DECIZIA DE PUNERE ÎN APLICARE (UE) 2022/483 A COMISIEI

din 21 martie 2022

de modificare a Deciziei de punere în aplicare (UE) 2021/1073 de stabilire a specificațiilor tehnice și a regulilor de punere în aplicare a cadrului de încredere pentru certificatul digital al UE privind COVID instituit prin Regulamentul (UE) 2021/953 al Parlamentului European și al Consiliului

(Text cu relevanță pentru SEE)

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) 2021/953 al Parlamentului European și al Consiliului din 14 iunie 2021 privind cadrul pentru eliberarea, verificarea și acceptarea certificatelor interoperabile de vaccinare, testare și vindecare de COVID-19 (certificatul digital al UE privind COVID) pentru a facilita libera circulație pe durata pandemiei de COVID-19 ([1]), în special articolul 9 alineatul (1),

întrucât:

(1) Regulamentul (UE) 2021/953 instituie certificatul digital al UE privind COVID care asigură dovada că o persoană a primit un vaccin împotriva COVID-19, un rezultat negativ la testul de depistare a infecției cu virusul SARS-CoV-2 sau s-a vindecat de COVID-19, cu scopul de a facilita exercitarea de către titulari a dreptului lor la liberă circulație în timpul pandemiei de COVID-19.

(2) Regulamentul (UE) 2021/954 al Parlamentului European și al Consiliului ([2]) prevede că statele membre trebuie să aplice normele prevăzute în Regulamentul (UE) 2021/953 resortisanților țărilor terțe care nu intră sub incidența regulamentului respectiv, dar care se află în situație de ședere legală sau au reședință legală pe teritoriul lor și care au dreptul de a călători în alte state membre în conformitate cu dreptul Uniunii.

(3) Recomandarea (UE) 2022/290 a Consiliului de modificare a Recomandării (UE) 2020/912 privind restricția temporară asupra călătoriilor neesențiale către UE și posibila eliminare a acestei restricții ([3]) prevede că resortisanții țărilor terțe care doresc să efectueze călătorii neesențiale dintr-o țară terță către Uniune ar trebui să dețină o dovadă valabilă a vaccinării sau a vindecării, cum ar fi un certificat digital al UE privind COVID sau un certificat privind COVID-19 eliberat de o țară terță care face obiectul unui act de punere în aplicare adoptat în temeiul articolului 8 alineatul (2) din Regulamentul (UE) 2021/953.

(4) Pentru ca certificatul digital al UE privind COVID să fie operațional în întreaga Uniune, Comisia a adoptat Decizia de punere în aplicare (UE) 2021/1073 ([4]), care stabilește specificații tehnice și reguli care să asigure completarea, eliberarea în condiții de siguranță și verificarea certificatelor digitale ale UE privind COVID, garantarea protecției datelor cu caracter personal, stabilirea structurii comune a identificatorului unic al certificatului și emiterea unui cod de bare valabil, securizat și interoperabil.

(5) În conformitate cu articolul 4 din Regulamentul (UE) 2021/953, Comisia și statele membre trebuie să instituie și să mențină un cadru de încredere pentru certificatul digital al UE privind COVID. Acest cadru de încredere poate sprijini schimbul bilateral de liste cu certificate revocate, care conțin identificatorii unici ai certificatelor revocate.

([1]) JO L 211, 15.6.2021, p. 1.

([2]) Regulamentul (UE) 2021/954 al Parlamentului European și al Consiliului din 14 iunie 2021 privind cadrul pentru eliberarea, verificarea și acceptarea certificatelor interoperabile de vaccinare, testare și vindecare de COVID-19 (certificatul digital al UE privind COVID) referitor la resortisanții țărilor terțe aflați în situație de ședere legală sau care au reședință legală pe teritoriul statelor membre, pe durata pandemiei de COVID-19 (JO L 211, 15.6.2021, p. 24).

([3]) Recomandarea (UE) 2022/290 a Consiliului din 22 februarie 2022 de modificare a Recomandării (UE) 2020/912 privind restricția temporară asupra călătoriilor neesențiale către UE și posibila eliminare a acestei restricții (JO L 43, 24.2.2022, p. 79).

([4]) Decizia de punere în aplicare (UE) 2021/1073 a Comisiei din 28 iunie 2021 de stabilire a specificațiilor tehnice și a regulilor de punere în aplicare a cadrului de încredere pentru certificatul digital al UE privind COVID instituit prin Regulamentul (UE) 2021/953 al Parlamentului European și al Consiliului (JO L 230, 30.6.2021, p. 32).

(6) La 1 iulie 2021, a devenit operațional gateway-ul pentru certificatele digitale ale UE privind COVID („gateway-ul”), care reprezintă partea centrală a cadrului de încredere și care permite schimbul fiabil și în condiții de siguranță între statele membre de chei publice utilizate pentru verificarea certificatelor digitale ale UE privind COVID.

(7) Datorită implementării lor cu succes și pe scară largă, certificatele digitale ale UE privind COVID au devenit o țintă pentru autorii fraudelor care încearcă să găsească modalități de a elibera certificate frauduloase. Prin urmare, aceste certificate frauduloase trebuie revocate. În plus, anumite certificate digitale ale UE privind COVID pot fi revocate de statele membre la nivel național din motive medicale și de sănătate publică, de exemplu deoarece un lot de vaccinuri administrate s-a dovedit ulterior a fi defectuos.

(8) Deși sistemul de certificate digitale ale UE privind COVID este capabil să depisteze imediat certificatele falsificate, certificatele autentice care sunt eliberate ilegal pe baza unor documente false, accesul neautorizat sau cu intenție frauduloasă nu pot fi detectate în alte state membre, cu excepția cazului în care listele cu certificatele revocate generate la nivel național fac obiectul unui schimb între statele membre. Același lucru este valabil și pentru certificatele care au fost revocate din motive medicale și de sănătate publică. Faptul că aplicațiile de verificare ale statelor membre nu detectează certificatele revocate de alte state membre reprezintă o amenințare pentru sănătatea publică și subminează încrederea cetățenilor în sistemul de certificate digitale ale UE privind COVID.

(9) Astfel cum se menționează în considerentul 19 din Regulamentul (UE) 2021/953, statele membre, din motive medicale și de sănătate publică și în cazul certificatelor eliberate sau obținute în mod fraudulos, ar trebui să poată întocmi și transmite altor state membre, în scopul respectivului regulament și în anumite cazuri, liste cu certificatele revocate, în special în ceea ce privește certificatele eliberate în mod greșit, ca rezultat al fraudei sau în urma suspendării unui lot de vaccinuri împotriva COVID-19 defectuoase. Statele membre nu ar trebui să poată revoca certificatele eliberate de alte state membre. Listele cu certificatele revocate care fac obiectul schimburilor ar trebui să nu conțină alte date cu caracter personal decât identificatorii unici ai certificatelor. În special, acestea nu ar trebui să includă motivul pentru care a fost revocat un certificat.

(10) În plus față de informațiile generale privind posibilitatea revocării unor certificate și posibilele motive pentru aceasta, titularii certificatelor revocate ar trebui să fie informați prompt de către autoritatea emitentă responsabilă cu privire la revocarea certificatelor lor și la motivele revocării. Cu toate acestea, în unele cazuri, în special în cazul certificatelor digitale ale UE privind COVID eliberate pe suport de hârtie, urmărirea și informarea titularului cu privire la revocare s-ar putea dovedi imposibile sau ar putea implica un efort disproporționat. Statele membre nu ar trebui să colecteze date cu caracter personal suplimentare care nu sunt necesare pentru procesul de eliberare doar pentru a putea informa titularii certificatelor în cazul în care certificatele lor sunt revocate.

(11) Prin urmare, este necesar să se consolideze cadrul de încredere pentru certificatul digital al UE privind COVID prin sprijinirea schimbului bilateral de liste cu certificatele revocate între statele membre.

(12) Prezenta decizie nu se referă la suspendarea temporară a certificatelor pentru cazurile de utilizare la nivel național care nu intră în domeniul de aplicare al regulamentului referitor la certificatul digital al UE privind COVID, de exemplu situațiile în care titularul unui certificat de vaccinare a obținut un rezultat pozitiv la testul de depistare a SARS-CoV-2. Aceasta nu aduce atingere procedurilor stabilite de verificare a normelor operaționale privind valabilitatea certificatelor.

(13) Deși, din punct de vedere tehnic, sunt fezabile diferite arhitecturi pentru schimbul de liste de revocare, schimbul acestora prin intermediul gateway-ului este cel mai adecvat, deoarece limitează schimburile de date la cadrul de încredere deja instituit și reduce la minimum atât numărul punctelor posibile de eșec, cât și al schimburilor dintre statele membre în comparație cu un sistem alternativ *peer-to-peer*.

(14) În consecință, gateway-ul pentru certificatul digital al UE privind COVID ar trebui consolidat pentru a sprijini schimbul securizat de certificate digitale ale UE privind COVID revocate în scopul verificării lor în condiții de siguranță prin intermediul gateway-ului. În acest sens, ar trebui puse în aplicare măsuri de securitate adecvate pentru a proteja datele cu caracter personal prelucrate în cadrul gateway-ului. Pentru a asigura un nivel ridicat de protecție, statele membre ar trebui să pseudonimizeze atributele certificatelor prin intermediul unui *hash* ireversibil care să fie inclus pe listele de revocare. Într-adevăr, identificatorul unic ar trebui să fie considerat drept date pseudonimizate pentru operațiunile de prelucrare efectuate în cadrul gateway-ului.

(15) Totodată ar trebui să fie stabilite dispoziții privind rolul statelor membre și al Comisiei în ceea ce privește schimbul de liste cu certificatele revocate.

(16) Prelucrarea datelor cu caracter personal ale titularilor de certificate, care se efectuează sub responsabilitatea statelor membre sau a altor organizații publice sau organisme oficiale din statele membre, ar trebui să se efectueze în conformitate cu Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului ([5]). Prelucrarea datelor cu caracter personal sub responsabilitatea Comisiei în scopul gestionării și al asigurării securității gateway-ului pentru certificatul digital al UE privind COVID ar trebui să respecte Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului ([6]).

(17) Statele membre, reprezentate de organismele oficiale sau autoritățile naționale desemnate, stabilesc împreună scopul și mijloacele de prelucrare a datelor cu caracter personal prin gateway-ul pentru certificatul digital al UE privind COVID și, prin urmare, sunt operatori asociați. Articolul 26 din Regulamentul (UE) 2016/679 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. Articolul menționat prevede, de asemenea, posibilitatea ca aceste responsabilități să fie stabilite în dreptul Uniunii sau al statului membru care li se aplică operatorilor. Modalitatea menționată la articolul 26 ar trebui să fie inclusă în anexa III la prezenta decizie.

(18) Regulamentul (UE) 2021/953 atribuie Comisiei sarcina de a sprijini astfel de schimburi. Cea mai adecvată modalitate de a îndeplini acest mandat este de a reuni, în numele statelor membre, listele cu certificatele revocate. Prin urmare, Comisiei ar trebui să i se atribuie rolul de persoană împuternicită de operator pentru a sprijini aceste schimburi prin facilitarea schimbului de liste prin intermediul gateway-ului pentru certificatul digital al UE privind COVID, în numele statelor membre.

(19) Comisia, în calitate de furnizor de soluții tehnice și organizaționale pentru gateway-ul pentru certificatele digitale ale UE privind COVID, prelucrează datele cu caracter personal din listele de revocare din gateway în numele statelor membre care au calitatea de operatori asociați. Prin urmare, Comisia acționează în calitate de persoană împuternicită de acestea. În temeiul articolului 28 din Regulamentul (UE) 2016/679 și al articolului 29 din Regulamentul (UE) 2018/1725, prelucrarea de către o persoană împuternicită de operator trebuie 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. Prin urmare, este necesar să se prevadă norme privind prelucrarea datelor de către Comisie în calitate de persoană împuternicită de operator.

(20) Sarcina Comisiei de a acorda sprijin nu implică instituirea unei baze de date centrale, astfel cum se menționează în considerentul 52 din Regulamentul (UE) 2021/953. Această interdicție este menită să evite crearea unui registru central al tuturor certificatelor digitale ale UE privind COVID care au fost eliberate și nu împiedică statele membre să facă schimb de liste de revocare, astfel cum se prevede în mod expres la articolul 4 alineatul (2) din Regulamentul (UE) 2021/953.

(21) Atunci când prelucrează date cu caracter personal în cadrul gateway-ului pentru certificatele digitale ale UE privind COVID, Comisia trebuie să respecte Decizia (UE, Euratom) 2017/46 ([7]).

(22) Articolul 3 alineatul (10) din Regulamentul (UE) 2021/953 permite Comisiei să adopte acte de punere în aplicare prin care să stabilească echivalența cu certificatele privind COVID-19 eliberate în temeiul prezentului regulament a certificatelor privind COVID-19 eliberate de o țară terță cu care Uniunea și statele membre au încheiat un acord privind libera circulație a persoanelor care permite părților contractante să restricționeze libera circulație din motive de sănătate publică într-un mod nediscriminatoriu și care nu conține un mecanism de încorporare a actelor juridice ale Uniunii. Pe această bază, Comisia a adoptat, la 8 iulie 2021, Decizia de punere în aplicare (UE) 2021/1126 a Comisiei ([8]) de stabilire a echivalenței certificatelor COVID-19 eliberate de Elveția.

([5]) 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).

([6]) 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).

([7]) 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

([8]) Decizia de punere în aplicare (UE) 2021/1126 a Comisiei din 8 iulie 2021 de stabilire a echivalenței certificatelor COVID-19 eliberate de Elveția cu certificatele eliberate în conformitate cu Regulamentul (UE) 2021/953 al Parlamentului European și al Consiliului (JO L 243, 9.7.2021, p. 49).

(23) Articolul 8 alineatul (2) din Regulamentul (UE) 2021/953 permite Comisiei să adopte un act de punere în aplicare prin care să stabilească faptul că certificatele privind COVID-19 eliberate de către o țară terță în conformitate cu standardele și sistemele tehnologice interoperabile cu cadrul de încredere pentru certificatul digital al UE privind COVID, care permit verificarea autenticității, a valabilității și a integrității certificatului și care cuprind datele prevăzute în anexa la regulament, trebuie considerate echivalente cu certificatele digitale ale UE privind COVID cu scopul de a facilita exercitarea de către titulari a dreptului lor la liberă circulație pe teritoriul Uniunii. Astfel cum se menționează în considerentul 28 din Regulamentul (UE) 2021/953, articolul 8 alineatul (2) din regulamentul respectiv se referă la acceptarea certificatelor eliberate de țări terțe cetățenilor Uniunii și membrilor familiilor acestora. Comisia a adoptat deja mai multe astfel de acte de punere în aplicare.

(24) Pentru a se evita lacunele în ceea ce privește detectarea certificatelor revocate care fac obiectul unor astfel de acte de punere în aplicare, ar trebui să fie posibil, de asemenea, ca țările terțe ale căror certificate privind COVID-19 au fost considerate echivalente în temeiul articolului 3 alineatul (10) și al articolului 8 alineatul (2) din Regulamentul (UE) 2021/953 să poată transmite listele relevante cu certificatele revocate pe gateway-ul pentru certificatele digitale ale UE privind COVID.

(25) Resortisanți ai țărilor terțe care dețin certificate privind COVID-19 revocate eliberate de o țară terță ale cărei certificate privind COVID-19 au fost considerate echivalente în temeiul Regulamentului (UE) 2021/953 pot să nu intre în domeniul de aplicare al regulamentului menționat anterior sau al Regulamentului (UE) 2021/954 în momentul în care țara terță respectivă generează o listă de revocare ce include certificatele acestora. Cu toate acestea, în momentul în care țara terță respectivă generează o listă cu certificatele revocate nu se poate ști dacă toți resortisanții țărilor terțe care dețin certificate revocate intră în domeniul de aplicare al unuia dintre cele două regulamente. Prin urmare, încercarea de a exclude persoanele care nu intră în domeniul de aplicare al niciunuia dintre aceste regulamente de pe listele cu certificatele revocate ale țărilor respective nu este fezabilă, iar încercarea de a face acest lucru ar conduce la imposibilitatea statelor membre de a detecta certificatele revocate deținute de resortisanții țărilor terțe care călătoresc în Uniune pentru prima dată. Cu toate acestea, chiar și certificatele revocate ale resortisanților respectivei țări terțe ar fi verificate de statele membre atunci când titularii acestora intră pe teritoriul Uniunii și, ulterior, când călătoresc pe teritoriul Uniunii. Țările terțe ale căror certificate au fost considerate echivalente în temeiul Regulamentului (UE) 2021/953 nu sunt implicate în guvernanța gateway-ului și, prin urmare, nu se califică drept operatori asociați.

(26) În plus, sistemul de certificate digitale ale UE privind COVID s-a dovedit a fi singurul sistem de certificate privind COVID-19 operațional la nivel internațional pe scară largă. Prin urmare, certificatul digital al UE privind COVID a dobândit o importanță tot mai mare la nivel mondial și contribuie la combaterea pandemiei la nivel internațional, prin facilitarea călătoriilor internaționale în condiții de siguranță și a redresării globale. În procesul de adoptare a unor acte de punere în aplicare suplimentare în temeiul articolului 8 alineatul (2) din Regulamentul (UE) 2021/953, apar noi nevoi în ceea ce privește completarea certificatului digital al UE privind COVID. În conformitate cu normele prevăzute în Decizia de punere în aplicare (UE) 2021/1073, numele de familie este un câmp obligatoriu în conținutul tehnic al certificatului. Este necesar să se modifice această cerință pentru a promova incluziunea și interoperabilitatea cu alte sisteme, având în vedere că, în unele țări terțe, există persoane fără nume de familie. În cazurile în care numele titularului certificatului nu poate fi împărțit în două părți, numele ar trebui introdus în același câmp (nume sau prenume) din certificatul digital al UE privind COVID, ca și în cazul documentului de călătorie sau de identitate al titularului. De asemenea, această modificare ar alinia mai bine conținutul tehnic al certificatelor cu specificațiile valabile în prezent privind documentele de călătorie care pot fi citite automat, publicate de Organizația Aviației Civile Internaționale.

(27) Prin urmare, Decizia de punere în aplicare (UE) 2021/1073 ar trebui modificată în consecință.

(28) 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 vineri, 11 martie 2022.

(29) Pentru a acorda statelor membre și Comisiei suficient timp pentru a pune în aplicare modificările necesare care să permită schimbul de liste cu certificatele revocate prin intermediul gateway-ului pentru certificatul digital al UE privind COVID, prezenta decizie ar trebui să înceapă să se aplice la patru săptămâni de la intrarea în vigoare.

(30) Măsurile prevăzute în prezenta decizie sunt conforme cu avizul comitetului instituit în temeiul articolului 14 din Regulamentul (UE) 2021/953,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Decizia de punere în aplicare (UE) 2021/1073 se modifică după cum urmează:

1. se inserează următoarele articole 5a, 5b și 5c:

„*Articolul 5a*

Schimbul de liste cu certificatele revocate

(1) Cadrul de încredere pentru certificatul digital al UE privind COVID permite schimbul de liste cu certificatele revocate prin intermediul gateway-ului pentru certificatele digitale ale UE privind COVID („gateway-ul"), în conformitate cu specificațiile tehnice din anexa I.

(2) În situația în care statele membre revocă anumite certificate digitale ale UE privind COVID, acestea pot transmite gateway-ului liste cu certificatele revocate.

(3) În cazul în care statele membre transmit liste cu certificatele revocate, autoritățile emitente păstrează o listă cu certificatele revocate.

(4) În cazul în care se face schimb de date cu caracter personal prin intermediul gateway-ului, prelucrarea se limitează la scopul de a sprijini schimbul de informații privind revocarea. Aceste date cu caracter personal se utilizează numai în scopul verificării statutului de revocare a certificatelor digitale ale UE privind COVID eliberate în cadrul domeniului de aplicare al Regulamentului (UE) 2021/953.

(5) Informațiile transmise gateway-ului cuprind următoarele date, în conformitate cu specificațiile tehnice din anexa I:

(a) identificatorii unici pseudonimizați ai certificatelor revocate;

(b) o dată de expirare pentru lista cu certificatele revocate depusă.

(6) În cazul în care o autoritate emitentă revocă anumite certificate digitale ale UE privind COVID pe care le-a eliberat în temeiul Regulamentului (UE) 2021/953 sau al Regulamentului (UE) 2021/954 și intenționează să facă schimb de informații relevante prin intermediul gateway-ului, aceasta poate transmite gateway-ului informațiile menționate la alineatul (5) sub forma unor liste cu certificatele revocate, într-un format securizat, în conformitate cu specificațiile tehnice prevăzute în anexa I.

(7) Autoritățile emitente furnizează, în măsura posibilului, o soluție pentru a informa, în momentul revocării, titularii certificatelor revocate cu privire la statutul de revocare al certificatelor lor și la motivul revocării.

(8) Gateway-ul colectează listele cu certificatele revocate primite și furnizează instrumente pentru distribuirea listelor către statele membre. Acesta șterge automat listele în conformitate cu datele de expirare indicate de autoritatea emitentă pentru fiecare listă depusă.

(9) Autoritățile naționale sau organismele oficiale desemnate ale statelor membre care prelucrează date cu caracter personal în gateway sunt operatori asociați ai datelor prelucrate. Responsabilitățile respective ale operatorilor asociați se atribuie în conformitate cu anexa VI.

(10) Comisia este persoana împuternicită de operator în ceea ce privește datele cu caracter personal prelucrate în cadrul gateway-ului. În calitatea sa de persoană împuternicită de operator în numele statelor membre, Comisia asigură securitatea transmiterii și a găzduirii datelor cu caracter personal în gateway și respectă obligațiile care îi revin persoanei împuternicite de operator prevăzute în anexa VII.

(11) Eficacitatea măsurilor tehnice și organizatorice pentru asigurarea securității prelucrării datelor cu caracter personal în cadrul gateway-ului este testată, examinată și evaluată periodic de Comisie și de operatorii asociați.

Articolul 5b

Transmiterea de către țările terțe de liste cu certificatele revocate

Țările terțe care eliberează certificate privind COVID-19 pentru care Comisia a adoptat un act de punere în aplicare în temeiul articolului 3 alineatul (10) sau al articolului 8 alineatul (2) din Regulamentul (UE) 2021/953 pot prezenta liste cu certificatele privind COVID-19 revocate care fac obiectul unui astfel de act de punere în aplicare, pentru a fi prelucrate de Comisie în numele operatorilor asociați, în cadrul gateway-ului, astfel cum se menționează la articolul 5a, în conformitate cu specificațiile tehnice prevăzute în anexa I.

Articolul 5c

Guvernanța prelucrării datelor cu caracter personal în gateway-ul central pentru certificatele digitale ale UE privind COVID

(1) Procesul decizional al operatorilor asociați este reglementat de un grup de lucru instituit în cadrul comitetului menționat la articolul 14 din Regulamentul (UE) 2021/953.

(2) Autoritățile naționale sau organismele oficiale desemnate ale statelor membre care prelucrează date cu caracter personal în cadrul gateway-ului în calitate de operatori asociați desemnează reprezentanți în acest grup.”

2. Anexa I se modifică în conformitate cu anexa I la prezenta decizie.

3. Anexa V se modifică în conformitate cu anexa II la prezenta decizie.

4. Textul din anexa III la prezenta decizie se adaugă ca anexa VI.

5. Textul din anexa IV la prezenta decizie se adaugă ca anexa VII.

Articolul 2

Prezenta decizie intră în vigoare în a treia zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Se aplică după patru săptămâni de la intrarea sa în vigoare.

Adoptată la Bruxelles, 21 martie 2022.

Pentru Comisie
Președinta
Ursula VON DER LEYEN

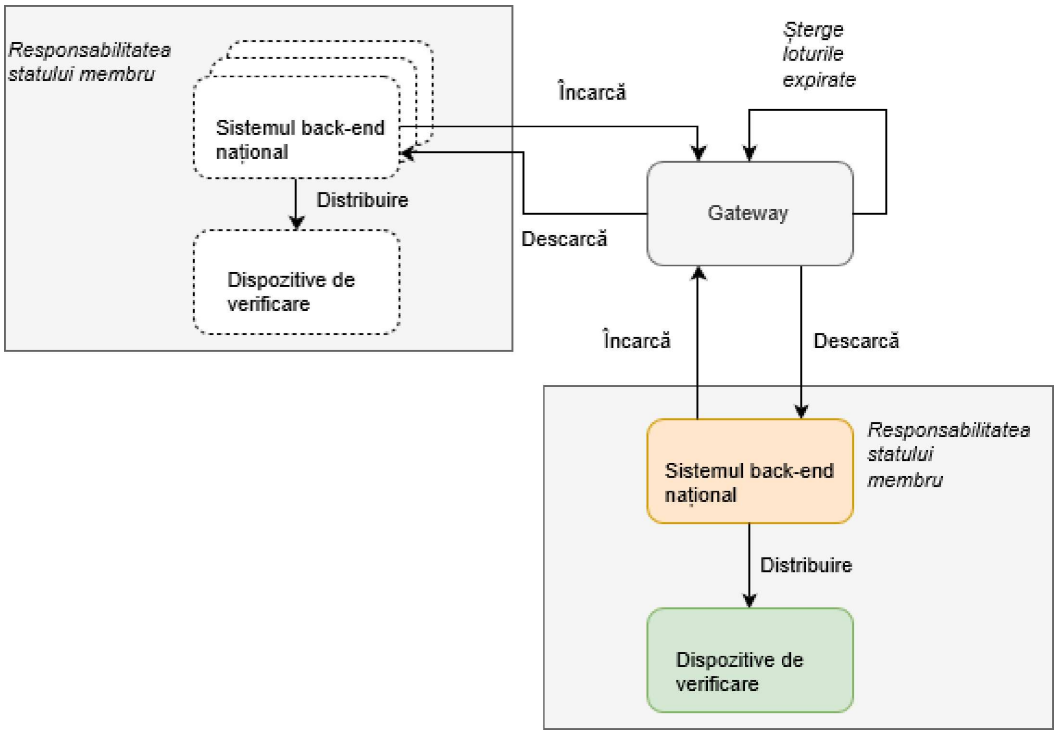
ANEXA I

În anexa I la Decizia de punere în aplicare (UE) 2021/1073 se adaugă următoarea secțiune 9:

„9. **SOLUȚIA REVOCĂRII**

9.1. **Dispoziție privind lista DCC revocate (DRL)**

Gateway-ul asigură puncte finale și funcționalitatea pentru a păstra și a gestiona listele de revocare:



9.2. **Modelul de încredere**

Toate conexiunile sunt stabilite de modelul de încredere standard al DCCG prin intermediul certificatelor NB_{TLS} și NB_{UP} (a se vedea guvernanța certificatelor). Toate informațiile sunt regrupate și încărcate prin mesaje CMS pentru a se asigura integritatea.

9.3. **Construirea loturilor**

9.3.1. *Lotul*

Fiecare listă de revocare conține una sau mai multe intrări și este regrupată în loturi care conțin un set de hash-uri și metadatele acestora. Un lot este imuabil și stabilește o dată de expirare care indică momentul în care lotul poate fi șters. Data expirării tuturor elementelor din lot trebuie să fie exact aceeași – ceea ce înseamnă că loturile trebuie grupate în funcție de data expirării și prin semnarea DSC. Fiecare lot conține maximum 1 000 de intrări. În cazul în care lista de revocare cuprinde mai mult de 1 000 de intrări, se creează mai multe loturi. Orice intrare poate avea loc în cel mult un lot. Lotul este grupat într-o structură CMS și este semnat de certificatul NB_{up} al țării care îl încarcă.

9.3.2. *Indexul loturilor*

Atunci când se creează un lot, acestuia i se atribuie un identificator unic de către gateway și se adaugă automat la index. Indexul loturilor este ordonat în funcție de data modificată, în ordine cronologică crescătoare.

9.3.3. *Comportamentul gateway-ului*

Gateway-ul prelucrează loturi de revocare fără nicio modificare: acesta nu poate nici să actualizeze, nici să elimine și nici să adauge vreo informație în loturi. Loturile sunt trimise tuturor țărilor autorizate (a se vedea capitolul 9.6).

Gateway-ul observă în mod activ datele de expirare a loturilor și elimină loturile expirate. După ce lotul este șters, gateway-ul returnează un răspuns «HTTP 410 Gone» pentru URL-ul lotului șters. Prin urmare, lotul apare în indexul loturilor ca fiind «șters».

9.4. **Tipuri de hash**

Lista de revocare conține hash-uri care pot reprezenta diferite tipuri/atribute de revocare. Aceste tipuri sau atribute sunt indicate odată cu transmiterea listelor de revocare. Tipurile curente sunt:

Tip	Atribut	Calculul hash
SEMNĂTURA	DCC Signature	SHA256 of DCC Signature
UCI	UCI (identificator unic al certificatului)	SHA256 of UCI
COUNTRYCODEUCI	Issuing Country Code + UCI	SHA256 of Issuing CountryCode + UCI

Doar primii 128 de biți de hash-uri codificați ca șiruri base64 sunt introduși în loturi și utilizați pentru a identifica DCC revocat ([1]).

9.4.1. *Tipul de hash SHA256(DCC Signature)*

În acest caz, hash-ul se calculează pe octeți ai semnăturii COSE_SIGN1 din CWT. Pentru semnăturile RSA, întreaga semnătură va fi utilizată ca intrare. Formula pentru certificatele semnate de EC DSA utilizează valoarea r ca intrare:

SHA256(r)

[necesar pentru toate noile implementări]

9.4.2. *Tipul de hash SHA256(UCI)*

În acest caz, hash-ul se calculează pe șirul UCI codificat în UTF-8 și convertit într-o rețea de octeți.

[perimat ([2]), dar susținut pentru compatibilitatea inversă]

9.4.3. *Tipul de hash SHA256[Codul țării emitente(CountryCode)+UCI]*

În acest caz, CountryCode codificat ca un șir UTF-8 concatenat cu UCI codificat cu un șir UTF-8. Acesta este apoi transformat într-o rețea de octeți și utilizat ca intrare în funcția de hash.

[perimat[2], dar susținut pentru compatibilitatea inversă]

9.5. **Structura API**

9.5.1. *API care asigură intrarea revocării*

9.5.1.1. Obiectivul

API asigură intrările din lista de revocare în loturi, inclusiv un index al loturilor.

9.5.1.2. Puncte finale

([1]) Vă rugăm să luați în considerare, de asemenea, punctul 9.5.1.2 pentru descrierile detaliate ale API.

([2]) Perimat înseamnă că această caracteristică nu trebuie luată în considerare pentru noile implementări, ci trebuie sprijinită pentru implementările existente pentru o perioadă de timp bine definită.

9.5.1.2.1. Punctul final pentru descărcarea listei lotului

Punctele finale urmează un model simplu, returnând o listă de loturi cu un *wrapper* de mici dimensiuni care furnizează metadate. Loturile sunt sortate după *dată* în ordine *crescătoare (cronologică)*:

/revocation-list

Verb: GET

Content-Type: application/json

Response: JSON Array

```
{
    'more':true|false,
    'batches':
        [{
            'batchId': '{uuid}',
            'country': 'XY',
            'date': '2021-11-01T00:00:00Z'
            'deleted': true | false
        }, ..
        ]
}
```

Notă: Rezultatul este limitat, implicit, la 1 000. Dacă indicatorul «more» este setat la «true», răspunsul indică faptul că sunt disponibile mai multe loturi în vederea descărcării. Pentru a descărca mai multe elemente, clientul trebuie să seteze antetul If-Modified-Since la o dată care să nu fie anterioară ultimei intrări primite.

Răspunsul conține o rețea JSON cu următoarea structură:

Câmp	Definiție
more	Indicatorul boolean care indică faptul că există mai multe loturi.
loturi	Rețea cu loturile existente.
batchId	https://en.wikipedia.org/wiki/Universally_unique_identifier
country	Codul de țară ISO 3166
date	Data UTC ISO 8601. Data la care lotul a fost adăugat sau șters.
deleted	boolean. «True» dacă este șters. Când indicatorul este setat la șters, intrarea poate fi eliminată în cele din urmă din rezultatele interogării după 7 zile.

9.5.1.2.1.1. *Coduri* de răspuns

Codul	Descrierea
200	Toate sunt în ordine.
204	Nu există conținut dacă antetul «If-Modified-Since» nu are un corespondent.

Antetul cererii

Antet	Obligatoriu	Descrierea
If-Modified-Since	Da	Acest antet conține ultima dată descărcată pentru a obține doar cele mai noi rezultate. La solicitarea inițială, antetul ar trebui setat la «2021-06-01T00:00:00Z»

9.5.1.2.2. Punctul final pentru descărcarea lotului

Loturile conțin o listă de identificatori ai certificatelor:

/revocation-list/{batchId}

Verb: GET

Accepts: application/cms

Response:CMS with Content

{

‘country’: ‘XY’,

‘expires’: ‘2022-11-01T00:00:00Z’,

‘kid’:’23S+33f=’,

‘hashType’:’SIGNATURE’,

‘entries’:[{

‘hash’:’e2e2e2e2e2e2e2e2’

}, ..]

}

Răspunsul conține un CMS care include o semnătură care trebuie să corespundă certificatului NB_{UP}al țării. Toate elementele din rețeaua JSON conțin următoarea structură:

Câmp	Obligatoriu	Tip	Definiție
expires	Da	String	Data la care elementul poate fi eliminat. Data/Ora ISO8601 UTC
country	Da	String	Codul de țară ISO 3166
hashType	Da	String	Tipul de hash al intrărilor furnizate (a se vedea tipurile de hash)]
entries	Da	JSON Object Array	A se vedea tabelul Intrări
kid	Da	String	KID al DSC codificat în base64 utilizat pentru a semna DCC. Dacă nu se cunoaște KID, atunci se poate folosi seria `UNKNOWN_KID`(excluzând `).

Note:

— Loturile sunt grupate în funcție de data expirării și DSC – toate elementele expiră în același timp și au fost semnate cu aceeași cheie.

— Data expirării este o dată/oră în UTC deoarece EU-DCC este un sistem global și nu trebuie să existe ambiguitate temporală.

— Data de expirare a unui DCC revocat permanent este stabilită la data de expirare a DSC-ului corespunzător utilizat pentru a semna DCC-ul sau data expirării DCC-ului revocat (în acest caz se consideră că timpul indicat în data numerică/perioada utilizat este în fusul orar UTC).

— Sistemul back-end național (NB) elimină elemente din lista lor de revocare atunci când se ajunge la data **expirării**.

— NB poate elimina elemente din lista lor de revocare în cazul în care **kidul** utilizat pentru semnarea DCC-ului este revocat.

9.5.1.2.2.1. Intrări

Câmp	Obligatoriu	Tip	Definiție
hash	Da	String	Primii 128 de biți ai hash-ului SHA256 codificați ca șir în base64

Notă: Obiectul intrărilor conține în prezent doar un hash, dar pentru a fi compatibil cu modificările viitoare a fost ales un obiect în locul unei rețele json.

9.5.1.2.2.2. Coduri de răspuns

Codul	Descrierea
200	Toate sunt în ordine.
410	Lot ieșit. Lotul poate fi șters în sistemul back-end național.

9.5.1.2.2.3. Antete de răspuns

Antet	Descriere
ETag	Identificatorul lotului.

9.5.1.2.3. Punctul final pentru încărcarea lotului

Încărcarea se face pe același punct final prin comanda POST:

/revocation-list

Verb: POST

Accepts: application/cms

Request: CMS with Content

ContentType: application/cms

Content:

{

‘country’: ‘XY’,

‘expires’: ‘2022-11-01T00:00:00Z’,

‘kid’:’23S+33f=’,

'hashType':'SIGNATURE',

'entries':[{

'hash':'e2e2e2e2e2e2e2e2'

}, ..]

}

Lotul va fi semnat utilizându-se certificatul NB_{UP}. Gateway-ul va verifica dacă semnătura a fost stabilită de NB_{UP} pentru *țara* respectivă. Dacă verificarea semnăturii eșuează, atunci eșuează și încărcarea.

NOTĂ: Fiecare lot este imuabil și nu poate fi schimbat după încărcare. Cu toate acestea, poate fi șters. ID-ul fiecărui lot șters este stocat, iar încărcarea unui lot nou cu același ID este respinsă.

9.5.1.2.4. Punctul final pentru ștergerea lotului

Un lot poate fi șters pe același punct final prin comanda DELETE:

/revocation-list

Verb: DELETE

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

'batchId': '...'

}

Sau, din motive de compatibilitate, la următorul punct final cu comanda POST:

/revocation-list/delete

Verb: POST

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

'batchId': '...'

}

9.6. **Protecția API/RGPD**

Această secțiune specifică măsurile de implementare pentru respectarea dispozițiilor Regulamentului (UE) 2021/953 în ceea ce privește prelucrarea datelor cu caracter personal.

9.6.1. *Autentificarea existentă*

Gateway-ul utilizează în prezent certificatul NB_{TLS} pentru autentificarea țărilor care se conectează la gateway. Această autentificare poate fi utilizată pentru a stabili identitatea țării conectate la gateway. Această identitate poate fi apoi utilizată pentru a pune în aplicare controlul accesului.

9.6.2. *Controlul accesului*

Pentru a putea prelucra în mod legal datele cu caracter personal, gateway-ul implementează un mecanism de control al accesului.

Gateway-ul implementează o listă de control al accesului combinată cu securitatea bazată pe roluri. În această schemă se mențin două tabele - un tabel care descrie care sunt rolurile care pot aplica anumite operațiuni anumitor resurse, celălalt tabel descrie ce roluri se atribuie și căror utilizatori.

Pentru a pune în aplicare controalele cerute în conformitate cu prezentul document sunt necesare trei roluri, și anume:

RevocationListReader

RevocationUploader

RevocationDeleter

Următoarele puncte finale verifică dacă utilizatorul are rolul de RevocationListReader; dacă așa este, se acordă acces, dacă nu, se returnează un răspuns HTTP 403 Forbidden:

GET/revocation-list/

GET/revocation-list/{batchId}

Următoarele puncte finale verifică dacă utilizatorul are rolul de RevocationUploader; dacă așa este, se acordă acces, dacă nu, se returnează un răspuns HTTP 403 Forbidden:

POST/revocation-list

Următoarele puncte finale verifică dacă utilizatorul are rolul de RevocationDeleter; dacă așa este, se acordă acces, dacă nu, se returnează un răspuns HTTP 403 Forbidden:

DELETE/revocation-list

POST/revocation-list/delete

Gateway-ul asigură, de asemenea, o metodă fiabilă prin care administratorii pot gestiona rolurile care sunt legate de utilizatori astfel încât să se reducă riscul apariției unor erori umane fără a împovăra însă administratorii funcționali.”

ANEXA II

Secțiunea 3 din anexa V la Decizia de punere în aplicare (UE) 2021/1073 se înlocuiește cu următorul text:

„3. ***Structuri comune și cerințe generale***

Un certificat digital al UE privind COVID nu se eliberează dacă, din cauza lipsei de informații, nu pot fi completate corect toate câmpurile de date în conformitate cu această specificație. **Acest lucru nu trebuie înțeles ca afectând obligația statelor membre de a elibera certificate digitale ale UE privind COVID.**

Informațiile din toate câmpurile pot fi furnizate utilizând setul complet de caractere UNICODE 13.0 codificate utilizând UTF-8, cu excepția cazului în care caracterele sunt limitate în mod specific la seturi de valori sau la seturi mai restrânse de caractere.

Structura comună este următoarea:

«JSON»:{

«ver»:< informații privind versiunea>,

«nam»:{

<Informații privind numele persoanei>

}

«dob»:<data nașterii>,

«v» sau «t» sau «r»:[

{< informații despre doza de vaccin, testare sau vindecare, o intrare>}

]

}

În secțiunile următoare sunt furnizate informații detaliate privind grupurile și câmpurile individuale.

În cazul în care normele indică faptul că un câmp va fi omis, aceasta înseamnă că va fi gol conținutul său și că nu sunt permise în conținuturi nici numele și nici valoarea câmpului.

3.1. ***Versiune***

Se furnizează informații privind versiunea. Versiunile respectă Semantic Versioning (semver: https://semver.org). În faza de producție, aceasta trebuie să fie una dintre versiunile lansate oficial (cea curentă sau una dintre versiunile mai vechi lansate oficial). A se vedea secțiunea referitoare la locația schemei JSON pentru mai multe detalii.

ID-ul câmpului	Denumirea câmpului	Instrucțiuni
ver	Versiunea schemei	Trebuie să corespundă identificatorului versiunii schemei utilizate pentru producerea certificatelor digitale ale UE privind COVID. Exemplu: «ver»:«1.3.0»

3.2. ***Numele persoanei și data nașterii***

Numele persoanei este numele oficial complet al persoanei, care corespunde numelui menționat pe documentele de călătorie. Identificatorul structurii este *nam*. Se completează exact 1 (un) nume de persoană.

ID-ul câmpului	Denumirea câmpului	Instrucțiuni
nam/fn	Numele de familie	Numele de familie al (ale) titularului. În cazul în care titularul nu are nume de familie și are un prenume, câmpul se omite. În toate celelalte cazuri, se completează exact 1 (un) câmp care nu poate rămâne gol, toate numele de familie fiind incluse în acesta. În cazul mai multor nume de familie, acestea se separă printr-un spațiu. Cu toate acestea, numele compuse, care cuprind cratime sau caractere similare, nu trebuie modificate.

		Exemple: «fn»:«Musterfrau-Gößinger» «fn»:«Musterfrau-Gößinger Müller»
nam/fn	Nume standardizat(e)	Numele de familie al (ale) titularului transliterat(e) utilizând aceeași convenție precum cea utilizată în documentele de călătorie ale titularului care pot fi citite automat (cum ar fi normele definite în documentul OACI 9303 partea 3). În cazul în care titularul nu are nume de familie și are prenume, câmpul se omite. În toate celelalte cazuri, se completează exact 1 (un) câmp care nu poate rămâne gol și care cuprinde numai caracterele A-Z și <. Lungime maximă: 80 de caractere (conform specificației OACI 9303). Exemple: «fnt»:«MUSTERFRAU<GOESSINGER» «fnt»:«MUSTERFRAU<GOESSINGER<MUELLER»
nam/fn	Prenume	Prenumele titularului, cum ar fi numele de botez. În cazul în care titularul nu are prenume și are nume de familie, câmpul se omite. În toate celelalte cazuri, se completează exact 1 (un) câmp care nu poate rămâne gol, toate prenumele fiind incluse în acesta. În cazul mai multor prenume, acestea se separă printr-un spațiu. Exemplu: «gn»:«Isolde Erika»
nam/gnt	Prenume standardizat(e)	Prenumele titularului transliterat(e) utilizând aceeași convenție precum cea utilizată în documentele de călătorie ale titularului care pot fi citite automat (cum ar fi normele definite în documentul OACI 9303 partea 3). În cazul în care titularul nu are prenume și are nume de familie, câmpul se omite. În toate celelalte cazuri, se completează exact 1 (un) câmp care nu poate rămâne gol și care cuprinde numai caracterele A-Z și <. Lungime maximă: 80 de caractere. Exemplu: «gnt»:«ISOLDE<ERIKA»
dob	Data nașterii	Data nașterii titularului DCC. Data completă sau parțială fără oră, limitată la intervalul 1900-01-01 până la 2099-12-31. În cazul în care se cunoaște data completă sau parțială a nașterii, se completează exact 1 (un) câmp care nu poate rămâne gol. Dacă data nașterii nu este cunoscută nici măcar parțial, câmpul se setează la un șir gol «». Acesta ar trebui să corespundă informațiilor furnizate în documentele de călătorie. În cazul în care sunt disponibile informații privind data nașterii, se utilizează unul dintre următoarele formate ISO 8601. Alte opțiuni nu sunt acceptate. AAAA-LL-ZZ AAAA-LL AAAA (Aplicația de verificare poate indica părțile lipsă din data nașterii utilizând convenția XX precum cea utilizată în documentele de călătorie care pot fi citite automat, de exemplu 1990-XX-XX.) Exemple: «dob»:«1979-04-14» «dob»:«1901-08» «dob»:«1939» «dob»:«»

3.3. ***Grupuri pentru informații specifice tipului de certificat***

Schema JSON acceptă trei grupuri de intrări care cuprind informații specifice tipului de certificat. Fiecare DCCUE conține exact 1 (un) grup. Grupurile goale nu sunt permise.

Identificatorul grupului	**Denumirea grupului**	**Intrări**
v	Grupul de vaccinare	Dacă există, trebuie să conțină exact 1 (o) intrare care să descrie exact 1 (o) doză de vaccinare (o doză).
t	Grupul de testare	Dacă există, trebuie să conțină exact 1 (o) intrare care să descrie exact 1 (un) rezultat al testului.
r	Grupul de vindecare	Dacă există, trebuie să conțină exact 1 (o) intrare care să descrie exact 1 (o) declarație de vindecare.”

ANEXA III

„ANEXA VI

RESPONSABILITĂȚILE STATELOR MEMBRE ÎN CALITATE DE OPERATORI ASOCIAȚI PENTRU GATEWAY-UL PENTRU CERTIFICATUL DIGITAL AL UE PRIVIND COVID ÎN VEDEREA SCHIMBULUI DE LISTE CU DCC-URILE UE REVOCATE

SECȚIUNEA 1

Subsecțiunea 1

Repartizarea responsabilităților

1. Operatorii asociați prelucrează datele cu caracter personal prin intermediul gateway-ului, în conformitate cu specificațiile tehnice din anexa I.

2. Autoritățile emitente ale statelor membre rămân unicii operatori pentru colectarea, utilizarea, divulgarea și orice altă prelucrare a informațiilor privind revocarea în afara gateway-ului, inclusiv pentru procedura care conduce la revocarea unui certificat.

3. Fiecare operator este responsabil pentru prelucrarea datelor cu caracter personal în gateway-ul care constituie cadrul de încredere, în conformitate cu articolele 5, 24 și 26 din Regulamentul general privind protecția datelor.

4. 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.

5. Un subgrup de lucru instituit de comitetul menționat la articolul 14 din Regulamentul (UE) 2021/953 este mandatat să decidă cu privire la toate problemele care decurg din schimbul de liste de revocare și din operarea asociată a prelucrării aferente de date cu caracter personal, precum și să faciliteze transmiterea de instrucțiuni coordonate Comisiei, în calitate de persoană împuternicită de operatori. Procesul decizional al operatorilor asociați este reglementat de grupul de lucru respectiv și de regulamentul de procedură care urmează să fie adoptat de acesta. Ca regulă de bază, neparticiparea niciunuia dintre operatorii asociați la o reuniune a acestui grup de lucru, care a fost anunțată cu cel puțin șapte (7) zile înainte de a fi convocată în scris, se consideră a fi un acord tacit cu rezultatele reuniunii grupului de lucru. Oricare dintre operatorii asociați poate convoca o reuniune a acestui grup de lucru.

6. Instrucțiunile către persoana împuternicită de operatori sunt transmise de oricare dintre punctele de contact ale operatorilor asociați, în acord cu ceilalți operatori asociați, în conformitate cu procesul decizional al grupului de lucru precizat la punctul 5 de mai sus. Operatorul asociat care furnizează instrucțiunea ar trebui să o furnizeze persoanei împuternicite de operator în scris și să îi informeze pe toți ceilalți operatori asociați cu privire la acest lucru. Dacă chestiunea în cauză este suficient de urgentă ca să nu permită o reuniune a grupului de lucru menționat la punctul 5 de mai sus, se poate furniza totuși o instrucțiune, dar aceasta poate fi anulată de grupul de lucru. Această instrucțiune ar trebui să fie furnizată în scris, iar toți ceilalți operatori asociați ar trebui să fie informați în acest sens în momentul furnizării instrucțiunii.

7. Grupul de lucru, astfel cum este stabilit la punctul 5 de mai sus, nu aduce atingere niciuneia dintre competențele individuale ale operatorilor asociați de a-și informa autoritatea de supraveghere competentă, în conformitate cu articolele 33 și 24 din Regulamentul general privind protecția datelor. O astfel de notificare nu necesită consimțământul niciunuia dintre ceilalți operatori asociați.

8. 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 de încredere al gateway-ului.

9. Fiecare autoritate emitentă păstrează o evidență a activităților de prelucrare aflate în responsabilitatea sa. Operarea asociată poate fi indicată în evidență.

Subsecțiunea 2

Responsabilitățile și rolurile în ceea ce privește tratarea cererilor persoanelor vizate și informarea acestora

1. Fiecare operator, în calitatea sa de autoritate emitentă, furnizează persoanelor fizice ale căror certificate au fost revocate (denumite în continuare «persoanele vizate») informații cu privire la revocarea respectivă și la prelucrarea datelor lor cu caracter personal în gateway-ul pentru certificatul digital al UE privind COVID în scopul sprijinirii schimbului de liste de revocare, în conformitate cu articolul 14 din Regulamentul general privind protecția datelor, cu excepția cazului în care acest lucru se dovedește imposibil sau ar implica un efort disproporționat.

2. Fiecare operator acționează ca punct de contact pentru persoanele fizice al căror certificat l-a revocat și tratează cererile depuse de persoanele vizate sau de reprezentanții acestora în exercitarea drepturilor lor în conformitate cu Regulamentul general privind protecția datelor. În cazul în care un operator asociat primește o cerere din partea unei persoane vizate, care se referă la un certificat eliberat de un alt operator asociat, acesta informează persoana vizată cu privire la identitatea și datele de contact ale respectivului operator asociat responsabil. Dacă li se solicită de către un alt operator asociat, operatorii asociați își acordă asistență reciprocă pentru tratarea cererilor persoanelor vizate și își răspund reciproc, fără întârzieri nejustificate și cel târziu în termen de o lună de la primirea unei cereri de asistență. În cazul în care o cerere se referă la date transmise de o țară terță, operatorul care primește cererea o tratează și informează persoana vizată cu privire la identitatea și datele de contact ale autorității emitente din țara terță.

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 gateway-ul pentru certificatul digital al UE privind COVID.

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

   (a) orice risc potențial sau real la adresa disponibilității, a confidențialității și/sau a integrității datelor cu caracter personal care fac obiectul prelucrării în cadrul de încredere al gateway-ului;

   (b) orice încălcare a securității datelor cu caracter personal, consecințele probabile ale încălcării securității datelor cu caracter personal și evaluarea riscurilor la adresa drepturilor și a 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 a libertăților persoanelor fizice;

   (c) orice încălcare a garanțiilor tehnice și/sau organizaționale ale operațiunii de prelucrare în cadrul de încredere al gateway-ului.

3. Operatorii asociați comunică orice încălcare a securității datelor cu caracter personal în ceea ce privește operațiunile de prelucrare din cadrul de încredere al gateway-ului Comisiei, autorităților de supraveghere competente și, dacă este cazul, persoanelor vizate, în conformitate cu articolele 33 și 34 din Regulamentul general privind protecția datelor sau în urma notificării de către Comisie.

4. Fiecare autoritate competentă pune în aplicare măsuri tehnice și organizatorice adecvate, menite:

   (a) să asigure și să protejeze disponibilitatea, integritatea și confidențialitatea datelor cu caracter personal prelucrate în comun;

   (b) să ofere protecție împotriva prelucrării, pierderii, utilizării, divulgării, dobândirii sau a accesării neautorizate sau ilegale a oricăror date cu caracter personal pe care le deține;

   (c) să se asigure că accesul la datele cu caracter personal nu este divulgat sau permis niciunei alte persoane cu excepția destinatarilor sau a persoanelor împuternicite de operatori.

SECȚIUNEA 3

Evaluarea impactului asupra protecției datelor

1. Dacă, pentru a-și îndeplini obligațiile prevăzute la articolele 35 și 36 din Regulamentul (UE) 2016/679, 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 4. Al doilea operator depune toate eforturile pentru a furniza informațiile respective.”

ANEXA IV

„ANEXA VII

RESPONSABILITĂȚILE COMISIEI ÎN CALITATE DE PERSOANĂ ÎMPUTERNICITĂ DE OPERATOR PENTRU GATEWAY-UL PENTRU CERTIFICATUL DIGITAL AL UE PRIVIND COVID ÎN VEDEREA SPRIJINIRII SCHIMBULUI DE LISTE CU DCC-URILE UE REVOCATE

Comisia:

1. Crearea și asigurarea unei infrastructuri de comunicații sigure și fiabile în numele statelor membre, care să sprijine schimbul de liste de revocare transmise gateway-ului pentru certificatul digital al UE privind COVID.

2. Pentru a-și îndeplini obligațiile care îi revin în calitate de persoană împuternicită de operator a cadrului de încredere al gateway-ului pentru statele membre, Comisia poate angaja părți terțe ca subcontractanți; Comisia informează operatorii asociați cu privire la orice modificare preconizată privind adăugarea sau înlocuirea altor subcontractanți, oferind astfel operatorilor posibilitatea de a formula, împreună, obiecții față de aceste modificări. Comisia se asigură că acestor subcontractanți li se aplică aceleași obligații în materie de protecție a datelor ca cele prevăzute în prezenta decizie.

3. 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 asociați 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.

   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 5a alineatul (3) din decizie, 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 gateway-ul pentru certificatul digital al UE privind COVID;

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

   (e) ștergerea datelor la data lor de expirare sau în urma instrucțiunilor operatorului care le-a transmis;

   (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.

4. Ia toate măsurile de securitate organizaționale, fizice și logice de ultimă generație pentru a menține gateway-ul pentru certificatul digital al UE privind COVID. În acest scop, Comisia:

   (a) desemnează o entitate responsabilă pentru gestionarea securității la nivelul gateway-ului pentru certificatul digital al UE privind COVID, comunică operatorilor asociați informațiile sale de contact și asigură disponibilitatea sa de reacție la amenințări la adresa securității;

   (b) își asumă responsabilitatea pentru securitatea gateway-ului pentru certificatul digital al UE privind COVID, inclusiv prin efectuarea periodică de teste, de analize și de evaluări ale măsurilor de securitate;

   (c) se asigură că toate persoanele cărora li se acordă acces la gateway-ul pentru certificatul digital al UE privind COVID 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 gateway-ul pentru certificatul digital al UE privind COVID. Aceasta 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) a defini condițiile în care să autorizeze, inclusiv la cererea operatorilor, și să contribuie la efectuarea auditurilor independente, inclusiv a inspecțiilor și a examinărilor privind măsurile de securitate, sub rezerva condițiilor care respectă Protocolul nr. 7 la TFUE privind privilegiile și imunitățile Uniunii Europene;

(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 asociați 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 afectați, pentru a informa fără întârziere operatorii astfel încât aceștia să informeze 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 gateway-ului pentru certificatul digital al UE privind COVID 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 de la serverele back-end naționale la cadrul de încredere al gateway-ului pentru certificatul digital al UE privind COVID;

(f) se asigură că persoanele care accesează gateway-ul pentru certificatul digital al UE privind COVID sunt identificate și autentificate;

(g) reexaminează drepturile de autorizare legate de accesul la gateway-ul pentru certificatul digital al UE privind COVID în cazul unei încălcări a securității care afectează această infrastructură;

(h) menține integritatea informațiilor transmise prin intermediul gateway-ului pentru certificatul digital al UE privind COVID;

(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 gateway-ul pentru certificatul digital al UE privind COVID din domeniul autorităților emitente (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 cadrului de încredere al gateway-ului, elaborează statistici periodice și păstrează evidențe.

10. Oferă sprijin în limba engleză pentru toate serviciile cadrului de încredere al gateway-ului, 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 gateway-ului pentru certificatul digital al UE privind COVID și serviciile lor de asistență respective, responsabilii de proiect și persoanele desemnate din cadrul Comisiei.

11. Oferă asistență operatorilor asociați, prin măsuri tehnice și organizaționale adecvate, în măsura posibilului, în conformitate cu articolul 12 din Regulamentul (UE) 2018/1725, 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 asociați prin furnizarea de informații privind gateway-ul pentru certificatul digital al UE privind COVID, în vederea implementării obligațiilor prevăzute la articolele 32, 33, 34, 35 și 36 din Regulamentul general privind protecția datelor.

13. Se asigură că datele prelucrate în cadrul gateway-ului pentru certificatul digital al UE privind COVID sunt neinteligibile pentru orice persoană care nu este autorizată să le acceseze.

14. Ia toate măsurile relevante pentru a preveni accesul neautorizat al operatorilor gateway-ului pentru certificatul digital al UE privind COVID la datele transmise.

15. Ia măsuri pentru a facilita interoperabilitatea și comunicarea dintre operatorii desemnați ai gateway-ului pentru certificatul digital al UE privind COVID.

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