO SPOLOČNÝCH PREVÁDZKOVATEĽOV FEDERAČNEJ BRÁNY PRE CEZHRANIČNÉ SPRACÚVANIE INFORMÁCIÍ MEDZI VNÚTROŠTÁTNYMI APLIKÁCIAMI NA VYHĽADÁVANIE KONTAKTOV A VAROVANIE

ODDIEL 1

Pododdiel 1

Rozdelenie povinností

1. Spoloční prevádzkovatelia spracúvajú osobné údaje vo federačnej bráne v súlade s technickými špecifikáciami stanovenými sieťou elektronického zdravotníctva ([1]).

2. Každý prevádzkovateľ je zodpovedný za spracúvanie osobných údajov vo federačnej bráne v súlade so všeobecným nariadením o ochrane údajov a smernicou 2002/58/ES.

3. Každý prevádzkovateľ zriadi kontaktné miesto s funkčnou e-mailovou schránkou, ktorá bude slúžiť na komunikáciu medzi spoločnými prevádzkovateľmi a medzi spoločnými prevádzkovateľmi a sprostredkovateľom.

4. Úlohou preskúmať všetky otázky vyplývajúce z interoperability vnútroštátnych mobilných aplikácií na vyhľadávanie kontaktov a varovanie, ako aj zo spoločného prevádzkovania súvisiaceho spracúvania osobných údajov na uľahčenie koordinovaných pokynov pre Komisiu ako sprostredkovateľa je poverená dočasná podskupina zriadená sieťou elektronického zdravotníctva v súlade s článkom 5 ods. 4 Okrem iných otázok môžu prevádzkovatelia v rámci dočasnej podskupiny pracovať na spoločnom prístupe k uchovávaniu údajov v ich vnútroštátnych zálohových serveroch, pričom sa zohľadní obdobie uchovávania stanovené vo federačnej bráne.

5. Pokyny pre sprostredkovateľa posiela ktorékoľvek kontaktné miesto spoločných prevádzkovateľov po dohode s ostatnými spoločnými prevádzkovateľmi v uvedenej podskupine.

6. Prístup k osobným údajom používateľov, ktoré sa vymieňajú vo federačnej bráne, majú iba povolané osoby určené vnútroštátnymi orgánmi resp. verejnými subjektmi.

7. Určený vnútroštátny orgán alebo verejný subjekt prestáva byť spoločným prevádzkovateľom od dátumu zrušenia svojej účasti vo federačnej bráne. Je však aj naďalej zodpovedný za spracúvanie údajov vo federačnej bráne, ku ktorému došlo pred zrušením účasti.

Pododdiel 2

Povinnosti a úlohy pri vybavovaní žiadostí a informovaní dotknutých osôb

1. Každý prevádzkovateľ poskytuje používateľom mobilných aplikácií na vyhľadávanie kontaktov a varovanie vo svojej krajine (ďalej len „dotknuté osoby“) informácie o spracúvaní ich osobných údajov vo federačnej bráne na účely cezhraničnej interoperability uvedených mobilných aplikácií v súlade s článkami 13 a 14 všeobecného nariadenia o ochrane údajov.

2. Každý prevádzkovateľ vystupuje ako kontaktné miesto pre používateľov mobilných aplikácií na vyhľadávanie kontaktov a varovanie vo svojej krajine a vybavuje žiadosti týkajúce sa výkonu práv dotknutých osôb, ktoré títo používatelia alebo ich zástupcovia predložili, v súlade so všeobecným nariadením o ochrane údajov. Každý prevádzkovateľ stanoví osobitné kontaktné miesto určené na vybavovanie žiadostí od dotknutých osôb. Ak spoločný prevádzkovateľ dostane od dotknutej osoby žiadosť, ktorá nespadá do rozsahu jeho zodpovednosti, bezodkladne ju postúpi zodpovednému spoločnému prevádzkovateľovi. Na požiadanie si spoloční prevádzkovatelia pri vybavovaní žiadostí dotknutých osôb navzájom pomáhajú a vzájomne si odpovedajú bez zbytočného odkladu, a to najneskôr do 15 dní od doručenia žiadosti o pomoc.

([1]) Konkrétne špecifikáciami interoperability pre cezhraničné reťazce šírenia nákazy medzi schválenými aplikáciami zo 16. júna 2020, ktoré sú dostupné na adrese: https://ec.europa.eu/health/ehealth/key_documents_en#anchor0.

3. Každý prevádzkovateľ sprístupní dotknutým osobám obsah tejto prílohy vrátane opatrení stanovených v bodoch 1 a 2.

ODDIEL 2

Riadenie kybernetických incidentov vrátane prípadov porušenia ochrany osobných údajov

1. Spoloční prevádzkovatelia si navzájom pomáhajú pri identifikácii a riešení všetkých bezpečnostných incidentov vrátane prípadov porušenia ochrany osobných údajov, ktoré sú spojené so spracúvaním vo federačnej bráne.

2. Spoloční prevádzkovatelia sa navzájom informujú najmä o týchto skutočnostiach:

a) všetkých potenciálnych alebo skutočných rizikách týkajúcich sa dostupnosti, dôvernosti a/alebo integrity osobných údajov, ktoré sa spracúvajú vo federačnej bráne;

b) všetkých bezpečnostných incidentoch súvisiacich so spracovateľskými operáciami vo federačnej bráne;

c) všetkých prípadoch porušenia ochrany osobných údajov, pravdepodobných dôsledkoch porušenia ochrany osobných údajov a posúdení rizika v súvislosti s právami a slobodami fyzických osôb, ako aj o všetkých prijatých opatreniach na riešenie porušovania ochrany osobných údajov a zmierňovanie rizika v súvislosti s právami a slobodami fyzických osôb;

d) všetkých prípadoch porušenia technických a/alebo organizačných záruk týkajúcich sa spracovateľských operácií vo federačnej bráne.

3. Spoloční prevádzkovatelia oznamujú Komisii, príslušným orgánom dohľadu a v prípade potreby dotknutým osobám všetky prípady porušenia ochrany osobných údajov týkajúce sa spracovateľských operácií vo federačnej bráne v súlade s článkami 33 a 34 nariadenia (EÚ) 2016/679 alebo po oznámení Komisie.

ODDIEL 3

Posúdenie vplyvu na ochranu údajov

Ak prevádzkovateľ v záujme plnenia povinností stanovených v článkoch 35 a 36 všeobecného nariadenia o ochrane údajov potrebuje informácie od iného prevádzkovateľa, zašle osobitnú žiadosť do funkčnej e-mailovej schránky uvedenej v oddiele 1 pododdiele 1 bode 3. Oslovený prevádzkovateľ vynaloží maximálne úsilie na poskytnutie týchto informácií.

PRÍLOHA III

POVINNOSTI KOMISIE AKO SPROSTREDKOVATEĽA FEDERAČNEJ BRÁNY PRE CEZHRANIČNÉ SPRACÚVANIE INFORMÁCIÍ MEDZI VNÚTROŠTÁTNYMI APLIKÁCIAMI NA VYHĽADÁVANIE KONTAKTOV A VAROVANIE

Komisia:

1. Vytvára a zaisťuje bezpečnú a spoľahlivú komunikačnú infraštruktúru, ktorá členským štátom zapojeným do federačnej brány prepája ich vnútroštátne aplikácie na vyhľadávanie kontaktov a varovanie. Komisia môže v rámci plnenia svojich povinností sprostredkovateľa vo federačnej bráne využívať služby tretích strán ako subdelegovaných sprostredkovateľov; Komisia informuje spoločných prevádzkovateľov o všetkých zamýšľaných zmenách týkajúcich sa pridania ďalších subdelegovaných sprostredkovateľov alebo ich nahradenia, a tým prevádzkovateľom poskytuje možnosť spoločne vzniesť voči takýmto zmenám námietky, ako sa stanovuje v oddiele 1 pododdiele 1 bode 4 prílohy II. Komisia zabezpečuje, aby sa na týchto subdelegovaných sprostredkovateľov vzťahovali rovnaké povinnosti v oblasti ochrany údajov, ako sú povinnosti stanovené v tomto rozhodnutí.

2. Spracúva osobné údaje len na základe zdokumentovaných pokynov prevádzkovateľov, pokiaľ to nevyžaduje právo Únie alebo členského štátu; v takom prípade Komisia oznámi prevádzkovateľom túto právnu požiadavku pred spracúvaním, pokiaľ dané právo predkladanie takéhoto oznámenia zo závažných dôvodov verejného záujmu nezakazuje.

3. Zo spracúvania osobných údajov Komisiou vyplývajú tieto skutočnosti:

a) autentifikácia vnútroštátnych zálohových severov založená na vnútroštátnych osvedčeniach zálohových serverov;

b) získavanie údajov uvedených v článku 7a ods. 3 vykonávacieho rozhodnutia, ktoré boli nahrané vnútroštátnymi zálohovými servermi, a to poskytnutím aplikačného programového rozhrania, ktoré umožní vnútroštátnym zálohovým serverom príslušné údaje nahrať;

c) uchovávanie údajov vo federačnej bráne po ich získaní z vnútroštátnych zálohových serverov;

d) sprístupnenie údajov na stiahnutie prostredníctvom vnútroštátnych zálohových serverov;

e) vymazanie údajov, potom, čo si ich stiahnu všetky zapojené zálohové servery, alebo 14 dní po ich získaní, podľa toho, čo nastane skôr;

f) vymazanie všetkých zostávajúcich údajov po skončení poskytovania služieb, pokiaľ právo Únie alebo práva členského štátu nevyžaduje tieto osobné údaje uchovávať.

Sprostredkovateľ prijíma všetky opatrenia potrebné na zachovanie integrity spracúvaných údajov.

4. Prijíma všetky špičkové organizačné, fyzické a logické bezpečnostné opatrenia na spravovanie federačnej brány. Komisia na tento účel:

a) určí zodpovedný subjekt na riadenie bezpečnosti na úrovni federačnej brány, oznámi prevádzkovateľom údajov jeho kontaktné údaje a zabezpečí, aby bol subjekt k dispozícii, ak bude potrebné reagovať na bezpečnostné hrozby;

b) nesie zodpovednosť za bezpečnosť federačnej brány;

c) zabezpečuje, aby sa na všetky osoby, ktorým je udelený prístup do federačnej brány, vzťahovala zmluvná, profesionálna alebo zákonná povinnosť zachovávať dôvernosť.

5. Prijíma všetky potrebné bezpečnostné opatrenia, aby nedošlo k ohrozeniu bezproblémového fungovania vnútroštátnych zálohových serverov. Komisia na tento účel zavedie osobitné postupy týkajúce sa pripojenia zo zálohových serverov do federačnej brány. To zahŕňa:

a) postup na posúdenie rizika s cieľom identifikovať a odhadnúť potenciálne hrozby pre systém;

b) audit a preskúmanie s cieľom:

   i) overiť zhodu medzi zavádzanými bezpečnostnými opatreniami a platnou bezpečnostnou politikou;

   ii) pravidelne kontrolovať integritu súborov systému, bezpečnostné parametre a udelené autorizácie;

   iii) monitorovať prípady narušenia bezpečnosti a neoprávnených vniknutí;

   iv) vykonať zmeny na zmiernenie existujúcich nedostatkov v zabezpečení;

   v) umožniť, a to aj na žiadosť prevádzkovateľov, vykonávanie nezávislých auditov vrátane inšpekcií a vykonávanie preskúmaní bezpečnostných opatrení a prispievať k týmto auditom a preskúmaniam, a to za podmienok, ktoré sú v súlade s protokolom (č. 7) k ZFEÚ o výsadách a imunitách Európskej únie ([2]);

([2]) Protokol č. 7 o výsadách a imunitách Európskej únie (Ú. v. EÚ C 326, 26.10.2012, s. 266).

c) zmenu postupu kontroly s cieľom zdokumentovať a odmerať vplyv zmeny pred jej vykonaním a informovať prevádzkovateľov o všetkých zmenách, ktoré môžu ovplyvniť komunikáciu s ich infraštruktúrami a/alebo ich bezpečnosť;

d) stanovenie postupu údržby a opravy s cieľom špecifikovať pravidlá a podmienky, ktoré treba dodržať pri údržbe a/alebo oprave vybavenia;

e) stanovenie postupu týkajúceho sa kybernetických incidentov s cieľom stanoviť systém hlásení a eskalácie, bezodkladne informovať prevádzkovateľov, ako aj európskeho dozorného úradníka pre ochranu údajov o akomkoľvek prípade narušenia bezpečnosti a stanoviť disciplinárne konanie pre prípady narušenia bezpečnosti.

6. Prijíma špičkové fyzické a/alebo logické bezpečnostné opatrenia pre zariadenia, v ktorých sa nachádza federačná brána, a pre logické kontroly prístupu k údajom a prístupu k zabezpečeniu. Komisia na tento účel:

a) zaisťuje fyzickú bezpečnosť s cieľom vytvoriť osobitné bezpečnostné zóny a umožniť odhalenie prípadov narušenia;

b) kontroluje prístup do zariadení a vedie register návštevníkov na účely sledovania;

c) zabezpečuje, aby externé osoby, ktorým bol udelený prístup do priestorov, sprevádzali riadne autorizovaní zamestnanci;

d) zabezpečuje, aby vybavenie nebolo možné pridať, nahradiť ani odstrániť bez predchádzajúcej autorizácie určených zodpovedných orgánov;

e) kontroluje prístup z/do vnútroštátnych zálohových serverov prepojených s federačnou bránou

f) zabezpečuje, aby všetci jednotlivci, ktorí využívajú prístup do federačnej brány, boli identifikovaní a overení;

g) preskúmava prístupové práva týkajúce sa prístupu do federačnej brány v prípade narušenia bezpečnosti, ktoré má vplyv na túto infraštruktúru;

h) zachováva integritu informácií prenášaných prostredníctvom federačnej brány;

i) realizuje technické a organizačné bezpečnostné opatrenia s cieľom zabrániť neoprávnenému prístupu k osobným údajom;

j) v prípade potreby realizuje opatrenia na zablokovanie neoprávneného prístupu do federačnej brány z domény vnútroštátnych orgánov (t. j.: blokovanie určenia polohy/IP adresy).

7. Podniká kroky na ochranu svojej domény vrátane prerušenia pripojení v prípade výraznej odchýlky od zásad a koncepcií v oblasti kvality alebo bezpečnosti.

8. Vypracúva a aktualizuje plán riadenia rizík v oblasti svojej pôsobnosti.

9. Monitoruje – v reálnom čase – vykonávanie všetkých zložiek služby v rámci svojich služieb federačnej brány, zostavuje pravidelnú štatistiku a vedie záznamy.

10. Poskytuje podporu všetkým službám federačnej brány v angličtine, a to 24 hodín denne a 7 dní v týždni cez telefón, mailom alebo cez webový portál a prijíma hovory od autorizovaných volajúcich, ktorými sú: koordinátori federačnej brány a ich príslušnej technickej podpory, projektoví manažéri a určené osoby z Komisie.

11. Primeranými technickými a organizačnými opatreniami a pokiaľ je to možné, pomáha prevádzkovateľom pri plnení ich povinnosti reagovať na žiadosti o výkon práv dotknutej osoby stanovených v kapitole III všeobecného nariadenia o ochrane údajov.

12. Podporuje prevádzkovateľov tým, že im poskytuje informácie týkajúce sa federačnej brány, aby sa splnili povinnosti vyplývajúce z článkov 32, 35 a 36 všeobecného nariadenia o ochrane údajov.

13. Zabezpečuje, aby boli údaje spracúvané v rámci federačnej brány zašifrované pre všetky osoby, ktoré nemajú oprávnenie na prístup k nim.

14. Prijíma všetky príslušné opatrenia, ktorými sa zabraňuje, aby mali prevádzkovatelia federačnej brány neoprávnený prístup k prenášaným údajom.

15. Prijíma opatrenia na uľahčenie interoperability a komunikácie medzi určenými prevádzkovateľmi federačnej brány.

16. Vedie záznamy o spracovateľských činnostiach vykonávaných v mene prevádzkovateľov v súlade s článkom 31 ods. 2 nariadenia (EÚ) 2018/1725.“