►B

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

[notificată cu numărul C(2019) 7460]

(Text cu relevanță pentru SEE)

(JO L 270, 24.10.2019, p. 83)

Astfel cum a fost modificată prin:

		Jurnalul Oficial		
		NR.	Pagina	Data
►M1	Decizia de punere în aplicare (UE) 2020/1023 a Comisiei din 15 iulie 2020	L 227 I	1	16.7.2020

▼B

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

[notificată cu numărul C(2019) 7460]

(Text cu relevanță pentru SEE)

Articolul 1

Obiect

Prezenta decizie stabilește normele necesare pentru înființarea, gestionarea și funcționarea rețelei de e-sănătate a autorităților naționale responsabile cu e-sănătatea, astfel cum este prevăzut la articolul 14 din Directiva 2011/24/UE.

Articolul 2

Definiții

(1) În sensul prezentei decizii:

(a) „rețeaua de e-sănătate” înseamnă rețeaua voluntară care conectează autoritățile naționale responsabile cu e-sănătatea, desemnate de statele membre, și care urmărește obiectivele stabilite la articolul 14 din Directiva 2011/24/UE;

(b) „puncte de contact naționale pentru e-sănătate” înseamnă canale organizatorice și tehnice pentru furnizarea de servicii transfrontaliere de informații privind e-sănătatea sub responsabilitatea statelor membre;

(c) „servicii transfrontaliere de informații privind e-sănătatea” înseamnă serviciile existente care sunt prelucrate prin intermediul punctelor de contact naționale pentru e-sănătate și printr-o platformă centrală de servicii dezvoltată de Comisie în scopul asistenței medicale transfrontaliere;

(d) „infrastructura de servicii digitale de e-sănătate pentru serviciile transfrontaliere de informații privind e-sănătatea” înseamnă infrastructura care permite furnizarea de servicii transfrontaliere de informații privind e-sănătatea prin intermediul punctelor de contact naționale pentru e-sănătate și al platformei centrale europene de servicii. Această infrastructură include atât servicii generice, astfel cum sunt definite la articolul 2 alineatul (2) litera (e) din Regulamentul (UE) nr. 283/2014, dezvoltate de statele membre, cât și o platformă centrală de servicii, astfel cum este definită la articolul 2 alineatul (2) litera (d) din același regulament, dezvoltată de Comisie;

(e) „alte servicii europene de e-sănătate partajate” înseamnă servicii digitale care pot fi dezvoltate în cadrul rețelei de e-sănătate și partajate între statele membre;

▼B

(f) „model de guvernanţă” înseamnă un set de norme privind desemnarea organismelor care participă la procesele decizionale referitoare la infrastructura de servicii digitale de e-sănătate pentru serviciile transfrontaliere de informaţii privind e-sănătatea sau la alte servicii europene de e-sănătate partajate, dezvoltate în cadrul reţelei de e-sănătate, precum și descrierea acestor procese;

▼M1

(g) „utilizator al aplicaţiei” înseamnă o persoană aflată în posesia unui dispozitiv inteligent care a descărcat și rulează o aplicaţie mobilă de depistare a contacţilor și de avertizare autorizată;

(h) „depistarea contacţilor” înseamnă măsurile puse în aplicare în vederea depistării persoanelor care au fost expuse la o sursă de ameninţări transfrontaliere grave pentru sănătate în sensul articolului 3 litera (c) din Decizia 1082/2013/UE a Parlamentului European și a Consiliului ([1]);

(i) „aplicaţie mobilă naţională de depistare a contacţilor și de avertizare” înseamnă o aplicaţie software aprobată la nivel naţional, care rulează pe dispozitive inteligente, în special pe telefoane inteligente, concepută de obicei pentru o interacţiune amplă și orientată cu resurse web, care prelucrează date de proximitate și alte informaţii contextuale colectate de mulţi senzori aflaţi 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 aplicaţii mobile pot detecta prezenţa altor dispozitive utilizând Bluetooth și pot face schimb de informaţii cu servere *back-end* prin internet;

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

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

(l) „verificarea infecţiei” înseamnă metoda aplicată pentru confirmarea unei infecţii cu SARS-CoV-2, și anume dacă a fost autoraportată de utilizatorul aplicaţiei sau a rezultat în urma confirmării de către o autoritate naţională de sănătate sau a unui test de laborator;

(m) „ţări de interes” înseamnă statul membru sau statele în care s-a aflat un utilizator al aplicaţiei în ultimele 14 zile înainte de data încărcării cheilor și unde a descărcat aplicaţia mobilă naţională de depistare a contacţilor și de avertizare autorizată și/sau unde a călătorit;

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

▼M1

(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.

▼B

(2) Definițiile de la articolul 4 punctele 1, 2, 7 și 8 din Regulamentul (UE) 2016/679 se aplică în consecință.

Articolul 3

Componența rețelei de e-sănătate

(1) Membrii rețelei de e-sănătate sunt autoritățile statelor membre responsabile cu e-sănătatea, desemnate de statele membre care participă la rețeaua de e-sănătate.

(2) Statele membre care doresc să participe la rețeaua de e-sănătate notifică în scris Comisia cu privire la:

(a) decizia de a participa la rețeaua de e-sănătate;

(b) autoritatea națională responsabilă cu e-sănătatea, care va deveni membru al rețelei de e-sănătate, precum și numele reprezentantului și cel al supleantului său.

(3) Membrii notifică în scris Comisiei următoarele:

(a) decizia lor de a se retrage din rețeaua de e-sănătate;

(b) orice modificare a informațiilor menționate la alineatul (2) litera (b).

(4) Comisia pune la dispoziția publicului lista membrilor care participă la rețeaua de e-sănătate.

Articolul 4

Activitățile rețelei de e-sănătate

(1) În vederea realizării obiectivului menționat la articolul 14 alineatul (2) litera (a) din Directiva 2011/24/UE, rețeaua de e-sănătate poate, în special:

(a) să faciliteze o interoperabilitate sporită a sistemelor naționale de tehnologie a informației și comunicațiilor și transferabilitatea transfrontalieră a datelor medicale electronice în cadrul asistenței medicale transfrontaliere;

(b) să ofere orientări statelor membre, în cooperare cu alte autorități de supraveghere competente, în legătură cu schimbul de date medicale între statele membre și cu asigurarea posibilității pentru cetățeni de a avea acces la propriile date medicale și de a le partaja;

▼B

(c) să ofere orientări statelor membre și să faciliteze schimbul de bune practici în ceea ce privește dezvoltarea unor servicii digitale de sănătate diferite, cum ar fi telemedicina, m-sănătatea sau noile tehnologii în domeniul volumelor mari de date și al inteligenţei artificiale, ţinând seama de acţiunile în curs de desfășurare la nivelul UE;

(d) să ofere orientări statelor membre în ceea ce privește sprijinirea promovării sănătăţii, a prevenirii bolilor și a îmbunătăţirii furnizării de asistenţă medicală printr-o mai bună utilizare a datelor medicale și prin îmbunătăţirea competenţelor digitale ale pacienţilor și ale profesioniștilor în domeniul sănătăţii;

(e) să ofere orientări statelor membre și să faciliteze schimbul voluntar de bune practici în domeniul investiţiilor în infrastructura digitală;

(f) să ofere orientări statelor membre, în colaborare cu alte organisme și părţi interesate relevante, cu privire la cazurile de utilizare necesare pentru interoperabilitatea clinică și instrumentele pentru realizarea acesteia;

(g) să ofere orientări membrilor în ceea ce privește securitatea infrastructurii de servicii digitale de e-sănătate pentru serviciile transfrontaliere de informaţii privind e-sănătatea sau a altor servicii europene de e-sănătate partajate dezvoltate în cadrul reţelei de e-sănătate, ţinând seama de legislaţia și documentele elaborate la nivelul Uniunii, în special din domeniul securităţii, precum și de recomandările din domeniul securităţii cibernetice, în strânsă cooperare cu Grupul de cooperare în materie de securitate a reţelelor și a informaţiilor și cu Agenţia Uniunii Europene pentru Securitatea Reţelelor și a Informaţiilor, precum și cu autorităţile naţionale, dacă este cazul;

▼M1

(h) să ofere orientări statelor membre cu privire la schimbul transfrontalier de date cu caracter personal, prin intermediul portalului federativ, dintre aplicaţiile mobile naţionale de depistare a contacţilor și de avertizare.

▼B

(2) La elaborarea orientărilor privind metodele eficace pentru a permite utilizarea informaţiilor medicale pentru sănătatea publică și pentru cercetare menţionate la articolul 14 alineatul (2) litera (b) punctul (ii) din Directiva 2011/24/UE, reţeaua de e-sănătate ţine seama de orientările adoptate de Comitetul european pentru protecţia datelor și, dacă este cazul, îl consultă. Aceste orientări pot viza, de asemenea, informaţiile schimbate prin intermediul infrastructurii de servicii digitale de e-sănătate pentru serviciile transfrontaliere de informaţii privind e-sănătatea sau al altor servicii europene de e-sănătate partajate.

Articolul 5

Funcţionarea reţelei de e-sănătate

(1) Reţeaua de e-sănătate își stabilește propriul regulament de procedură cu majoritatea simplă a membrilor.

(2) Reţeaua de e-sănătate adoptă un program de lucru multianual și un instrument de evaluare privind punerea în aplicare a acestui program.

▼B

(3) În vederea îndeplinirii sarcinilor sale, reţeaua de e-sănătate poate înfiinţa subgrupuri permanente pentru sarcini specifice, în special referitoare la infrastructura de servicii digitale de e-sănătate pentru serviciile transfrontaliere de informaţii privind e-sănătatea sau la celelalte servicii europene de e-sănătate partajate, dezvoltate în cadrul reţelei de e-sănătate.

(4) De asemenea, reţeaua de e-sănătate poate înfiinţa subgrupuri temporare, inclusiv cu experţi, pentru examinarea unor aspecte specifice, pe baza unui mandat definit de reţeaua de e-sănătate. Aceste subgrupuri sunt desfiinţate imediat după ce și-au îndeplinit mandatul.

(5) În cazul în care membrii reţelei de e-sănătate decid să își intensifice cooperarea în unele domenii care intră în sfera sarcinilor reţelei de e-sănătate, aceștia ar trebui să cadă de acord asupra normelor acestei cooperări intensificate și să le respecte.

(6) În îndeplinirea obiectivelor sale, reţeaua de e-sănătate lucrează în strânsă cooperare cu acţiunile comune care sprijină activităţile reţelei de e-sănătate, acolo unde există astfel de acţiuni comune, cu părţile interesate sau cu alte organisme ori mecanisme de sprijin implicate și ţine seama de rezultatele obţinute în cadrul acestor activităţi.

(7) Reţeaua de e-sănătate elaborează, împreună cu Comisia, modelele de guvernanţă ale infrastructurii de servicii digitale de e-sănătate pentru serviciile transfrontaliere de informaţii privind e-sănătatea și participă la această guvernanţă prin:

(i) stabilirea de comun acord a priorităţilor infrastructurii de servicii digitale de e-sănătate și prin supravegherea funcţionării lor;

(ii) elaborarea de orientări și cerinţe privind funcţionarea, inclusiv selectarea standardelor utilizate pentru infrastructura de servicii digitale de e-sănătate pentru serviciile transfrontaliere de informaţii privind e-sănătatea;

(iii) ajungerea la un acord privind acordarea permisiunii ca membrii reţelei de e-sănătate să iniţieze și să continue schimbul de date medicale electronice prin intermediul infrastructurii de servicii digitale de e-sănătate pentru serviciile transfrontaliere de informaţii privind e-sănătatea, prin punctele lor de contact naţionale pentru e-sănătate, pe baza conformităţii lor cu cerinţele stabilite de reţeaua de e-sănătate, astfel cum a fost evaluată în cadrul testelor furnizate și a auditurilor efectuate de Comisie;

(iv) aprobarea planului anual de lucru pentru infrastructura de servicii digitale de e-sănătate pentru serviciile transfrontaliere de informaţii privind e-sănătatea.

(8) Reţeaua de e-sănătate poate elabora, împreună cu Comisia, modelele de guvernanţă ale altor servicii europene de e-sănătate partajate, dezvoltate în cadrul reţelei de e-sănătate și poate participa la guvernanţa acestora. De asemenea, reţeaua poate să stabilească prioritățile, împreună cu Comisia, și să elaboreze orientări pentru funcţionarea acestor servicii europene de e-sănătate partajate.

▼B

(9) Regulamentul de procedură poate prevedea posibilitatea ca ţările, altele decât statele membre, care aplică Directiva 2011/24/UE, să participe la reuniunile reţelei de e-sănătate în calitate de observatori.

(10) Membrii reţelei de e-sănătate și reprezentanţii acestora, precum și experţii și observatorii invitaţi trebuie să respecte obligaţiile privind secretul profesional prevăzute la articolul 339 din tratat, precum și normele în materie de securitate ale Comisiei referitoare la protecţia informaţiilor clasificate ale UE, astfel cum sunt prevăzute în Decizia (UE, Euratom) 2015/444 a Comisiei [1]. În cazul nerespectării acestor obligaţii, președintele reţelei de e-sănătate poate lua toate măsurile adecvate prevăzute în regulamentul de procedură.

Articolul 6

Relaţia dintre reţeaua de e-sănătate și Comisie

(1) Comisia:

(a) participă la reuniunile reţelei de e-sănătate și asigură copreședinţia acestora împreună cu reprezentantul membrilor;

(b) cooperează cu reţeaua de e-sănătate și îi oferă sprijin în legătură cu activităţile sale;

(c) furnizează servicii de secretariat reţelei de e-sănătate;

(d) elaborează, pune în aplicare și menţine măsuri tehnice și organizatorice adecvate legate de serviciile centrale ale infrastructurii de servicii digitale de e-sănătate pentru serviciile transfrontaliere de informaţii privind e-sănătatea;

(e) sprijină reţeaua de e-sănătate în stabilirea conformităţii tehnice și organizatorice a punctelor de contact naţionale pentru e-sănătate cu cerinţele pentru schimbul transfrontalier de date medicale, furnizând și efectuând testele și auditurile necesare. Auditorii Comisiei pot fi asistaţi de către experţi din statele membre;

▼M1

(f) dezvoltă, implementează și menţine măsuri tehnice și organizatorice adecvate legate de securitatea transmiterii și găzduirii de date cu caracter personal în portalul federativ pentru a asigura interoperabilitatea aplicaţiilor mobile naţionale de depistare a contacţilor și de avertizare;

(g) sprijină reţeaua de e-sănătate în ceea ce privește stabilirea conformităţii tehnice și organizatorice a autorităţilor naţionale cu cerinţele pentru schimbul transfrontalier de date cu caracter personal prin portalul federativ, punând la dispoziţie și efectuând testele și auditurile necesare. Auditorii Comisiei pot fi asistaţi de experţi din statele membre.

▼B

(2) Comisia poate participa la reuniunile subgrupurilor din cadrul reţelei de e-sănătate.

(3) Comisia poate consulta reţeaua de e-sănătate cu privire la chestiuni referitoare la domeniul e-sănătăţii la nivelul Uniunii și la schimbul de bune practici în materie de e-sănătate.

[1] Decizia (UE, Euratom) 2015/444 a Comisiei din 13 martie 2015 privind normele de securitate pentru protecţia informaţiilor UE clasificate (JO L 72, 17.3.2015, p. 53).

▼B

(4) Comisia pune la dispoziţia publicului informaţii privind activităţile desfășurate de reţeaua de e-sănătate.

Articolul 7

▼M1

Protecţia datelor cu caracter personal prelucrate prin intermediul infrastructurii de servicii digitale de e-sănătate

▼B

(1) Statele membre, reprezentate de autorităţile naţionale relevante sau de alte organisme desemnate, sunt considerate drept operatori ai datelor cu caracter personal pe care le procesează prin intermediul infrastructurii de servicii digitale de e-sănătate pentru serviciile transfrontaliere de informaţii privind e-sănătatea și trebuie să aloce în mod clar și transparent responsabilităţile între operatori.

(2) Comisia este considerată persoană împuternicită de operator pentru datele cu caracter personal ale pacienţilor prelucrate prin intermediul infrastructurii de servicii digitale de e-sănătate pentru serviciile transfrontaliere de informaţii privind e-sănătatea. În calitatea sa de persoană împuternicită de operator, Comisia gestionează serviciile centrale ale infrastructurii de servicii digitale de e-sănătate pentru serviciile transfrontaliere de informaţii privind e-sănătatea și respectă obligaţiile unei persoane împuternicite de operator prevăzute în ►M1 anexa I ◄ la prezenta decizie. Comisia nu are acces la datele cu caracter personal ale pacienţilor prelucrate prin intermediul infrastructurii de servicii digitale de e-sănătate pentru serviciile transfrontaliere de informaţii privind e-sănătatea.

(3) Comisia este considerată operator al prelucrării datelor cu caracter personal necesare pentru a acorda și a gestiona drepturile de acces la serviciile centrale ale infrastructurii de servicii digitale de e-sănătate pentru serviciile transfrontaliere de informaţii privind e-sănătatea. Aceste date sunt datele de contact ale utilizatorilor, inclusiv numele, prenumele și adresa de e-mail și afilierea acestora.

▼M1

Articolul 7a

Schimbul transfrontalier de date dintre aplicaţiile mobile naţionale de depistare a contacţilor 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 aplicaţiilor mobile naţionale de depistare a contacţilor și de avertizare în cadrul portalului federativ, precum și continuitatea depistării contacţilor într-un context transfrontalier.

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

▼M1

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

(a) cheile transmise de aplicaţiile mobile naţionale de depistare a contacţilor 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 specificaţiile tehnice utilizat în ţara de origine a cheilor;

(c) verificarea infecţiei;

(d) ţările de interes și ţara de origine a cheilor.

(4) Organismele oficiale sau autoritățile naţionale desemnate care prelucrează date cu caracter personal în cadrul portalului federativ sunt operatori asociaţi ai datelor prelucrate în cadrul portalului federativ. Responsabilităţile respective ale operatorilor asociaţi sunt alocate în conformitate cu anexa II. Fiecare stat membru care dorește să participe la schimbul de date transfrontalier dintre aplicaţiile mobile naţionale de depistare a contacţilor și de avertizare notifică Comisiei intenţia sa, înainte de a se alătura acestui schimb de date, și indică organismul oficial sau autoritatea naţională 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 obligaţiile unei persoane împuternicite de operator, prevăzute în anexa III.

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

(7) Fără a se aduce atingere deciziei operatorilor asociaţi de a pune capăt prelucrării în cadrul portalului federativ, funcţionarea portalului federativ este dezactivată cel târziu la 14 zile de la data la care toate aplicaţiile mobile naţionale de depistare a contacţilor și de avertizare au încetat să mai transmită chei prin intermediul portalului federativ.

▼B

Articolul 8

Cheltuieli

(1) Participanţii la activităţile reţelei de e-sănătate nu sunt remuneraţi de Comisie pentru serviciile lor.

▼B

(2) Cheltuielile de deplasare și de ședere suportate de participanţii la activităţile reţelei de e-sănătate sunt rambursate de Comisie în conformitate cu dispoziţiile în vigoare în cadrul Comisiei pentru rambursarea cheltuielilor suportate de persoanele din afara Comisiei invitate să participe la reuniuni în calitate de experţi. Cheltuielile respective se rambursează în limitele creditelor disponibile alocate în cadrul procedurii anuale de alocare a resurselor.

Articolul 9

Abrogare

Decizia de punere în aplicare 2011/890/UE se abrogă. Trimiterile la decizia abrogată se interpretează ca trimiteri la prezenta decizie.

Articolul 10

Destinatarii

Prezenta decizie se adresează statelor membre.

▼M1

ANEXĂ I

▼B

RESPONSABILITĂȚILE COMISIEI ÎN CALITATE DE PERSOANĂ ÎMPUTERNICITĂ DE OPERATOR PENTRU INFRASTRUCTURA DE SERVICII DIGITALE DE e-SĂNĂTATE PENTRU SERVICIILE TRANSFRONTALIERE DE INFORMAȚII PRIVIND e-SĂNĂTATEA

Comisia:

1. Stabilește și asigură o infrastructură de comunicații sigură și fiabilă, care interconectează rețelele membrilor rețelei de e-sănătate implicate în infrastructura de servicii digitale de e-sănătate pentru serviciile transfrontaliere de informații privind e-sănătatea („infrastructura securizată centrală de comunicații”). În vederea îndeplinirii obligațiilor care îi revin, Comisia poate recurge la părți terțe. Comisia se asigură că aceleași obligații în materie de protecție a datelor prevăzute în prezenta decizie se aplică acestor părți terțe.

2. Configurează o parte din infrastructura securizată centrală de comunicații, astfel încât punctele de contact naționale pentru e-sănătate să poată face schimb de informații într-un mod sigur, fiabil și eficient.

3. Comisia prelucrează datele cu caracter personal pe baza instrucțiunilor documentate primite de la operatori.

4. Ia toate măsurile de securitate organizațională, fizică și logică necesare pentru a întreține infrastructura securizată centrală de comunicații. În acest scop, Comisia:

   (a) desemnează o entitate responsabilă pentru managementul securității la nivelul infrastructurii securizate centrale de comunicații, comunică operatorilor de date informațiile sale de contact și asigură disponibilitatea de reacție a acesteia la amenințări la adresa securității;

   (b) își asumă responsabilitatea pentru securitatea infrastructurii securizate centrale de comunicații;

   (c) se asigură că toate persoanele cărora li se acordă acces la infrastructura securizată centrală de comunicații fac obiectul obligației contractuale, profesionale sau statutare de confidențialitate;

   (d) se asigură că personalul care are acces la informații clasificate îndeplinește criteriile corespunzătoare de autorizare și confidențialitate.

5. Ia toate măsurile de securitate necesare pentru a evita compromiterea bunei funcționări operaționale a domeniului celeilalte părți. În acest scop, Comisia instituie procedurile specifice legate de conectarea la infrastructura securizată centrală de comunicații. Aceste informații cuprind:

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

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

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

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

      (iii) a întreprinde acțiuni de monitorizare în vederea depistării încălcărilor securității și a intruziunilor;

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

▼B

(v) a defini condițiile pentru a autoriza, inclusiv la cererea operatorilor, și a contribui la efectuarea de audituri independente, inclusiv de inspecții și de analize privind măsurile de securitate;

(c) procedura de control al modificărilor, cu scopul de a documenta și a măsura impactul unei modificări înainte de punerea în aplicare a acesteia și a informa punctele de contact naționale pentru e-sănătate cu privire la orice modificare care poate afecta comunicarea cu celelalte infrastructuri naționale și/sau securitatea acestora;

(d) procedura de întreținere și reparare, pentru a specifica regulile și condițiile care trebuie urmate atunci când ar trebui să fie efectuate lucrări de întreținere și/sau reparare a echipamentelor;

(e) procedura privind incidentele de securitate, pentru a defini sistemul de raportare și escaladare, pentru a informa fără întârziere administrația națională responsabilă, precum și Autoritatea Europeană pentru Protecția Datelor cu privire la orice încălcare a securității și pentru a defini un proces disciplinar care să trateze cazurile de încălcare a securității.

6. Ia măsuri de securitate fizică și/sau logică pentru instalațiile care găzduiesc echipamentele infrastructurii securizate centrale de comunicații și pentru controalele accesului la datele logice și controalele accesului securizat. În acest scop, Comisia:

(a) asigură securitatea fizică pentru a stabili perimetre de securitate distinctive 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 al organizației sale;

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

(e) controlează accesul la și dintr-o altă rețea (alte rețele) interconectată (interconectate) la infrastructura securizată centrală de comunicații;

(f) se asigură că persoanele care accesează infrastructura securizată centrală de comunicații sunt identificate și autentificate;

(g) revizuiește drepturile de autorizare legate de accesul la infrastructura securizată centrală de comunicații în cazul unei încălcări a securității care afectează această infrastructură;

(h) păstrează integritatea informațiilor transmise prin intermediul infrastructurii securizate centrale de comunicații;

(i) pune în aplicare măsuri de securitate tehnică și organizațională 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 infrastructura securizată centrală de comunicații din domeniul punctelor de contact naționale pentru e-sănătate (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.

▼B

9. Monitorizează – în timp real – performanţa tuturor componentelor de servicii ale serviciilor infrastructurii sale securizate centrale de comunicaţii, elaborează statistici periodice și păstrează evidenţe.

10. Asigură asistenţă în limba engleză 24/7 prin telefon, e-mail sau portal web pentru toate serviciile infrastructurii securizate centrale de comunicaţii și acceptă apeluri din partea apelanţilor autorizaţi: coordonatorii infrastructurii securizate centrale de comunicaţii și birourile lor de asistenţă („helpdesk”), responsabilii de proiect și persoanele desemnate din partea Comisiei.

11. Sprijinirea operatorilor prin furnizarea de informaţii privind infrastructura securizată centrală de comunicaţii a infrastructurii de servicii digitale de e-sănătate pentru serviciile transfrontaliere de informaţii privind e-sănătatea, în vederea punerii în aplicare a obligaţiilor prevăzute la articolele 35 și 36 din Regulamentul (UE) 2016/679.

12. Se asigură că datele transferate în cadrul infrastructurii securizate centrale de comunicaţii sunt criptate.

13. Ia toate măsurile relevante pentru a preveni accesul neautorizat al operatorilor infrastructurii securizate centrale de comunicaţii la datele transferate.

14. Ia măsuri pentru a facilita interoperabilitatea și comunicarea între administraţiile naţionale competente desemnate ale infrastructurii securizate centrale de comunicaţii.

▼M1

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

([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.

▼M1

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.

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.

▼M1

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:

▼M1

(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 ([1]);

(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:

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

▼**M1**

(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.

▼**M1**

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.