►B

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

[oznámené pod číslom C(2019) 7460]

(Text s významom pre EHP)

(Ú. v. EÚ L 270, 24.10.2019, s. 83)

Zmenené a doplnené:

		Úradný vestník		
		Č.	Strana	Dátum
►M1	Vykonávacie rozhodnutie Komisie (EÚ) 2020/1023 z 15. júla 2020	L 227 I	1	16.7.2020

▼B

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

[oznámené pod číslom C(2019) 7460]

(Text s významom pre EHP)

Článok 1

Predmet úpravy

Týmto rozhodnutím sa stanovujú potrebné pravidlá týkajúce sa zriadenia, riadenia a fungovania siete elektronického zdravotníctva spájajúcej vnútroštátne orgány zodpovedné za elektronické zdravotníctvo podľa článku 14 smernice 2011/24/EÚ.

Článok 2

Vymedzenie pojmov

1. Na účely tohto rozhodnutia:

a) „sieť elektronického zdravotníctva“ je dobrovoľná sieť spájajúca vnútroštátne orgány zodpovedné za elektronické zdravotníctvo, ktoré určili členské štáty a ktoré sledujú ciele stanovené v článku 14 smernice 2011/24/EÚ;

b) „národné kontaktné miesta pre elektronické zdravotníctvo“ sú organizačné a technické brány na poskytovanie cezhraničných informačných služieb elektronického zdravotníctva, za ktoré sú zodpovedné členské štáty;

c) „cezhraničné informačné služby elektronického zdravotníctva“ sú existujúce služby, ktoré sa spracúvajú prostredníctvom národných kontaktných miest pre elektronické zdravotníctvo a prostredníctvom platformy základných služieb, ktorú vytvorila Komisia na účely cezhraničnej zdravotnej starostlivosti;

d) „infraštruktúra digitálnych služieb elektronického zdravotníctva pre cezhraničné informačné služby elektronického zdravotníctva“ je infraštruktúra, ktorá umožňuje poskytovanie cezhraničných informačných služieb elektronického zdravotníctva prostredníctvom národných kontaktných miest pre elektronické zdravotníctvo a platformy základných služieb. Táto infraštruktúra zahŕňa generické služby vymedzené v článku 2 ods. 2 písm. e) nariadenia (EÚ) č. 283/2014 vyvinuté členskými štátmi a platformu základných služieb vymedzenú v jeho článku 2 ods. 2 písm. d) vyvinutú Komisiou;

e) „iné spoločné európske služby“ sú digitálne služby, ktoré sa môžu vyvinúť v rámci siete elektronického zdravotníctva a ktoré môžu členské štáty využívať spoločne;

▼B

f) „model riadenia“ je súbor pravidiel týkajúcich sa určenia orgánov zapojených do rozhodovacích procesov v súvislosti s infraštruktúrou digitálnych služieb elektronického zdravotníctva pre cezhraničné informačné služby elektronického zdravotníctva alebo inými spoločnými európskymi službami elektronického zdravotníctva vyvinutými v rámci siete elektronického zdravotníctva, ako aj opis uvedených procesov;

▼M1

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 ([1]);

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;

([1]) 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).

▼M1

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.

▼B

2. Zodpovedajúcim spôsobom sa uplatňuje vymedzenie pojmov podľa článku 4 bodov 1, 2, 7 a 8 nariadenia (EÚ) 2016/679.

Článok 3

Členstvo v sieti elektronického zdravotníctva

1. Členmi siete elektronického zdravotníctva sú orgány členských štátov zodpovedné za elektronické zdravotníctvo, ktoré určili členské štáty zapojené do siete elektronického zdravotníctva.

2. Členské štáty, ktoré sa chcú zapojiť do siete elektronického zdravotníctva, písomne oznámia Komisii:

a) rozhodnutie zapojiť sa do siete elektronického zdravotníctva;

b) vnútroštátny orgán zodpovedný za elektronické zdravotníctvo, ktorý sa stane členom siete elektronického zdravotníctva, ako aj meno zástupcu a jeho/jej náhradníka.

3. Členské štáty oznámia Komisii tieto informácie:

a) rozhodnutie vystúpiť zo siete elektronického zdravotníctva;

b) zmeny v informáciách uvedených v odseku 2 písm. b).

4. Komisia sprístupní verejnosti zoznam členov zapojených do siete elektronického zdravotníctva.

Článok 4

Aktivity siete elektronického zdravotníctva

1. Pri plnení cieľa uvedeného v článku 14 ods. 2 písm. a) smernice 2011/24/EÚ môže sieť elektronického zdravotníctva najmä:

a) umožňovať väčšiu interoperabilitu vnútroštátnych systémov informačných a komunikačných technológií a cezhraničnú prenosnosť elektronických údajov týkajúcich sa zdravia pri cezhraničnej zdravotnej starostlivosti;

b) poskytovať v spolupráci s inými príslušnými orgánmi dohľadu usmernenia členským štátom v súvislosti so zdieľaním údajov týkajúcich sa zdravia medzi členskými štátmi a s možnosťou, aby mali občania prístup k svojim vlastným údajom týkajúcim sa zdravia a aby ich mohli sami zdieľať;

▼B

c) poskytovať usmernenia členským štátom a uľahčovať výmenu osvedčených postupov týkajúcich vyvíjania rôznych digitálnych služieb zdravotnej starostlivosti, ako je napr. telemedicína, mobilné zdravotníctvo alebo nové technológie v oblasti veľkých dát a umelej inteligencie s ohľadom na prebiehajúce akcie na úrovni EÚ;

d) poskytovať členským štátom usmernenia týkajúce sa podpory zdravia, prevencie chorôb a zdokonaleného poskytovania zdravotnej starostlivosti prostredníctvom lepšieho využívania údajov týkajúcich sa zdravia a zlepšenia digitálnych zručností pacientov a zdravotníckych pracovníkov;

e) poskytovať usmernenia členským štátom a uľahčovať dobrovoľnú výmenu najlepších postupov v súvislosti s investíciami do digitálnej infraštruktúry;

f) poskytovať členským štátom v spolupráci s inými príslušnými orgánmi a zainteresovanými stranami usmernenia o potrebných možnostiach použitia v záujme klinickej interoperability a nástrojoch na jej dosiahnutie;

g) poskytovať členským štátom v úzkej spolupráci so skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti a s Agentúrou Európskej únie pre sieťovú a informačnú bezpečnosť, ako aj s vnútroštátnymi orgánmi usmernenia o bezpečnosti infraštruktúry digitálnych služieb elektronického zdravotníctva pre cezhraničné informačné služby elektronického zdravotníctva alebo iných spoločných európskych služieb elektronického zdravotníctva vyvinutých v rámci siete elektronického zdravotníctva s ohľadom na právne predpisy a dokumenty vypracované na úrovni Únie, najmä v oblasti bezpečnosti, ako aj odporúčania v oblasti kybernetickej bezpečnosti;

▼M1

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

▼B

2. Sieť elektronického zdravotníctva pri vypracúvaní usmernení o účinných metódach umožňujúcich využívanie lekárskych informácií v záujme verejného zdravia a výskumu uvedených v článku 14 ods. 2 písm. b) bode ii) smernice 2011/24/EÚ zohľadňuje usmernenia, ktoré prijal Európsky výbor pre ochranu údajov, a v príslušných prípadoch s ním uskutočňuje konzultácie. Tieto usmernenia sa môžu zaoberať aj informáciami vymieňanými prostredníctvom infraštruktúry digitálnych služieb elektronického zdravotníctva pre cezhraničné informačné služby elektronického zdravotníctva alebo iných spoločných európskych služieb elektronického zdravotníctva.

Článok 5

Fungovanie siete elektronického zdravotníctva

1. Sieť elektronického zdravotníctva stanoví svoj rokovací poriadok jednoduchou väčšinou svojich členov.

2. Sieť elektronického zdravotníctva prijme viacročný program činnosti a nástroj hodnotenia vykonávania tohto programu.

▼B

3. V záujme dosiahnutia svojich cieľov môže sieť elektronického zdravotníctva zriadiť stále podskupiny na plnenie konkrétnych úloh týkajúcich sa najmä infraštruktúry digitálnych služieb elektronického zdravotníctva pre cezhraničné informačné služby elektronického zdravotníctva alebo iné spoločné európske služby elektronického zdravotníctva vyvinuté v rámci siete elektronického zdravotníctva.

4. Sieť elektronického zdravotníctva môže okrem toho zriadiť dočasné podskupiny, aj s expertmi, na preskúmanie konkrétnych otázok na základe mandátu, ktorý vymedzila samotná sieť elektronického zdravotníctva. Takéto podskupiny sa hneď po splnení svojej úlohy zrušia.

5. Keď sa členovia siete elektronického zdravotníctva rozhodnú prehĺbiť svoju spoluprácu v niektorých oblastiach, ktoré sú zahrnuté v úlohách siete, mali by sa dohodnúť na pravidlách prehĺbenej spolupráce a tieto pravidlá dodržiavať.

6. Sieť elektronického zdravotníctva pri plnení svojich cieľov úzko spolupracuje s jednotnými akciami, ktoré podporujú aktivity siete elektronického zdravotníctva (ak takéto spoločné akcie existujú), so zainteresovanými stranami a inými príslušnými orgánmi a podpornými mechanizmami a zohľadňuje výsledky dosiahnuté v rámci uvedených aktivít.

7. Sieť elektronického zdravotníctva spolu s Komisiou vypracuje modely riadenia infraštruktúry digitálnych služieb elektronického zdravotníctva pre cezhraničné informačné služby elektronického zdravotníctva a zúčastní sa na uvedenom riadení tým, že:

i) sa dohodne na prioritách infraštruktúry digitálnych služieb elektronického zdravotníctva a kontroluje ich prevádzku;

ii) vypracuje usmernenia a požiadavky na prevádzku vrátane výberu noriem používaných v prípade infraštruktúry digitálnych služieb elektronického zdravotníctva pre cezhraničné informačné služby elektronického zdravotníctva;

iii) sa dohodne, či by členovia siete elektronického zdravotníctva mali byť oprávnení začať a ďalej si vymieňať elektronické údaje týkajúce sa zdravia prostredníctvom infraštruktúry digitálnych služieb elektronického zdravotníctva pre cezhraničné informačné služby elektronického zdravotníctva cez svoje národné kontaktné miesta pre elektronické zdravotníctvo na základe ich súladu s požiadavkami stanovenými sieťou elektronického zdravotníctva, ktorý sa vyhodnotil na základe testov stanovených a auditov vykonaných Komisiou;

iv) schváli ročný pracovný program pre infraštruktúru digitálnych služieb elektronického zdravotníctva pre cezhraničné informačné služby elektronického zdravotníctva.

8. Sieť elektronického zdravotníctva môže spolu s Komisiou vypracovať modely riadenia iných spoločných európskych služieb elektronického zdravotníctva vyvinutých v rámci siete elektronického zdravotníctva a zúčastniť sa na ich riadení. Okrem toho môže sieť stanoviť priority v spolupráci s Komisiou a vypracovať usmernenia na fungovanie takýchto spoločných európskych služieb elektronického zdravotníctva.

▼B

9. V rokovacom poriadku sa môže stanoviť, že krajiny iné ako členské štáty, ktoré uplatňujú smernicu 2011/24/EÚ, sa môžu zúčastňovať na zasadnutiach siete elektronického zdravotníctva ako pozorovatelia.

10. Členovia siete elektronického zdravotníctva a ich zástupcovia, ako aj pozvaní experti a pozorovatelia dodržiavajú povinnosť služobného tajomstva stanovenú v článku 339 zmluvy, ako aj bezpečnostné predpisy Komisie týkajúce ochrany utajovaných informácií EÚ v zmysle rozhodnutia Komisie (EÚ, Euratom) 2015/444 ([1]). V prípade nedodržania týchto povinností môže predseda siete elektronického zdravotníctva prijať všetky vhodné opatrenia stanovené v rokovacom poriadku.

Článok 6

Vzťah medzi sieťou elektronického zdravotníctva a Komisiou

1. Komisia:

a) sa zúčastňuje na zasadnutiach siete elektronického zdravotníctva a spolu so zástupcom členov im spolupredsedá;

b) spolupracuje so sieťou elektronického zdravotníctva a poskytuje jej podporu v súvislosti s jej aktivitami;

c) poskytuje sekretárske služby pre sieť elektronického zdravotníctva;

d) vyvíja, zavádza a zachováva primerané technické a organizačné opatrenia týkajúce sa základných služieb infraštruktúry digitálnych služieb elektronického zdravotníctva pre cezhraničné informačné služby elektronického zdravotníctva;

e) pomáha sieti elektronického zdravotníctva pri overovaní technického a organizačného súladu národných kontaktných miest pre elektronické zdravotníctvo s požiadavkami na cezhraničnú výmenu údajov týkajúcich sa zdravia tým, že stanovuje a vykonáva potrebné testy a audity. Audítorom Komisie môžu pomáhať experti z členských štátov;

▼M1

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.

▼B

2. Komisia sa môže zúčastňovať na zasadnutiach podskupín siete elektronického zdravotníctva.

3. Komisia môže konzultovať so sieťou elektronického zdravotníctva o otázkach týkajúcich sa elektronického zdravotníctva na úrovni Únie a o výmene najlepších postupov v oblasti elektronického zdravotníctva.

([1]) Rozhodnutie Komisie (EÚ, Euratom) 2015/444 z 13. marca 2015 o bezpečnostných predpisoch na ochranu utajovaných skutočností EÚ (Ú. v. EÚ L 72, 17.3.2015, s. 53).

▼B

4. Komisia sprístupňuje verejnosti informácie o aktivitách siete elektronického zdravotníctva.

Článok 7

▼M1

Ochrana osobných údajov spracúvaných prostredníctvom infraštruktúry digitálnych služieb elektronického zdravotníctva

▼B

1. Členské štáty, ktoré sú zastúpené príslušnými vnútroštátnymi orgánmi alebo inými určenými subjektmi, sa považujú za prevádzkovateľov osobných údajov, ktoré spracúvajú prostredníctvom infraštruktúry digitálnych služieb elektronického zdravotníctva pre cezhraničné informačné služby elektronického zdravotníctva, a jasne a transparentne určujú zodpovednosti jednotlivých prevádzkovateľov.

2. Komisia sa považuje za sprostredkovateľa v prípade osobných údajov pacientov spracúvaných prostredníctvom infraštruktúry digitálnych služieb elektronického zdravotníctva pre cezhraničné informačné služby elektronického zdravotníctva. Komisia ako sprostredkovateľ riadi základné služby infraštruktúry digitálnych služieb elektronického zdravotníctva pre cezhraničné informačné služby elektronického zdravotníctva a dodržiava povinnosti sprostredkovateľa stanovené v ►M1 prílohe I ◄ k tomuto rozhodnutiu. Komisia nemá prístup k osobným údajom pacientov spracúvaným prostredníctvom infraštruktúry digitálnych služieb elektronického zdravotníctva pre cezhraničné informačné služby elektronického zdravotníctva.

3. Komisia sa považuje za prevádzkovateľa v súvislosti so spracúvaním osobných údajov potrebných na udelenie a riadenie práv prístupu k základným službám infraštruktúry digitálnych služieb elektronického zdravotníctva pre cezhraničné informačné služby elektronického zdravotníctva. Takýmito údajmi sú kontaktné údaje používateľov vrátane mena, priezviska a e-mailovej adresy a ich príslušnosti.

▼M1

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.

▼M1

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.

▼B

Článok 8

Výdavky

1. Účastníci aktivít siete elektronického zdravotníctva nedostávajú od Komisie odmenu za svoje služby.

▼B

2. Cestovné náklady a náklady spojené s pobytom, ktoré účastníkom vznikli v súvislosti s aktivitami siete elektronického zdravotníctva, nahrádza Komisia v súlade s ustanoveniami platnými v rámci Komisie týkajúcimi náhrady nákladov a výdavkov osôb mimo Komisie, ktoré sú pozvané na zasadnutia ako experti. Tieto výdavky sa uhrádzajú v medziach dostupných rozpočtových prostriedkov pridelených v rámci ročného postupu prideľovania finančných prostriedkov.

Článok 9

Zrušenie

Vykonávacie rozhodnutie 2011/890/EÚ sa zrušuje. Odkazy na zrušené rozhodnutie sa považujú za odkazy na toto rozhodnutie.

Článok 10

Adresáti

Toto rozhodnutie je určené členským štátom.

▼M1

PRÍLOHA I

▼B

ÚLOHY KOMISIE AKO SPROSTREDKOVATEĽA V RÁMCI INFRAŠTRUKTÚRY DIGITÁLNYCH SLUŽIEB ELEKTRONICKÉHO ZDRAVOTNÍCTVA PRE CEZHRANIČNÉ INFORMAČNÉ SLUŽBY ELEKTRONICKÉHO ZDRAVOTNÍCTVA

Komisia:

1. Vytvára a zaisťuje zabezpečenú a spoľahlivú komunikačnú infraštruktúru, ktorá prepája siete členov siete elektronického zdravotníctva zapojených do infraštruktúry digitálnych služieb elektronického zdravotníctva pre cezhraničné informačné služby elektronického zdravotníctva („centrálna zabezpečená komunikačná infraštruktúra“). Komisia môže v rámci plnenia svojich povinností využívať služby tretích strán. Komisia zabezpečuje, aby sa na tieto tretie strany vzťahovali rovnaké povinnosti v oblasti ochrany údajov, ako sú povinnosti stanovené v tomto rozhodnutí.

2. Konfiguruje časť zabezpečenej komunikačnej infraštruktúry tak, aby si národné kontaktné miesta pre elektronické zdravotníctvo mohli vymieňať informácie bezpečne, spoľahlivo a efektívne.

3. Komisia spracúva osobné údaje na základe zdokumentovaných pokynov prevádzkovateľov.

4. Prijíma všetky organizačné, fyzické a logické bezpečnostné opatrenia na spravovanie centrálnej zabezpečenej komunikačnej infraštruktúry. Komisia na tento účel:

   a) určí zodpovedný subjekt na riadenie bezpečnosti na úrovni centrálnej zabezpečenej komunikačnej infraštruktúry, oznámi prevádzkovateľom údajov jeho kontaktné údaje a zabezpečí, že subjekt bude k dispozícii, ak bude potrebné reagovať na bezpečnostné hrozby;

   b) nesie zodpovednosť za bezpečnosť centrálnej zabezpečenej komunikačnej infraštruktúry;

   c) zabezpečuje, aby sa na všetky osoby, ktorým je udelený prístup do centrálnej zabezpečenej komunikačnej infraštruktúry, vzťahovala zmluvná, profesionálna alebo zákonná povinnosť zachovávať dôvernosť;

   d) zabezpečuje, aby personál, ktorý má prístup k utajovaným skutočnostiam, spĺňal príslušné kritériá na previerku a zachovávanie dôvernosti.

5. Prijíma všetky potrebné bezpečnostné opatrenia, aby nedošlo k ohrozeniu bezproblémového fungovania domény druhej strany. Komisia na tento účel zavedie osobitné postupy týkajúce sa pripojenia k centrálnej zabezpečenej komunikačnej infraštruktúre. Informácie zahŕňajú:

   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 uplatňovanou bezpečnostnou politikou;

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

      iii) monitorovať prípady narušenia bezpečnosti a neoprávnených vniknutí;

      iv) vykonať zmeny, aby sa odstránili existujúce nedostatky v zabezpečení, a

▼B

v) stanoviť podmienky, za ktorých je možné udeliť autorizáciu, a to aj na žiadosť prevádzkovateľov, a prispieť k vykonávaniu nezávislých auditov vrátane inšpekcií a k vykonávaniu preskúmaní bezpečnostných opatrení;

c) postup kontroly zmien s cieľom zdokumentovať a odmerať vplyv zmeny pred jej vykonaním a informovať národné kontaktné miesta pre elektronické zdravotníctvo o všetkých zmenách, ktoré môžu ovplyvniť komunikáciu s ostatnými vnútroštátnymi infraštruktúrami a/alebo ich bezpečnosť;

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

e) postup týkajúci sa kybernetických incidentov s cieľom stanoviť systém hlásení a eskalácie, bezodkladne informovať zodpovednú vnútroštátnu správu, ako aj európskeho dozorného úradníka pre ochranu údajov o akomkoľvek narušení bezpečnosti a stanoviť disciplinárne konanie pre prípad narušenia bezpečnosti.

6. Prijíma fyzické a/alebo logické bezpečnostné opatrenia pre zariadenia, v ktorých sa nachádza vybavenie centrálnej zabezpečenej komunikačnej infraštruktúry, a pre logické kontroly prístupu k údajom a prístupu k zabezpečeniu. Komisia na tento účel:

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

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

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

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

e) kontroluje prístup z a do iných sietí prepojených s centrálnou zabezpečenou komunikačnou infraštruktúrou;

f) zabezpečuje, aby všetci jednotlivci, ktorí využívajú prístup do centrálnej zabezpečenej komunikačnej infraštruktúry, boli identifikovaní a overení;

g) preskúmava prístupové práva týkajúce sa prístupu k centrálnej zabezpečenej komunikačnej infraštruktúre v prípade narušenia bezpečnosti, ktoré má vplyv na túto infraštruktúru;

h) zachováva integritu prenášaných informácií v rámci centrálnej zabezpečenej komunikačnej infraštruktúry;

i) realizuje technické a organizačné bezpečnostné opatrenia na zabránenie neoprávnenému prístupu k osobným údajom;

j) v prípade potreby realizuje opatrenia na zablokovanie neoprávneného prístupu k centrálnej zabezpečenej komunikačnej infraštruktúre z domény národných kontaktných miest pre elektronické zdravotníctvo (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.

▼B

9. Monitoruje – v reálnom čase – vykonávanie všetkých zložiek služby v rámci svojich služieb centrálnej zabezpečenej komunikačnej infraštruktúry, zostavuje pravidelnú štatistiku a vedie záznamy.

10. Poskytuje podporu všetkým službám centrálnej zabezpečenej komunikačnej infraštruktúry v angličtine 24/7 cez telefón, mailom alebo cez webový portál a prijíma hovory od autorizovaných volajúcich, ktorými sú: koordinátori centrálnej zabezpečenej komunikačnej infraštruktúry a ich príslušnej technickej podpory, projektoví manažéri a určené osoby z Komisie.

11. Podporuje prevádzkovateľov tým, že im poskytuje informácie týkajúce centrálnej zabezpečenej komunikačnej infraštruktúry v rámci infraštruktúry digitálnych služieb elektronického zdravotníctva pre cezhraničné informačné služby elektronického zdravotníctva, aby sa splnili povinnosti vyplývajúce z článkov 35 a 36 nariadenia (EÚ) 2016/679.

12. Zabezpečuje, aby boli informácie prenášané v rámci centrálnej zabezpečenej komunikačnej infraštruktúry zašifrované.

13. Prijíma všetky príslušné opatrenia, ktorými sa zabraňuje, aby mali prevádzkovatelia centrálnej zabezpečenej komunikačnej infraštruktúry neoprávnený prístup k prenášaným údajom.

14. Prijíma opatrenia na uľahčenie interoperability a komunikácie medzi určenými vnútroštátnymi príslušnými správnymi orgánmi centrálnej zabezpečenej komunikačnej infraštruktúry.

▼M1

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

([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.

▼M1

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.

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.

▼M1

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:

▼M1

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 ([1]);

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:

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

▼M1

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.

▼**M1**

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.