II

(Acte fără caracter legislativ)

DECIZII

DECIZIA DE PUNERE ÎN APLICARE (UE) 2020/1023 A COMISIEI

din 15 iulie 2020

de modificare a Deciziei de punere în aplicare (UE) 2019/1765 în ceea ce privește schimbul transfrontalier de date dintre aplicațiile mobile naționale de depistare a contacților și de avertizare în contextul combaterii pandemiei de COVID-19

(Text cu relevanță pentru SEE)

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Directiva 2011/24/UE a Parlamentului European și a Consiliului din 9 martie 2011 privind aplicarea drepturilor pacienților în cadrul asistenței medicale transfrontaliere ([1]), în special articolul 14 alineatul (3),

întrucât:

(1) Prin articolul 14 din Directiva 2011/24/UE, Uniunii îi este atribuită sarcina de a sprijini și de a facilita cooperarea și schimbul de informații dintre statele membre care operează în cadrul unei rețele voluntare ce conectează autoritățile naționale responsabile cu e-sănătatea desemnate de statele membre („rețeaua de e-sănătate”).

(2) Decizia de punere în aplicare a Comisiei (UE) 2019/1765 ([2]) prevede normele pentru înființarea, gestionarea și funcționarea rețelei de autorități naționale responsabile cu e-sănătatea. Articolul 4 din decizia respectivă încredințează rețelei de e-sănătate sarcina de a facilita o interoperabilitate sporită a sistemelor naționale de tehnologie a informației și a comunicațiilor și transferabilitatea transfrontalieră a datelor medicale electronice în cadrul asistenței medicale transfrontaliere.

(3) Având în vedere criza de sănătate publică provocată de pandemia de COVID-19, mai multe state membre au creat aplicații mobile care sprijină depistarea contacților și permit utilizatorilor acestor aplicații să fie avertizați, pentru a lua măsurile adecvate, precum testarea sau autoizolarea, dacă au fost potențial expuși la virus prin apropierea de un alt utilizator al acestor aplicații care a raportat un diagnostic pozitiv. Aceste aplicații se bazează pe tehnologia Bluetooth pentru a detecta apropierea dintre dispozitive. Întrucât restricțiile privind călătoriile dintre statele membre au fost ridicate începând cu luna iunie 2020, între statele membre din cadrul rețelei de e-sănătate trebuie realizată o interoperabilitate sporită a sistemelor naționale de tehnologie a informației și a comunicațiilor, prin implementarea unei infrastructuri digitale care să permită interoperabilitatea aplicațiilor mobile naționale care sprijină depistarea contacților și avertizarea.

([1]) JO L 88, 4.4.2011, p. 45.

([2]) Decizia de punere în aplicare (UE) 2019/1765 a Comisiei din 22 octombrie 2019 de stabilire a normelor pentru înființarea, gestionarea și funcționarea rețelei de autorități naționale responsabile cu e-sănătatea și de abrogare a Deciziei de punere în aplicare 2011/890/UE (JO L 270, 24.10.2019, p. 83).

(4) Comisia sprijină statele membre în ceea ce privește aplicațiile mobile menționate mai sus. La 8 aprilie 2020, Comisia a adoptat o Recomandare privind un set comun de instrumente la nivelul Uniunii pentru utilizarea tehnologiei și a datelor în scopul de a combate criza provocată de pandemia de COVID-19 și de a ieși din această criză, în special în ceea ce privește aplicațiile mobile și utilizarea datelor anonimizate privind mobilitatea (denumită în continuare „recomandarea Comisiei") ([3]). Statele membre din cadrul rețelei de e-sănătate au adoptat, cu sprijinul Comisiei, un set comun de instrumente la nivelul UE pentru statele membre, privind aplicațiile mobile de sprijinire a depistării contacților ([4]), precum și orientări privind interoperabilitatea aplicațiilor mobile de depistare a contacților autorizate în UE ([5]). Acest set de instrumente explică cerințele naționale pentru aplicațiile mobile naționale de depistare a contacților și de avertizare, în special faptul că trebuie să fie voluntare, aprobate de autoritatea națională de sănătate respectivă, să protejeze viața privată și să fie scoase din uz de îndată ce nu mai sunt necesare. În urma celor mai recente evoluții ale crizei provocate de pandemia de COVID-19, atât Comisia ([6]), cât și Comitetul european pentru protecția datelor ([7]) au emis orientări privind aplicațiile mobile și instrumentele de depistare a contacților, în legătură cu protecția datelor. Concepția aplicațiilor mobile ale statelor membre și a infrastructurii digitale care permite interoperabilitatea acestora se bazează pe setul comun de instrumente la nivelul UE, pe orientările menționate mai sus și pe specificațiile tehnice convenite în cadrul rețelei de e-sănătate.

(5) Pentru a facilita interoperabilitatea aplicațiilor mobile naționale de depistare a contacților și de avertizare, statele membre care participă la rețeaua de e-sănătate și care au decis în mod voluntar să progreseze în ceea ce privește cooperarea lor în acest domeniu au dezvoltat o infrastructură digitală, cu sprijinul Comisiei, ca instrument informatic pentru schimbul de date. Această infrastructură digitală este denumită „portalul federativ".

(6) Prezenta decizie stabilește dispoziții privind rolul statelor membre participante și al Comisiei în legătură cu funcționarea portalului federativ pentru interoperabilitatea transfrontalieră a aplicațiilor mobile naționale de depistare a contacților și de avertizare.

(7) Prelucrarea datelor cu caracter personal ale utilizatorilor aplicațiilor mobile de depistare a contacților și de avertizare, care se realizează sub responsabilitatea statelor membre sau a altor organizații sau organisme publice din statele membre, trebuie să fie efectuată în conformitate cu Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului ([8]) („Regulamentul general privind protecția datelor") și cu Directiva 2002/58/CE a Parlamentului European și a Consiliului ([9]). Prelucrarea datelor cu caracter personal sub responsabilitatea Comisiei în scopul gestionării și asigurării securității portalului federativ trebuie să respecte Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului ([10]).

(8) Portalul federativ trebuie să constea într-o infrastructură informatică securizată care pune la dispoziție o interfață comună în cadrul căreia organismele oficiale sau autoritățile naționale desemnate pot schimba între ele un set minim de date privind contactele cu persoanele infectate cu SARS-CoV-2, pentru a îi informa pe ceilalți cu privire la expunerea lor potențială la infecția respectivă, și care promovează o cooperare eficace în domeniul asistenței medicale între statele membre prin facilitarea schimbului de informații relevante.

(9) Prin urmare, prezenta decizie trebuie să stabilească modalitățile pentru schimbul transfrontalier de date dintre organismele oficiale sau autoritățile naționale desemnate, prin intermediul portalului federativ, în cadrul UE.

([3]) Recomandarea (UE) 2020/518 a Comisiei din 8 aprilie 2020 privind un set comun de instrumente la nivelul Uniunii pentru utilizarea tehnologiei și a datelor în scopul de a combate criza provocată de pandemia de COVID-19 și de a ieși din această criză, în special în ceea ce privește aplicațiile mobile și utilizarea datelor anonimizate privind mobilitatea (JO L 114, 14.4.2020, p. 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]) Comunicare a Comisiei intitulată „Orientări în domeniul protecției datelor privind aplicațiile care sprijină combaterea pandemiei de COVID-19" (JO C 124I, 17.4.2020, p. 1).

([7]) Orientările 04/2020 privind utilizarea datelor de localizare și a instrumentelor de depistare a contacților în contextul pandemiei de COVID-19 și Declarația CEPD din 16 iunie 2020 privind impactul interoperabilității aplicațiilor de depistare a contacților asupra protecției datelor, ambele disponibile la adresa: https://edpb.europa.eu

([8]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

([9]) Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) (JO L 201, 31.7.2002, p. 37).

([10]) Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39).

(10) Statele membre participante, reprezentate de organismele oficiale sau autoritățile naționale desemnate, stabilesc împreună scopul și mijloacele de prelucrare a datelor cu caracter personal prin portalul federativ și, prin urmare, sunt operatori asociați. Articolul 26 din Regulamentul general privind protecția datelor prevede obligația operatorilor asociați care efectuează operațiuni de prelucrare a datelor cu caracter personal de a stabili, în mod transparent, responsabilitățile fiecăruia în ceea ce privește respectarea obligațiilor care le revin în temeiul regulamentului respectiv. De asemenea, prevede posibilitatea ca aceste responsabilități să fie stabilite prin legislația de la nivelul Uniunii sau al statului membru care li se aplică operatorilor. Fiecare operator trebuie să se asigure că dispune de un temei juridic la nivel național pentru a desfășura operațiuni de prelucrare în cadrul portalului federativ.

(11) Comisia, în calitate de furnizor de soluții tehnice și organizatorice pentru portalul federativ, prelucrează date cu caracter personal pseudonimizate în numele statelor membre participante la portalul federativ ca operatori asociați și, prin urmare, este o persoană împuternicită de operator. În conformitate cu articolul 28 din Regulamentul general privind protecția datelor și cu articolul 29 din Regulamentul (UE) 2018/1725, prelucrarea de către o persoană împuternicită de operator este reglementată printr-un contract sau un act juridic în temeiul dreptului Uniunii sau al dreptului statului membru, care are caracter obligatoriu pentru persoana împuternicită de operator în raport cu operatorul și care precizează aspecte referitoare la prelucrare. Prezenta decizie stabilește norme privind prelucrarea de către Comisie în calitate de persoană împuternicită de operator.

(12) Atunci când prelucrează date cu caracter personal în cadrul portalului federativ, Comisia trebuie să respecte Decizia (UE, Euratom) 2017/46 a Comisiei ([11]).

(13) Ținând seama de faptul că scopurile pentru care operatorii prelucrează date cu caracter personal în cadrul aplicațiilor mobile naționale de depistare a contacților și de avertizare nu necesită în mod neapărat identificarea unei persoane vizate, este posibil ca operatorii să nu fie întotdeauna în măsură să asigure aplicarea drepturilor persoanelor vizate. Prin urmare, este posibil ca drepturile menționate la articolele 15-20 din Regulamentul general privind protecția datelor să nu se aplice atunci când sunt îndeplinite condițiile prevăzute la articolul 11 din regulamentul respectiv.

(14) Anexa existentă la Decizia de punere în aplicare (UE) 2019/1765 trebuie renumerotată în urma adăugării a două noi anexe.

(15) Prin urmare, Decizia de punere în aplicare (UE) 2019/1765 trebuie modificată în consecință.

(16) Având în vedere caracterul urgent al situației provocate de pandemia de COVID-19, prezenta decizie trebuie să se aplice începând din ziua următoare datei publicării în *Jurnalul Oficial al Uniunii Europene*.

(17) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 42 alineatul (1) din Regulamentul (UE) 2018/1725 și a emis un aviz la 9 iulie 2020.

(18) Măsurile prevăzute în prezenta decizie sunt conforme cu avizul comitetului instituit în temeiul articolului 16 din Directiva 2011/24/UE,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Decizia de punere în aplicare (UE) 2019/1765 se modifică după cum urmează:

1. La articolul 2 alineatul (1) se introduc următoarele litere (g), (h), (i), (j), (k), (l), (m), (n) și (o):

„(g) «utilizator al aplicației» înseamnă o persoană aflată în posesia unui dispozitiv inteligent care a descărcat și rulează o aplicație mobilă de depistare a contacților și de avertizare autorizată;

(h) «depistarea contacților» înseamnă măsurile puse în aplicare în vederea depistării persoanelor care au fost expuse la o sursă de amenințări transfrontaliere grave pentru sănătate în sensul articolului 3 litera (c) din Decizia 1082/2013/UE a Parlamentului European și a Consiliului (*);

([11]) Decizia (UE, Euratom) 2017/46 a Comisiei din 10 ianuarie 2017 privind securitatea sistemelor informatice și de comunicații în cadrul Comisiei Europene (JO L 6, 11.1.2017, p. 40). Comisia publică informații suplimentare privind standardele de securitate care se aplică tuturor sistemelor informatice ale Comisiei Europene la adresa https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_ro

(i) «aplicație mobilă națională de depistare a contacților și de avertizare» înseamnă o aplicație software aprobată la nivel național, care rulează pe dispozitive inteligente, în special pe telefoane inteligente, concepută de obicei pentru o interacțiune amplă și orientată cu resurse web, care prelucrează date de proximitate și alte informații contextuale colectate de mulți senzori aflați în dispozitivele inteligente, în scopul depistării contactelor cu persoane infectate cu SARS-CoV-2 și al alertării persoanelor care este posibil să fi fost expuse la SARS-CoV-2. Aceste aplicații mobile pot detecta prezența altor dispozitive utilizând Bluetooth și pot face schimb de informații cu servere *back-end* prin internet;

(j) «portalul federativ» înseamnă un portal de acces la rețea gestionat de Comisie prin intermediul unui instrument informatic securizat care primește, stochează și pune la dispoziție un set minim de date cu caracter personal între serverele *back-end* ale statelor membre, pentru a asigura interoperabilitatea aplicațiilor mobile naționale de depistare a contactelor și de avertizare;

(k) «cheie» înseamnă un identificator unic efemer legat de raportarea de către un utilizator al aplicației a faptului că a fost infectat cu SARS-CoV-2 sau că este posibil să fi fost expus la SARS-CoV-2;

(l) «verificarea infecției» înseamnă metoda aplicată pentru confirmarea unei infecții cu SARS-CoV-2, și anume dacă a fost autoraportată de utilizatorul aplicației sau a rezultat în urma confirmării de către o autoritate națională de sănătate sau a unui test de laborator;

(m) «țări de interes» înseamnă statul membru sau statele în care s-a aflat un utilizator al aplicației în ultimele 14 zile înainte de data încărcării cheilor și unde a descărcat aplicația mobilă națională de depistare a contacților și de avertizare autorizată și/sau unde a călătorit;

(n) «țara de origine a cheilor» înseamnă statul membru unde se află serverul *back-end* care a încărcat cheile în portalul federativ;

(o) «date din registrul de activitate» înseamnă o evidență automată a unei activități legate de schimbul de și accesul la date prelucrate prin intermediul portalului federativ, care arată în special tipul de activitate de prelucrare, data și ora activității de prelucrare, precum și identificatorul persoanei care prelucrează datele.

(*) Decizia nr. 1082/2013/UE a Parlamentului European și a Consiliului din 22 octombrie 2013 privind amenințările transfrontaliere grave pentru sănătate și de abrogare a Deciziei nr. 2119/98/CE (JO L 293, 5.11.2013, p. 1).”

2. La articolul 4 alineatul (1) se introduce următoarea literă (h):

„(h) să ofere orientări statelor membre cu privire la schimbul transfrontalier de date cu caracter personal, prin intermediul portalului federativ, dintre aplicațiile mobile naționale de depistare a contacților și de avertizare.”

3. La articolul 6 alineatul (1) se introduc următoarele litere (f) și (g):

„(f) dezvoltă, implementează și menține măsuri tehnice și organizatorice adecvate legate de securitatea transmiterii și găzduirii de date cu caracter personal în portalul federativ pentru a asigura interoperabilitatea aplicațiilor mobile naționale de depistare a contacților și de avertizare;

(g) sprijină rețeaua de e-sănătate în ceea ce privește stabilirea conformității tehnice și organizatorice a autorităților naționale cu cerințele pentru schimbul transfrontalier de date cu caracter personal prin portalul federativ, punând la dispoziție și efectuând testele și auditurile necesare. Auditorii Comisiei pot fi asistați de experți din statele membre.”

4. Articolul 7 se modifică după cum urmează:

(a) titlul se înlocuiește cu „Protecția datelor cu caracter personal prelucrate prin intermediul infrastructurii de servicii digitale de e-sănătate”;

(b) la alineatul (2), cuvântul „anexă” se înlocuiește cu „anexa I”.

5. Se introduce următorul articol 7a:

„*Articolul 7a*

Schimbul transfrontalier de date dintre aplicațiile mobile naționale de depistare a contacților și de avertizare prin intermediul portalului federativ

(1) Atunci când se face schimb de date cu caracter personal prin intermediul portalului federativ, prelucrarea se limitează la scopul de a facilita interoperabilitatea aplicațiilor mobile naționale de depistare a contacților și de avertizare în cadrul portalului federativ, precum și continuitatea depistării contacților într-un context transfrontalier.

(2) Datele cu caracter personal menționate la alineatul (3) se transmit către portalul federativ într-un format pseudonimizat.

(3) Datele cu caracter personal pseudonimizate care sunt schimbate și prelucrate în cadrul portalului federativ cuprind doar următoarele informații:

(a) cheile transmise de aplicațiile mobile naționale de depistare a contacților și de avertizare cu până la 14 zile înainte de data încărcării cheilor;

(b) datele din registrul de activitate asociate cheilor respective, în conformitate cu protocolul privind specificațiile tehnice utilizat în țara de origine a cheilor;

(c) verificarea infecției;

(d) țările de interes și țara de origine a cheilor.

(4) Organismele oficiale sau autoritățile naționale desemnate care prelucrează date cu caracter personal în cadrul portalului federativ sunt operatori asociați ai datelor prelucrate în cadrul portalului federativ. Responsabilitățile respective ale operatorilor asociați sunt alocate în conformitate cu anexa II. Fiecare stat membru care dorește să participe la schimbul de date transfrontalier dintre aplicațiile mobile naționale de depistare a contacților și de avertizare notifică Comisiei intenția sa, înainte de a se alătura acestui schimb de date, și indică organismul oficial sau autoritatea națională desemnat(ă) ca operator responsabil.

(5) Comisia este persoana împuternicită de operator în ceea ce privește datele cu caracter personal prelucrate în cadrul portalului federativ. În calitate de persoană împuternicită de operator, Comisia asigură securitatea prelucrării, inclusiv transmiterea și găzduirea, datelor cu caracter personal în cadrul portalului federativ și respectă obligațiile unei persoane împuternicite de operator, prevăzute în anexa III.

(6) Eficacitatea măsurilor tehnice și organizatorice de asigurare a securității prelucrării datelor cu caracter personal în cadrul portalului federativ este testată, analizată și evaluată periodic de Comisie și de autoritățile naționale autorizate să acceseze portalul federativ.

(7) Fără a se aduce atingere deciziei operatorilor asociați de a pune capăt prelucrării în cadrul portalului federativ, funcționarea portalului federativ este dezactivată cel târziu la 14 zile de la data la care toate aplicațiile mobile naționale de depistare a contacților și de avertizare au încetat să mai transmită chei prin intermediul portalului federativ.”

6. Anexa devine „Anexa I”.

7. Se adaugă anexele II și III, al căror text figurează în anexa la prezenta decizie.

Articolul 2

Prezenta decizie intră în vigoare în ziua următoare datei publicării în *Jurnalul Oficial al Uniunii Europene*.

Adoptată la Bruxelles, 15 iulie 2020.

Pentru Comisie
Președintele
Ursula VON DER LEYEN

ANEXĂ

La Decizia de punere în aplicare (UE) 2019/1765 se adaugă următoarele anexe II și III:

„ANEXA II

RESPONSABILITĂȚILE STATELOR MEMBRE PARTICIPANTE, ÎN CALITATE DE OPERATORI ASOCIAȚI AI PORTALULUI FEDERATIV DE PRELUCRARE TRANSFRONTALIERĂ ÎNTRE APLICAȚIILE MOBILE NAȚIONALE DE DEPISTARE A CONTACȚILOR ȘI DE AVERTIZARE

SECȚIUNEA 1

Subsecțiunea 1

Împărțirea responsabilităților

1. Operatorii asociați prelucrează datele cu caracter personal prin intermediul portalului federativ în conformitate cu specificațiile tehnice stabilite de rețeaua de e-sănătate ([1]).

2. Fiecare operator este responsabil pentru prelucrarea datelor cu caracter personal în cadrul portalului federativ în conformitate cu Regulamentul general privind protecția datelor și cu Directiva 2002/58/CE.

3. Fiecare operator stabilește un punct de contact cu o adresă de e-mail funcțională care va servi la comunicarea dintre operatorii asociați și dintre operatorii asociați și persoana împuternicită de operatori.

4. Un subgrup temporar instituit de rețeaua de e-sănătate în conformitate cu articolul 5 alineatul (4) are sarcina de a examina toate problemele care decurg din interoperabilitatea aplicațiilor mobile naționale de depistare a contacților și de avertizare și din operarea asociată a prelucrării aferente de date cu caracter personal, precum și de a facilita transmiterea de instrucțiuni coordonate Comisiei, în calitate de persoană împuternicită de operatori. Printre altele, operatorii pot colabora, în cadrul subgrupului temporar, în direcția unei abordări comune în ceea ce privește păstrarea datelor în serverele lor *back-end* naționale, ținând seama de perioada de păstrare prevăzută în cadrul portalului federativ.

5. Instrucțiunile către persoana împuternicită de operatori sunt transmise de oricare dintre punctele de contact ale operatorilor asociați, în acord cu celălalt operator asociat în cadrul subgrupului menționat mai sus.

6. Numai persoanele autorizate de organismele oficiale sau de autoritățile naționale desemnate pot accesa datele cu caracter personal ale utilizatorilor care au făcut obiectul schimburilor de date în cadrul portalului federativ.

7. Fiecare organism oficial sau autoritate națională desemnat(ă) încetează să mai fie operator asociat începând de la data retragerii participării sale la portalul federativ. Cu toate acestea, el/ea rămâne responsabil(ă) pentru prelucrările din cadrul portalului federativ care au avut loc înainte de retragerea sa.

Subsecțiunea 2

Responsabilități și roluri în ceea ce privește tratarea cererilor persoanelor vizate și informarea acestora

1. Fiecare operator furnizează utilizatorilor aplicației sale mobile naționale de depistare a contacților și de avertizare («persoanele vizate») informații cu privire la prelucrarea datelor lor cu caracter personal în cadrul portalului federativ în scopul interoperabilității transfrontaliere a aplicațiilor mobile naționale de depistare a contacților și de avertizare, în conformitate cu articolele 13 și 14 din Regulamentul general privind protecția datelor.

2. Fiecare operator acționează ca punct de contact pentru utilizatorii aplicației sale mobile naționale de depistare a contacților și de avertizare și tratează cererile legate de exercitarea drepturilor persoanelor vizate în conformitate cu Regulamentul general privind protecția datelor, depuse de utilizatorii respectivi sau de reprezentanții acestora. Fiecare operator desemnează un punct de contact specific pentru cererile primite de la persoanele vizate. Dacă un operator asociat primește o cerere din partea unei persoane vizate care nu intră în responsabilitatea sa, el transmite imediat această cerere operatorului asociat responsabil. Dacă li se solicită, operatorii asociați își acordă asistență reciprocă pentru tratarea cererilor persoanelor vizate și își răspund reciproc, fără întârzieri nejustificate și cel târziu în termen de 15 zile de la primirea unei cereri de asistență.

([1]) În special specificațiile de interoperabilitate pentru lanțurile de transmisie transfrontalieră dintre aplicații autorizate, din 16 iunie 2020, disponibile la adresa: https://ec.europa.eu/health/ehealth/key_documents_ro#anchor0.

3. Fiecare operator pune la dispoziția persoanelor vizate conținutul prezentei anexe, inclusiv măsurile prevăzute la punctele 1 și 2.

SECȚIUNEA 2

Gestionarea incidentelor de securitate, inclusiv a încălcării securității datelor cu caracter personal

1. Operatorii asociați își acordă asistență reciprocă pentru identificarea și tratarea oricăror incidente de securitate, inclusiv a încălcării securității datelor cu caracter personal, legate de prelucrarea în cadrul portalului federativ.

2. În special, operatorii asociați își notifică reciproc următoarele:

(a) orice riscuri potențiale sau reale la adresa disponibilității, confidențialității și/sau integrității datelor cu caracter personal care fac obiectul prelucrării în cadrul portalului federativ;

(b) orice incidente de securitate care sunt legate de operațiunea de prelucrare din cadrul portalului federativ;

(c) orice încălcare a securității datelor cu caracter personal, consecințele probabile ale încălcării securității datelor cu caracter personal și evaluarea riscurilor la adresa drepturilor și libertăților persoanelor fizice, precum și orice măsuri luate pentru a remedia încălcarea securității datelor cu caracter personal și pentru a atenua riscul la adresa drepturilor și libertăților persoanelor fizice;

(d) orice încălcare a garanțiilor tehnice și/sau organizaționale ale operațiunii de prelucrare în cadrul portalului federativ.

3. Operatorii asociați comunică orice încălcare a securității datelor cu caracter personal în ceea ce privește operațiunile de prelucrare din cadrul portalului federativ către Comisie, către autoritățile de supraveghere competente și, dacă este cazul, către persoanele vizate, în conformitate cu articolele 33 și 34 din Regulamentul (UE) 2016/679 sau în urma notificării de către Comisie.

SECȚIUNEA 3

Evaluarea impactului asupra protecției datelor

Dacă, pentru a-și îndeplini obligațiile prevăzute la articolele 35 și 36 din Regulamentul general privind protecția datelor, un operator are nevoie de informații de la un alt operator, cel dintâi transmite o cerere specifică la adresa de e-mail funcțională menționată în secțiunea 1 subsecțiunea 1 punctul 3. Operatorul destinatar depune toate eforturile pentru a furniza informațiile respective.

ANEXA III

RESPONSABILITĂȚILE COMISIEI, ÎN CALITATE DE PERSOANĂ ÎMPUERNICITĂ DE OPERATORI PENTRU PORTALUL FEDERATIV DE PRELUCRARE TRANSFRONTALIERĂ ÎNTRE APLICAȚIILE MOBILE NAȚIONALE DE DEPISTARE A CONTACȚILOR ȘI DE AVERTIZARE

Comisia:

1. Instituie și asigură o infrastructură de comunicații securizată și fiabilă care interconectează aplicațiile mobile naționale de depistare a contacților și de avertizare ale statelor membre care participă la portalul federativ. Pentru a-și îndeplini obligațiile care îi revin în calitate de persoană împuternicită de operatorii portalului federativ, Comisia poate angaja părți terțe ca subcontractanți; Comisia informează operatorii asociați cu privire la orice modificări preconizate în ceea ce privește adăugarea sau înlocuirea altor subcontractanți, oferind astfel operatorilor posibilitatea de a se opune în comun unor astfel de modificări, astfel cum se prevede în secțiunea 1 subsecțiunea 1 punctul 4 din anexa II. Comisia se asigură că acestor subcontractanți li se aplică aceleași obligații în materie de protecție a datelor ca cele prevăzute în prezenta decizie.

2. Prelucrează datele cu caracter personal, numai pe baza unor instrucțiuni documentate din partea operatorilor, cu excepția cazului în care legislația Uniunii sau a statului membru îi impune să facă acest lucru; în acest caz, Comisia informează operatorii cu privire la cerința legală respectivă, înainte de prelucrare, cu excepția cazului în care legislația interzice transmiterea unor astfel de informații din motive importante de interes public.

3. Prelucrarea de către Comisie implică următoarele:

(a) autentificarea serverelor *back-end* naționale, pe baza certificatelor serverelor *back-end* naționale;

(b) primirea datelor menționate la articolul 7a alineatul (3) din decizia de punere în aplicare, încărcate de serverele *back-end* naționale, prin furnizarea unei interfețe de programare a aplicațiilor care să permită serverelor *back-end* naționale să încarce datele relevante;

(c) stocarea datelor în portalul federativ, după primirea lor de la serverele *back-end* naționale;

(d) punerea la dispoziție a datelor pentru descărcarea de către serverele *back-end* naționale;

(e) ștergerea datelor atunci când toate serverele *back-end* participante le-au descărcat sau la 14 zile de la primirea lor, oricare dintre aceste date survine prima;

(f) după încheierea furnizării serviciului, ștergerea oricăror date rămase, cu excepția cazului în care legislația Uniunii sau a statului membru impune stocarea datelor cu caracter personal.

Persoana împuternicită de operatori ia măsurile necesare pentru a menține integritatea datelor prelucrate.

4. Ia toate măsurile de securitate organizaționale, fizice și logice de ultimă generație pentru a menține portalul federativ. În acest scop, Comisia:

(a) desemnează o entitate responsabilă pentru gestionarea securității la nivelul portalului federativ, comunică operatorilor informațiile sale de contact și asigură disponibilitatea sa de reacție la amenințări la adresa securității;

(b) își asumă responsabilitatea pentru securitatea portalului federativ;

(c) se asigură că toate persoanele cărora li se acordă acces la portalul federativ fac obiectul obligației contractuale, profesionale sau statutare de confidențialitate.

5. Ia toate măsurile de securitate necesare pentru a evita compromiterea bunei funcționări operaționale a serverelor *back-end* naționale. În acest scop, Comisia instituie proceduri specifice referitoare la conexiunea de la serverele *back-end* la portalul federativ. Acest lucru include:

(a) procedura de evaluare a riscurilor, pentru a identifica și a estima potențialele amenințări la adresa sistemului;

(b) procedura de audit și de reexaminare, pentru:

(i) a verifica corespondența dintre măsurile de securitate puse în aplicare și politica de securitate aplicabilă;

(ii) a controla periodic integritatea fișierelor sistemului, parametrii de securitate și autorizațiile acordate;

(iii) a desfășura activități de monitorizare în vederea depistării încălcărilor securității și a intruziunilor;

(iv) a pune în aplicare modificări cu scopul de a atenua deficiențele de securitate existente;

(v) permite, inclusiv la cererea operatorilor, și contribuie la efectuarea de audituri independente, inclusiv de inspecții, și de analize privind măsurile de securitate, sub rezerva unor condiții care respectă Protocolul nr. 7 la TFUE privind privilegiile și imunitățile Uniunii Europene ([2]);

([2]) Protocolul nr. 7 privind privilegiile și imunitățile Uniunii Europene (JO C 326, 26.10.2012, p. 266).

(c) modificarea procedurii de control pentru a documenta și a măsura impactul unei modificări înainte de punerea în aplicare a acesteia și pentru a informa operatorii cu privire la orice modificare care poate afecta comunicarea cu infrastructurile lor și/sau securitatea acestora;

(d) stabilirea unei proceduri de întreținere și de reparare, pentru a specifica regulile și condițiile care trebuie respectate atunci când trebuie efectuate lucrări de întreținere și/sau de reparare a echipamentelor;

(e) stabilirea unei proceduri privind incidentele de securitate, pentru a defini sistemul de raportare și de escaladare, pentru a informa fără întârziere operatorii, precum și Autoritatea Europeană pentru Protecția Datelor, cu privire la orice încălcare legată de datele cu caracter personal și pentru a defini un proces disciplinar care să trateze cazurile de încălcare a securității.

6. Ia măsuri de securitate fizică și/sau logică de ultimă generație pentru instalațiile care găzduiesc echipamentele portalului federativ și pentru controalele accesului la datele logice și controalele accesului de securitate. În acest scop, Comisia:

(a) asigură securitatea fizică pentru a stabili perimetre de securitate distincte și pentru a permite depistarea încălcărilor;

(b) controlează accesul la instalații și menține un registru al vizitatorilor în scopuri de trasabilitate;

(c) se asigură că persoanele din exterior cărora li s-a acordat accesul în incinte sunt escortate de personal autorizat în mod corespunzător;

(d) se asigură că nu se pot adăuga, înlocui sau elimina echipamente fără autorizarea prealabilă a organismelor responsabile desemnate;

(e) controlează accesul dintre serverele *back-end* naționale și portalul federativ;

(f) se asigură că persoanele care accesează portalul federativ sunt identificate și autentificate;

(g) reexaminează drepturile de autorizare legate de accesul la portalul federativ în cazul unei încălcări a securității care afectează această infrastructură;

(h) menține integritatea informațiilor transmise prin intermediul portalului federativ;

(i) pune în aplicare măsuri de securitate tehnice și organizaționale pentru a preveni accesul neautorizat la date cu caracter personal;

(j) pune în aplicare, ori de câte ori este necesar, măsuri pentru blocarea accesului neautorizat la portalul federativ din domeniul autorităților naționale (și anume, blocarea unei locații/adrese IP).

7. Ia măsuri pentru protejarea domeniului său, inclusiv întreruperea conexiunilor, în caz de abateri semnificative de la principiile și conceptele privind calitatea sau securitatea.

8. Menține un plan de gestionare a riscurilor aferent domeniului său de responsabilitate.

9. Monitorizează – în timp real – performanța tuturor componentelor de servicii ale portalului federativ, elaborează statistici periodice și păstrează evidențe.

10. Oferă sprijin în limba engleză pentru toate serviciile portalului federativ, 24 de ore din 24 și 7 zile din 7, prin telefon, e-mail sau portal web, și acceptă apeluri din partea apelanților autorizați: coordonatorii portalului federativ și serviciile lor de asistență respective, responsabilii de proiect și persoanele desemnate din cadrul Comisiei.

11. Oferă asistență operatorilor, prin măsuri tehnice și organizaționale adecvate, în măsura posibilului, pentru îndeplinirea obligației operatorului de a răspunde la cererile de exercitare a drepturilor persoanelor vizate prevăzute în capitolul III din Regulamentul general privind protecția datelor.

12. Sprijină operatorii prin furnizarea de informații privind portalul federativ, în vederea implementării obligațiilor prevăzute la articolele 32, 35 și 36 din Regulamentul general privind protecția datelor.

13. Se asigură că datele prelucrate în cadrul portalului federativ sunt neinteligibile pentru orice persoană care nu este autorizată să le acceseze.

14. Ia toate măsurile relevante pentru a preveni accesul neautorizat al operatorilor portalului federativ la datele transmise.

15. Ia măsuri pentru a facilita interoperabilitatea și comunicarea dintre operatorii desemnați ai portalului federativ.

16. Ține evidența activităților de prelucrare efectuate în numele operatorilor în conformitate cu articolul 31 alineatul (2) din Regulamentul (UE) 2018/1725.”