Usmernenia

Usmernenia 4/2020 týkajúce sa lokalizačných údajov a iných nástrojov na sledovanie kontaktov v kontexte vypuknutia nákazy COVID-19

Prijaté 21. apríla 2020

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

prijaté

Obsah

Obsah 2
1 Úvod & kontext 3
2 Použitie lokalizačných údajov 5
2.1 Zdroje lokalizačných údajov 5
2.2 Zameranie sa na používanie anonymizovaných lokalizačných údajov 5
3 Aplikácie na sledovanie kontaktov 7
3.1 Všeobecná právna analýza 7
3.2 Odporúčania a požiadavky na funkčnosť 9
4 Záver 11
Príloha -- Aplikácie na sledovanie kontaktov Analytická príručka 12

Európsky výbor pre ochranu údajov

so zreteľom na článok 70 ods. 1 písm. e) nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (ďalej len „všeobecné nariadenie o ochrane údajov“),

so zreteľom na Dohodu o EHP, a najmä na prílohu XI a protokol 37 k tejto dohode, ktoré boli zmenené rozhodnutím Spoločného výboru EHP č. 154/2018 zo 6. júla 2018[1],

so zreteľom na článok 12 a článok 22 svojho rokovacieho poriadku,

PRIJAL TIETO USMERNENIA

1 ÚVOD & KONTEXT

1 Vlády a súkromné subjekty chcú v rámci reakcie na pandémiu COVID-19 využívať aj riešenia založené na údajoch, čo vyvoláva viaceré obavy v súvislosti s ochranou súkromia.

2 Európsky výbor pre ochranu údajov zdôrazňuje, že právny rámec ochrany údajov bol navrhnutý tak, aby bol flexibilný, a ako taký je schopný zabezpečiť účinnú reakciu, ktorou sa obmedzí šírenie pandémie a pritom budú chránené základné ľudské práva a slobody.

3 Európsky výbor pre ochranu údajov je pevne presvedčený, že ak je na zvládanie pandémie COVID-19 nevyhnutné spracúvanie osobných údajov, tak pre budovanie dôvery, vytvorenie podmienok na spoločenskú prijateľnosť akéhokoľvek riešenia, a teda pre zabezpečenie účinnosti navrhovaných opatrení je zásadné dôležitá ochrana údajov. Keďže vírus nepozná hranice, zdá sa, že je vhodnejšie vyvinúť spoločný európsky prístup k súčasnej kríze alebo aspoň zaviesť interoperabilný rámec.

4 Európsky výbor pre ochranu údajov sa vo všeobecnosti domnieva, že údaje a technológie používané na boj proti COVID-19 by sa mali používať skôr na posilnenie postavenia jednotlivcov, ako na ich kontrolu, stigmatizáciu či trestanie. Navyše, hoci údaje a technológie môžu byť dôležitými nástrojmi, sú im vlastné určité obmedzenia a môžu len zvyšovať účinnosť iných opatrení v oblasti verejného zdravia. Každé opatrenie prijaté členskými štátmi alebo inštitúciami EÚ, ktoré sa týka spracovania osobných údajov na boj proti COVID-19, sa musí riadiť všeobecnými zásadami účinnosti, nevyhnutnosti a primeranosti.

5 V týchto usmerneniach sa objasňujú podmienky a zásady primeraného používania lokalizačných údajov a nástrojov na sledovanie kontaktov, a to na dva konkrétne účely:

- použitie lokalizačných údajov na podporu reakcie na pandémiu prostredníctvom modelovania šírenia vírusu s cieľom vyhodnotiť celkovú účinnosť opatrení na obmedzenie pohybu;
- sledovanie kontaktov, ktorého cieľom je upovedomiť jednotlivcov o skutočnosti, že boli v tesnej blízkosti niekoho, u koho sa napokon potvrdí, že je nositeľom vírusu, a to so zámerom čo najskôr prerušiť reťazce nákazy.

6 Účinný prínos aplikácií na sledovanie kontaktov k zvládnutiu pandémie závisí od mnohých faktorov (napr. percenta ľudí, ktorí by si aplikáciu mali nainštalovať; vymedzenia „kontaktu“ z hľadiska blízkosti a trvania). Takéto aplikácie navyše musia byť súčasťou komplexnej

1 Odkazy na „členské štáty“ v tomto dokumente by sa mali chápať ako odkazy na „členské štáty EHP“.

stratégie v oblasti verejného zdravia zameranej na boj proti pandémii, ktorá by okrem iného mala zahŕňať testovanie a následné manuálne sledovanie kontaktov s cieľom odstrániť pochybnosti. Ich zavádzanie by malo byť sprevádzané podpornými opatreniami s cieľom zabezpečiť, aby sa informácie používateľom poskytovali v kontexte a aby boli varovania užitočné pre systém verejného zdravotníctva. Inak tieto aplikácie nemusia dosiahnuť plný účinok.

7 Európsky výbor pre ochranu údajov zdôrazňuje, že všeobecné nariadenie o ochrane údajov aj smernica 2002/58/ES (ďalej len „smernica“) obsahujú osobitné pravidlá, ktoré umožňujú použitie anonymných alebo osobných údajov na podporu orgánov verejnej moci a ďalších aktérov na vnútroštátnej úrovni a na úrovni EÚ pri monitorovaní a obmedzovaní šírenia vírusu SARS-CoV-2[2].

8 V tejto súvislosti Európsky výbor pre ochranu údajov už zaujal stanovisko ku skutočnosti, že používanie aplikácií na sledovanie kontaktov by malo byť dobrovoľné a nemalo by byť založené na sledovaní jednotlivých pohybov, ale skôr na informáciách o blízkosti vo vzťahu k používateľom.[3]

[2] Pozri predchádzajúce vyhlásenie Európskeho úradu na ochranu údajov k vypuknutiu nákazy COVID 19.
[3] [3] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

2 POUŽITIE LOKALIZAČNÝCH ÚDAJOV

2.1 Zdroje lokalizačných údajov

9 Na modelovanie šírenia vírusu a celkovej účinnosti opatrení na obmedzenie pohybu sú k dispozícii dva hlavné zdroje lokalizačných údajov:

- lokalizačné údaje získané poskytovateľmi elektronických komunikačných služieb (ako sú operátori mobilných telekomunikačných služieb) v priebehu poskytovania služieb a
- lokalizačné údaje získané aplikáciami poskytovateľov služieb informačnej spoločnosti, ktorých funkčnosť si vyžaduje používanie takýchto údajov (napr. navigácia, dopravné služby atď.).

10 Európsky výbor pre ochranu údajov pripomína, že lokalizačné údaje[4] získané od poskytovateľov elektronických komunikácií sa môžu spracúvať iba v rozsahu stanovenom článkami 6 a 9 smernice. To znamená, že tieto údaje sa môžu zasielať orgánom verejnej moci alebo iným tretím stranám iba vtedy, ak ich poskytovateľ anonymizoval alebo ak ide o údaje udávajúce geografickú polohu koncového zariadenia používateľa, ktoré nie sú prevádzkovými údajmi, a s predchádzajúcim súhlasom používateľov[5].

11 Pokiaľ ide o informácie zhromaždené priamo z koncového zariadenia vrátane lokalizačných údajov, uplatňuje sa článok 5 ods. 3 smernice. Uchovávanie informácií v zariadení používateľa alebo získavanie prístupu k informáciám, ktoré sú už uchovávané, je povolené len vtedy, ak i) používateľ dal súhlas[6] alebo ak je ii) uchovávanie a/alebo sprístupnenie nevyhnutne potrebné pre službu informačnej spoločnosti, o ktorú používateľ výslovne požiadal.

12 Výnimky z práv a povinností stanovených v smernici sú však možné podľa článku 15, ak predstavujú nevyhnutné, primerané a proporcionálne opatrenie na dosiahnutie určitých cieľov v demokratickej spoločnosti[7].

13 Ak ide o opakované použitie lokalizačných údajov získaným poskytovateľom služieb informačnej spoločnosti na účely modelovania (napr. prostredníctvom operačného systému alebo nejakej predtým nainštalovanej aplikácie), musia byť splnené ďalšie podmienky. Ak sa údaje získali v súlade s článkom 5 ods. 3 smernice, môžu sa ďalej spracúvať iba s dodatočným súhlasom dotknutej osoby alebo na základe práva Únie alebo členského štátu, ktoré v demokratickej spoločnosti predstavuje nevyhnutné a primerané opatrenie na ochranu cieľov uvedených v článku 23 ods. 1 všeobecného nariadenia o ochrane údajov[8].

2.2 Zameranie sa na používanie anonymizovaných lokalizačných údajov

14 Európsky výbor pre ochranu údajov zdôrazňuje, že pokiaľ ide o používanie lokalizačných údajov, malo by sa vždy uprednostniť spracúvanie anonymizovaných údajov, a nie osobných údajov.

15 Pojmom anonymizácia sa označuje použitie súboru techník na odstránenie schopnosti pri vynaložení „primeraného“ úsilia prepojiť údaje s identifikovanou alebo identifikovateľnou fyzickou osobou. V tejto „skúške primeranosti“ sa musia zohľadniť objektívne aspekty (čas, technické prostriedky) a kontextové prvky, ktoré sa môžu v jednotlivých prípadoch líšiť (vzácnosť javu pri zvážení hustoty obyvateľstva, povahy a množstva údajov). Ak údaje neprejdú touto skúškou, potom neboli anonymizované, a preto zostávajú v rozsahu pôsobnosti všeobecného nariadenia o ochrane údajov.

---

[4] Pozri článok 2 písm. c) smernice.
[5] Pozri články 6 a 9 smernice.
[6] Pojem súhlas v smernici zodpovedá pojmu súhlas vo všeobecnom nariadení o ochrane údajov a musí spĺňať všetky požiadavky súhlasu stanovené v článku 4 ods. 11 a článku 7 všeobecného nariadenia o ochrane údajov.
[7] V súvislosti s výkladom článku 15 smernice pozri aj rozsudok Súdneho dvora Európskej únie z 29. januára 2008 vo veci C-275/06, Productores de Música de España (Promusicae)/Telefónica de España SAU.
[8] Pozri oddiel 1.5.3 usmernení 1/2020 o spracúvaní osobných údajov v súvislosti s pripojenými vozidlami.

16 Hodnotenie spoľahlivosti anonymizácie sa opiera o tri kritériá: i) vyčlenenie (izolácia jednotlivca v rámci väčšej skupiny na základe údajov); ii) prepojiteľnosť (prepojenie dvoch záznamov týkajúcich sa tej istej osoby); a (iii) odvodenie (odvodenie, s významnou pravdepodobnosťou, neznámych informácií o jednotlivcovi).

17 Pojem anonymizácia sa často nechápe správne a mylne sa považuje za pseudonymizáciu. Anonymizácia umožňuje použitie údajov bez akýchkoľvek obmedzení, pseudonymizované údaje však stále patria do rozsahu pôsobnosti všeobecného nariadenia o ochrane údajov.

18 Existuje veľa možností účinnej anonymizácie[9], treba však byť obozretný. Údaje nemôžu byť anonymizované samé osebe, čo znamená, že len celé dátové súbory môžu alebo nemôžu byť anonymizované. V tomto zmysle sa každý zásah do jedného vzoru údajov (pomocou šifrovania alebo akýchkoľvek iných matematických transformácií) môže v najlepšom prípade považovať za pseudonymizáciu.

19 Procesy anonymizácie a útoky opätovnej identifikácie sa aktívne zaoberá výskum. Je dôležité, aby každý prevádzkovateľ, ktorý vykonáva anonymizačné riešenia, sledoval najnovší vývoj v tejto oblasti, najmä pokiaľ ide o lokalizačné údaje (pochádzajúce od telekomunikačných operátorov a/alebo poskytovateľov služieb informačnej spoločnosti), o ktorých je známe, že sa ťažko anonymizujú.

20 V mnohých výskumoch sa skutočne potvrdilo[10], *že lokalizačné údaje, ktoré sa považujú za anonymizované,* také v skutočnosti nemusia byť. Stopy pohybu jednotlivcov sú vo svojej podstate úzko prepojené a jedinečné. Za určitých okolností preto môžu ľahko podliehať pokusom o opätovnú identifikáciu.

21 Jediný vzorec údajov sledujúci polohu jednotlivca počas významného časového obdobia nie je možné úplne anonymizovať. Toto posúdenie môže stále platiť, ak sa presnosť zaznamenaných zemepisných súradníc dostatočne nezníži, alebo ak sa odstránia podrobnosti o trase, a to aj vtedy, ak sa zachová iba poloha miest, kde dotknutá osoba zostáva značný čas. Platí to aj pre lokalizačné údaje, ktoré sú slabo agregované.

22 Na dosiahnutie anonymizácie musia byť lokalizačné údaje starostlivo spracované, aby splnili test primeranosti. V tomto zmysle takéto spracovanie zahŕňa posudzovanie súborov lokalizačných údajov ako celku, ako aj spracúvanie údajov od primerane veľkej skupiny jednotlivcov pomocou dostupných spoľahlivých anonymizačných techník za predpokladu, že sú primerane a účinne implementované.

23 A napokon, vzhľadom na komplexnosť procesov anonymizácie sa dôrazne odporúča transparentnosť v oblasti metodiky anonymizácie.

---

[9] de Montjoye et al., 2018. „On the privacy-conscientious use of mobile phone data (Využívanie údajov z mobilných telefónov v súlade s ochranou súkromia)".

[10] De Montjoye et al., 2013. „Unique in the Crowd: The privacy bounds of human mobility (Jedinečný v dave: Hranice súkromia pri ľudskej mobilite)", a Pyrgelis et al., 2017. „Knock Knock, Who's There?Membership Inference on Aggregate Location Data (Klop, klop, kto je tam?: Inferencia o členstve na základe agregovaných lokalizačných údajov)".

3 APLIKÁCIE NA SLEDOVANIE KONTAKTOV

3.1 Všeobecná právna analýza

24 Systematické a rozsiahle monitorovanie polohy a/alebo kontaktov medzi fyzickými osobami je vážnym zásahom do ich súkromia. Takýto zásah môže byť odôvodnený iba v prípade dobrovoľného prijatia používateľmi na každý z príslušných účelov. To by znamenalo najmä to, že jednotlivci, ktorí sa rozhodnú takéto aplikácie nepoužiť alebo ich nemôžu používať, by nemali byť nijakým spôsobom znevýhodnení.

25 Na zabezpečenie zodpovednosti by mal byť jasne určený prevádzkovateľ každej aplikácie na sledovanie kontaktov. Európsky výbor pre ochranu údajov sa domnieva, že prevádzkovateľmi by mohli byť orgány verejného zdravotníctva[11]; možno však navrhnúť aj iných prevádzkovateľov. V každom prípade, ak sú do zavádzania aplikácií na sledovanie kontaktov zapojení rôzni aktéri, ich úlohy a povinnosti sa musia od začiatku jasne stanoviť a vysvetliť používateľom.

26 Okrem toho, pokiaľ ide o zásadu obmedzenia účelu, tieto ciele musia byť dostatočne konkrétne na to, aby sa vylúčilo ďalšie spracovanie na účely nesúvisiace so zvládaním zdravotnej krízy COVID-19 (napr. obchodné účely alebo účely presadzovania práva). Keď bude cieľ jasne stanovený, bude potrebné zabezpečiť, aby použitie osobných údajov bolo primerané, nevyhnutné a proporcionálne.

27 V súvislosti s aplikáciou na sledovanie kontaktov by sa mala starostlivo zvážiť zásada minimalizácie údajov a zásada špecificky navrhnutej ochrany údajov a štandardnej ochrany údajov:

- v aplikáciách na sledovanie kontaktov sa nevyžaduje sledovanie polohy jednotlivých používateľov. Namiesto toho by sa mali používať údaje o blízkosti;
- keďže aplikácie na sledovanie kontaktov môžu fungovať bez priamej identifikácie jednotlivcov, mali by sa prijať vhodné opatrenia s cieľom predísť opätovnej identifikácii;
- získané informácie by sa mali nachádzať v koncových zariadeniach používateľa a v prípade, že je to absolútne nevyhnutné, mali by sa získavať iba relevantné informácie.

28 Pokiaľ ide o zákonnosť spracovania, Európsky výbor pre ochranu údajov poznamenáva, že aplikácie na sledovanie kontaktov zahŕňajú uchovávanie informácií a/alebo prístup k informáciám už uchovávaným v koncovom zariadení, na ktoré sa vzťahuje článok 5 ods. 3 smernice. Ak sú tieto operácie nevyhnutne potrebné na to, aby poskytovateľ aplikácie poskytoval službu výslovne vyžiadanú používateľom, spracovanie by si nevyžadovalo jeho súhlas. V prípade operácií, ktoré nie sú nevyhnutne potrebné, by poskytovateľ musel získať súhlas používateľa.

29 Európsky výbor pre ochranu údajov ďalej poznamenáva, že samotná skutočnosť, že k používaniu aplikácií na sledovanie kontaktov dochádza dobrovoľne, neznamená, že spracúvanie osobných údajov sa bude nevyhnutne zakladať na súhlase. Ak orgány verejnej moci poskytujú službu na základe udeleného mandátu a v súlade s požiadavkami stanovenými zákonom, zdá sa, že najvhodnejším právnym základom pre spracovanie je nevyhnutnosť splnenia úlohy vo verejnom záujme, t. j. článok 6 ods. 1 písm. e) všeobecného nariadenia o ochrane údajov.

30 V článku 6 ods. 3 všeobecného nariadenia o ochrane údajov sa vysvetľuje, že základom pre spracovanie uvedené v článku 6 ods. 1 písm. e) sú právne predpisy Únie alebo členského štátu, ktoré sa vzťahujú na prevádzkovateľa. Účel spracúvania sa stanoví na tomto právnom základe, alebo pokiaľ ide o spracúvanie uvedené v odseku 1 písm. e), ide o spracúvanie nevyhnutné na

[11] Pozri aj dokument Európskej komisie „Usmernenie týkajúce sa aplikácií podporujúcich boj proti pandémii COVID-19 v súvislosti s ochranou údajov“, Brusel, 16. 4. 2020 C (2020) 2523 final.

splnenie úlohy vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi.[12]

31 Právny základ alebo legislatívne opatrenie, ktoré poskytuje právny základ pre používanie aplikácií na sledovanie kontaktov, by však malo obsahovať zmysluplné záruky vrátane odkazu na dobrovoľnú povahu aplikácie. Mala by sa zahrnúť jasná špecifikácia účelu a výslovné obmedzenia týkajúce sa ďalšieho použitia osobných údajov, ako aj jasná identifikácia zúčastnených prevádzkovateľov. Mali by sa identifikovať aj kategórie údajov, ako aj subjekty (a účely, na ktoré sa osobné údaje môžu poskytovať). V závislosti od úrovne zasahovania by sa mali zahrnúť ďalšie záruky, a to s ohľadom na povahu, rozsah a účel spracovania. Európsky výbor pre ochranu údajov napokon odporúča, aby sa zároveň čo najskôr zahrnuli kritériá, na základe ktorých sa rozhodne, kedy bude aplikácia ukončená a ktorý subjekt bude zodpovedný za vykonanie tohto rozhodnutia.

32 Ak sa však spracovanie údajov zakladá na inom právnom základe, napríklad na súhlase □článok 6 ods. 1 písm. a)□[13], prevádzkovateľ bude musieť zabezpečiť splnenie prísnych požiadaviek na platnosť takéhoto právneho základu.

33 Použitie aplikácie na boj proti pandémii COVID-19 by navyše mohlo viesť k získavaniu údajov týkajúcich sa zdravia (napríklad o stave infikovanej osoby). Spracovanie takýchto údajov je povolené, ak je potrebné z dôvodov verejného záujmu v oblasti verejného zdravia a pri splnení podmienok článku 9 ods. 2 písm. i) všeobecného nariadenia o ochrane údajov[14] alebo na účely zdravotnej starostlivosti, ako sa uvádza v článku 9 ods. 2 písm. h) všeobecného nariadenia o ochrane údajov[15]. V závislosti od právneho základu by mohlo byť založené aj na výslovnom súhlase □článok 9 ods. 2 písm. a)□ všeobecného nariadenia o ochrane údajov.

34 V súlade s pôvodným účelom sa v článku 9 ods. 2 písm. j) všeobecného nariadenia o ochrane údajov umožňuje aj spracúvanie údajov týkajúcich sa zdravia, ak je to potrebné na účely vedeckého výskumu alebo na štatistické účely.

35 Súčasná zdravotná kríza by sa nemala využívať ako príležitosť na stanovenie neprimeraných mandátov na uchovávanie údajov. Pri minimalizácii uchovávania by sa mali brať do úvahy skutočné potreby a význam z lekárskeho hľadiska (napr. epidemiologické aspekty, ako je inkubačný čas atď.) a osobné údaje by sa mali uchovávať iba počas trvania krízy COVID-19. Po kríze by sa vo všeobecnosti všetky osobné údaje mali vymazať alebo anonymizovať.

36 Európsky výbor pre ochranu údajov chápe, že takéto aplikácie nemôžu nahradiť, ale iba podporovať manuálne sledovanie kontaktov vykonávané kvalifikovanými zdravotníckymi pracovníkmi, ktorí môžu rozlíšiť, či blízke kontakty môžu alebo nemôžu viesť k prenosu vírusu (napr. pri interakcii s niekým, kto je alebo nie je chránený primeranými prostriedkami – pokladníci a pod.). Európsky výbor pre ochranu údajov zdôrazňuje, že postupy a procesy vrátane príslušných algoritmov implementovaných aplikáciami na sledovanie kontaktov by mali fungovať pod prísnym dohľadom kvalifikovaných pracovníkov tak, aby sa obmedzil výskyt akýchkoľvek falošných pozitívnych alebo negatívnych výsledkov. Najmä poskytovanie poradenstva o ďalších krokoch by nemalo byť založené výhradne na automatizovanom spracovaní.

37 S cieľom zabezpečiť spravodlivosť a zodpovednosť algoritmov a všeobecnejšie ich súlad so zákonom musia byť algoritmy kontrolovateľné a mali by byť pravidelne skúmané nezávislými odborníkmi. S cieľom čo najširšej kontroly by sa mal zverejniť zdrojový kód aplikácie.

---

[12] Pozri odôvodnenie 41.

[13] Prevádzkovatelia (najmä orgány verejnej moci) musia venovať osobitnú pozornosť skutočnosti, že súhlas by sa nemal považovať za slobodne daný, ak jednotlivec nemá skutočnú možnosť odmietnuť alebo odvolať svoj súhlas bez toho, aby bol poškodený.

[14] Spracúvanie musí vychádzať z právnych predpisov Únie alebo členských štátov, v ktorých sa stanovujú vhodné a konkrétne opatrenia na ochranu práv a slobôd dotknutej osoby, najmä profesijného tajomstva.

[15] Pozri článok 9 ods. 2 písm. h) všeobecného nariadenia o ochrane údajov.

38 Falošne pozitívne výsledky sa v istej miere vždy vyskytujú. Keďže identifikácia rizika infekcie môže mať veľký vplyv na jednotlivcov, napríklad na zotrvanie v samoizolácii až do získania negatívnych výsledkov testov, schopnosť opraviť údaje a/alebo výsledky následnej analýzy sú nevyhnutné. Toto by sa, samozrejme, malo vzťahovať iba na scenáre a implementácie, keď sa údaje spracúvajú a/alebo uchovávajú spôsobom, ktorý takúto opravu technicky umožňuje, a v prípadoch, keď sa pravdepodobne vyskytnú uvedené nepriaznivé účinky.

39 Európsky výbor pre ochranu údajov sa napokon domnieva, že keďže spracovanie sa považuje za pravdepodobne vysoko rizikové (spracúvanie údajov týkajúcich sa zdravia, predpokladaná veľká miera prijatia, systematické monitorovanie, využívanie nového technologického riešenia), pred zavedením takéhoto nástroja sa musí vykonať posúdenie vplyvu na ochranu údajov[16]. Európsky výbor pre ochranu údajov dôrazne odporúča zverejnenie posúdení vplyvu na ochranu údajov.

3.2 Odporúčania a požiadavky na funkčnosť

40 Podľa zásady minimalizácie údajov by sa ako jedno z opatrení špecificky navrhnutej a štandardnej ochrany údajov[17] mali spracované údaje obmedziť na prísne minimum. V aplikácii by sa nemali získavať nesúvisiace alebo nepotrebné informácie, napríklad občiansky stav, identifikátory komunikácie, položky zoznamov v zariadení, správy, denníky hovorov, lokalizačné údaje, identifikátory zariadenia atď.

41 Údaje vysielané aplikáciami musia obsahovať iba niektoré jedinečné a pseudonymné identifikátory, ktoré aplikácia sama generuje a ktoré sú pre ňu špecifické. Tieto identifikátory sa musia pravidelne obnovovať, a to s frekvenciou, ktorá je zlučiteľná s účelom obmedziť šírenie vírusu a ktorá je postačujúca na zníženie rizika identifikácie a fyzického sledovania jednotlivcov.

42 Implementácie na sledovanie kontaktov môžu byť založené na centralizovanom alebo decentralizovanom prístupe[18]. Obidve možnosti by sa mali považovať za vhodné za predpokladu, že sa zavedú primerané bezpečnostné opatrenia, pričom každá z nich má niekoľko výhod a nevýhod. Koncepčná fáza vývoja aplikácií by preto vždy mala zahŕňať dôkladné zváženie obidvoch koncepcií, pričom sa starostlivo zvážia príslušné účinky na ochranu údajov/súkromia a možné vplyvy na práva jednotlivcov.

43 Každý server zapojený do systému sledovania kontaktov musí zhromažďovať iba históriu kontaktov alebo pseudonymné identifikátory používateľa, ktorý bol diagnostikovaný ako infikovaný na základe náležitého posúdenia orgánmi verejného zdravia a dobrovoľného úkonu používateľa. Druhou možnosťou je, že zoznam pseudonymných identifikátorov infikovaných používateľov alebo ich história kontaktov sa na serveri budú uchovávať iba tak dlho, aby boli potenciálne infikovaní používatelia informovaní o svojom vystavení nákaze, a nemala by sa vykonávať identifikácia potenciálne infikovaných používateľov.

44 Zavedenie globálnej metodiky sledovania kontaktov vrátane aplikácií a manuálneho sledovania si môže v niektorých prípadoch vyžiadať spracovanie ďalších informácií. V tejto súvislosti by tieto doplňujúce informácie mali zostať v koncovom zariadení používateľa a spracúvať sa iba v nevyhnutných prípadoch a s jeho predchádzajúcim a osobitným súhlasom.

---

[16] Pozri usmernenia pracovnej skupiny pre ochranu údajov zriadenej podľa článku 29 (prijaté Európskym výborom pre ochranu údajov) týkajúce sa posúdenia vplyvu na ochranu údajov a stanovenie toho, či na účely nariadenia 2016/679 spracúvanie „pravdepodobne povedie k vysokému riziku“.

[17] Pozri usmernenia Európskeho výboru pre ochranu údajov 4/2019 týkajúce sa špecificky navrhnutej a štandardnej ochrany údajov podľa článku 25

[18] Decentralizované riešenie je viac v súlade so zásadou minimalizácie.

45 Na zabezpečenie údajov uchovávaných na serveroch a v aplikáciách, pri komunikácii medzi aplikáciami a vzdialeným serverom sa musia implementovať najmodernejšie kryptografické techniky. Medzi aplikáciou a serverom sa musí sa vykonávať aj vzájomná autentifikácia.

46 Nahlasovanie používateľov infikovaných SARS-CoV-2 do aplikácie musí podliehať riadnemu schváleniu, napríklad prostredníctvom jednorazového kódu, ktorý bude viazaný na pseudonymnú totožnosť infikovanej osoby a prepojený s odberným miestom alebo so zdravotníckym pracovníkom. Ak nie je možné získať potvrdenie bezpečným spôsobom, nemalo by sa vykonať žiadne spracovanie údajov, pri ktorom sa predpokladá platnosť stavu používateľa.

47 Prevádzkovateľ musí v spolupráci s orgánmi verejnej moci jasne a výslovne informovať, odkiaľ si možno stiahnuť oficiálnu vnútroštátnu aplikáciu na sledovanie kontaktov s cieľom znížiť riziko, že jednotlivci budú používať aplikáciu tretej strany.

4 ZÁVER

48 Svet čelí vážnej kríze verejného zdravia. Kríza si vyžaduje dôrazné reakcie, ktoré budú mať vplyv aj po skončení núdzového stavu. Automatizované spracúvanie údajov a digitálne technológie môžu byť kľúčovými prvkami v boji proti COVID-19. Treba však zohľadniť potenciálne riziko, že opatrenia nebude možné úplne vrátiť späť. Je našou povinnosťou zabezpečiť, aby každé opatrenie prijaté za týchto mimoriadnych okolností bolo nevyhnutné, časovo obmedzené, minimálne a aby bolo predmetom pravidelného a dôkladného preskúmania, ako aj vedeckého hodnotenia.

49 Európsky výbor pre ochranu údajov zdôrazňuje, že by sme si účinná reakcia na súčasnú krízu by sa nemala vylučovať s ochranou našich základných práv: dokážeme dosiahnuť oboje a zásady ochrany údajov môžu navyše zohrávať veľmi dôležitú úlohu v boji proti vírusu. Európske právne predpisy o ochrane údajov umožňujú zodpovedné používanie osobných údajov na účely manažmentu zdravia a zároveň zabezpečujú, aby v tomto procese neboli narušené práva a slobody jednotlivcov.

Za Európsky výbor pre ochranu údajov

predsedníčka

(Andrea Jelinek)

PRÍLOHA -- APLIKÁCIE NA SLEDOVANIE KONTAKTOV ANALYTICKÁ PRÍRUČKA

0. Upozornenie

Toto usmernenie nie je ani normatívne, ani vyčerpávajúce a jeho jediným účelom je poskytnúť všeobecné usmernenie vývojárom a prevádzkovateľom aplikácií na sledovanie kontaktov. Možno použiť aj iné riešenia ako tie, ktoré sú tu opísané, a môžu byť zákonné, pokiaľ sú v súlade s príslušným právnym rámcom (t. j. so všeobecným nariadením o ochrane údajov a smernicou).

Treba takisto poznamenať, že ide o usmernenie všeobecnej povahy. Odporúčania a povinnosti obsiahnuté v tomto dokumente sa preto nesmú považovať za vyčerpávajúce. Vždy sa musí vykonávať posúdenie jednotlivých prípadov a v prípade konkrétnych aplikácií môžu byť potrebné ďalšie opatrenia, ktoré nie sú uvedené v tomto usmernení.

1. Zhrnutie

V mnohých členských štátoch zainteresované strany zvažujú použitie aplikácií *na sledovanie kontaktov*, aby pomohli obyvateľom zistiť, či boli v kontakte s osobou infikovanou vírusom SARS-Cov-2.

Podmienky, za ktorých takéto aplikácie účinne prispejú k zvládnutiu pandémie, zatiaľ nie sú stanovené. Takéto podmienky by bolo dobré stanoviť pred akoukoľvek implementáciou takej aplikácie. Je však dôležité poskytnúť usmernenia, v ktorých sa jednotlivým vývojovým tímom poskytnú príslušné informácie, aby sa zabezpečila ochrana osobných údajov už od počiatočnej fázy návrhu.

Treba poznamenať, že ide o usmernenie všeobecnej povahy. Odporúčania a povinnosti obsiahnuté v tomto dokumente sa preto nesmú považovať za vyčerpávajúce. Vždy sa musí vykonávať posúdenie jednotlivých prípadov a v prípade konkrétnych aplikácií môžu byť potrebné ďalšie opatrenia, ktoré nie sú uvedené v tomto usmernení. Účelom tohto dokumentu je poskytnúť všeobecné usmernenie vývojárom a prevádzkovateľom aplikácií na sledovanie kontaktov.

Niektoré kritériá môžu prekračovať rámec prísnych požiadaviek vyplývajúcich z rámca ochrany údajov. Ich cieľom je zabezpečiť najvyššiu úroveň transparentnosti s cieľom podporiť prijatie takýchto aplikácií na sledovanie kontaktov v spoločnosti.

Preto by vydavatelia aplikácií na sledovanie kontaktov mali zohľadniť tieto kritériá:

- Používanie takejto aplikácie musí byť prísne dobrovoľné. Nesmie sa ním podmieňovať prístup k akýmkoľvek právam zaručeným zákonom. Jednotlivci musia mať vždy úplnú kontrolu nad svojimi údajmi a mali by mať možnosť slobodne si zvoliť, či budú takúto aplikáciu používať.
- Aplikácie na sledovanie kontaktov môžu viesť k vysokému riziku pre práva a slobody fyzických osôb a pred ich zavedením bude potrebné vykonať posúdenie vplyvu na ochranu údajov.
- Informácie o blízkosti medzi používateľmi aplikácie možno získať bez toho, že sa bude zisťovať ich poloha. Pri tomto druhu aplikácie sa nevyžadujú lokalizačné údaje, a preto by sa nemali využívať.
- Ak sa u používateľa diagnostikuje infekcia vírusom SARS-Cov-2, mali by byť informované iba osoby, s ktorými bol používateľ v úzkom kontakte v epidemiologicky relevantnom retenčnom období.

- Pri prevádzke tohto druhu aplikácie sa v závislosti od zvolenej architektúry môže vyžadovať použitie centralizovaného servera. V takom prípade a v súlade so zásadami minimalizácie údajov a štandardnej ochrany údajov by sa údaje spracúvané centralizovaným serverom mali obmedziť na absolútne minimum:
    - ak sa u používateľa diagnostikuje infekcia, informácie týkajúce sa jeho predchádzajúcich blízkych kontaktov alebo identifikátory vysielané aplikáciou používateľa možno získavať iba so súhlasom používateľa. Treba vytvoriť metódu overenia, ktorá umožní určiť, že osoba je skutočne infikovaná bez toho, aby sa identifikoval používateľ. Technicky by sa to dalo dosiahnuť varovaním kontaktov až po zásahu zdravotníckeho pracovníka, napríklad pomocou osobitného jednorazového kódu.
    - Informácie uložené na centrálnom serveri by prevádzkovateľovi nemali umožňovať identifikáciu používateľov, u ktorých bola diagnostikovaná infekcia, či používateľov, ktorí boli s touto osobou v kontakte, a nemali by ani umožniť odvodenie vzorcov kontaktov, ktoré nie sú potrebné na určenie príslušných kontaktov.
- Prevádzka tohto druhu aplikácie si vyžaduje vysielanie údajov, ktoré čítajú zariadenia iných používateľov, a počúvanie týchto vysielaní.
    - Postačuje výmena pseudonymných identifikátorov medzi mobilnými zariadeniami používateľov (počítačmi, tabletmi, pripojenými hodinkami atď.), napríklad ich vysielaním (napr. prostredníctvom technológie Bluetooth Low Energy).
    - Identifikátory sa musia generovať pomocou najmodernejších kryptografických procesov.
    - Identifikátory sa musia pravidelne obnovovať, aby sa znížilo riziko fyzického sledovania a útokov s cieľom prepojenia údajov (angl. *linkage attacks*).
- Tento druh aplikácie musí byť zabezpečený tak, aby sa zaručili bezpečné technické procesy. Konkrétne:
    - aplikácia by používateľom nemala poskytovať informácie, ktoré im umožnia odvodiť totožnosť alebo diagnózu iných používateľov. Centrálny server nesmie mať schopnosť identifikovať používateľov ani odvodiť informácie o nich.

Vyhlásenie o odmietnutí zodpovednosti: Uvedené zásady sa týkajú deklarovaného účelu aplikácií na *sledovanie kontaktov* a iba tohto účelu, teda automatického informovania ľudí potenciálne vystavených vírusu (bez toho, aby sa musela zistiť ich totožnosť). Prevádzkovatelia aplikácie a jej infraštruktúry môžu byť kontrolovaní príslušným dozorným orgánom. Dodržiavanie všetkých usmernení alebo časti z nich nie je nevyhnutne dostatočné na zabezpečenie úplného súladu s rámcom ochrany údajov.

2. Vymedzenie pojmov

Kontakt	V prípade aplikácie na sledovanie kontaktov je kontaktom používateľ, ktorý sa zúčastnil na interakcii s používateľom potvrdeným za nositeľa vírusu, pričom trvanie a vzdialenosť interakcie vyvolávajú riziko významného vystavenia vírusovej infekcii. Parametre pre dĺžku vystavenia a vzdialenosť medzi ľuďmi musia odhadnúť orgány verejného zdravotníctva a môžu byť stanovené v aplikácii.
Lokalizačné údaje	Ide o všetky údaje spracované v elektronickej komunikačnej sieti alebo prostredníctvom elektronickej komunikačnej služby, ktoré udávajú geografickú polohu koncového zariadenia používateľa verejne dostupnej elektronickej komunikačnej služby (ako sa stanovuje v smernici), ako aj údaje z iných potenciálnych zdrojov týkajúce sa: – zemepisnej šírky, dĺžky alebo nadmorskej výšky koncového zariadenia; – smeru pohybu používateľa alebo – času zaznamenania informácií o polohe.
Interakcia	V kontexte aplikácie na sledovanie kontaktov sa interakcia vymedzuje ako výmena informácií medzi dvoma zariadeniami umiestnenými v tesnej vzájomnej blízkosti (v priestore a čase) v rozsahu použitej komunikačnej technológie (napr. Bluetooth). Toto vymedzenie vylučuje lokalizáciu dvoch používateľov interakcie.
Nositeľ vírusu	V tomto dokumente za nositeľov vírusu považujeme používateľov, u ktorých bol pozitívny výsledok testu a ktorí dostali oficiálnu diagnózu od lekárov alebo zdravotníckych stredísk.
Sledovanie kontaktov	Ľudia, ktorí boli v úzkom kontakte (podľa kritérií, ktoré definujú epidemiológovia) s jednotlivcom infikovaným vírusom, sú vystavení významnému riziku, že infikujú ďalších. Sledovanie kontaktov je metodika kontroly chorôb, pri ktorej sa vytvára zoznam všetkých ľudí, ktorí boli v tesnej blízkosti nositeľa vírusu, aby sa skontrolovalo, či im hrozí infekcia, a aby voči nim prijali príslušné hygienické opatrenia.

3. Všeobecné informácie

GEN-1	Aplikácia musí byť doplnkovým nástrojom k tradičným technikám sledovania kontaktov (najmä rozhovorom s infikovanými osobami), t. j. musí byť súčasťou širšieho programu v oblasti verejného zdravia. Smie sa používať iba do času, kým samotné techniky manuálneho sledovania kontaktov nedokážu zvládnuť množstvo nových infekcií.

GEN-2	Najneskôr, keď príslušné orgány verejnej moci rozhodnú o „návrate do normálu“, sa musí zaviesť postup na zastavenie získavania identifikátorov (globálna deaktivácia aplikácie, pokyny na odinštalovanie aplikácie, automatické odinštalovanie atď.) a na aktiváciu odstránenia všetkých získaných údajov zo všetkých databáz (mobilných aplikácií a serverov).
GEN-3	Zdrojový kód aplikácie a jej „backendu“ musí byť otvorený a technické špecifikácie musia byť zverejnené tak, aby ktorákoľvek zúčastnená strana mohla vykonať audit kódu, a ak je to relevantné – prispieť k vylepšeniu kódu, k opraveniu možných chýb a k zaisteniu transparentnosti spracovania osobných údajov.
GEN-4	Fázy zavádzania aplikácie musia umožňovať postupné potvrdzovanie jej účinnosti z hľadiska verejného zdravia. Na tento účel sa musí smerom nahor v reťazci vývoja stanoviť hodnotiaci protokol, v ktorom sa špecifikujú ukazovatele umožňujúce merať účinnosť aplikácie.

4. Účely

PUR-1	Aplikácia musí sledovať jediný účel sledovania kontaktov, t. j. aby mohli byť ľudia, ktorí boli potenciálne vystavení vírusu SARS-Cov-2, upozornení a aby sa im poskytla starostlivosť. Nesmie sa používať na iné účely.
PUR-2	Aplikácia sa nesmie odkloniť od svojho primárneho použitia na účely monitorovania dodržiavania karanténnych opatrení, opatrení na obmedzenie pohybu a/alebo obmedzenie kontaktu medzi ľuďmi.
PUR-3	Aplikácia sa nesmie používať na vyvodenie záverov o mieste pohybu používateľov na základe ich interakcie a alebo akýchkoľvek iných prostriedkov.

5. Funkčné hľadiská

FUNC-1	Aplikácia musí poskytovať funkcie, ktoré používateľom umožnia získať informáciu o tom, že boli potenciálne vystavení vírusu, pričom táto informácia je založená na blízkosti infikovaného používateľa počas X dní pred pozitívnym skríningovým testom (hodnotu X stanovia orgány verejného zdravotníctva).
FUNC-2	Aplikácia by mala používateľom, u ktorých sa zistilo, že boli potenciálne vystavení vírusu, poskytnúť odporúčania. Používateľom by mala sprostredkúvať pokyny týkajúce sa opatrení, ktoré by mali dodržiavať, a mala by im umožniť požiadať o radu. V takýchto prípadoch by bol povinný zásah človeka.
FUNC-3	Algoritmus merajúci riziko infekcie na základe faktorov vzdialenosti a času, a teda rozhodujúci o tom, kedy sa kontakt má pridať do zoznamu sledovania kontaktov, musí byť bezpečne upraviteľný tak, aby zohľadňoval najnovšie poznatky o šírení vírusu.

FUNC-4	**Používatelia musia byť informovaní v prípade, že boli vírusu vystavení**, alebo musia pravidelne dostávať informácie o tom, či boli v priebehu inkubačného času vírusu vystavení alebo nie.
FUNC-5	Aplikácia by mala byť interoperabilná s inými aplikáciami vyvinutými v členských štátoch, aby boli používatelia, ktorí cestujú medzi rôznymi členskými štátmi, riadne informovaní.

6. Údaje

DATA-1	Aplikácia musí byť schopná vysielať a prijímať dáta prostredníctvom bezkontaktných komunikačných technológií, ako je Bluetooth Low Energy, ktoré umožnia vykonávať sledovanie kontaktov.
DATA-2	Tieto vysielané údaje musia obsahovať kryptograficky silné pseudonáhodné identifikátory generované aplikáciou a špecifické pre aplikáciu.
DATA-3	Riziko kolízie medzi pseudonáhodnými identifikátormi by malo byť dostatočne nízke.
DATA-4	Pseudonáhodné identifikátory sa musia pravidelne obnovovať, a to s frekvenciou, ktorá je dostatočná na zníženie rizika opätovnej identifikácie, fyzického sledovania alebo prepojenia údajov jednotlivcov, a to kýmkoľvek vrátane prevádzkovateľov centrálnych serverov, iných používateľov aplikácií alebo tretích strán s nekalým úmyslom. Tieto identifikátory musia byť generované aplikáciou používateľa, prípadne na základe informácie poskytnutej centrálnym serverom.
DATA-5	V súlade so zásadou minimalizácie údajov sa v aplikácii nesmú zhromažďovať iné údaje ako tie, ktoré sú nevyhnutne potrebné na účely sledovania kontaktov.
DATA-6	V aplikácii sa nesmú na účely sledovania kontaktov zhromažďovať lokalizačné údaje. Lokalizačné údaje môžu byť spracúvané výlučne s cieľom umožniť aplikácii komunikovať s podobnými aplikáciami v iných krajinách a mali by sa presne obmedziť na to, čo je nevyhnutne potrebné na tento jediný účel.
DATA-7	V aplikácii by sa nemali zhromažďovať údaje týkajúce sa zdravia okrem tých, ktoré sú nevyhnutne potrebné na účely aplikácie, s výnimkou voliteľného a výhradného účelu pomoci pri rozhodovacom procese týkajúcom sa informovania používateľa.
DATA-8	Používatelia musia byť informovaní o všetkých osobných údajoch, ktoré sa budú získavať. Tieto údaje by sa mali získavať iba so súhlasom používateľa.

7. Technické vlastnosti

TECH-1	Aplikácia by mala využívať dostupné technológie, napríklad bezkontaktné komunikačné technológie (ako Bluetooth Low Energy) na detekciu používateľov v blízkosti zariadenia, na ktorom je aplikácia spustená.
TECH-2	Aplikácia by mala uchovávať históriu kontaktov používateľa v zariadení na vopred stanovené obmedzené časové obdobie.
TECH-3	Pri vykonávaní niektorých svojich funkcií sa aplikácia môže spoliehať na centrálny server.
TECH-4	Aplikácia musí byť založená na architektúre, ktorá sa v maximálnej možnej miere opiera o zariadenia používateľov.
TECH-5	Z iniciatívy používateľov, ktorí boli nahlásení ako infikovaní vírusom, a po potvrdení ich stavu primerane certifikovaným zdravotníckym pracovníkom by sa ich história kontaktov alebo ich vlastné identifikátory mali preniesť na centrálny server.

8. Bezpečnosť

SEC-1	Stav používateľov, ktorí boli v aplikácii nahlásení ako pozitívni na vírus SARS-CoV-2, sa musí overovať mechanizmom, ktorý napríklad poskytne jednorazový kód prepojený s odberovou stanicou alebo so zdravotníckym pracovníkom. Ak nie je možné bezpečným spôsobom získať potvrdenie, údaje sa nesmú spracovať.
SEC-2	Údaje zaslané na centrálny server sa musia prenášať zabezpečeným kanálom. Využívanie služieb odosielania oznámení poskytovaných poskytovateľmi platformy operačného systému by sa malo dôkladne posúdiť a nemalo by viesť k poskytnutiu žiadnych údajov tretím stranám.
SEC-3	Žiadosti musia byť odolné voči neoprávneným zásahom používateľov s nekalými úmyslami.
SEC-4	Na zabezpečenie komunikácie medzi aplikáciou a serverom a medzi aplikáciami navzájom a ako všeobecné pravidlo na ochranu informácií uložených v aplikáciách a na serveri sa musia implementovať najmodernejšie kryptografické techniky. Príklady techník, ktoré sa môžu použiť, zahŕňajú napríklad: symetrické a asymetrické šifrovanie, funkcie hašovania, test súkromného členstva (*private membership test*, PMT), križovatka súkromných súborov (*private set intersection, PSI*), filtre Bloom, získavanie súkromných informácií, homomorfné šifrovanie atď.
SEC-5	Na centrálnom serveri sa nesmú uchovávať identifikátory sieťového pripojenia (napr. IP adresy) žiadnych používateľov, a to ani tých, ktorí boli pozitívne diagnostikovaní a ktorí odoslali svoju históriu kontaktov alebo svoje vlastné identifikátory.
SEC-6	S cieľom vyhnúť sa vydávaniu sa za inú osobu alebo vytvoreniu falošných používateľov musí server aplikáciu overiť.
SEC-7	Aplikácia musí autentifikovať centrálny server.
SEC-8	Funkcie servera by mali byť chránené pred útokmi opakovaného prehrávania.

SEC-9	Informácie prenášané centrálnym serverom musia byť podpísané, čím sa potvrdí ich pôvod a integrita.
SEC-10	Prístup ku všetkým údajom uloženým na centrálnom serveri, ktoré nie sú verejne prístupné, sa musí obmedziť na oprávnené osoby.
SEC-11	Správca povolení zariadenia na úrovni operačného systému musí požadovať iba povolenia potrebné na prístup a použitie komunikačných modulov v prípade potreby, na uchovávanie údajov v koncovom zariadení a na výmenu informácií s centrálnym serverom.

9. Ochrana osobných údajov a súkromia fyzických osôb

Upozornenie: Ďalšie pokyny sa týkajú aplikácie, ktorej jediným účelom je sledovanie kontaktov.

PRIV-1	Pri výmene údajov sa musí rešpektovať súkromie používateľov (a najmä dodržiavať zásada minimalizácie údajov).
PRIV-2	Aplikácia nesmie pri používaní umožňovať priamu identifikáciu používateľov.
PRIV-3	Aplikácia nesmie umožňovať sledovanie pohybu používateľov.
PRIV-4	Používanie aplikácie by používateľom nemalo umožniť dozvedieť sa čokoľvek o iných používateľoch (najmä o tom, či sú alebo nie sú nositeľmi vírusu).
PRIV-5	Dôvera v centrálny server musí byť obmedzená. Správa centrálneho servera sa musí riadiť jasne stanovenými pravidlami riadenia a musí zahŕňať všetky potrebné opatrenia na zaistenie jeho bezpečnosti. Lokalizácia centrálneho servera by mala umožniť účinný dohľad zo strany príslušného dozorného orgánu.
PRIV-6	Musí sa vykonať posúdenie vplyvu na ochranu údajov, ktoré by sa malo zverejniť.
PRIV-7	Aplikácia by mala používateľovi odhaliť iba to, či bol vírusu vystavený, a pokiaľ je to možné bez toho, aby sa zverejnili informácie o iných používateľoch, počet kontaktov a dátumy vystavenia.
PRIV-8	Informácie poskytované aplikáciou nesmú používateľom umožniť identifikovať používateľov prenášajúcich vírus ani ich pohyb.
PRIV-9	Informácie poskytované aplikáciou nesmú orgánom verejného zdravotníctva umožniť identifikáciu používateľov potenciálne vystavených vírusu bez ich súhlasu.
PRIV-10	V žiadostiach aplikácie odoslaných na centrálny server sa nesmú odhaliť žiadne informácie o nositeľovi vírusu.
PRIV-11	V žiadostiach aplikácie odoslaných na centrálny server sa nesmú odhaliť žiadne zbytočné informácie o používateľovi okrem jeho pseudonymných identifikátorov a zoznamu kontaktov, ak je to nevyhnutné.
PRIV-12	Útoky s cieľom prepojenia údajov (angl. *linkage attacks*) nesmú byť možné.
PRIV-13	Používatelia musia mať možnosť uplatniť si prostredníctvom aplikácie svoje práva.
PRIV-14	Odstránenie aplikácie musí viesť k odstráneniu všetkých lokálne získaných údajov.
PRIV-15	V aplikácii by sa mali zhromažďovať iba údaje prenášané prostredníctvom inštancií aplikácie alebo ekvivalentných interoperabilných aplikácií. Nemala by získavať žiadne údaje týkajúce sa iných aplikácií a/alebo bezkontaktných komunikačných zariadení.
PRIV-16	S cieľom zabrániť opätovnej identifikácii centrálnym serverom by sa mali implementovať proxy servery. Účelom týchto *nekoordinovaných serverov (angl. non-colluding servers)* je zmiešať identifikátory viacerých používateľov (identifikátory nositeľov vírusu, ako aj identifikátory odoslané žiadateľmi) pred ich

	zaslaním na centrálny server tak, aby sa centrálnemu serveru zabránilo poznať identifikátory (napríklad IP adresy) používateľov.
PRIV-17	Aplikácia a server musia byť starostlivo vyvinuté a nakonfigurované tak, aby nezískavali zbytočné údaje (napr. v záznamoch servera by nemali byť zahrnuté žiadne identifikátory atď.) s cieľom zabrániť použitiu SDK tretích strán získavajúcich údaje na iné účely.

Väčšina aplikácií na sledovanie kontaktov, o ktorých sa aktuálne diskutuje, sa v prípade nahlásenia infikovaného používateľa v zásade riadi dvoma prístupmi: môžu na server buď posielať históriu blízkych kontaktov, ktoré získali skenovaním, alebo môžu posielať zoznam svojich vlastných identifikátorov, ktoré boli vysielané. Nasledujúce zásady sa podľa týchto dvoch prístupov zamietajú. Aj keď sa na tomto mieste analyzujú tieto dva prístupy, neznamená to, že nie sú možné či dokonca lepšie iné prístupy, napríklad prístupy, pri ktorých sa implementuje určitá forma šifrovania E2E alebo používajú iné technológie na zvýšenie bezpečnosti alebo ochrany súkromia.

9.1. Zásady, ktoré sa uplatňujú iba **vtedy, keď aplikácia odošle serveru zoznam kontaktov:**

CON-1	Centrálny server musí zbierať históriu kontaktov používateľov, ktorí boli hlásení ako pozitívni na SARS-CoV-2, na základe ich dobrovoľného úkonu.
CON-2	Centrálny server nesmie uchovávať ani rozširovať zoznam pseudonymných identifikátorov používateľov prenášajúcich vírus.
CON-3	História kontaktov uložená na centrálnom serveri sa musí vymazať, hneď ako budú používatelia upovedomení o ich blízkom kontakte s pozitívne diagnostikovanou osobou.
CON-4	S výnimkou prípadov, keď používateľ s pozitívnou diagnózou zašle svoju históriu kontaktov na centrálny server alebo keď používateľ požiada server, aby zistil svoje potenciálne vystavenia vírusu, nesmú z jeho zariadenia odísť žiadne údaje.
CON-5	Každý identifikátor zahrnutý do miestnej histórie sa musí odstrániť po X dňoch od jeho získania (hodnotu X stanovujú orgány verejného zdravotníctva).
CON-6	História kontaktov predložená jednotlivými používateľmi by sa nemala ďalej spracúvať, napr. krížovo prepájať s cieľom vytvoriť globálne mapy blízkosti.
CON-7	Údaje v záznamoch servera sa musia minimalizovať a musia spĺňať požiadavky na ochranu údajov.

9.2. Zásady, ktoré sa uplatňujú iba vtedy, keď aplikácia odošle na server zoznam svojich vlastných identifikátorov:

ID-1	Centrálny server musí zbierať aplikáciou vysielané identifikátory používateľov hlásených ako pozitívnych na SARS-CoV-2, ktoré títo používatelia dobrovoľne poskytli.

ID-2	Centrálny server nesmie uchovávať ani rozširovať históriu kontaktov používateľov, ktorí sú nositeľmi vírusu.
ID-3	Identifikátory uložené na centrálnom serveri sa musia po distribúcii do iných aplikácií odstrániť.
ID-4	S výnimkou prípadu, keď používateľ identifikovaný ako nakazený zašle svoje identifikátory centrálnemu serveru, nesmú jeho zariadenie opustiť žiadne údaje. Rovnako ani v prípade, keď používateľ požiada server o zistenie svojej potenciálnej expozície vírusu, nesmú z jeho zariadenia odísť žiadne údaje.
ID-5	Údaje v záznamoch servera sa musia minimalizovať a musia spĺňať požiadavky na ochranu údajov.