Orientări

Orientările 4/2020 privind utilizarea datelor de localizare și a instrumentelor de urmărire a contactelor în contextul pandemiei de COVID-19

Adoptate la 21 aprilie 2020

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Adoptate

Istoric versiuni

Versiunea 1.1	5 mai 2020	Corecturi minore
Versiunea 1.0	21 aprilie 2020	Adoptarea orientărilor

Cuprins

Comitetul european pentru protecția datelor,

având în vedere articolul 70 alineatul (1) litera (e) din 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 (denumit în continuare „RGPD”),

având în vedere Acordul privind SEE, în special anexa XI și Protocolul 37 la acesta, astfel cum a fost modificat prin Decizia nr. 154/2018 a Comitetului mixt al SEE din 6 iulie 2018[1],

având în vedere articolele 12 și 22 din Regulamentul său de procedură,

ADOPTĂ URMĂTOARELE ORIENTĂRI

1 INTRODUCERE ȘI CONTEXT

1 Guvernele şi entităţile private iau în calcul utilizarea unor soluţii bazate pe date ca parte a răspunsului la pandemia de COVID-19, ceea ce ridică numeroase probleme legate de protecţia vieţii private.

2 CEPD subliniază că, întrucât cadrul juridic privind protecţia datelor a fost conceput astfel încât să fie flexibil, acesta permite în mod eficace atât limitarea răspândirii pandemiei, cât şi protejarea drepturilor şi libertăţilor fundamentale ale omului.

3 Opinia fermă a CEPD este că, atunci când gestionarea pandemiei de COVID-19 impune prelucrarea de date cu caracter personal, este indispensabil să se asigure protecţia acestor date astfel încât să se consolideze încrederea, să se creeze condiţiile pentru acceptabilitatea socială a oricărei eventuale soluţii şi, prin urmare, să se garanteze eficacitatea acestor măsuri. Virusul nu cunoaşte frontiere, deci pare preferabil să se dezvolte o abordare europeană comună ca răspuns la criza actuală sau cel puţin să se instituie un cadru interoperabil.

4 CEPD consideră, în general, că datele şi tehnologiile avute în vedere pentru a contribui la combaterea COVID-19 ar trebui utilizate mai degrabă pentru a le conferi autonomie persoanelor, şi nu pentru a le controla, stigmatiza sau oprima. În plus, deşi datele şi tehnologia pot fi instrumente importante, acestea au limitări intrinseci şi pot doar să sporească eficacitatea altor măsuri din domeniul sănătăţii publice. Principiile generale ale eficacităţii, necesităţii şi proporţionalităţii trebuie să ghideze procesul de adoptare – de către statele membre sau instituţiile UE – a oricărei măsuri de combatere a COVID-19 ce implică prelucrarea datelor cu caracter personal.

5 Orientările de faţă clarifică condiţiile şi principiile de utilizare proporţională a datelor de localizare şi a instrumentelor de urmările a contactelor, în două scopuri specifice:

- utilizarea datelor de localizare pentru a sprijini răspunsul la pandemie prin modelarea răspândirii virusului, astfel încât să se evalueze eficacitatea globală a măsurilor de izolare;
- urmărirea contactelor pentru informarea persoanelor cu privire la faptul că s-au aflat în imediata apropiere a cuiva care ulterior va fi confirmat ca fiind purtător al virusului, astfel încât să se întrerupă cât mai rapid lanţurile de contaminare.

1Trimiterile la „statele membre” din prezentul document trebuie înţelese ca trimiteri la „statele membre ale SEE”.

6 Eficienţa pe care o pot avea aplicaţiile de urmărire a contactelor în gestionarea pandemiei depinde de mulţi factori (de exemplu, procentul de persoane care îşi vor instala o astfel de aplicaţie, definirea termenului „contact” din perspectiva proximităţii şi a duratei.) În plus, astfel de aplicaţii trebuie să facă parte dintr-o strategie cuprinzătoare în domeniul sănătăţii publice pentru combaterea pandemiei, care să includă, printre altele, testarea persoanelor şi urmărirea manuală ulterioară a contactelor acestora, cu scopul de a se elimina orice îndoială. Punerea la dispoziţie a acestor aplicaţii ar trebui să fie însoţită de măsuri de sprijin pentru a se asigura faptul că informaţiile care le sunt furnizate utilizatorilor sunt contextualizate şi că alertele generate pot fi utile pentru sistemul de sănătate publică. În caz contrar, este posibil ca aceste aplicaţii să nu poată avea impactul scontat.

7 CEPD subliniază că atât RGPD, cât şi Directiva 2002/58/CE (denumită în continuare „directiva”) conţin norme specifice care permit utilizarea datelor anonime sau a datelor cu caracter personal pentru a sprijini autorităţile publice şi alte entităţi de la nivel naţional şi de la nivelul UE în ceea ce priveşte monitorizarea şi limitarea răspândirii virusului SARS-CoV-2[2].

8 În această privinţă, CEPD a luat deja poziţie cu privire la faptul că utilizarea aplicaţiilor de urmărire a contactelor ar trebui să fie voluntară şi nu ar trebui să se bazeze pe urmărirea deplasărilor individuale, ci pe informaţii de proximitate referitoare la utilizatori[3].

[2] A se vedea declaraţia anterioară a CEPD privind pandemia de COVID-19.
[3] [3] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

2 UTILIZAREA DATELOR DE LOCALIZARE

2.1 Sursele datelor de localizare

9 Există două surse principale de date de localizare disponibile pentru modelarea răspândirii virusului şi sporirea eficacităţii generale a măsurilor de izolare:

- datele de localizare colectate de furnizorii de servicii de comunicaţii electronice (cum ar fi operatorii de telecomunicaţii mobile) atunci când furnizează aceste servicii şi
- datele de localizare colectate de acele aplicaţii ale furnizorilor de servicii ale societăţii informaţionale care au nevoie de acest tip de date pentru a funcţiona (de exemplu, aplicaţiile de navigaţie, cele privind serviciile de transport etc.).

10 CEPD reaminteşte că datele de localizare[4] colectate de la furnizorii de comunicaţii electronice pot fi prelucrate numai cu respectarea articolelor 6 şi 9 din directivă. Prin urmare, aceste date pot fi transmise autorităţilor sau altor terţi doar dacă au fost anonimizate de către furnizor sau, în cazul datelor care indică poziţia geografică a echipamentului terminal al unui utilizator, cu excepţia datelor de trafic, doar dacă utilizatorii şi-au dat consimţământul în prealabil[5].

11 În privinţa informaţiilor, inclusiv a datelor de localizare colectate direct din echipamentul terminal, se aplică articolul 5 alineatul (3) din directivă. Prin urmare, stocarea informaţiilor pe dispozitivul utilizatorului sau obţinerea accesului la informaţiile deja stocate este permisă numai dacă (i) utilizatorul şi-a dat consimţământul[6] sau (ii) stocarea şi/sau accesul sunt strict necesare pentru serviciul societăţii informaţionale cerut în mod explicit de către utilizator.

12 Cu toate acestea, în temeiul articolului 15, sunt posibile derogări de la drepturile şi obligaţiile prevăzute în directivă atunci când acestea constituie o măsură necesară, corespunzătoare şi proporţională în cadrul unei societăţi democratice, pentru anumite obiective[7].

13 În ceea ce priveşte reutilizarea datelor de localizare colectate de un furnizor de servicii ale societăţii informaţionale în scopul modelării (de exemplu, prin intermediul sistemului de operare sau al unor aplicaţii instalate anterior), trebuie îndeplinite condiţii suplimentare. Atunci când au fost colectate în conformitate cu articolul 5 alineatul (3) din directivă, datele pot fi prelucrate ulterior numai cu consimţământul suplimentar al persoanei vizate sau în temeiul unui act legislativ adoptat de Uniune sau de statele membre care constituie o măsură necesară şi proporţională într-o societate democratică şi este în măsură să asigure protejarea obiectivelor menţionate la articolul 23 alineatul (1) din RGPD[8].

2.2 Axarea pe utilizarea datelor de localizare anonimizate

14 CEPD subliniază că, atunci când este vorba de utilizarea datelor de localizare, ar trebui să se acorde întotdeauna prioritate prelucrării datelor anonimizate în locul datelor cu caracter personal.

15 Anonimizarea se referă la utilizarea unui set de tehnici pentru a se elimina posibilitatea corelării datelor cu o persoană fizică identificată sau identificabilă prin depunerea de eforturi „rezonabile”. Acest test al caracterului rezonabil al eforturilor trebuie să ia în considerare atât aspectele obiective (timpul, mijloacele tehnice), cât şi elementele contextuale care pot varia de la caz la caz (raritatea unui fenomen ţinând seama, de exemplu, de densitatea populaţiei,

---

[4] A se vedea articolul 2 litera (c) din directivă.
[5] A se vedea articolele 6 şi 9 din directivă.
[6] Noţiunea de consimţământ din directivă este identică cu noţiunea de consimţământ din RGPD şi trebuie să îndeplinească toate cerinţele în această materie prevăzute la articolul 4 punctul (11) şi la articolul 7 din RGPD.
[7] Pentru interpretarea articolului 15 din directivă, a se vedea, de asemenea, hotărârea CJUE din 29 ianuarie 2008 în cauza C-275/06, Productores de Música de España (Promusicae)/Telefónica de España SAU.
[8] A se vedea secţiunea 1.5.3 din Orientările 1/2020 privind prelucrarea datelor cu caracter personal în contextul vehiculelor conectate.

natura şi volumul datelor). Dacă datele nu trec acest test, atunci nu au fost anonimizate şi, prin urmare, se încadrează în continuare în domeniul de aplicare al RGPD.

16 Evaluarea eficacităţii anonimizării se bazează pe trei criterii: (i) capacitatea de individualizare (izolarea unei persoane dintr-un grup mai mare, pe baza datelor); (ii) capacitatea de corelare (capacitatea de a corela două seturi de date referitoare la aceeaşi persoană) şi (iii) capacitatea de deducţie (capacitatea de a deduce, cu o probabilitate semnificativă, informaţii necunoscute cu privire la o persoană).

17 Conceptul de anonimizare poate fi înţeles greşit şi adesea se confundă cu pseudonimizarea. Anonimizarea permite utilizarea datelor fără nicio restricţie, în timp ce datele pseudonimizate se încadrează în domeniul de aplicare al RGPD.

18 Există multe opţiuni eficace pentru asigurarea anonimizării[9], dar cu anumite rezerve. Datele în sine nu pot fi anonimizate, ceea ce înseamnă că numai seturile de date în ansamblu pot sau nu să fie anonimizate. În acest sens, orice intervenţie asupra unei anumite colecţii de date structurate (prin criptare sau orice alte transformări matematice) poate fi considerată, în cel mai bun caz, pseudonimizare.

19 Procesele de anonimizare şi atacurile care au ca obiect reidentificarea sunt în prezent domenii active de cercetare. Este esenţial ca orice operator care foloseşte soluţii de anonimizare să monitorizeze evoluţiile recente din acest domeniu, în special în ceea ce priveşte datele de localizare (care provin de la operatorii de telecomunicaţii şi/sau de la serviciile societăţii informaţionale), cunoscute ca fiind extrem de dificil de anonimizat.

20 Un număr mare de studii au demonstrat[10] că este posibil ca *datele de localizare despre care se considera că au fost anonimizate* să nu fie, în realitate, anonimizate. Datele privind deplasările persoanelor sunt în mod inerent strâns corelate şi unice. Prin urmare, acestea pot fi vulnerabile la tentative de reidentificare în anumite circumstanţe.

21 O colecţie de date structurate care urmăreşte localizarea unei persoane pe o perioadă semnificativă de timp nu poate fi complet anonimizată. Acest lucru poate fi valabil şi dacă precizia coordonatelor geografice înregistrate nu este redusă suficient sau dacă detaliile deplasării sunt eliminate şi se păstrează doar locaţia în care persoana vizată a rămas o perioadă considerabilă de timp. Acest lucru este valabil şi pentru datele de localizare care nu sunt agregate într-un mod suficient de riguros.

22 Pentru a fi anonimizate, datele de localizare trebuie să fie prelucrate cu atenţie astfel încât să poată trece testul caracterului rezonabil. Astfel, seturile de date de localizare trebuie avute în vedere în ansamblu, iar prelucrarea datelor trebuie să se facă utilizându-se un set rezonabil de mare de subiecţi şi tehnici de anonimizare fiabile, aplicate în mod adecvat şi eficace.

23 În cele din urmă, având în vedere complexitatea proceselor de anonimizare, se încurajează puternic ca metodologia de anonimizare să fie transparentă.

---

[9] (de Montjoye et al., 2018) On the privacy-conscientious use of mobile phone data

[10] (de Montjoye et al., 2013) Unique in the Crowd: The privacy bounds of human mobility şi (Pyrgelis et al., 2017) Knock Knock, Who's There? Membership Inference on Aggregate Location Data

3 APLICAȚII DE URMĂRIRE A CONTACTELOR

3.1 Analiză juridică generală

24 Monitorizarea sistematică şi pe scară largă a localizării şi/sau a contactelor dintre persoane fizice este o intruziune gravă în viaţa privată. Aceasta nu poate fi legitimată decât dacă se bazează pe consimţământul utilizatorilor pentru fiecare dintre scopurile respective. Acest lucru ar însemna, în special, că persoanele care decid să nu utilizeze astfel de aplicaţii nu ar trebui să sufere niciun dezavantaj.

25 Pentru a putea fi tras la răspundere, ar trebui să se definească în mod clar operatorul acestui tip de aplicaţii de urmărire a contactelor. CEPD consideră că autorităţile naţionale din domeniul sănătăţii ar putea fi operatori[11] pentru astfel de aplicaţii, dar pot fi avuţi în vedere şi alţi operatori. În orice caz, în cazul în care punerea la dispoziţie a aplicaţiilor de urmărire a contactelor implică actori diferiţi, rolurile şi responsabilităţile acestora trebuie să fie clar stabilite de la bun început şi să le fie explicate utilizatorilor.

26 În plus, în ceea ce priveşte principiul colectării datelor cu caracter personal numai în scopurile prevăzute, scopurile trebuie să fie suficient de specifice pentru a exclude prelucrarea ulterioară în scopuri care nu au legătură cu gestionarea crizei sanitare generate de COVID-19 (de exemplu, în scopuri comerciale sau de asigurare a respectării legii). Odată ce obiectivul a fost clar definit, va fi necesar să se asigure că utilizarea datelor cu caracter personal este adecvată, necesară şi proporţională.

27 În contextul unei aplicaţii de urmărire a contactelor, ar trebui să se acorde o atenţie deosebită principiului reducerii la minimum a datelor şi principiului protecţiei datelor începând cu momentul conceperii şi în mod implicit:

- aplicaţiile de urmărire a contactelor nu au nevoie să urmărească unde se află un utilizator, ci ar trebui să utilizeze în acest sens datele de proximitate;
- întrucât aplicaţiile de urmărire a contactelor pot funcţiona fără identificarea directă a persoanelor, ar trebui să se instituie măsuri corespunzătoare care să împiedice reidentificarea;
- informaţiile colectate ar trebui să rămână pe echipamentul terminal al utilizatorului şi să fie colectate numai informaţiile relevante atunci când este absolut necesar.

28 În ceea ce priveşte legalitatea prelucrării, CEPD constată că aplicaţiile de urmărire a contactelor implică stocarea informaţiilor şi/sau accesul la informaţii deja stocate în terminal, care face obiectul articolului 5 alineatul (3) din directivă. În cazul în care operaţiunile respective sunt strict necesare pentru ca furnizorul aplicaţiei să presteze serviciul solicitat în mod explicit de către utilizator, prelucrarea nu ar necesita consimţământul utilizatorului. Pentru operaţiuni care nu sunt strict necesare, furnizorul va trebui să solicite consimţământul utilizatorului.

29 În plus, CEPD reaminteşte că simplul fapt că utilizarea aplicaţiilor de urmărire a contactelor se face pe bază voluntară nu înseamnă că prelucrarea datelor cu caracter personal se va întemeia în mod necesar pe consimţământ. Atunci când autorităţile publice furnizează un serviciu în baza unui mandat care le-a fost încredinţat prin lege şi în conformitate cu cerinţele prevăzute de lege, se pare că temeiul juridic cel mai relevant pentru prelucrare este necesitatea îndeplinirii unei sarcini de interes public, şi anume articolul 6 alineatul (1) litera (e) din RGPD.

30 Articolul 6 alineatul (3) din RGPD clarifică faptul că temeiul pentru prelucrarea menţionată la articolul 6 alineatul (1) litera (e) trebuie să fie prevăzut de dreptul Uniunii sau de dreptul intern al statului membru care i se aplică operatorului. Scopul prelucrării trebuie stabilit în respectivul act legislativ sau, în ceea ce priveşte prelucrarea menţionată la alineatul (1)

[11] A se vedea, de asemenea, Comisia Europeană „Orientări în domeniul protecţiei datelor privind aplicaţiile care sprijină combaterea pandemiei de COVID-19”, Bruxelles, 16.4.2020, C (2020) 2523 final.

litera (e), este necesar pentru îndeplinirea unei sarcini care serveşte unui interes public sau care rezultă din exercitarea autorităţii publice cu care este învestit operatorul[12].

31 Cu toate acestea, actul legislativ sau măsura legislativă care oferă temeiul legal pentru utilizarea aplicaţiilor de urmărire a contactelor ar trebui să includă garanţii semnificative, inclusiv o trimitere la caracterul voluntar al utilizării aplicaţiei. Ar trebui să se includă o specificare clară a scopului şi restricţiile explicite privind utilizarea ulterioară a datelor cu caracter personal, precum şi o identificare clară a operatorului (operatorilor) implicat (implicaţi). De asemenea, ar trebui identificate categoriile de date, precum şi entităţile cărora li se pot divulga datele cu caracter personal (şi scopurile) în care se pot face aceste divulgări. În funcţie de nivelul de interferenţă, ar trebui incluse garanţii suplimentare, ţinând seama de natura, domeniul de aplicare şi scopurile prelucrării. În cele din urmă, CEPD recomandă, de asemenea, să se includă, cât de curând posibil, criteriile de stabilire a momentului în care aplicaţia va fi dezactivată şi entitatea care va fi responsabilă va putea fi trasă la răspundere pentru luarea acestei decizii.

32 Cu toate acestea, dacă prelucrarea datelor se bazează pe un alt temei juridic, cum ar fi, de exemplu, consimţământul [articolul 6 alineatul (1) litera (a)][13], operatorul va trebui să se asigure că sunt îndeplinite cerinţele stricte pentru ca un astfel de temei juridic să fie valabil.

33 În plus, utilizarea unei aplicaţii pentru combaterea pandemiei de COVID-19 ar putea duce la colectarea de date privind sănătatea (de exemplu, privind starea de sănătate a unei persoane infectate). Prelucrarea unor astfel de date este permisă dacă este necesară din motive de interes public în domeniul sănătăţii publice, sub rezerva îndeplinirii condiţiilor prevăzute la articolul 9 alineatul (2) litera (i) din RGPD[14] sau în scopurile din sfera asistenţei medicale prevăzute la articolul 9 alineatul (2) litera (h) din RGPD[15]. În funcţie de temeiul juridic, prelucrarea ar putea, de asemenea, să se bazeze pe consimţământul explicit [articolul 9 alineatul (2) litera (a) din RGPD].

34 În conformitate cu scopul iniţial, articolul 9 alineatul (2) litera (j) din RGPD permite, de asemenea, prelucrarea datelor privind sănătatea atunci când acest lucru este necesar în scopuri de cercetare ştiinţifică sau statistice.

35 Actuala criză din domeniul sănătăţii nu ar trebui să fie utilizată ca o oportunitate pentru a stabili reguli disproporţionate în materie de păstrare a datelor. Limitarea perioadei de păstrare a datelor ar trebui să ţină seama de necesităţile reale şi de relevanţa medicală (aceasta poate include consideraţii epidemiologice, precum perioada de incubaţie etc.), iar datele cu caracter personal ar trebui să fie păstrate numai pe durata crizei generate de pandemia de COVID-19. Ulterior, ca regulă generală, toate datele cu caracter personal ar trebui şterse sau anonimizate.

36 Opinia CEPD este că aceste aplicaţii nu pot înlocui, ci doar sprijini un sistem manual de urmărire a contactelor, efectuat de personal calificat în domeniul sănătăţii publice, care să verifice dacă aceste contacte apropiate sunt de natură să ducă la transmiterea virusului sau nu (de exemplu, atunci când persoana cu care s-a realizat interacţiunea purta un echipament adecvat de protecţie — casieri etc. — sau nu). CEPD subliniază că procedurile şi procesele, inclusiv algoritmii utilizaţi de aplicaţiile de urmărire a contactelor, ar trebui să fie supravegheate strict de personal calificat în acest sens pentru a se limita apariţia oricăror rezultate fals pozitive sau fals negative. În special, sarcina de a oferi consiliere cu privire la etapele următoare nu ar trebui să se bazeze exclusiv pe prelucrarea automată.

---

[12] A se vedea considerentul 41.

[13] Operatorii (în special autorităţile publice) trebuie să ţină seama de faptul că nu se poate considera că o persoană îşi dă consimţământul în mod liber dacă nu are posibilitatea reală de a refuza sau de a-şi retrage consimţământul fără a avea de suferit.

[14] Prelucrarea trebuie să se bazeze pe dreptul Uniunii sau pe cel al statelor membre care prevede măsuri adecvate şi specifice pentru protejarea drepturilor şi libertăţilor persoanei vizate, în special a secretului profesional.

[15] A se vedea articolul 9 alineatul (2) litera (h) din RGPD.

37 Pentru a se putea asigura tragerea la răspundere şi pentru a se garanta imparţialitatea şi, în sens mai larg, conformitatea algoritmilor cu legislaţia, aceştia trebuie să poată face obiectul unui audit şi alunei revizuiri periodice de către experţi independenţi. Codul sursă al aplicaţiei ar trebui să fie pus la dispoziţia publicului pentru a putea fi supus unei analize critice cât mai largi.

38 Rezultate fals pozitive vor exista întotdeauna într-o anumită măsură. Întrucât identificarea unui risc de infecţie poate avea un impact ridicat asupra persoanelor, cum ar fi autoizolarea până la obţinerea unui rezultat negativ în urma testării, este imperativ să se poată corecta datele şi/sau rezultatele analizelor ulterioare. Acest lucru ar trebui, bineînţeles, să se aplice numai în cazul scenariilor şi al implementărilor în care datele sunt prelucrate şi/sau stocate în aşa fel încât o astfel de corectare să fie fezabilă din punct de vedere tehnic şi să existe probabilitatea producerii efectelor negative menţionate mai sus.

39 În cele din urmă, CEPD consideră că o evaluare a impactului asupra protecţiei datelor trebuie efectuată înainte de adoptarea unui astfel de instrument, deoarece prelucrarea este considerată ca având un risc potenţial ridicat (date privind sănătatea, adoptare anticipată pe scară largă, monitorizare sistematică, utilizarea unei soluţii tehnologice noi)[16]. CEPD recomandă cu fermitate publicarea evaluărilor impactului asupra protecţiei datelor.

3.2 Recomandări și cerințe funcționale

40 Conform principiului reducerii la minimum a datelor, printre alte măsuri de protecţie a datelor începând cu momentul conceperii şi în mod implicit[17], ar trebui să se numere reducerea prelucrării datelor la minimul strict necesar. Aplicaţiile nu ar trebui să colecteze informaţii care nu au legătură cu scopul menţionat sau nu sunt necesare pentru atingerea acestuia, de exemplu privind starea civilă, identificatorii comunicaţiilor, elementele din directoarele echipamentului, mesajele, istoricul apelurilor, datele de localizare, identificatorii dispozitivului etc.

41 Datele transmise de aplicaţii trebuie să includă numai câţiva identificatori unici şi pseudonimi, generaţi de aplicaţie şi specifici acesteia. Aceşti identificatori trebuie să fie reînnoiţi în mod regulat, cu o frecvenţă compatibilă cu scopul limitării răspândirii virusului şi suficientă pentru a se limita riscul identificării şi urmăririi fizice a persoanelor.

42 Urmărirea contactelor se poate face centralizat sau descentralizat[18]. Ambele abordări ar trebui să fie considerate opţiuni viabile, cu condiţia să fie instituite măsuri de securitate adecvate, întrucât fiecare variantă presupune avantaje şi dezavantaje. Astfel, faza de concepţie a dezvoltării aplicaţiilor ar trebui să includă întotdeauna o analiză aprofundată a ambelor concepte, care să evalueze cu atenţie efectele lor respective asupra protecţiei vieţii private şi posibilul impact asupra drepturilor persoanelor.

43 Orice server implicat în sistemul de urmărire a contactelor trebuie să colecteze numai istoricul contactelor sau identificatorii pseudonimi ai unui utilizator diagnosticat ca infectat în urma unei evaluări adecvate efectuate de autorităţile din domeniul sănătăţii şi a unei acţiuni voluntare a utilizatorului. O altă opţiune este ca serverul să păstreze o listă a identificatorilor pseudonimi ai utilizatorilor infectaţi sau a istoricului contactelor acestora numai atât timp cât este necesar pentru a-i informa pe utilizatorii potenţial infectaţi cu privire la faptul că au fost expuşi; de asemenea, serverul nu ar trebui să încerce să îi identifice pe utilizatorii potenţial infectaţi.

---

[16] A se vedea Grupul de lucru „Articolul 29”, Orientări privind evaluarea impactului asupra protecţiei datelor şi stabilirea dacă prelucrarea este „susceptibilă să genereze un risc ridicat” în sensul Regulamentului 2016/679.

[17] A se vedea Orientările 4/2019 ale CEPD cu privire la articolul 25 privind protecţia datelor începând cu momentul conceperii şi în mod implicit

[18] În general, soluția descentralizată este mai compatibilă cu principiul reducerii la minimum a datelor.

44 Punerea în aplicare a unei metodologii globale de urmărire a contactelor care să includă atât aplicații, cât și o urmărire manuală poate necesita, în anumite cazuri, prelucrarea unor informații suplimentare. În acest context, informațiile suplimentare menționate ar trebui să rămână în terminalul utilizatorului și ar trebui să fie prelucrate numai atunci când acest lucru este strict necesar și cu consimțământul prealabil și specific al utilizatorului.

45 Pentru a asigura securitatea datelor stocate în servere și aplicații, precum și a schimburilor dintre aplicații și serverul de la distanță, trebuie folosite tehnici criptografice de ultimă generație. De asemenea, trebuie să se efectueze o autentificare reciprocă între aplicație și server.

46 Raportarea în aplicație a utilizatorilor infectați cu SARS-CoV-2 trebuie să facă obiectul unei autorizări adecvate, de exemplu printr-un cod de unică folosință legat de o identitate pseudonimă a persoanei infectate și de un laborator de testare sau de un cadru medical. Dacă nu se poate obține confirmarea într-un mod securizat, nu ar trebui să se efectueze prelucrarea datelor prezumându-se valabilitatea statutului utilizatorului.

47 Operatorul, în colaborare cu autoritățile publice, trebuie să prezinte în mod clar și explicit informații privind linkul care trebuie folosit pentru a descărca aplicația națională de urmărire a contactelor, astfel încât să se reducă riscul ca persoanele să utilizeze aplicații dezvoltate de terți.

4 CONCLUZIE

48 Ne confruntăm cu o criză de proporţii în domeniul sănătăţii publice, care necesită răspunsuri ferme, ce vor avea un impact şi după ce această situaţie de urgenţă va lua sfârşit. Prelucrarea automată a datelor şi tehnologiile digitale pot fi componente esenţiale în lupta împotriva COVID-19. Cu toate acestea, ar trebui să fim precauţi în ceea ce priveşte „efectul de clichet” (caracterul ireversibil al anumitor măsuri). Este responsabilitatea noastră să ne asigurăm că fiecare măsură luată în aceste circumstanţe extraordinare este necesară, limitată în timp, are o sferă de aplicare minimă şi va fi supusă unei revizuiri periodice şi efective şi unei evaluări ştiinţifice.

49 CEPD subliniază că nu ar trebui să fim nevoiţi să alegem între un răspuns eficace la criza actuală şi protecţia drepturilor noastre fundamentale: le putem asigura pe ambele şi, în plus, principiile de protecţie a datelor pot juca un rol foarte important în lupta împotriva virusului. Legislaţia europeană privind protecţia datelor permite utilizarea în mod responsabil a datelor cu caracter personal în scopul gestionării sănătăţii, asigurând în acelaşi timp că nu se restrâng drepturile şi libertăţile individuale în cursul acestui proces.

Pentru Comitetul european pentru protecţia datelor,

Preşedinta,

(Andrea Jelinek)

ANEXĂ -- GHID DE ANALIZĂ A APLICAȚIILOR DE URMĂRIRE A CONTACTELOR

0. Declinarea responsabilității

Orientările de față nu sunt nici prescriptive, nici exhaustive. Singurul lor scop este de a oferi îndrumări generale celor care concep și implementează aplicații de urmărire a contactelor. Pot fi utilizate și alte soluții decât cele descrise în prezentele orientări. Acestea sunt legale atât timp cât respectă cadrul juridic relevant (și anume RGPD și directiva).

Prezentele orientări au un caracter general. În consecință, recomandările și obligațiile din prezentul document nu trebuie considerate exhaustive. Orice evaluare trebuie efectuată de la caz la caz, iar aplicațiile specifice pot necesita măsuri suplimentare care nu sunt incluse în prezentul ghid.

1. Rezumat

În multe state membre, părțile interesate au în vedere utilizarea *aplicațiilor* de *urmărire* a *contactelor* pentru a ajuta populația să afle dacă au fost în contact cu o persoană infectată cu SARS-CoV-2.

Nu au fost încă stabilite condițiile în care astfel de aplicații ar contribui în mod eficace la gestionarea pandemiei. Aceste condiții ar trebui stabilite înainte de implementarea unei astfel de aplicații. Cu toate acestea, este relevant să se ofere orientări care să aducă informații relevante echipelor de dezvoltare în amonte, astfel încât protecția datelor cu caracter personal să poată fi garantată încă din faza de concepere.

Trebuie subliniat că ghidul de față are un caracter general. În consecință, recomandările și obligațiile din prezentul document nu trebuie considerate exhaustive. Orice evaluare trebuie efectuată de la caz la caz, iar aplicațiile specifice pot necesita măsuri suplimentare care nu sunt incluse în prezentul ghid. Singurul scop al orientărilor de față este de a oferi îndrumări generale celor care concep și implementează aplicații de urmărire a contactelor.

Unele criterii ar putea include cerințe mai stricte decât cele care decurg din cadrul privind protecția datelor. Acestea vizează asigurarea celui mai înalt nivel de transparență, pentru a favoriza acceptabilitatea socială a unor astfel de aplicații de urmărire a contactelor.

În acest scop, editorii de aplicații de urmărire a contactelor ar trebui să ia în considerare următoarele criterii:

- utilizarea unei astfel de aplicații trebuie să fie strict voluntară; aceasta nu are dreptul să condiționeze accesul la drepturi garantate prin lege de utilizarea sa; persoanele trebuie să dețină controlul deplin asupra datelor lor în orice moment și ar trebui să poată alege în mod liber dacă să utilizeze sau nu o astfel de aplicație.
- Aplicațiile de urmărire a contactelor sunt susceptibile să genereze un risc ridicat la adresa drepturilor și libertăților persoanelor fizice și să necesite, înainte de a fi puse la dispoziția publicului, o evaluare a impactului acestora asupra protecției datelor.
- Informațiile privind proximitatea dintre utilizatorii aplicației pot fi obținute fără localizarea acestora. Acest tip de aplicație nu are nevoie să utilizeze datele de localizare și, prin urmare, nu ar trebui să implice utilizarea acestor date.

- Atunci când un utilizator este diagnosticat cu SARS-CoV-2, de acest lucru ar trebui să fie informate doar persoanele cu care utilizatorul a fost în contact apropiat în perioada de păstrare a datelor privind urmărirea contactelor care este relevantă din punct de vedere epidemiologic.

- Funcționarea acestui tip de aplicație poate necesita, în funcție de arhitectura aleasă, utilizarea unui server centralizat. În acest caz și în conformitate cu principiul reducerii la minimum a datelor și cu principiul protecției datelor începând cu momentul conceperii și în mod implicit, datele prelucrate de serverul centralizat ar trebui să fie limitate la minimul necesar:

    - Atunci când un utilizator este diagnosticat ca infectat, se pot colecta informații referitoare la contactele sale apropiate sau la identificatorii transmiși de aplicația sa numai cu acordul utilizatorului. Trebuie să se stabilească o metodă de verificare care să permită să se afirme că persoana în cauză este într-adevăr infectată fără a se identifica utilizatorul. Din punct de vedere tehnic, acest lucru ar putea fi realizat prin alertarea contactelor numai în urma intervenției unui cadru medical, de exemplu prin utilizarea unui cod unic special.

    - Informațiile stocate pe serverul central nu ar trebui să îi permită operatorului să îi identifice pe utilizatorii diagnosticați ca infectați sau pe cei care au fost în contact cu acești utilizatori sau să deducă tipare în materie de interacțiuni între utilizatori care nu sunt necesare pentru stabilirea contactelor relevante.

- Funcționarea acestui tip de aplicație necesită transmiterea de date care să fie citite de dispozitivele altor utilizatori și interceptarea acestor date transmise:

    - Este suficient să se facă schimb de identificatori pseudonimi între echipamentele mobile ale utilizatorilor (computere, tablete, ceasuri conectate etc.), de exemplu prin transmiterea acestora (prin tehnologia Bluetooth cu consum energetic redus, de pildă).

    - Identificatorii trebuie generați utilizându-se procese criptografice de ultimă generație și

    - trebuie reînnoiți regulat pentru a se reduce riscul urmăririlor fizice și al atacurilor prin care se încearcă corelarea datelor cu persoanele în cauză.

- Acest tip de aplicație trebuie să fie securizată pentru a se garanta siguranța proceselor tehnice. În special:

    - Aplicația nu ar trebui să transmită utilizatorilor informații care să le permită acestora să deducă identitatea sau diagnosticul altor persoane. Serverul central nu trebuie să identifice utilizatorii sau să deducă informații cu privire la aceștia.

Declarație de declinare a responsabilității: Principiile menționate anterior sunt legate de scopul declarat al aplicațiilor de *urmărire a contactelor* și numai de acest scop, care vizează exclusiv informarea automată a persoanelor potențial expuse la virus (fără a fi necesară identificarea acestora). Operatorii aplicației și infrastructura sa pot fi supuse controlului autorității de supraveghere competente. Respectarea integrală sau parțială a prezentelor orientări nu este neapărat suficientă pentru a se asigura respectarea pe deplin a cadrului privind protecția datelor.

2. Definiții

Contact	În contextul unei aplicații de urmărire a contactelor, un contact este un utilizator care a participat la o interacțiune cu un utilizator confirmat ca fiind purtător al virusului, pe o durată și la o distanță care determină un risc de expunere semnificativă la infecția virală. Parametrii privind durata expunerii și distanța dintre persoane trebuie să fie estimați de autoritățile din domeniul sănătății și pot fi stabiliți în aplicație.
Date de localizare	Înseamnă toate datele prelucrate într-o rețea de comunicații electronice sau de un serviciu de comunicații electronice care indică poziția geografică a echipamentului terminal al unui utilizator al unui serviciu public de comunicații electronice (astfel cum este definit în directivă), precum și datele din alte surse potențiale referitoare la: – latitudinea, longitudinea sau altitudinea echipamentului terminal; – direcția de deplasare a utilizatorului sau – momentul în care au fost înregistrate informațiile de localizare.
Interacțiune	În contextul unei aplicații de urmărire a contactelor, o interacțiune este definită ca schimbul de informații dintre două dispozitive aflate în imediată apropiere (în spațiu și timp) în raza de acțiune a tehnologiei de comunicații utilizate (de exemplu, Bluetooth). Această definiție exclude localizarea celor doi utilizatori ai interacțiunii.
Purtător al virusului	În documentul de față, sunt considerați purtători ai virusului utilizatorii care au fost depistați pozitiv în urma testării și care au primit un diagnostic oficial din partea unui medic sau a unui centru medical.
Urmărire a contactelor	Persoanele care au fost în contact apropiat (conform unor criterii care urmează a fi definite de epidemiologi) cu o persoană infectată cu virusul au un risc semnificativ de a fi la rândul lor infectate și de a infecta alte persoane. Urmărirea contactelor este o metodologie de control al transmisiei bolilor prin care se întocmește o listă cu toate persoanele care au fost în imediata apropiere a unui purtător al virusului, astfel încât să se verifice dacă acestea sunt expuse riscului de infecție și să se ia măsurile sanitare corespunzătoare.

3. Observații generale

GEN-1	Aplicația trebuie să fie un instrument complementar tehnicilor tradiționale de urmărire a contactelor (în special al interviurilor cu persoanele infectate), adică să facă parte dintr-un program de sănătate publică mai larg. Aceasta trebuie folosită numai până când numărul de noi infectări va putea fi gestionat exclusiv prin intermediul tehnicilor manuale de urmărire a contactelor.

GEN-2	Cel târziu în momentul în care autoritățile publice competente vor decide revenirea la normal, trebuie instituită o procedură pentru a opri colectarea identificatorilor (dezactivarea globală a aplicației, instrucțiuni pentru dezinstalarea aplicației, dezinstalarea automată etc.) și pentru a activa ștergerea tuturor datelor colectate din toate bazele de date (aplicații mobile și servere).
GEN-3	Codul sursă al aplicației și backendul acesteia trebuie să fie deschise, iar specificațiile tehnice trebuie să fie făcute publice, astfel încât orice parte interesată să poată audita codul și, dacă este cazul, să contribuie la îmbunătățirea codului, să corecteze eventualele erori și să asigure transparența prelucrării datelor cu caracter personal.
GEN-4	Aplicația ar trebui să fie pusă la dispoziție gradual, iar fiecare nouă etapă trebuie să permită validarea progresivă a eficacității sale din perspectiva sănătății publice. În acest scop, trebuie definit în amonte un protocol de evaluare care să specifice indicatorii care trebuie urmăriți pentru a aprecia eficacitatea aplicației.

4. Scopuri

PUR-1	Aplicația trebuie să aibă drept scop unic urmărirea contactelor, astfel încât persoanele potențial expuse la SARS-CoV-2 să primească alerte în acest sens și să poată primi îngrijirile corespunzătoare. Aplicația nu trebuie utilizată în alte scopuri
PUR-2	și nu trebuie deturnată de la utilizarea sa principală, care este aceea de a monitoriza respectarea măsurilor de carantină sau de izolare și/sau distanțare socială.
PUR-3	Aplicația nu trebuie să fie utilizată pentru a trage concluzii cu privire la localizarea utilizatorilor pe baza interacțiunii acestora și/sau a oricăror altor mijloace.

5. Considerații de ordin funcțional

FUNC-1	Aplicația trebuie să ofere o funcționalitate care să le permită utilizatorilor să fie informați că au fost potențial expuși la virus, pe baza proximității față de un utilizator infectat într-un interval de X zile înainte de primirea de către acesta a unui rezultat pozitiv la testul de depistare (valoarea X fiind definită de autoritățile din domeniul sănătății).
FUNC-2	Aplicația ar trebui să le ofere recomandări utilizatorilor identificați ca fiind potențial expuși la virus. Ar trebui să ofere instrucțiuni privind măsurile de urmat și ar trebui să îi permită utilizatorului să solicite sfaturi, caz în care intervenția umană ar fi obligatorie.

FUNC-3	Algoritmul care măsoară riscul de infecție prin luarea în considerare a factorilor distanță și timp și care determină în acest mod momentul în care un contact trebuie să fie înscris pe lista de urmărire a contactelor trebuie să poată fi ajustat în mod securizat pentru a se ține seama de cele mai recente cunoștințe privind răspândirea virusului.
FUNC-4	**Utilizatorii trebuie să fie informați în cazul în care au fost expuși la virus** sau trebuie să obțină periodic informații cu privire la expunerea la virus pe parcursul perioadei de incubație a virusului.
FUNC-5	Aplicația ar trebui să fie interoperabilă cu alte aplicații dezvoltate în statele membre, astfel încât utilizatorii care călătoresc în diferite state membre să poată fi notificați în mod eficient.

6. Date

DATA-1	Aplicația trebuie să fie în măsură să transmită și să recepționeze date prin intermediul tehnologiilor de comunicații de proximitate, cum ar fi tehnologia Bluetooth cu consum energetic redus, astfel încât să se poată efectua urmărirea contactelor.
DATA-2	Aceste date transmise trebuie să includă identificatori pseudoaleatorii și puternici din punct de vedere criptografic, generați de aplicație și specifici acesteia.
DATA-3	Riscul de coliziune între identificatorii pseudoaleatorii trebuie să fie suficient de scăzut.
DATA-4	Identificatorii pseudoaleatorii trebuie reînnoiți regulat, cu o frecvență suficientă pentru a se limita riscul ca orice persoană, inclusiv operatorii serverelor centrale, alți utilizatori de aplicații sau terți răuvoitori, să reidentifice un utilizator, să îl urmărească fizic sau să coreleze datele cu acesta. Acești identificatori trebuie să fie generați de aplicația utilizatorului, eventual pe baza unor valori inițiale furnizate de serverul central.
DATA-5	În conformitate cu principiul reducerii la minimum a datelor, aplicația nu trebuie să colecteze alte date decât cele strict necesar pentru urmărirea contactelor.
DATA-6	Aplicația nu trebuie să colecteze datele de localizare în scopul urmăririi contactelor. Datele de localizare pot fi prelucrate cu unicul scop de a permite aplicației să interacționeze cu aplicații similare în alte țări și ar trebui să fie limitate în ceea ce privește precizia la ceea ce este strict necesar pentru acest scop unic.
DATA-7	Aplicația nu ar trebui să colecteze alte date privind sănătatea în afara celor strict necesare pentru îndeplinirea scopului aplicației, decât cu titlu facultativ și cu unicul scop de a sprijini procesul decizional de informare a utilizatorului.

DATA-8	Utilizatorii trebuie să fie informați cu privire la toate datele cu caracter personal care vor fi colectate. Aceste date ar trebui să fie colectate numai cu autorizația utilizatorului.

7. Proprietăți tehnice

TECH-1	Aplicația ar trebui să folosească tehnologii disponibile precum tehnologia de comunicații de proximitate (de exemplu tehnologia Bluetooth cu consum energetic redus) pentru a-i detecta pe utilizatorii din vecinătatea dispozitivului pe care rulează aplicația.
TECH-2	Aplicația ar trebui să păstreze istoricul contactelor unui utilizator în echipament pe o perioadă de timp limitată și predefinită.
TECH-3	Pentru o parte dintre funcționalitățile sale, aplicația se poate baza pe un server central,
TECH-4	însă arhitectura acesteia trebuie să se bazeze cât mai mult posibil pe dispozitivele utilizatorilor.
TECH-5	La inițiativa utilizatorilor raportați în aplicație ca fiind infectați cu virusul și după confirmarea stării lor de sănătate de către un cadru medical care deține toate calificările necesare, istoricul contactelor lor sau identificatorii proprii ar trebui transmiși serverului central.

8. Securitate

SEC-1	Trebuie să existe un mecanism care să verifice starea de sănătate a utilizatorilor care au fost raportați în aplicație ca fiind purtători ai SARS-CoV-2, de exemplu prin furnizarea unui cod de unică folosință legat de un laborator de testare sau de un cadru medical. Dacă nu se poate obține confirmarea în mod securizat, datele nu trebuie prelucrate.
SEC-2	Transmiterea datelor către serverul central trebuie să aibă loc prin intermediul unui canal securizat. Utilizarea serviciilor de notificare puse la dispoziție de furnizorii de platforme de sisteme de operare ar trebui evaluată cu atenție și nu ar trebui să conducă la divulgarea oricăror date către părți terțe.
SEC-3	Solicitările nu trebuie să fie vulnerabile la eventualele manipulări frauduloase ale unor utilizatori rău-intenționați.
SEC-4	Trebuie folosite tehnici criptografice de ultimă generație pentru securizarea schimburilor dintre aplicație și server și între aplicații și, ca regulă generală, pentru a proteja informațiile stocate în aplicații și pe server. Printre tehnicile care pot fi utilizate se numără: criptarea simetrică și asimetrică, funcțiile hash, testul de apartenență la un domeniu privat, intersectarea seturilor private, filtrele Bloom, extragerea de informații cu caracter privat, criptarea homomorfică etc.

SEC-5	Serverul central nu trebuie să păstreze identificatorii conexiunii de rețea (de exemplu, adresele IP) a niciunui utilizator, în special a celor care au fost diagnosticați pozitiv și care și-au transmis istoricul contactelor sau identificatorii proprii.
SEC-6	Pentru a evita asumarea unor identități false sau crearea de utilizatori falși, serverul trebuie să autentifice aplicația.
SEC-7	Aplicația trebuie să autentifice serverul central.
SEC-8	Funcționalitățile serverului ar trebui să fie protejate împotriva atacurilor prin retransmiterea conținutului.
SEC-9	Informațiile transmise de serverul central trebuie să fie semnate pentru se autentifica originea și integritatea acestora.
SEC-10	Accesul la toate datele stocate în serverul central și care nu sunt disponibile publicului trebuie limitat la persoanele autorizate.
SEC-11	Administratorul autorizațiilor dispozitivului la nivelul sistemului de operare trebuie să solicite doar aprobările necesare pentru accesarea și utilizarea, atunci când este necesar, a modulelor de comunicații, pentru stocarea datelor în terminal și pentru schimbul de informații cu serverul central.

9. Protecția datelor cu caracter personal și a vieții private a persoanelor fizice

Atenție: următoarele orientări se referă la o aplicație al cărei unic scop este urmărirea contactelor.

PRIV-1	Schimburile de date trebuie să respecte viața privată a utilizatorilor (și, în special, principiul reducerii la minimum a datelor).
PRIV-2	Aplicația nu trebuie să permită identificarea directă a utilizatorilor pe durata utilizării.
PRIV-3	Aplicația nu trebuie să permită urmărirea deplasărilor efectuate de utilizatori.
PRIV-4	Utilizarea aplicației nu ar trebui să permită utilizatorilor să obțină informații despre alți utilizatori (și, în special, dacă aceștia sunt purtători sau nu ai virusului).
PRIV-5	Încrederea în serverul central trebuie să fie limitată. Gestionarea serverului central trebuie să respecte norme de guvernanță clar definite și să includă toate măsurile necesare pentru asigurarea securității acestuia. Localizarea serverului central ar trebui să îi permită autorității de supraveghere competente să efectueze o supraveghere eficace a acestuia.
PRIV-6	Trebuie efectuată o evaluare a impactului asupra protecției datelor, ale cărei rezultate trebuie publicate.
PRIV-7	Aplicația ar trebui să îl informeze pe utilizator doar dacă a fost expus la virus, fără a dezvălui, dacă este posibil, informații cu privire la alți utilizatori, de câte ori și când a fost expus.
PRIV-8	Informațiile transmise prin aplicație nu trebuie să le permită utilizatorilor să îi identifice pe utilizatorii care sunt purtători ai virusului sau să identifice deplasările acestora.
PRIV-9	Informațiile transmise prin aplicație nu trebuie să le permită autorităților din domeniul sănătății să îi identifice pe utilizatorii potențial expuși la virus, cu excepția cazului în care aceștia și-au exprimat acordul în acest sens.
PRIV-10	Solicitările adresate serverului central de aplicație nu trebuie să dezvăluie nicio informație în legătură cu purtătorul virusului.
PRIV-11	Solicitările adresate serverului central de aplicație nu trebuie să dezvăluie nicio informație inutilă cu privire la utilizator, cu excepția, eventual și numai atunci când este necesar, a identificatorilor săi pseudonimi și a listei sale de contacte.
PRIV-12	Atacurile prin care se încearcă corelarea datelor cu persoanele nu trebuie să fie posibile.
PRIV-13	Utilizatorii trebuie să își poată exercita drepturile prin intermediul aplicației.
PRIV-14	Ștergerea aplicației trebuie să atragă după sine ștergerea tuturor datelor colectate local.
PRIV-15	Aplicația ar trebui să colecteze doar datele transmise de către instanțe ale aplicației sau aplicații echivalente interoperabile. Nu se vor colecta date referitoare la alte aplicații și/sau dispozitive de comunicații de proximitate.

PRIV-16	Pentru a evita reidentificarea de către serverul central, ar trebui să fie folosite servere proxy. Scopul acestor *servere care nu au un comportament coluziv este* de a amesteca identificatorii mai multor utilizatori (atât cei ai purtătorilor virusului, cât și cei trimiși de solicitanți) înainte de a îi transmite serverului central, astfel încât acesta să nu poată cunoaște identificatorii utilizatorilor (cum ar fi adresele IP).
PRIV-17	Aplicația și serverul trebuie să fie atent dezvoltate și configurate pentru a nu colecta date inutile (de exemplu, niciun identificator nu ar trebui inclus în jurnalele serverului etc.) și pentru a se evita situația ca kiturile de dezvoltare de software (SDK) ale terților să colecteze date în alte scopuri.

Cele mai multe dintre aplicațiile de urmărire a contactelor care sunt analizate în prezent aplică, practic, două abordări atunci când un utilizator este declarat infectat: fie trimit unui server istoricul contactelor de proximitate pe care le-au obținut prin analiza acestora, fie trimit lista propriilor identificatori care au fost transmiși. Din aceste două abordări decurg următoarele principii: deși în documentul de față sunt analizate aceste abordări, nu înseamnă că nu sunt posibile sau chiar preferabile alte abordări, de exemplu soluții care realizează o anumită formă de criptare E2E (de la un capăt la altul) sau care aplică alte tehnologii de sporire a securității sau a protecției vieții private.

9.1. **Principii care se aplică** numai **atunci când aplicația trimite unui server o listă de contacte**

CON-1	În urma unei acțiuni voluntare din partea utilizatorilor, serverul central trebuie să colecteze istoricul contactelor avute de utilizatorii raportați în aplicație ca depistați pozitiv cu SARS-CoV-2.
CON-2	Serverul central nu trebuie să păstreze sau să distribuie o listă a identificatorilor pseudonimi ai utilizatorilor purtători ai virusului.
CON-3	Istoricul contactelor, care este stocat pe serverul central, trebuie șters de îndată ce utilizatorii sunt informați cu privire la faptul că s-au aflat în apropierea unei persoane diagnosticate pozitiv.
CON-4	Cu excepția cazului în care utilizatorul depistat pozitiv își partajează istoricul contactelor cu serverul central sau a cazului în care utilizatorul trimite o solicitare serverului pentru a afla dacă a fost expus potențial la virus, datele nu trebuie să părăsească echipamentul utilizatorului.
CON-5	Orice identificator inclus în istoricul local trebuie șters după X zile de la colectare (valoarea X fiind definită de autoritățile din domeniul sănătății).
CON-6	Istoricul contactelor trimis de utilizatori nu ar trebui prelucrat ulterior, de exemplu, prin corelare încrucișată pentru a se crea hărți de proximitate la nivel mondial.
CON-7	Datele din jurnalele serverului trebuie reduse la minimum și trebuie să respecte cerințele privind protecția datelor.

9.2. Principii care se aplică numai atunci când aplicația trimite unui server o listă cu identificatorii proprii

ID-1	Serverul central trebuie să colecteze identificatorii transmiși de aplicația utilizatorilor raportați ca depistați pozitiv cu SARS-CoV-2 în urma unei acțiuni voluntare din partea acestora.
ID-2	Serverul central nu trebuie să păstreze sau să distribuie istoricul contactelor utilizatorilor purtători ai virusului.
ID-3	Identificatorii stocați pe serverul central trebuie șterși după ce au fost distribuiți celorlalte aplicații.
ID-4	Cu excepția cazului în care utilizatorul depistat pozitiv își partajează identificatorii cu serverul central sau a celui în care utilizatorul trimite o solicitare serverului pentru a afla dacă a fost expus potențial la virus, datele nu trebuie să părăsească echipamentul utilizatorului.
ID-5	Datele din jurnalele serverului trebuie reduse la minimum și trebuie să respecte cerințele privind protecția datelor.