Iránymutatások

# 04/2020 sz. iránymutatás a COVID19-járvánnyal összefüggésben a helymeghatározó adatok és a kontaktkövető eszközök használatáról

## Elfogadás időpontja: 2020. április 21.

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

elfogadva

# Verziótörténet

| | | |
|---|---|---|
| 1.1 verzió | 2020. május 5. | Kisebb javítások |
| 1.0 verzió | 2020. április 21. | Az iránymutatás elfogadása |

# Tartalomjegyzék

## Az Európai Adatvédelmi Testület,

tekintettel a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet (a továbbiakban: általános adatvédelmi rendelet) 70. cikke (1) bekezdésének e) pontjára,

tekintettel az EGT-megállapodásra és különösen annak az EGT Vegyes Bizottság 2018. július 6-i 154/2018 határozatával módosított XI. mellékletére és 37. jegyzőkönyvére[1],

tekintettel eljárási szabályzatának 12. és 22. cikkére,

**ELFOGADTA A KÖVETKEZŐ IRÁNYMUTATÁST:**

# 1 BEVEZETÉS ÉS HÁTTÉR

1 A kormányok és a magánszereplők a COVID19-világjárványra adott válasz részeként az adatközpontú megoldások alkalmazása felé fordulnak, ami számos adatvédelmi aggályt vet fel.

2 Az Európai Adatvédelmi Testület hangsúlyozza, hogy az adatvédelmi jogi keretet úgy alakították ki, hogy rugalmas legyen, és az így egyszerre képes hatékonyan hozzájárulni a világjárvány korlátozásához, illetve megvédeni az alapvető emberi jogokat és szabadságokat.

3 Az Európai Adatvédelmi Testület szilárd meggyőződése, hogy amikor a COVID19-világjárvány kezelése személyes adatok feldolgozását teszi szükségessé, az adatvédelem elengedhetetlen a bizalom kiépítéséhez, a megoldások társadalmi elfogadhatóságához szükséges feltételek megteremtéséhez, és ezáltal a megoldást célzó intézkedések hatékonyságának garantálásához. Mivel a vírus nem ismer határokat, célszerű közös európai megközelítést kidolgozni, vagy legalábbis egy interoperabilitási keretet létrehozni, a jelenlegi válságra adott válaszként.

4 Az Európai Adatvédelmi Testület általánosságban úgy véli, hogy a COVID19 elleni küzdelemhez használt adatokat és technológiát inkább az egyének szerepvállalásának növelésére, mintsem ellenőrzésére, megbélyegzésére vagy elnyomására kell felhasználni. Továbbá, bár az adatok és a technológia fontos eszközök lehetnek, inherens korlátaik miatt pusztán kiegészítő szerepet játszhatnak más közegészségügyi intézkedések hatékonyságának növelése útján. A COVID19 elleni küzdelem érdekében a tagállamok vagy az uniós intézmények által elfogadott, személyes adatok feldolgozásával járó intézkedéseket az eredményesség, a szükségesség és az arányosság általános elveinek kell vezérelniük.

5 Ez az iránymutatás két konkrét célból pontosítja a helymeghatározó adatok és a kontaktkövető eszközök arányos használatára vonatkozó feltételeket és elveket:

- helymeghatározó adatok használata a világjárványra való reagálás támogatására a vírus terjedésének modellezésével, a kijárási korlátozások általános hatékonyságának értékelése céljából;
- kontaktkövetés, amelynek célja, hogy a fertőzési lánc mielőbbi megszakítása érdekében az egyéneket értesítsék arról, hogy olyan személy közvetlen közelében tartózkodtak, akiről később megállapítást nyert, hogy vírushordozó.

1 A jelen dokumentumban a „tagállamokra” történő bármely hivatkozást „EGT-tagállamokra” történő hivatkozásként kell értelmezni.

6 Számos tényezőtől függ, hogy a kontaktkövető alkalmazások milyen hatékonyan képesek hozzájárulni a világjárvány kezeléséhez (ilyen tényező például az alkalmazást telepíteni köteles személyek aránya vagy a „kontaktus” fogalmának definiálása a térbeli közelség és az időtartam vonatkozásában). Ezen túlmenően az ilyen eszközöknek a világjárvány elleni küzdelemre irányuló átfogó, többek között – a bizonyosság érdekében – a tesztelést és a manuális kontaktkövetést is magában foglaló népegészségügyi stratégia részét kell képezniük. Alkalmazásukat egyéb, támogató intézkedéseknek kell kísérniük annak biztosítása érdekében, hogy a felhasználóknak nyújtott információk megfelelő keretbe illeszkedjenek, és hogy a figyelmeztető jelzések hasznosak legyenek a népegészségügyi rendszer számára. Ellenkező esetben előfordulhat, hogy a szóban forgó alkalmazások nem fejtik ki maradéktalanul potenciális hatásukat.

7 Az Európai Adatvédelmi Testület hangsúlyozza, hogy az általános adatvédelmi rendelet és a 2002/58/EK irányelv (a továbbiakban: az irányelv) egyaránt tartalmaz olyan konkrét szabályokat, amelyek lehetővé teszik anonim vagy személyes adatok felhasználását abban a küzdelemben, amit a hatóságok és más nemzeti és uniós szintű szereplők a SARS-CoV-2 vírus terjedésének nyomon követése és megfékezése érdekében folytatnak[2].

8 E tekintetben az Európai Adatvédelmi Testület már állást foglalt azzal kapcsolatban, hogy a kontaktkövetésre szolgáló alkalmazások használatának önkéntesnek kell lennie, és nem az egyéni mozgások nyomon követésén, hanem a felhasználók közelségére vonatkozó információkon kell alapulnia[3].

[2] Lásd az Európai Adatvédelmi Testület a COVID19-járvánnyal kapcsolatos előző állásfoglalását.
[3] [3] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

# 2 A HELYMEGHATÁROZÓ ADATOK FELHASZNÁLÁSA

## 2.1 A helymeghatározó adatok forrásai

9 A vírus terjedésének és a kijárási korlátozások általános hatékonyságának modellezése céljából a helymeghatározó adatoknak két fő forrása áll rendelkezésre:

- az elektronikus hírközlési szolgáltatók (például mobil távközlési szolgáltatók) által a szolgáltatásnyújtás során gyűjtött helymeghatározó adatok; valamint
- az információs társadalommal összefüggő szolgáltatást nyújtó szolgáltatók olyan alkalmazásai által gyűjtött helymeghatározó adatok, amelyek működése ilyen adatok felhasználását teszi szükségessé (pl. navigáció, szállítási szolgáltatások stb.).

10 Az Európai Adatvédelmi Testület emlékeztet arra, hogy az elektronikus hírközlési szolgáltatóktól gyűjtött helymeghatározó adatokat[4] csak az irányelv 6. és 9. cikkének alkalmazási körén belül lehet feldolgozni. Ez azt jelenti, hogy ezek az adatok csak akkor továbbíthatók hatóságok vagy más harmadik felek részére, ha azokat a szolgáltató anonimizálta, vagy a felhasználó végberendezésének földrajzi helyzetét jelző adatok esetében, amelyek nem forgalmi adatok, a felhasználók előzetes hozzájárulásával[5].

11 Ami a közvetlenül a végberendezésről gyűjtött információkat – köztük a helymeghatározó adatokat – illeti, az irányelv 5. cikkének (3) bekezdése alkalmazandó. Ezért a felhasználó eszközén történő információtárolás vagy a már tárolt információkhoz való hozzáférés csak akkor megengedett, ha i. a felhasználó hozzájárult ahhoz[6], vagy ii. a tárolás és/vagy a hozzáférés feltétlenül szükséges a felhasználó által kifejezetten kért, információs társadalommal összefüggő szolgáltatáshoz.

12 Az irányelvben meghatározott jogoktól és kötelezettségektől azonban az 15. cikk értelmében el lehet térni, amennyiben azok bizonyos célkitűzések tekintetében egy demokratikus társadalomban szükséges, megfelelő és arányos intézkedésnek minősülnek[7].

13 Az információs társadalommal összefüggő szolgáltatást nyújtó szolgáltató által gyűjtött helymeghatározó adatok modellezési célokra (pl. operációs rendszeren vagy korábban telepített alkalmazáson keresztül) történő további felhasználása további feltételekhez kötött. Amennyiben az adatokat a irányelv 5. cikkének (3) bekezdésével összhangban gyűjtötték, azokat csak az érintett további hozzájárulásával vagy olyan uniós vagy tagállami jogszabály alapján lehet tovább feldolgozni, amely egy demokratikus társadalomban az általános adatvédelmi rendelet 23. cikkének (1) bekezdésében említett célkitűzések biztosításához szükséges és arányos intézkedésnek minősül[8].

## 2.2 Az anonimizált helymeghatározó adatok használatának előtérbe helyezése

14 Az Európai Adatvédelmi Testület hangsúlyozza, hogy a helymeghatározó adatok használatakor a személyes adatok helyett mindig az anonimizált adatok feldolgozását kell előnyben részesíteni.

15 Az anonimizálás olyan technikák alkalmazását jelenti, amelyek célja, hogy megszüntessék az adatoknak egy azonosított vagy azonosítható természetes személlyel való összekapcsolhatóságát bármely „észszerű” erőfeszítéssel szemben. Ennek az „észszerűségi vizsgálatnak” mind az objektív szempontokat (idő, technikai eszközök), mind az egyes

---

[4] Lásd az irányelv 2. cikkének c) pontját.
[5] Lásd az irányelv 6. és 9. cikkét.
[6] Az irányelvben szereplő hozzájárulás fogalma továbbra is megfelel az általános adatvédelmi rendeletben szereplő hozzájárulás fogalmának, és annak teljesítenie kell az általános adatvédelmi rendelet 4. cikkének (11) bekezdésében és 7. cikkében a hozzájárulás tekintetében előírt valamennyi követelményt.
[7] Az irányelv 15. cikkének értelmezéséhez lásd még az Európai Unió Bíróságának a C-275/06. sz. Productores de Música de España (Promusicae) kontra Telefónica de España SAU ügyben 2008. január 29-én hozott ítéletét.
[8] Lásd a személyes adatok hálózatba kapcsolt járművekkel összefüggésben történő feldolgozásáról szóló 1/2020. sz. iránymutatás 1.5.3. szakaszát.

esetekben változó kontextuális elemeket (a jelenség ritkasága, tekintettel például népsűrűségre, az adatok jellege és mennyisége) figyelembe kell vennie. Ha az adatok a vizsgálaton nem felelnek meg, akkor azokat nem anonimizálták, és ezért továbbra is az általános adatvédelmi rendelet hatálya alá tartoznak.

16 Az anonimizálás megalapozottságának értékelése három kritériumon alapul: i. különválasztás (egy nagyobb csoportba tartozó egyén izolálása az adatok alapján); ii. összekapcsolhatóság (az ugyanarra az egyénre vonatkozó két rekord összekapcsolása); és iii. következtetések (az egyénre vonatkozó ismeretlen információk nagy valószínűséggel történő levonása).

17 Az anonimizálás fogalma könnyen félreérthető, és gyakran összetévesztik az álnevesítéssel. Míg az anonimizálás korlátozás nélkül lehetővé teszi az adatok felhasználását, az álnevesített adatok továbbra is az általános adatvédelmi rendelet hatálya alá tartoznak.

18 A hatékony anonimizálásra számos lehetőség kínálkozik[9], de fenntartások mellett. Adatok önmagukban nem anonimizálhatók, ami azt jelenti, hogy az anonimizálás vagy annak hiánya csak adatkészletek egészére értelmezhető. Ebben az értelemben az egyetlen adatmintán (titkosítással vagy bármely más matematikai transzformációval) történő beavatkozás legfeljebb álnevesítésnek tekinthető.

19 Az anonimizálási folyamatok és az újraazonosítási támadások termékeny kutatási területek. Alapvető fontosságú, hogy az anonimizálási megoldásokat alkalmazó adatkezelők figyelemmel kísérjék az e területen a közelmúltban bekövetkezett fejleményeket, különösen a helymeghatározó adatok tekintetében (távközlési szolgáltatóktól és/vagy információs társadalmi szolgáltatásoktól származó adatok), amelyek közismerten igen nehezen anonimizálhatók.

20 Számos kutatás rámutatott[10], hogy az *anonimizáltnak vélt helymeghatározó adatok* valójában nem feltétlenül anonimizáltak. Az egyének mobilitási nyomai eredendően nagymértékben korreláltak és egyediek. Ezért bizonyos körülmények között ki vannak téve az újraazonosítási kísérleteknek.

21 Nem lehet teljes mértékben anonimizálni azt az egyedi adatmintát, amely egy adott személy helyzetét követi le jelentős időn át. Ez az értékelés akkor is helytálló lehet, ha a rögzített földrajzi koordináták pontossága nem csökken elegendő mértékben, vagy ha a nyomvonalra vonatkozó részletes adatokat eltávolítják, sőt akkor is, ha csak azon helyek helyzeti adatait őrzik meg, ahol az érintett huzamosabb ideig tartózkodott. Ez vonatkozik a nem megfelelően aggregált helymeghatározó adatokra is.

22 Az anonimizálás során a helymeghatározó adatokat gondosan kell kezelni az észszerűségi vizsgálat sikeres elvégzése érdekében. Ebben az értelemben az ilyen adatkezelés magában foglalja a helymeghatározó adatkészletek egészének figyelembevételét, valamint az egyének viszonylag nagy csoportjától származó adatok kezelését a rendelkezésre álló megbízható anonimizálási technikák alkalmazásával, feltéve, hogy azokat megfelelően és hatékonyan alkalmazzák.

23 Végül, tekintettel az anonimizálási folyamatok összetettségére, igen fontos az anonimizálási módszertan átláthatóságának biztosítása.

---

[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 és Pyrgelis et al. (2017): Knock Knock, Who's There? Membership Inference on Aggregate Location Data.

# 3 KONTAKTKÖVETŐ ALKALMAZÁSOK

## 3.1 Általános jogi elemzés

24 A természetes személyek tartózkodási helyének és/vagy kapcsolatainak szisztematikus és széles körű nyomon követése súlyosan sérti a magánéletüket. Ez kizárólag a felhasználóknak az egyes célok tekintetében adott önkéntes hozzájárulásán alapulhat. Ennek különösen azzal kell járnia, hogy azok a személyek, akik úgy döntenek, hogy nem használják vagy nem képesek használni ezeket az alkalmazásokat, semmilyen hátrányt nem szenvedhetnek.

25 Az elszámoltathatóság biztosítása érdekében minden kontaktkövető alkalmazás adatkezelőjét egyértelműen meg kell határozni. Az Európai Adatvédelmi Testület úgy véli, hogy a nemzeti egészségügyi hatóságok lehetnek az ilyen alkalmazások adatkezelői[11]; mindazonáltal más adatkezelők is elképzelhetők. Minden olyan esetben, amikor a kontaktkövető alkalmazások telepítése különböző szereplőket érint, szerepüket és felelősségüket a kezdetektől fogva egyértelműen meg kell határozni, és el kell magyarázni a felhasználóknak.

26 Emellett a célhoz kötöttség elve tekintetében a céloknak kellően konkrétnak kell lenniük ahhoz, hogy kizárják a COVID19 egészségügyi válság kezeléséhez nem kapcsolódó (pl. kereskedelmi vagy bűnüldözési célú) további feldolgozást. A célkitűzés egyértelmű meghatározását követően biztosítani kell, hogy a személyes adatok felhasználása megfelelő, szükséges és arányos legyen.

27 A kontaktkövető alkalmazásokkal összefüggésben gondosan mérlegelni kell az adattakarékosság és a beépített és alapértelmezett adatvédelem elvét:

- a kontaktkövető alkalmazásokhoz nincs szükség az egyéni felhasználók helyének nyomon követésére; ehelyett közelségi adatokat kell használni;
- mivel a kontaktkövető alkalmazások az egyének közvetlen azonosítása nélkül is működhetnek, megfelelő intézkedéseket kell hozni az újraazonosítás megakadályozására;
- az összegyűjtött információkat a felhasználó végberendezésén kell elhelyezni, és csak a releváns információk gyűjthetők össze, ha feltétlenül szükséges.

28 Az adatfeldolgozás jogszerűségét illetően az Európai Adatvédelmi Testület megjegyzi, hogy a kontaktkövető alkalmazások használata a végberendezésben már eltárolt adatok tárolását és/vagy az azokhoz való hozzáférést biztosítja, és erre az irányelv 5. cikkének (3) bekezdése vonatkozik. Ha e műveletek feltétlenül szükségesek ahhoz, hogy az alkalmazás szolgáltatója a felhasználó által kifejezetten kért szolgáltatást nyújthassa, az adatkezeléshez nem szükséges a felhasználó hozzájárulása. A nem feltétlenül szükséges műveletek esetében a szolgáltatónak ki kell kérnie a felhasználó hozzájárulását.

29 Az Európai Adatvédelmi Testület megjegyzi továbbá, hogy pusztán az a tény, hogy a kontaktkövető alkalmazások használata önkéntes alapon történik, nem jelenti azt, hogy a személyes adatok kezelése szükségszerűen hozzájáruláson alapul. Amennyiben a hatóságok jogszabályban meghatározott felhatalmazás alapján és azzal összhangban nyújtanak szolgáltatást, az adatkezelés legfontosabb jogalapja nyilvánvalóan a közérdekű feladat végrehajtásának szükségessége, azaz az általános adatvédelmi rendelet 6. cikke (1) bekezdésének e) pontja.

30 Az általános adatvédelmi rendelet 6. cikkének (3) bekezdése egyértelművé teszi, hogy a 6. cikk (1) bekezdésének e) pontjában említett adatkezelés alapját uniós jogszabály vagy az adatkezelőre alkalmazandó tagállami jogszabály határozza meg. Az adatkezelés célját e jogalapra hivatkozással kell meghatározni, illetve az (1) bekezdés e) pontjában említett adatkezelés tekintetében annak szükségesnek kell lennie valamely közérdekű vagy az

[11] Lásd még: „Iránymutatás az adatvédelemmel összefüggésben a COVID19-világjárvány elleni küzdelmet támogató alkalmazásokról”, Brüsszel, 2020.4.16. C (2020) 2523 final.

adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához.[12]

31 A kontaktkövető alkalmazások használatának jogszerű alapját képező jogalapnak vagy jogalkotási intézkedésnek azonban érdemi biztosítékokat kell tartalmaznia, ideértve az alkalmazás önkéntes jellegére való hivatkozást is. Idetartozik az adatkezelés céljának világos meghatározása és a személyes adatok további felhasználására vonatkozó kifejezett korlátozás, valamint az érintett adatkezelő(k) egyértelmű azonosítása. Emellett meg kell határozni az adatkategóriákat, valamint azokat a jogalanyokat amelyekkel a személyes adatok közölhetők (illetve az ilyen adatközlés céljait). A beavatkozás mértékétől függően további biztosítékokat kell beépíteni, figyelembe véve az adatkezelés jellegét, hatókörét és céljait. Végezetül az Európai Adatvédelmi Testület azt is ajánlja, hogy a lehető leghamarabb építsék be azokat a kritériumokat is, amelyek meghatározzák, hogy az alkalmazást mikor kell eltávolítani, és azt, hogy mely szervezet felelős és számoltatható el ezek meghatározásáért.

32 Ha azonban az adatfeldolgozás más jogalapon, például hozzájáruláson (a 6. cikk (1) bekezdésének a) pontja) alapul[13], az adatkezelőnek biztosítania kell, hogy teljesüljenek az ilyen jogalap érvényességére vonatkozó szigorú követelmények.

33 Ezenkívül a COVID19-világjárvány elleni küzdelemre irányuló alkalmazás használata egészségügyi adatok gyűjtéséhez vezethet (például fertőzött személy státusz). Az ilyen adatok kezelése akkor megengedett, ha az az általános adatvédelmi rendelet 9. cikke (2) bekezdésének i) pontjában foglalt feltételeknek megfelelően[14] a népegészségügy területét érintő közérdekből vagy az általános adatvédelmi rendelet 9. cikke (2) bekezdésének h) pontjában említett egészségügyi célokból[15] szükséges. A jogalaptól függően az adatkezelés kifejezett hozzájáruláson is alapulhat (az általános adatvédelmi rendelet 9. cikke (2) bekezdésének a) pontja).

34 Az eredeti céllal összhangban az általános adatvédelmi rendelet 9. cikke (2) bekezdésének j) pontja lehetővé teszi az egészségügyi adatok tudományos kutatási vagy statisztikai célból történő kezelését is.

35 A jelenlegi egészségügyi válságot nem szabad arra felhasználni, hogy aránytalan adatmegőrzési jogosítványok jöjjenek létre. A tárolási korlátozásnak figyelembe kell vennie a valós igényeket és az orvosi relevanciát (ide tartozhatnak a járványtani megfontolások, például a lappangási időszak hossza stb.); a személyes adatok csak a COVID19-válság időtartama során őrizhetők meg. Ezt követően általános szabályként minden személyes adatot törölni vagy anonimizálni kell.

36 Az Európai Adatvédelmi Testület értelmezése szerint az ilyen alkalmazások nem helyettesíthetik, hanem csak támogathatják a népegészségügyi szakemberek által végzett manuális kontaktkövetést, mert ezek a szakemberek azok, akik ki tudják szűrni, hogy a szoros érintkezés valószínűleg fertőzést eredményez-e vagy sem (pl. amikor az érintkezés megfelelő védőfelszereléssel ellátott személlyel – pénztárosokkal stb. – történik). Az Európai Adatvédelmi Testület hangsúlyozza, hogy a kontaktkövető alkalmazások által működtetett eljárásoknak és folyamatoknak – beleértve a vonatkozó algoritmusokat is – képzett személyzet szigorú felügyelete alatt kell működniük annak érdekében, hogy korlátozzák a hamis pozitív és negatív eredmények előfordulását. Különösen fontos, hogy az alkalmazás használatát követő lépésekre vonatkozó tanácsadás nem alapulhat kizárólag automatizált feldolgozáson.

---

[12] Lásd a (41) preambulumbekezdést.

[13] Az adatkezelőknek (különösen a hatóságoknak) különös figyelmet kell fordítaniuk arra a tényre, hogy a hozzájárulás nem tekinthető önkéntesnek, ha az egyénnek nincs valódi választása a hozzájárulás hátrányos megkülönböztetés nélküli megtagadására vagy visszavonására.

[14] Az adatkezelésnek olyan uniós vagy tagállami jogon kell alapulnia, amely megfelelő és konkrét intézkedéseket ír elő az érintett jogainak és szabadságainak védelme érdekében, különös tekintettel a szakmai titoktartásra.

[15] Lásd az általános adatvédelmi rendelet 9. cikke (2) bekezdésének h) pontját.

37 A méltányos, elszámoltatható és – tágabb értelemben – jogkövető működés biztosítása érdekében az algoritmusoknak ellenőrizhetőnek kell lenniük, és azokat független szakértőknek rendszeresen felül kell vizsgálniuk. Az alkalmazás forráskódját a lehető legszélesebb körű vizsgálat céljából nyilvánosan hozzáférhetővé kell tenni.

38 Hamis pozitív találatok bizonyos mértékben mindig előfordulnak. Mivel a fertőzési kockázat azonosítása valószínűleg nagy hatással lesz az egyénekre (például az illető a negatív teszteredményig önkéntes karanténban maradhat), biztosítani kell az adatok és/vagy az azt követő elemzési eredmények helyesbítésének lehetőségét. Ez természetesen csak olyan forgatókönyvekre és alkalmazásokra vonatkozik, amelyek esetében az adatokat oly módon kezelik és/vagy tárolják, amely műszakilag lehetővé teszi az ilyen korrekciót, és ahol a fent említett káros hatások valószínűsíthetően bekövetkeznek.

39 Végezetül az Európai Adatvédelmi Testület úgy véli, hogy minden ilyen eszköz bevezetése előtt adatvédelmi hatásvizsgálatot kell végezni, mivel az adatkezelés valószínűsíthetően magas kockázattal jár (egészségügyi adatok, várható széles körű elfogadás, rendszeres nyomon követés, új technológiai megoldás alkalmazása)[16]. Az Európai Adatvédelmi Testület nyomatékosan ajánlja adatvédelmi hatásvizsgálatok közzétételét.

## 3.2 Ajánlások és funkcionális követelmények

40 Az adattakarékosság elve szerint a beépített és alapértelmezett adatvédelem[17] egyéb intézkedései mellett a kezelt adatok mennyiségét a szükséges minimumra kell csökkenteni. Az alkalmazás nem gyűjthet nem kapcsolódó vagy nem szükséges információkat, amelyek magukban foglalhatják a családi állapotot, a kommunikációs azonosítókat, a berendezés címjegyzékének elemeit, az üzeneteket, a hívásnaplókat, a helymeghatározó adatokat, az eszközazonosítókat stb.

41 Az alkalmazások által közvetített adatok csak az alkalmazás által generált és arra specifikusan jellemző egyedi és álnevesített azonosítókat tartalmazhatnak. Ezeket az azonosítókat rendszeresen meg kell újítani, olyan gyakorisággal, amely összeegyeztethető a vírus terjedésének megfékezésére irányuló céllal, és elegendő ahhoz, hogy korlátozza az egyének azonosításának és fizikai nyomon követésének kockázatát.

42 A kontaktkövetés végrehajtása központosított vagy decentralizált megközelítésen alapulhat[18]. Mindkettőt működőképes lehetőségnek kell tekinteni, feltéve, hogy megfelelő biztonsági intézkedések vannak érvényben, amelyek mindegyike számos előnnyel és hátránnyal jár. Ezért az alkalmazásfejlesztés koncepcionális szakaszának mindig magában kell foglalnia mindkét megközelítés alapos mérlegelését, gondosan felmérve azok adatvédelemre/magánéletre gyakorolt hatásait és az egyének jogaira gyakorolt lehetséges hatásokat.

43 A kontaktkövetés rendszerében részt vevő szerverek csak azon felhasználók kontaktustörténetét vagy álneves azonosítóit gyűjthetik össze – és csak a felhasználó önkéntes fellépése nyomán –, akiket az egészségügyi hatóságok által végzett megfelelő értékelés alapján fertőzöttnek találtak. Emellett a szerver csak addig tárolhatja a fertőzött felhasználók álneves azonosítóinak vagy kontaktustörténetének listáját, amíg a potenciálisan fertőzött felhasználókat tájékoztatják kitettségükről, továbbá a szerver nem kísérelheti meg a potenciálisan fertőzött felhasználók azonosítását.

44 Az alkalmazásokra és a manuális kontaktkövetésre egyaránt kiterjedő globális kontaktkövetési módszertan bevezetése bizonyos esetekben további információk feldolgozását teheti szükségessé. Ebben az összefüggésben ezeknek a kiegészítő információknak a felhasználói

[16] Lásd: WP 29 – Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár”-e.
[17] Lásd az Európai Adatvédelmi Testület 4/2019. sz. iránymutatását a beépített és alapértelmezett adatvédelemről.
[18] Általánosságban a decentralizált megoldás jobban összhangban van az adattakarékosság elvével.

terminálon kell maradniuk, és csak akkor dolgozhatók fel, ha feltétlenül szükséges, és akkor is csak a felhasználó előzetes és kifejezett hozzájárulásával.

45 A szervereken és alkalmazásokon tárolt adatok biztonsága érdekében, valamint az alkalmazások és a távoli szerverek közötti cserék esetében a legkorszerűbb kriptográfiai technikákat kell alkalmazni. Az alkalmazás és a szerver közötti kölcsönös hitelesítést is el kell végezni.

46 A felhasználóknak az alkalmazásban SARS-CoV-2-fertőzöttként való bejelentését megfelelő engedélyezéshez kell kötni, például a fertőzött személy álnevesített személyazonosságához kötött és tesztállomáshoz vagy egészségügyi szakemberhez kapcsolt egyszer használatos kód révén. Ha a megerősítés nem szerezhető be biztonságos módon, nem kerülhet sor olyan adatkezelésre, amely feltételezi a felhasználó státuszának érvényességét.

47 Az adatkezelőnek a hatóságokkal együttműködve egyértelműen és kifejezetten tájékoztatnia kell a potenciális felhasználókat a hivatalos nemzeti kontaktkövető alkalmazás letöltéséhez vezető linkről annak érdekében, hogy csökkentse az idegen alkalmazások használatának kockázatát.

# 4 KÖVETKEZTETÉS

48 A világ jelentős népegészségügyi válsággal néz szembe, amely határozott válaszlépéseket tesz szükségessé, és amely e vészhelyzet elmúltával is éreztetni fogja hatását. Az automatizált adatfeldolgozás és a digitális technológiák kulcsfontosságú elemei lehetnek a COVID19 elleni küzdelemnek. Óvakodnunk kell azonban az ún. „racsni-hatástól". Feladatunk annak biztosítása, hogy az ilyen rendkívüli körülmények között hozott valamennyi intézkedés szükséges, időben korlátozott, minimális mértékű legyen, továbbá rendszeres és tényleges felülvizsgálat, valamint tudományos értékelés tárgyát képezze.

49 Az Európai Adatvédelmi Testület hangsúlyozza, hogy nem szabad választani a jelenlegi válságra adott hatékony válasz és az alapvető jogaink védelme között: mindkettő megvalósítható, és az adatvédelmi elvek nagyon fontos szerepet játszhatnak a vírus elleni küzdelemben. Az európai adatvédelmi jog lehetővé teszi a személyes adatok felelősségteljes használatát az egészségmenedzsmentben, ugyanakkor biztosítja, hogy az egyéni jogok és szabadságok ne sérüljenek ebben a folyamatban.

Az Európai Adatvédelmi Testület részéről

az elnök

(Andrea Jelinek)

# MELLÉKLET – KONTAKTKÖVETŐ ALKALMAZÁSOK ELEMZÉSI ÚTMUTATÓ

## 0. Felelősségkizáró nyilatkozat

Az alábbi iránymutatás nem előíró és nem kimerítő jellegű. Egyedüli célja, hogy általános iránymutatást nyújtson a kontaktkövető alkalmazások tervezői és használói számára. Az itt leírtaktól eltérő megoldások is alkalmazhatók és jogszerűek lehetnek, amennyiben megfelelnek a vonatkozó jogi keretnek (pl. az általános adatvédelmi rendeletnek és az irányelvnek).

Megjegyzendő továbbá, hogy ez az útmutató általános jellegű. Következésképpen az e dokumentumban foglalt ajánlások és kötelezettségek nem tekinthetők teljes körűnek. Minden értékelést eseti alapon kell elvégezni, és az egyes konkrét alkalmazások esetében olyan kiegészítő intézkedésekre lehet szükség, amelyek nem szerepelnek ebben az útmutatóban.

## 1. Összefoglalás

Számos tagállamban az érdekelt felek *kontaktkövető** alkalmazások használatának lehetőségét vizsgálják. Ezek az alkalmazások segítik az egyéni felhasználókat annak kiderítésében, hogy kapcsolatba kerültek-e SARS-Cov-2 vírussal fertőzött személlyel.

Azok a feltételek, amelyek mellett az ilyen alkalmazások hatékonyan hozzájárulhatnak a világjárvány kezeléséhez, még nem kerültek megállapításra. Ezeket a feltételeket ugyanakkor az ilyen alkalmazások bevezetése előtt meg kell határozni. Ebben az összefüggésben fontos, hogy a fejlesztők releváns információkat tartalmazó iránymutatást kapjanak annak érdekében, hogy a személyes adatok védelme már a tervezés korai szakaszától garantálható legyen.

Megjegyzendő, hogy a jelen útmutató általános jellegű. Következésképpen az e dokumentumban foglalt ajánlások és kötelezettségek nem tekinthetők teljes körűnek. Minden értékelést eseti alapon kell elvégezni, és az egyes konkrét alkalmazások esetében olyan kiegészítő intézkedésekre lehet szükség, amelyek nem szerepelnek ebben az útmutatóban. Ezen iránymutatás célja, hogy általános útmutatóval szolgáljon a kontaktkövető alkalmazások tervezői és végrehajtói számára.

Egyes kritériumok meghaladhatják az adatvédelmi keretből eredő szigorú követelményeket. Céljuk a legmagasabb szintű átláthatóság biztosítása a kontaktkövető alkalmazások társadalmi elfogadottságának előmozdítása érdekében.

E célból a kontaktkövető alkalmazások fejlesztőinek a következő kritériumokat kell figyelembe venniük:

- Az ilyen alkalmazásnak szigorúan önkéntesnek kell lennie. Nem korlátozhatja a törvény által biztosított jogokhoz való hozzáférést. Az egyének számára biztosítani kell, hogy mindenkor teljes körű ellenőrzést gyakoroljanak az adataik felett, és lehetővé kell tenni számukra, hogy szabadon dönthessenek az alkalmazás használatáról.
- A kontaktkövető alkalmazások valószínűsíthetően magas kockázattal járnak a természetes személyek jogaira és szabadságaira nézve, ezért működésbe állításuk előtt adatvédelmi hatásvizsgálatot kell végezni.

- Az alkalmazás felhasználóinak közelségére vonatkozó információk helymeghatározás nélkül is beszerezhetők. Az ilyen típusú alkalmazáshoz nincs szükség helymeghatározó adatok felhasználására, ezért az nem foglalhat magában helymeghatározó adatokat.
- Ha a felhasználó a SARS-Cov-2 vírussal fertőzöttnek bizonyult, csak azokat a személyeket kell tájékoztatni, akikkel a felhasználó a kontaktkövetés céljából járványügyileg releváns adatmegőrzési időszakon belül közeli kontaktusban volt.
- Az ilyen típusú alkalmazások működtetéséhez – a választott architektúrától függően – szükség lehet központi szerver használatára. Ilyen esetben és az adattakarékosság és a beépített adatvédelem elveivel összhangban a központi szerver által feldolgozott adatok mennyiségét a lehető legkisebbre kell korlátozni:
    - Ha a felhasználót fertőzöttként diagnosztizálják, csak a felhasználó beleegyezésével gyűjthetők a korábbi közeli kontaktusaira vagy a felhasználó alkalmazásán keresztül közvetített azonosítókra vonatkozó információk. Olyan ellenőrzési módszert kell kidolgozni, amely a felhasználó azonosítása nélkül teszi lehetővé annak megállapítását, hogy az adott személy valóban fertőzött-e. Ez technikailag úgy érhető el, ha a kontaktszemélyeket csak egészségügyi szakember beavatkozását követően figyelmeztetik, például egy külön egyszeri kód használatával.
    - A központi szerveren tárolt információk nem tehetik lehetővé az adatkezelő számára, hogy azonosítsa azokat a felhasználókat, akikről megállapították, hogy fertőzöttek vagy kapcsolatba kerültek fertőzött felhasználókkal, továbbá nem tehetik lehetővé olyan érintkezési minták kikövetkeztetését sem, amelyek nem szükségesek a releváns kontaktok meghatározásához.
- Az ilyen típusú alkalmazások működtetéséhez más felhasználók eszközei által leolvasandó adatok közvetítésére és az ilyen üzenetek meghallgatására van szükség:
    - Elegendő álneves azonosítókat cserélni a felhasználók mobil berendezései (számítógépek, táblagépek, hálózatba kapcsolt órák stb.) között, például azok közvetítése révén (pl. Bluetooth LE technológián keresztül).
    - Az azonosítókat a legkorszerűbb kriptográfiai eljárásokkal kell generálni.
    - Az azonosítókat rendszeresen meg kell újítani a fizikai nyomon követés és a kapcsolati támadások kockázatának csökkentése érdekében.
- Az ilyen típusú alkalmazásokban garantáltan biztonságos műszaki eljárásokat kell alkalmazni. Így különösen:
    - Az alkalmazás nem közvetítheti a felhasználók felé azokat az információkat, amelyek lehetővé teszik számukra mások személyazonosságának vagy diagnózisának kikövetkeztetését. A központi szerver nem azonosíthatja a felhasználókat, és nem következtethet rájuk vonatkozó információkra.

**Felelősségkizáró nyilatkozat**: A fenti elvek a *kontaktkövető* alkalmazások kifejezett céljához, és csakis ehhez a célhoz kapcsolódnak, amely a vírusnak potenciálisan kitett személyek automatikus tájékoztatása (e személyek azonosítása nélkül).Az alkalmazás üzemeltetőit és infrastruktúráját az illetékes felügyeleti hatóság ellenőrizheti. Ezen iránymutatás egészének vagy egy részének követése nem feltétlenül elegendő az adatvédelmi keretnek való teljes megfelelés biztosításához.

## 2. Fogalommeghatározások

| | |
|---|---|
| **Kontaktszemély** | A kontaktkövető alkalmazások vonatkozásában a kontaktszemély olyan felhasználó, aki interakcióba került bizonyítottan vírushordozó felhasználóval, mely interakció időtartama és távolsága a vírusfertőzésnek való jelentős kitettség kockázatát idézi elő. A kitettség időtartamára és az emberek közötti távolságra vonatkozó paramétereket az egészségügyi hatóságoknak kell megbecsülniük, és azokat az alkalmazásban be lehet állítani. |
| **Helymeghatározó adatok** | Az elektronikus hírközlő hálózatban vagy elektronikus hírközlési szolgáltatás keretében kezelt minden olyan adat, amely jelzi a nyilvánosan elérhető elektronikus hírközlési szolgáltatás felhasználója végberendezésének földrajzi helyzetét (az irányelv fogalommeghatározása), valamint az esetleges egyéb forrásokból származó, a következőkkel kapcsolatos adatok:<br>• a felhasználói végberendezés elhelyezkedésének földrajzi szélessége, hosszúsága és tengerszint feletti magassága;<br>• a felhasználó mozgásának iránya; vagy<br>• a helymeghatározó információ rögzítésének időpontja. |
| **Interakció** | A kontaktkövető alkalmazások vonatkozásában az interakció az alkalmazott kommunikációs technológia (pl. Bluetooth) tartományán belül, (térben és időben) egymás közvetlen közelében található két eszköz közötti információcsere. Ennek a meghatározásnak nem része az interakcióba lépő két felhasználó helye. |
| **Vírushordozó** | Ebben a dokumentumban azokat a felhasználókat tekintjük vírushordozónak, akiknek vírustesztje pozitív lett, és akik orvosoktól vagy más egészségügyi szervtől hivatalos diagnózist kaptak. |
| **Kontaktkövetés** | Azon személyek tekintetében, akik (a járványügyi szakemberek által meghatározandó kritériumok szerinti) szoros kapcsolatban álltak a vírussal fertőzött egyénnel, fennáll a megfertőződés, illetve mások megfertőzésének jelentős kockázata.<br>A kontaktkövetés olyan járványvédelmi módszer, amelynek során felkutatják mindazokat a személyeket, akik a vírushordozó közvetlen közelében tartózkodtak. Célja az ilyen személyek fertőzöttségének ellenőrzése és vonatkozásukban a megfelelő egészségügyi intézkedések foganatosítása. |

## 3. Általános kérdések

| | |
|---|---|
| GEN-1 | Az alkalmazásnak a hagyományos kontaktkövetési technikákat (nevezetesen a fertőzött személyekkel folytatott interjúkat) kiegészítő eszköznek kell lennie, azaz egy tágabb népegészségügyi program részét kell képeznie. Az alkalmazás |

| | |
|---|---|
| | csak addig használható, amíg a manuális kontaktkövetési technikák önmagukban nem tudják kezelni az új fertőzések mennyiségét. |
| GEN-2 | Legkésőbb az illetékes hatóságoknak a vészhelyzet megszüntetéséről hozott döntésekor be kell fejezni az azonosítók gyűjtését (az alkalmazás globális deaktiválása, az alkalmazás eltávolítására vonatkozó utasítások, automatikus eltávolítás stb.), és a gyűjtött adatokat az összes adatbázisból (mobilalkalmazásokból és szerverekből) törölni kell. |
| GEN-3 | Az alkalmazás és a „backend” forráskódjának nyitottnak kell lennie, és a műszaki leírásokat közzé kell tenni annak érdekében, hogy bármely érintett fél ellenőrizhesse a kódot, és adott esetben hozzá tudjon járulni a kód javításához, az esetleges hibák kijavításához és a személyes adatok kezelése átláthatóságának biztosításához. |
| GEN-4 | Az alkalmazás bevezetése során az egyes szakaszoknak lehetővé kell tenniük az alkalmazás népegészségügyi hatékonyságának fokozatos validálását. E célból előre ki kell dolgozni egy értékelési protokollt, amely meghatározza az alkalmazás hatékonyságának mérését lehetővé tevő mutatókat. |

## 4. Célok

| | |
|---|---|
| PUR-1 | Az alkalmazásnak nem lehet más célja, mint a kontaktkövetés annak érdekében, hogy a SARS-CoV-2 vírusnak potenciálisan kitett személyek riasztást kaphassanak és gondozásba kerülhessenek. Az alkalmazás egyéb célt nem szolgálhat. |
| PUR-2 | Az alkalmazás nem használható a karanténintézkedések, kijárási korlátozások és/vagy a távolságtartási szabályok betartásának ellenőrzésére. |
| PUR-3 | Az alkalmazás nem használható arra sem, hogy a felhasználók elhelyezkedésére vonatkozó következtetéseket vonjanak le interakcióik alapján és/vagy bármely más módon. |

## 5. Funkcionális megfontolások

| | |
|---|---|
| FUNC-1 | Az alkalmazásnak biztosítania kell, hogy a felhasználók értesüljenek arról, hogy potenciálisan ki voltak téve a vírusnak; ez az információ a fertőzött felhasználóhoz való olyan fizikai közelségen alapul, amely a pozitív szűrővizsgálatot megelőző X napon belül következett be (az X értéket az egészségügyi hatóságok határozzák meg). |
| FUNC-2 | Az alkalmazásnak ajánlásokat kell megfogalmaznia azon felhasználók számára, akikről megállapítást nyert, hogy potenciálisan ki voltak téve a vírusnak. Tájékoztatást kell adnia a követendő intézkedésekről, és lehetővé kell tennie a |

| | |
|---|---|
| | felhasználó számára, hogy tanácsot kérjen. Ilyen esetekben kötelezővé kell tenni az emberi beavatkozást. |
| FUNC-3 | Annak az algoritmusnak, amely a távolság és az idő tényezőinek figyelembevételével méri a fertőzés kockázatát, és ez alapján meghatározza, hogy mikor kell a kontaktszemélyt felvenni a kontaktkövetési listára, biztonságosan kalibrálhatónak kell lennie a vírus terjedésével kapcsolatos legújabb ismeretek figyelembevétele érdekében. |
| FUNC-4 | **A felhasználókat tájékoztatni kell, ha ki voltak téve a vírusnak**, vagy azoknak rendszeresen informálódniuk kell arról, hogy ki voltak-e téve a vírusnak a vírus lappangási idején belül. |
| FUNC-5 | Az alkalmazásnak interoperábilisnak kell lennie a tagállamokban kifejlesztett más alkalmazásokkal, hogy hatékonyan lehessen értesíteni a különböző tagállamok között utazó felhasználókat. |

## 6. Adatok

| | |
|---|---|
| DATA-1 | A sikeres kontaktkövetés érdekében az alkalmazásnak képesnek kell lennie az adatok továbbítására és fogadására olyan közelkörzeti kommunikációs technológiákon keresztül, mint a Bluetooth LE. |
| DATA-2 | Az alkalmazások által közvetített adatoknak az alkalmazás által generált és arra specifikusan jellemző, kriptográfiailag erős, pszeudovéletlen azonosítókat kell tartalmazniuk. |
| DATA-3 | A pszeudovéletlen azonosítók közötti ütközés kockázatának kellően alacsonynak kell lennie. |
| DATA-4 | A pszeudovéletlen azonosítókat rendszeresen meg kell újítani, éspedig olyan gyakorisággal, amely elegendő azon kockázat korlátozásához, hogy az egyéneket bárki – beleértve a központi szerverüzemeltetőket, más alkalmazásfelhasználókat vagy rosszindulatú harmadik feleket – újraazonosítsa, fizikailag nyomon kövesse vagy egymással összekapcsolja. Ezeket az azonosítókat a felhasználói alkalmazásnak kell generálnia, lehetőség szerint a központi szerver által biztosított kiindulási érték (seed) alapján. |
| DATA-5 | Az adattakarékosság elvének megfelelően az alkalmazás kizárólag a kontaktkövetéshez feltétlenül szükséges adatokat gyűjthet. |
| DATA-6 | Az alkalmazás nem gyűjthet helymeghatározó adatokat kontaktkövetés céljából. A helymeghatározó adatok kizárólag abból a célból kezelhetők, hogy lehetővé tegyék az alkalmazás számára a más országokban lévő hasonló alkalmazásokkal való interakciót, és pontosságukat az e kizárólagos cél eléréséhez feltétlenül szükséges mértékre kell korlátozni. |

| | |
|---|---|
| DATA-7 | Az alkalmazás a céljaihoz feltétlenül szükséges adatokon kívül nem gyűjthet egészségügyi adatokat, kivéve választható alapon és kizárólag abból a célból, hogy hozzájáruljon a felhasználó tájékoztatására vonatkozó döntéshozatalhoz. |
| DATA-8 | A felhasználókat tájékoztatni kell minden gyűjtött személyes adatról. Ezeket az adatokat csak a felhasználó engedélyével lehet gyűjteni. |

## 7. Műszaki tulajdonságok

| | |
|---|---|
| TECH-1 | Az alkalmazásnak az alkalmazást futtató eszköz közelében lévő felhasználók észlelésére olyan, rendelkezésre álló technológiákat kell használnia, mint például a közelkommunikációs technológia (pl. Bluetooth Low Energy). |
| TECH-2 | Az alkalmazásnak előre meghatározott, korlátozott ideig meg kell őriznie a berendezésben a felhasználó kontaktustörténetét. |
| TECH-3 | Egyes funkcióinak végrehajtásához az alkalmazás központi szerverre támaszkodhat. |
| TECH-4 | Az alkalmazásnak olyan architektúrán kell alapulnia, amely a lehető legnagyobb mértékben a felhasználó eszközeire támaszkodik. |
| TECH-5 | A vírussal fertőzöttnek bizonyult felhasználó kontaktustörténetét vagy saját azonosítóját az illető kezdeményezésére továbbítani kell a központi szerverre, miután egy megfelelően képzett egészségügyi szakember megerősítette ebbéli státuszukat. |

## 8. Biztonság

| | |
|---|---|
| SEC-1 | A SARS-CoV-2-pozitív eredményt kapott felhasználók státuszát egy erre a célra kialakított mechanizmus révén – például egy tesztállomáshoz vagy egészségügyi szakemberhez kapcsolódó egyszer használatos kód megadásával – ellenőrizni kell az alkalmazásban. Ha ez a megerősítés nem biztosítható biztonságos módon, az adatok nem kezelhetők. |
| SEC-2 | A központi szerverre küldött adatokat biztonságos csatornán keresztül kell továbbítani.<br>Az operációsrendszer-szolgáltatók által nyújtott értesítési szolgáltatások igénybevételét gondosan meg kell vizsgálni; e szolgáltatások igénybevétele nem vezethet semmilyen adat harmadik felek számára történő felfedéséhez. |
| SEC-3 | A lekérések nem lehetnek kitéve rosszindulatú felhasználó általi illetéktelen beavatkozásnak. |
| SEC-4 | A legkorszerűbb kriptográfiai technikákat kell alkalmazni az alkalmazás és a szerver, valamint az alkalmazások közötti biztonságos információcsere, illetve általános szabályként az alkalmazásokban és a szerveren tárolt információk védelme érdekében. Az alkalmazható technikák közé tartoznak például a következők: szimmetrikus és aszimmetrikus titkosítás, hash-funkciók, bizalmas tagsági teszt (PMT), bizalmas metszetképzés, Bloom-szűrők, bizalmas információk visszakeresése, homomorfikus titkosítás stb. |

| | |
|---|---|
| SEC-5 | A központi szerver nem őrizheti meg egyetlen felhasználó hálózati csatlakozási azonosítóját (pl. IP-címét) sem, így azokét sem, akiknek diagnózisa pozitív lett, és akik továbbították kontaktustörténetüket vagy saját azonosítóikat. |
| SEC-6 | A hasonmássággal való visszaélés és a hamis felhasználók létrehozásának megakadályozása érdekében a szervernek hitelesítenie kell az alkalmazást. |
| SEC-7 | Az alkalmazásnak hitelesítenie kell a központi szervert. |
| SEC-8 | A szerver funkcióit védeni kell a visszajátszásos támadásokkal szemben. |
| SEC-9 | A központi szerver által továbbított információkat eredetük és integritásuk hitelesítéséhez alá kell írni. |
| SEC-10 | A központi szerveren tárolt és a nyilvánosság számára nem hozzáférhető valamennyi adathoz való hozzáférést az arra jogosult személyekre kell korlátozni. |
| SEC-11 | Az eszköz engedélykezelője az operációs rendszer szintjén csak azokat az engedélyeket kérheti meg, amelyek a kommunikációs modulokhoz való hozzáféréshez és azok szükség szerinti használatához, az adatok végberendezésben való tárolásához, valamint a központi szerverrel való információcseréhez szükségesek. |

## 9. A természetes személyek személyes adatainak és magánéletének védelme

*Emlékeztető: az alábbi iránymutatások olyan alkalmazásra vonatkoznak, amelynek kizárólagos célja a kontaktkövetés.*

| | |
|---|---|
| PRIV-1 | Az adatcserének tiszteletben kell tartania a felhasználók magánéletét (és különösen az adattakarékosság elvét). |
| PRIV-2 | Az alkalmazás nem teheti lehetővé a felhasználók közvetlen azonosítását az alkalmazás használata során. |
| PRIV-3 | Az alkalmazás nem teheti lehetővé a felhasználók mozgásának nyomon követését. |
| PRIV-4 | Az alkalmazás használata nem teheti lehetővé a felhasználók számára, hogy bármit megtudjanak más felhasználókról (különösen arról, hogy vírushordozók-e vagy sem). |
| PRIV-5 | A központi szerver csak korlátozottan tekinthető megbízhatónak. A központi szerver irányításának világosan meghatározott irányítási szabályokat kell követnie, és magában kell foglalnia a szerver biztonságának garantálásához szükséges valamennyi intézkedést. A központi szerver elhelyezésének lehetővé kell tennie az illetékes felügyeleti hatóság általi hatékony felügyeletet. |
| PRIV-6 | Adatvédelmi hatásvizsgálatot kell végezni, és azt nyilvánosságra kell hozni. |
| PRIV-7 | Az alkalmazásnak csak azt kell jeleznie a felhasználó számára, hogy ki volt-e téve a vírusnak, valamint – lehetőség szerint más felhasználókra vonatkozó információk felfedése nélkül – azt, hogy az illető hány alkalommal és mely napokon volt exponált helyzetben. |
| PRIV-8 | Az alkalmazás által továbbított információk nem tehetik lehetővé a felhasználók számára, hogy azonosítsák a vírushordozó felhasználókat vagy azok mozgását. |
| PRIV-9 | Az alkalmazás által továbbított információk nem tehetik lehetővé az egészségügyi hatóságok számára a potenciálisan veszélyeztetett felhasználók azonosítását azok beleegyezése nélkül. |
| PRIV-10 | Az alkalmazás által a központi szerverhez továbbított kérések nem tárhatnak fel semmilyen információt a vírushordozóról. |
| PRIV-11 | A központi szerverhez továbbított kérések nem tartalmazhatnak szükségtelen információt a felhasználóról, kivéve, esetlegesen és csak szükség esetén, álneves azonosítóit és kontaktlistáját. |
| PRIV-12 | Ki kell zárni a kapcsolati támadások lehetőségét. |
| PRIV-13 | A felhasználók számára lehetővé kell tenni, hogy jogaikat az alkalmazáson keresztül gyakorolhassák. |
| PRIV-14 | Az alkalmazás eltávolításának az összes helyben gyűjtött adat törlését kell eredményeznie. |
| PRIV-15 | Az alkalmazás csak az alkalmazás további példányai vagy az azzal egyenértékű interoperábilis alkalmazások példányai által továbbított adatokat gyűjthet. Nem |

| | |
|---|---|
| | gyűjthetők más alkalmazásokra és/vagy közelkommunikációs eszközökre vonatkozó adatok. |
| PRIV-16 | A központi szerver általi újraazonosítás elkerülése érdekében proxyszervereket kell létrehozni. E *nem együttműködő szerverek* célja, hogy összekeverjék a felhasználók (a vírushordozók és a kérelmezők) azonosítóit, mielőtt azokat megosztanák a központi szerverrel, így akadályozva meg, hogy a központi szerver megismerje ezeket az azonosítókat (például IP-címeket). |
| PRIV-17 | Az alkalmazás és a szerver fejlesztése és konfigurálása során ügyelni kell arra, hogy a szerver ne gyűjtsön szükségtelen adatokat (pl. a szervernaplók nem tartalmazhatnak azonosítókat stb.), valamint arra, hogy harmadik felektől származó szoftvercsomagok ne gyűjthessenek más célokra adatokat. |

A legtöbb olyan kontaktkövető alkalmazás, amelynek bevezetése jelenleg megfontolás tárgyát képezi, alapvetően két megközelítést követ, amikor a felhasználót fertőzöttnek nyilvánítják: vagy a letapogatás útján szerzett kontaktustörténetet, vagy a közvetített saját azonosítóik listáját küldi el a szervernek. Az alkalmazott megközelítéstől függően az alábbiakban részletezett elvek érvényesítendők. Az, hogy itt e két megközelítést taglaljuk, nem jelenti azt, hogy nem lehetséges, vagy akár nem célszerűbb más megközelítést alkalmazni, például olyan megközelítést, amelyik az E2E-titkosítás valamilyen formáját, vagy más, a biztonságot vagy a magánélet védelmét erősítő technológiát alkalmaz.

**9.1. Azon elvek, amelyek** csak **akkor alkalmazandók, ha az alkalmazás a kontaktlistát küldi el a szervernek:**

| | |
|---|---|
| CON-1 | A központi szervernek a SARS-CoV-2-fertőzöttként diagnosztizált személy önkéntes fellépése nyomán kell összegyűjtenie az illető kontaktustörténetét. |
| CON-2 | A központi szerver nem őrizheti meg és nem terjesztheti a vírushordozó felhasználók álneves azonosítóinak listáját. |
| CON-3 | A központi szerveren tárolt kontaktustörténetet törölni kell, amint a felhasználók értesítést kaptak a fertőzöttként diagnosztizált személyhez való közelségükről. |
| CON-4 | Annak kivételével, amikor a fertőzöttként diagnosztizált felhasználó megosztja kontaktustörténetét a központi szerverrel, vagy amikor a felhasználó arra kéri a szervert, hogy tájékoztassa őt a vírusnak való potenciális kitettségéről, semmilyen adat nem hagyhatja el a felhasználó berendezését. |
| CON-5 | A helyi előzményekben szereplő azonosítókat a gyűjtésüktől számított X nap elteltével törölni kell (az X értékét az egészségügyi hatóságok határozzák meg). |
| CON-6 | A különböző felhasználók által továbbított kontaktustörténetek nem vethetők alá további adatkezelésnek, például globális közelségtérképek összeállításához kapcsolódó keresztkorrelációs eljárásnak. |
| CON-7 | A szervernaplóban tárolt adatok mennyiségét a lehető legkisebbre kell csökkenteni, és ezen adatoknak meg kell felelniük az adatvédelmi követelményeknek. |

**9.2. Azon elvek, amelyek csak akkor alkalmazandók, ha az alkalmazás a saját azonosítók listáját küldi el a szervernek:**

| | |
|---|---|
| ID-1 | A központi szervernek a SARS-CoV-2-fertőzöttként diagnosztizált személy önkéntes fellépése nyomán kell összegyűjtenie az illető alkalmazása által továbbított azonosítókat. |
| ID-2 | A központi szerver nem őrizheti meg és nem terjesztheti a vírushordozó felhasználók kontaktustörténetét. |
| ID-3 | A központi szerveren tárolt azonosítókat a többi alkalmazáshoz való továbbításukat követően törölni kell. |
| ID-4 | Annak kivételével, amikor a fertőzöttként diagnosztizált felhasználó megosztja azonosítóit a központi szerverrel, vagy amikor a felhasználó arra kéri a szervert, hogy tájékoztassa őt a vírusnak való potenciális kitettségéről, semmilyen adat nem hagyhatja el a felhasználó berendezését. |
| ID-5 | A szervernaplóban tárolt adatok mennyiségét a lehető legkisebbre kell csökkenteni, és ezen adatoknak meg kell felelniük az adatvédelmi követelményeknek. |