Riktlinjer 4/2020 om användning av lokaliseringsuppgifter och kontaktspårningsverktyg i samband med covid-19-utbrottet

Antagna den 21 april 2020

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

antaget

Versionshistorik

Version 1.1	5 maj 2020	Mindre korrigeringar
Version 1.0	21 april 2020	Antagande av riktlinjerna

Innehållsförteckning

Europeiska dataskyddsstyrelsen har

med beaktande av artikel 70.1e i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning),

med beaktande av EES-avtalet, särskilt bilaga XI och protokoll 37, ändrat genom gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018[1], och

med beaktande av artiklarna 12 och 22 i arbetsordningen,

ANTAGIT FÖLJANDE RIKTLINJER.

1 INLEDNING OCH BAKGRUND

1 Regeringar och privata aktörer intresserar sig alltmer för dataunderstödda lösningar som ett inslag i insatserna mot covid-19-pandemin, vilket aktualiserar ett stort antal integritetsfrågor.

2 Europeiska dataskyddsstyrelsen (nedan kallad *styrelsen*) vill understryka att den rättsliga ramen för dataskydd utformades för att vara flexibel. Tack vare den flexibiliteten är det möjligt att både verkningsfullt begränsa pandemin och skydda de grundläggande mänskliga fri- och rättigheterna.

3 Styrelsen är fast övertygad om att när det krävs behandling av personuppgifter för att hantera covid-19-pandemin, är dataskyddet en nödvändighet för att bygga förtroende och skapa förutsättningar för att åtgärderna ska accepteras av allmänheten, och därmed garantera att de blir verkningsfulla. Eftersom viruset inte känner några gränser, framstår det som motiverat att utveckla en gemensam europeisk strategi som svar på den aktuella krisen, eller åtminstone att införa en kompatibel ram.

4 Styrelsen anser generellt att data och teknik som utnyttjas i kampen mot covid-19 bör användas för att ge människor större inflytande, snarare än att kontrollera, stigmatisera eller förtrycka enskilda individer. Visserligen kan data och teknik vara viktiga verktyg, men de har också inneboende begränsningar och kan endast bli en hävstång för att höja andra folkhälsoåtgärders verkningsgrad. De allmänna principerna effektivitet, nödvändighet och proportionalitet måste vara vägledande för alla åtgärder som vidtas av medlemsstater eller EU-institutioner och som innebär behandling av personuppgifter för att bekämpa covid-19.

5 I föreliggande riktlinjer beskrivs villkoren och principerna för en proportionell användning av lokaliseringsuppgifter och kontaktspårningsverktyg inom två särskilda användningsområden:

- lokaliseringsuppgifter till stöd för åtgärder mot pandemin genom modellering av virusets spridning för att bedöma isoleringsåtgärdernas övergripande verkningsgrad,
- kontaktspårning i syfte att upplysa enskilda individer om att de befunnit sig i närheten av någon som senare kommer att bekräftas som virusbärare för att därigenom bryta smittkedjorna så tidigt som möjligt.

6 Det finns många faktorer som avgör effektiviteten i kontaktspårningsapparnas bidrag till hanteringen av pandemin (t.ex. andel av befolkningen som skulle behöva installera dem och definitionen av ”kontakt” med avseende på närhet och varaktighet). Vidare måste apparna

1Hänvisningar till ”medlemsstater” i detta dokument bör förstås som hänvisningar till ”medlemsstater i EES”.

också ingå som en del i en heltäckande folkhälsostrategi för bekämpande av pandemin med bl.a. testning och efterföljande manuell kontaktspårning för att skingra alla tvivel. När apparna börjar släppas, måste det samtidigt säkerställas att informationen till användarna sätts in i ett sammanhang och att varningarna verkligen kommer det offentliga hälso- och sjukvårdssystemet till godo. Om detta inte kan garanteras, finns det en risk att apparna inte kan utnyttjas maximalt.

7 Styrelsen betonar att både den allmänna dataskyddsförordningen (nedan kallad *dataskyddsförordningen*) och direktiv 2002/58/EG (nedan kallat *direktivet*) innehåller särskilda regler som medger användning av anonyma uppgifter eller personuppgifter till stöd för myndigheter och andra aktörer på nationell nivå och EU-nivå vid övervakningen och begränsningen av sars-cov-2-viruset[2].

8 Mot bakgrund av detta har styrelsen redan tagit ställning till det faktum att användningen av kontaktspårningsappar bör vara frivillig och inte bör bygga på spårning av enskilda rörelser utan snarare på uppgifter om närheten mellan användare[3].

[2] Se styrelsens tidigare uttalande om covid-19-utbrottet.
[3] [3] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

2 ANVÄNDNING AV LOKALISERINGSUPPGIFTER

2.1 Källor till lokaliseringsuppgifter

9 Det finns två huvudsakliga källor till lokaliseringsuppgifter som kan användas för modellering av virusets spridning och isoleringsåtgärdernas övergripande verkningsgrad:

- Lokaliseringsuppgifter som samlats in av leverantörer av elektronisk kommunikation (t.ex. telekomoperatörer) i samband med tillhandahållandet av tjänsten.
- Lokaliseringsuppgifter som samlats in av appar som tillhandahålls av leverantörer av informationssamhällets tjänster och som inte fungerar utan användning av sådana uppgifter (t.ex. navigation och transporttjänster).

10 Styrelsen erinrar om att lokaliseringsuppgifter[4] som samlats in från leverantörer av elektronisk kommunikation får behandlas enbart inom ramen för artiklarna 6 och 9 i direktivet. Detta innebär att uppgifterna kan överlämnas till myndigheter eller andra tredje parter först efter att ha anonymiserats av leverantören, eller med användarens samtycke när det gäller uppgifter som inte är trafikuppgifter och som visar den geografiska positionen för en användares terminalutrustning[5].

11 Vad gäller information, även lokaliseringsuppgifter, som samlats in direkt från terminalutrustningen, är artikel 5.3 i direktivet tillämplig. Därför är lagring av information om användarens enhet eller tillgång till redan lagrad information tillåten endast om i) användaren har lämnat sitt samtycke[6] eller ii) lagringen och/eller tillgången är absolut nödvändig för den av informationssamhällets tjänster som uttryckligen begärs av användaren.

12 Enligt artikel 15 i direktivet är det dock möjligt att göra en inskränkning av gällande rättigheter och skyldigheter när i ett demokratiskt samhälle en sådan inskränkning är nödvändig, lämplig och proportionell för vissa ändamål[7].

13 Vad gäller återanvändning av lokaliseringsuppgifter som samlats in av en leverantör av informationssamhällets tjänster i modelleringssyfte (t.ex. genom operativsystemet eller någon tidigare installerad app), måste också andra villkor vara uppfyllda. När uppgifter har samlats in i enlighet med artikel 5.3. i direktivet får de vidarebehandlas endast med den registrerades samtycke eller på grundval av en sådan lagstiftningsåtgärd i unionsrätten eller en medlemsstats nationella rätt som utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa de mål som avses i artikel 23.1 i den allmänna dataskyddsförordningen[8].

2.2 Fokus på användningen av anonymiserade lokaliseringsuppgifter

14 Styrelsen betonar att vid användning av lokaliseringsuppgifter bör alltid behandling av anonymiserade uppgifter prioriteras framför personuppgifter.

15 Med anonymisering avses användningen av särskilda tekniker för att undanröja möjligheten att, med varje ”rimlig” insats, koppla uppgifterna till en identifierad eller identifierbar fysisk person. I detta ”rimlighetstest” måste inte bara objektiva aspekter (tid och teknisk utrustning) beaktas, utan också faktorer i det större sammanhanget, vilka kan variera från fall till fall (ett fenomens sällsynthet med hänsyn till exempelvis befolkningstätheten, uppgifternas art och

---

[4] Se artikel 2 c i direktivet.
[5] Se artiklarna 6 och 9 i direktivet.
[6] Begreppet samtycke i direktivet är detsamma som begreppet samtycke i dataskyddsförordningen och måste uppfylla alla krav på samtycke enligt artiklarna 4.11 och 7 i dataskyddsförordningen.
[7] För tolkningen av artikel 15 i direktivet om integritet och elektronisk kommunikation, se även EU-domstolens dom av den 29 januari 2008 i mål C-275/06, Productores de Música de España (Promusicae) mot Telefónica de España SAU.
[8] Se avsnitt 1.5.3 i guidelines 1/2020 on processing personal data in the context of connected vehicles (”riktlinjer 1/2020 om behandling av personuppgifter i samband med uppkopplade fordon”).

omfattning). Om testet visar på luckor är uppgifterna inte anonymiserade och omfattas därför fortfarande av dataskyddsförordningen.

16 Utvärderingen av anonymiseringens hållbarhet utgår från tre testoperationer (kriterier): i) peka ut någon (isolering av en enskild person i en större grupp på grundval av uppgifterna), ii) sammanlänka uppgifter (sammanlänka två poster som rör samma person), samt iii) dra slutsatser (med stor sannolikhet sluta sig till okänd information om en enskild person).

17 Anonymiseringsbegreppet missförstås ofta och tolkas då felaktigt som pseudonymisering. Medan anonymisering medger obegränsad användning av uppgifterna, omfattas pseudonymiserade uppgifter fortfarande av dataskyddsförordningen.

18 Det finns många möjligheter till faktisk anonymisering[9], dock med ett förbehåll. Uppgifter kan inte anonymiseras enskilt, vilket innebär att endast hela dataset kan anonymiseras eller inte. I denna mening kan ingrepp i ett enskilt datamönster (genom kryptering eller andra matematiska omvandlingar) i bästa fall betraktas som pseudonymisering.

19 Anonymiseringsprocesser och avanonymiseringsattacker är två aktiva forskningsområden. Det är helt avgörande att alla personuppgiftsansvariga som inför anonymiseringslösningar följer den senaste utvecklingen på detta område, särskilt när det gäller lokaliseringsuppgifter (som härrör från telekomoperatörer och/eller informationssamhällets tjänster) som är kända för att alltid vara svåra att anonymisera.

20 Det finns mycket forskning som visar[10] att *lokaliseringsuppgifter som uppfattats anonymiserade* kanske inte varit det. Spåren efter enskilda personers rörlighet är inbördes starkt korrelerande och unika. Därför kan de under vissa omständigheter användas till att avanonymisera uppgifter.

21 Ett enskilt datamönster som spårar en individs lokalisering under en längre tid kan inte fullständigt anonymiseras. Detta kan stämma även om precisionsgraden för de registrerade geografiska koordinaterna sänks, om uppgifterna om spåret tas bort eller om endast de platser där den registrerade vistas under längre tid lokaliseras och sparas. Detta gäller även lokaliseringsuppgifter med låg systematiseringsgrad.

22 För att uppnå anonymisering måste lokaliseringsuppgifter hanteras noggrant för att uppfylla rimlighetstestets krav. "Detta innebär att lokaliseringsdataset ska behandlas som en helhet och att behandlingen ska gälla uppgifter från en relativt stor grupp individer och ske med hjälp av tillgängliga robusta anonymiseringstekniker, under förutsättning att dessa tillämpas på ett lämpligt och effektivt sätt.

23 Med tanke på anonymiseringsprocessernas komplexitet uppmuntras slutligen öppenhet i fråga om anonymiseringsmetoden starkt.

---

[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” och (Pyrgelis et al., 2017) ”Knock Knock, Who’s There? Membership Inference on Aggregate Location Data”

3 KONTAKTSPÅRNINGSAPPAR

3.1 Allmän rättslig analys

24 Systematisk och storskalig övervakning av fysiska personers lokalisering och/eller kontakter innebär ett allvarligt intrång i deras personliga integritet. Legitimitet för detta kan skapas endast om användarna frivilligt godtar det för de olika aktuella syftena. Detta skulle i synnerhet innebära att enskilda som inte vill eller kan använda sådana appar inte skulle drabbas av någon nackdel.

25 För att säkerställa ansvarsskyldigheten bör det tydligt anges vem som är personuppgiftansvarig för kontaktspårningsappen. Styrelsen anser att de nationella hälsomyndigheterna borde kunna vara personuppgiftsansvariga[11] för en sådan app. Andra personuppgiftsansvariga kan också komma i fråga. Om flera aktörer står bakom apparna, måste deras roller och ansvarsområden i alla händelser klargöras från första början och förklaras för användarna.

26 När det gäller principen om ändamålsbegränsning, måste ändamålet vara tillräckligt specifikt för att utesluta ytterligare behandling för ändamål som saknar samband med hanteringen av hälsokrisen till följd av covid-19 (t.ex. kommersiella syften eller brottsbekämpningsändamål). När ändamålet väl har fastställts, blir det nödvändigt att se till att användningen av personuppgifter sker på ett adekvat, nödvändigt och proportionerligt sätt.

27 I fråga om kontaktspårningsappar bör principen om uppgiftsminimering samt inbyggt dataskydd och dataskydd som standard noggrant övervägas:

- Kontaktspårningsappar kräver inte spårning av enskilda användares lokalisering. I stället bör närhetsdata användas.
- Eftersom kontaktspårningsappar fungerar också utan direkt identifiering av enskilda personer, bör lämpliga åtgärder vidtas för att förhindra avanonymisering.
- Den insamlade informationen bör lagras i användarens terminalutrustning, och enbart relevant information bör samlas in och endast när så är absolut nödvändigt.

28 När det gäller frågan om behandlingens lagenlighet, noterar styrelsen att kontaktspårningsappar lagrar och/eller har tillgång till information som redan är lagrad i terminalutrustningen. Sådan information omfattas av artikel 5.3 i direktivet. Om dessa operationer är absolut nödvändiga för att leverantören av appen ska kunna tillhandahålla den tjänst som användaren uttryckligen har begärt, kräver behandlingen inte vederbörandes samtycke. Vad gäller operationer som inte är strikt nödvändiga, måste leverantören begära användarens samtycke.

29 Vidare konstaterar styrelsen att även om användningen av kontaktspårningsappar sker på frivillig grund, innebär detta inte att behandlingen av personuppgifter nödvändigtvis också är grundad på samtycke. När myndigheter tillhandahåller en tjänst på grundval av ett lagstadgat mandat, förefaller den mest relevanta rättsliga grunden för behandlingen vara att den är nödvändig för att utföra en uppgift av allmänt intresse, vilket innebär att artikel 6.1 e i dataskyddsförordningen är tillämplig.

30 I artikel 6.3 i förordningen fastställs att grunden för den behandling som avses i artikel 6.1 e ska fastställas i enlighet med unionsrätten eller en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av. Syftet med behandlingen ska fastställas i den rättsliga grunden eller, i fråga om behandling enligt punkt 1 e, vara nödvändigt för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.[12]

---

[11] Se även kommissionens meddelande Vägledning om appar till stöd för kampen mot covid-19-pandemin med avseende på dataskydd, Bryssel, 16.4.2020, C(2020) 2523 final.
[12] Se skäl 41.

31 Den rättsliga grund eller lagstiftningsåtgärd som utgör den lagenliga grunden för användningen av kontaktspårningsappar bör dock inbegripa meningsfulla skyddsåtgärder samt en hänvisning till att användningen av appen är frivillig. Det bör finnas en tydlig precisering av syftet och uttryckliga begränsningar när det gäller den fortsatta behandlingen av personuppgifter, samt tydlig uppgift om den eller de berörda personuppgiftansvariga. Kategorierna av uppgifter och enheter till vilka (samt de ändamål för vilka) personuppgifterna får lämnas ut bör också fastställas. Beroende på graden av inblandning bör ytterligare skyddsåtgärder införas, med beaktande av behandlingens art, omfattning och ändamål. Slutligen rekommenderar styrelsen också att ta med de kriterier som, så snart det är praktiskt möjligt, ska avgöra när appen ska avvecklas och vilken enhet som ska vara ansvarig och ansvarsskyldig för att avgöra detta.

32 Om behandlingen av uppgifterna däremot bygger på en annan rättslig grund, såsom samtycke (artikel 6.1 a)[13], måste den personuppgiftsansvarige förvissa sig om att de strikta kraven för att en sådan rättslig grund ska vara giltig är uppfyllda.

33 Vidare kan användningen av en app för bekämpande av covid-19-pandemin leda till insamling av hälsouppgifter (t.ex. om den smittades hälsostatus). Behandling av sådana uppgifter är tillåten om behandlingen är nödvändig av hänsyn till allmänintresset på folkhälsoområdet och uppfyller villkoren i artikel 9.2 i i dataskyddsförordningen[14] eller för hälso- och sjukvårdsändamål enligt artikel 9.2 h i förordningen[15]. Beroende på den rättsliga grunden kan behandlingen också grundas på uttryckligt samtycke (artikel 9.2 a i dataskyddsförordningen).

34 I enlighet med det ursprungliga syftet medger artikel 9.2 j i dataskyddsförordningen också att hälsouppgifter behandlas när så är nödvändigt för vetenskapliga forskningsändamål eller statistiska ändamål.

35 Den rådande hälsokrisen bör inte utnyttjas som ett tillfälle att fastställa oproportionerliga mandat för lagring av uppgifter. Lagringsbegränsningen bör beakta de verkliga behoven och den medicinska relevansen (detta kan inbegripa epidemiologiska överväganden som inkubationstid osv.) och personuppgifter bör endast bevaras så länge som covid-19-krisen pågår. Efteråt bör den allmänna regeln vara att alla personuppgifter raderas eller anonymiseras.

36 Såsom styrelsen förstår saken, kan sådana appar inte ersätta, utan endast stödja, manuell kontaktspårning utförd av kvalificerad personal inom offentlig hälso- och sjukvård, som kan reda ut huruvida nära kontakter sannolikt kan leda till överföring av virus eller ej (t.ex. vid interaktion med någon som skyddas av lämplig utrustning – kassapersonal osv. – eller ej). Styrelsen understryker att förfaranden och processer som inbegriper algoritmer vilka utnyttjas i kontaktspårningsappar bör användas under sträng övervakning genomförd av kvalificerad personal för att begränsa förekomsten av falska positiva och negativa resultat. Särskilt uppgiften att ge råd om lämpliga åtgärder bör inte grunda sig enbart på automatiserad behandling.

37 För att säkerställa att algoritmerna är rättvisa, tydligt visar var ansvarsskyldigheten ligger och, mer allmänt, följer gällande lagstiftning, måste de kunna granskas och regelbundet ses över av oberoende experter. Appens källkod bör göras tillgänglig för allmänheten så att den kan granskas så brett som möjligt.

38 Det kommer alltid att finnas ett visst antal positiva träffresultat som visar sig vara felaktiga. Eftersom identifieringen av en smittrisk sannolikt kan ha stor inverkan på enskilda individer, t.ex. om de måste hålla sig i självisolering till dess att de testats med negativt resultat, är det

---

[13] Personuppgiftsansvariga (särskilt myndigheter) måste särskilt uppmärksamma att samtycke inte bör betraktas som frivilligt om den enskilde inte har något verkligt val att vägra eller återkalla sitt samtycke utan att drabbas av nackdelar.

[14] Behandlingen måste grunda sig på unionslagstiftningen eller en medlemsstats lagstiftning som föreskriver lämpliga och specifika åtgärder för att skydda den registrerades fri- och rättigheter, särskilt tystnadsplikt.

[15] Se artikel 9.2 h dataskyddsförordningen

nödvändigt att kunna korrigera uppgifter och/eller analysresultat. Detta bör naturligtvis endast gälla situationer och tillämpningar där uppgifter behandlas och/eller lagras på ett sätt som tekniskt medger sådan korrigering och där de negativa effekter som nämns ovan sannolikt kommer att inträffa.

39 Slutligen anser styrelsen att en konsekvensbedömning avseende dataskyddet måste genomföras innan ett sådant verktyg införs, eftersom behandlingen anses inbegripa hög risk (hälsouppgifter, förväntad användning i stor skala, systematisk övervakning och användning av ny teknisk lösning)[16]. Styrelsen rekommenderar starkt att konsekvensbedömningarna avseende dataskydd offentliggörs.

3.2 Rekommendationer och funktionskrav

40 Enligt principen om uppgiftsminimering bör, bland andra åtgärder som inbyggt dataskydd och dataskydd som standard[17], de uppgifter som behandlas reduceras till ett strikt minimum. Appen bör inte samla in ovidkommande eller onödig information, som kan omfatta civilstånd, kommunikationsidentifierare, utrustningsförteckningar, meddelanden, samtalsloggar, lokaliseringsuppgifter, produktidentifieringar osv.

41 Uppgifter som översänts av appar får endast innehålla vissa unika och pseudonymiserade identifierare som genereras av och är specifika för appen. Dessa identifierare måste regelbundet förnyas med en frekvens som är förenlig med ändamålet att begränsa virusets spridning och som är tillräcklig för att begränsa risken för identifiering och fysisk spårning av individer.

42 Åtgärderna för kontaktspårning kan vidtas enligt en centraliserad eller decentraliserad strategi[18]. Båda bör betraktas som genomförbara alternativ, förutsatt att lämpliga säkerhetsåtgärder vidtas, som var och en är förknippade med en rad fördelar och nackdelar. Under konceptstadiet av utvecklingen av appen bör man därför alltid noga beakta båda koncepten och noggrant gå igenom de olika effekterna på dataskyddet och den personliga integriteten samt den eventuella effekten på enskildas rättigheter.

43 De servrar som ingår i kontaktspårningssystemet får endast samla in kontakthistorik eller pseudonymiserade identifierare från en användare som konstaterats smittad efter en grundlig bedömning utförd av hälsomyndigheterna och som en frivillig åtgärd från användarens sida. Alternativt måste det på servern bevaras en förteckning över infekterade användares pseudonymiserade identifierare eller deras kontakthistorik endast under den tid som behövs för att underrätta potentiellt smittade användare om deras exponering. Servern bör inte ha möjligheten att kunna identifiera potentiellt smittade användare.

44 Införandet av en global kontaktspårningsmetod med både appar och manuell spårning kan kräva att ytterligare information behandlas i vissa fall. I detta sammanhang bör denna ytterligare information bevaras i användarterminalen och behandlas endast när så är absolut nödvändigt och då med särskilt samtycke.

45 Modern kryptografisk teknik måste användas för att säkra såväl de uppgifter som lagras på servrar och i appar som utbyten mellan appar och fjärrservern. En ömsesidig autentisering mellan appen och servern måste också effektueras.

46 Rapporteringen av användare såsom sars-cov-2-smittade i appen måste godkännas på vederbörligt sätt, t.ex. genom en engångskod knuten till en smittad persons pseudonymiserade identitet och till en teststation eller anställd inom hälso- och sjukvården. Om bekräftelse inte

---

[16] Se WP29 riktlinjer (antagna av styrelsen) om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679.
[17] Se EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default
[18] Den decentraliserade lösningen överensstämmer generellt bättre med principen om uppgiftsminimering.

kan erhållas på ett säkert sätt, bör det inte äga rum någon uppgiftsbehandling som förutsätter att användarens status är giltig.

47 Den personuppgiftsansvarige måste, i samarbete med myndigheterna, tydligt och uttryckligen informera om länken för nedladdning av den officiella nationella kontaktspårningsappen för att därigenom minska risken för att enskilda personer använder en tredjeparts app.

4 SLUTSATS

48 Världen befinner sig mitt uppe i en omfattande folkhälsokris som kräver kraftfulla svar med följder som går långt utöver själva nödsituationen. Automatisk uppgiftsbehandling och digital teknik kan bli nyckelinslag i kampen mot covid-19. Man bör dock vara medveten om ”avstängningseffekten”. Vi måste ta ansvar för att varje åtgärd som vidtas under dessa extraordinära omständigheter är nödvändig, begränsad i tiden, av minimal omfattning och föremål för regelbunden och genuin granskning och vetenskaplig utvärdering.

49 Styrelsen understryker att man inte ska behöva välja mellan ett verkningsfullt svar på den pågående krisen och skyddet av våra grundläggande rättigheter. Inget av dessa båda värden behöver väljas bort och dessutom kan dataskyddsprinciperna spela en mycket viktig roll i kampen mot viruset. EU:s dataskyddslagstiftning medger en ansvarsfull användning av personuppgifter för hälsoförvaltningsändamål, samtidigt som det säkerställs att individuella rättigheter och friheter inte urholkas i processen.

För Europeiska dataskyddsstyrelsen

Ordföranden

(Andrea Jelinek)

BILAGA – KONTAKTSPÅRNINGSAPPAR – ANALYS OCH VÄGLEDNING

0. Ansvarsfriskrivning

Följande vägledning är varken föreskrivande eller uttömmande. Dess enda syfte är att ge dem som utvecklar och realiserar kontaktspårningsappar allmän vägledning. Andra lösningar än de som beskrivs här kan också användas och kan vara lagenliga så länge de överensstämmer med den gällande rättsliga ramen (dvs. den allmänna dataskyddsförordningen och direktivet).

Vägledningen är av allmän karaktär. Följaktligen bör rekommendationerna och skyldigheterna i detta dokument inte betraktas som uttömmande. Alla bedömningar måste göras från fall till fall, och vissa appar kan kräva ytterligare åtgärder som inte beskrivs här.

1. Sammanfattning

I många medlemsstater överväger berörda parter möjligheten att använda *kontaktspårningsappar** för att hjälpa folk att upptäcka om de har varit i kontakt med en person som är smittad med sars-cov-2.

De förutsättningar under vilka sådana appar skulle kunna bidra verkningsfullt till hanteringen av pandemin har ännu inte fastställts. Dessa villkor måste fastställas innan någon sådan app tas i bruk. Det är ändå lämpligt att tillhandahålla riktlinjer och därigenom förmedla relevant information till utvecklingsgrupper uppströms, så att personuppgiftsskyddet kan säkerställas redan på ett tidigt utvecklingsstadium.

Denna vägledning är av allmän karaktär. Följaktligen bör rekommendationerna och skyldigheterna i detta dokument inte betraktas som uttömmande. Alla bedömningar måste göras från fall till fall, och särskilda tillämpningar kan kräva ytterligare åtgärder som inte beskrivs här. Syftet med den här vägledningen är att ge utvecklare och realisatörer av kontaktspårningsappar allmän vägledning.

Vissa kriterier kan gå utöver de strikta krav som följer av regelverket för dataskydd. Syftet är att säkerställa största möjliga öppenhet i avsikt att främja social acceptans för sådana kontaktspårningsappar.

För detta ändamål bör utgivare av kontaktspårningsappar beakta följande kriterier:

- Användningen av en sådan app måste vara helt frivillig. Tillgången till lagstadgade rättigheter får inte villkoras av användningen av en sådan app. Enskilda personer måste alltid ha full kontroll över sina uppgifter och fritt kunna välja om de vill använda en sådan app.
- Kontaktspårningsappar kommer sannolikt att medföra en hög risk för fysiska personers rättigheter och friheter samt kräva att en konsekvensbedömning avseende dataskyddet görs innan de släpps.
- Information om närheten mellan användare av appen kan erhållas utan att de blir lokaliserade. Denna typ av app behöver inte några lokaliseringsuppgifter och bör därför inte omfatta användning av sådana uppgifter.

- När en användare diagnostiserats med sars-cov-2-viruset, bör endast de personer som användaren har varit i nära kontakt med under den epidemiologiskt relevanta lagringsperioden för kontaktspårning underrättas.
- Denna typ av app kan, beroende på vilken arkitektur som väljs, på grund av sitt funktionssätt kräva användning av en centraliserad server. I ett sådant fall, och i enlighet med principerna om uppgiftsminimering och inbyggt dataskydd, bör de uppgifter som behandlas av den centrala servern begränsas till ett minimum:
    - När en användare diagnostiseras som smittad, kan information om vederbörandes tidigare nära kontakter eller identifierare som sänts ut av användaren samlas in, dock endast med användarens samtycke. Det måste beslutas om en kontrollmetod som gör det möjligt att fastställa att personen verkligen är smittad utan att användaren identifieras. Tekniskt skulle detta kunna uppnås genom att kontakten tas först sedan hälso- och sjukvårdspersonal har bekräftat smittan, t.ex. genom användning av en särskild engångskod.
    - Den information som lagras på den centrala servern bör inte medge att den personuppgiftsansvarige kan identifiera användare som diagnostiserats som smittade eller som personer som varit i kontakt med dessa användare. Inte heller bör den medge att slutsatser dras om kontaktmönster som inte är nödvändiga för att fastställa relevanta kontakter.
- Tillämpningen av detta slags app kräver sändning av uppgifter som andra användares apparater kan avläsa och avlyssna:
    - Det räcker med utbyte av pseudonymiserade identifierare mellan användarnas mobila utrustning (datorer, surfplattor, smartklockor osv.), t.ex. genom att de sänds ut (t.ex. med tekniken Bluetooth Low Energy).
    - Identifierare måste genereras med hjälp av uppdaterade kryptografiska processer.
    - Identifierarna måste regelbundet förnyas för att minska risken för fysisk spårning och länkningsattacker.
- Denna typ av app måste vara säkrad på ett sätt som gör att den garanterar säkra tekniska processer. Särskilt gäller följande:
    - Appen bör inte ge användarna information som medger att andras identitet eller diagnos kan härledas. Den centrala servern får varken identifiera användare eller härleda information om dem.

Friskrivning: Ovanstående principer gäller det angivna syftet *kontaktspårning* med hjälp av appar, och endast detta syfte, som enbart går ut på att automatiskt underrätta de personer som kan ha exponerats för viruset (utan att behöva identifiera dem). Den behöriga tillsynsmyndigheten har rätt att kontrollera appoperatörerna och appens infrastruktur. Att följa dessa riktlinjer helt eller delvis är inte nödvändigtvis tillräckligt för att säkerställa efterlevnaden av regelverket för dataskydd.

2. Definitioner

Kontakt	Vid kontaktspårning avses med kontakt en användare som har varit i interaktion med en användare som bekräftats vara virusbärare under en tidsperiod och på ett avstånd som medför risk för betydande exponering för virusinfektionen. Parametrarna för exponeringens varaktighet och avståndet mellan personerna ska avgöras av hälso- och sjukvårdsmyndigheterna. Parametrarna kan sedan programmeras in i appen.
Lokaliseringsuppgifter	Med detta avses alla uppgifter som behandlas i ett elektroniskt kommunikationsnät eller av en elektronisk kommunikationstjänst med angivande av den geografiska positionen för terminalutrustningen tillhörande en användare av en allmänt tillgänglig elektronisk kommunikationstjänst (enligt definitionen i direktivet), samt uppgifter från andra potentiella källor avseende: - terminalutrustningens latitud, longitud eller altitud, - användarens färdriktning, eller - tidpunkten för registreringen av lokaliseringsinformationen.
Interaktion	När det gäller kontaktspårningsappar, definieras interaktion som utbyte av information mellan två enheter i närheten av varandra (i tid och rum), inom ramen för den kommunikationsteknik som används (t.ex. Bluetooth). Denna definition utesluter lokalisering av de två användarna i interaktionen.
Virusbärare	I föreliggande dokument avses med virusbärare en användare som har testats positivt för viruset och som har fått en officiell diagnos från läkare eller en vårdinrättning.
Kontaktspårning	Personer som har varit i nära kontakt (enligt kriterier som ska fastställas av epidemiologer) med en person som är smittad med viruset löper stor risk att också smittas och att smitta andra i sin tur. Kontaktspårning är en metod för sjukdomsbekämpning, som förtecknar alla personer som befunnit sig i närheten av en virusbärare, för att kontrollera om dessa kan ha smittas och vidta lämpliga sanitära åtgärder.

3. Allmänt

GEN-1	Appen måste vara ett kompletterande verktyg till traditionella metoder för kontaktspårning (särskilt intervjuer med smittade personer). Den måste med andra ord ingå i ett bredare folkhälsoprogram. Den får endast användas så länge som enbart manuella kontaktspårningsmetoder inte räcker till för att hantera antalet nya infektioner.

GEN-2	Senast vid den tidpunkt då ”återgång till normalläge” beslutats av behöriga myndigheter, måste åtgärder vidtas för att stoppa insamlingen av identifierare (global avaktivering av appen, instruktioner för avinstallation av appen, automatisk avinstallation osv.) och aktivera radering av alla insamlade uppgifter från alla databaser (mobila appar och servrar).
GEN-3	Appens och dess backendsystems källkod måste vara öppna, och de tekniska specifikationerna måste offentliggöras så att alla berörda parter kan granska koden och i förekommande fall bidra till att förbättra den, korrigera eventuella programfel och säkerställa insyn i behandlingen av personuppgifter.
GEN-4	När appen släpps, måste det ske i etapper så att den successivt kan utvärderas ur ett folkhälsoperspektiv. Redan i ett tidigt skede måste ett utvärderingsprotokoll, med angivande av indikatorer som medger mätning av appens ändamålsenlighet, fastställas för detta ändamål.

4. Syften

PUR-1	Appen ska ha kontaktspårning som sitt enda syfte, så att personer som kan komma att exponeras för sars-cov-2-viruset kan varnas och tas om hand. Den får inte användas i något annat syfte.
PUR-2	Appen får inte användas utanför sitt primära användningsområde i syfte att kontrollera efterlevnaden av karantän- eller isoleringsåtgärder och/eller social distansering.
PUR-3	Appen får inte användas för att dra slutsatser om var användarna befinner sig utifrån deras interaktion och/eller på något annat sätt.

5. Frågor med avseende på funktionen

FUNC-1	Appen måste ha en funktion som informerar användarna om att de kan ha exponerats för viruset. Denna information bygger på närhet till en smittad användare inom en period av X dagar före det positiva resultatet av screeningtestet (X-värdet fastställs av hälso- och sjukvårdsmyndigheterna).
FUNC-2	Användare som identifierats som potentiellt exponerade för viruset bör kunna få rekommendationer i appen. Den bör ge upplysningar om vad man bör göra och användaren bör kunna få rådgivning genom appen. I det fallet är en mänsklig kontakt obligatorisk.
FUNC-3	Algoritmen som mäter smittorisken genom att beakta avstånd och tid, och därigenom avgör när en kontakt ska registreras i kontaktspårningsförteckningen, måste på ett säkert sätt kunna beakta de senaste rönen om virusets spridning.

FUNC-4	**Användarna måste informeras i de fall där de har exponerats för viruset**, eller regelbundet få ta del av information om huruvida de har utsatts för viruset eller inte, under virusets inkubationstid.
FUNC-5	Appen bör vara kompatibel med andra appar som utvecklats i medlemsstaterna, så att användare som reser mellan olika medlemsländer faktiskt kan underrättas.

6. Uppgifter

DATA-1	Appen måste kunna sända och ta emot uppgifter genom närkommunikationsteknik, t.ex. Bluetooth Low Energy, så att kontaktspårning medges.
DATA-2	Dessa sändningsdata måste innehålla kryptografiskt starka pseudoslumpidentifierare som genereras av appen och är specifika för denna.
DATA-3	Risken för kollision mellan pseudoslumpidentifierare bör vara tillräckligt låg.
DATA-4	Pseudoslumpidentifierare måste regelbundet bytas ut. Detta måste ske med en frekvens som är tillräcklig för att begränsa risken för att vem som helst – även operatörer av centrala servrar, andra appanvändare eller tredje parter med ont uppsåt – kan avanonymisera, fysiskt spåra eller koppla samman enskilda personer. Dessa identifierare måste genereras av användarens app, eventuellt med hjälp av ett frö som tillhandahålls av den centrala servern.
DATA-5	Enligt principen om uppgiftsminimering får appen inte samla in andra uppgifter än vad som är absolut nödvändigt i syfte att genomföra kontaktspårning.
DATA-6	Appen får inte samla in lokaliseringsuppgifter i syfte att genomföra kontaktspårning. Lokaliseringsuppgifter får behandlas enbart i syfte att medge interaktion med liknande appar i andra länder och deras precision bör begränsas till vad som är absolut nödvändigt för detta enda syfte.
DATA-7	Appen bör inte samla in andra hälsouppgifter än de som är strikt nödvändiga för tillämpningen av appen, förutom på frivillig grund och i det enda syftet att bidra till beslutet om att underrätta användaren.
DATA-8	Användare måste underrättas om vilka personuppgifter som kommer att samlas in. Dessa uppgifter bör samlas in endast med användarens godkännande.

7. Tekniska egenskaper

TECH-1	Appen bör använda tillgänglig teknik, såsom teknik för närhetskommunikation (t.ex. Bluetooth Low Energy), för att upptäcka användare i närheten av en apparat med appen installerad.

TECH-2	Appen bör spara historiken över en användares kontakter i apparaten under en i förväg fastställd begränsad period.
TECH-3	Appen får använda en central server för att fullgöra vissa funktioner.
TECH-4	Appen måste bygga på en arkitektur som så långt möjligt utgår från användarnas apparater.
TECH-5	På initiativ av användare som rapporterats som smittade av viruset, och efter att deras status har bekräftats av vederbörligen certifierad hälso- och sjukvårdspersonal, bör deras kontakthistorik eller deras egna identifierare översändas till den centrala servern.

8. Säkerhet

SEC-1	Det måste finnas en mekanism som kan verifiera statusen för de användare som rapporteras som sars-cov-2-positiva i appen, t.ex. genom att en engångskod kopplad till en teststation eller professionell hälso- och sjukvårdsinrättning tillhandahålls. Om bekräftelse inte kan erhållas på ett säkert sätt, får uppgifterna inte behandlas.
SEC-2	De uppgifter som skickas till den centrala servern måste överföras via en säker kanal. Användningen av aviseringstjänster som tillhandahålls av operativsystemleverantörer bör ingående bedömas och får inte leda till att några uppgifter lämnas ut till tredjeparter.
SEC-3	En begäran får inte kunna manipuleras av en användare med ont uppsåt.
SEC-4	Aktuell kryptografisk teknik måste användas för att åstadkomma ett säkert utbyte mellan appen och servern och mellan appar, samt som en allmän regel till skydd för den information som lagras i apparna och på servern. Exempel på tekniker som kan användas: symmetrisk och asymmetrisk kryptering, hashfunktioner, privat medlemskapstest, privata setsnitt, Bloom-filter, insamling av privat information, homomorfisk kryptering osv.
SEC-5	Identifierare för nätverksanslutningar (t.ex. IP-adresser) för användare får inte sparas på den centrala servern. Detta gäller även dem som har testats positivt och som har överfört sin kontakthistorik eller sina egna identifierare.
SEC-6	För att undvika identitetsbedrägeri eller skapande av falska användare måste appen autentiseras av servern.
SEC-7	Den centrala servern måste autentiseras av appen.
SEC-8	Serverfunktionerna bör vara skyddade för omtagningsattacker.
SEC-9	Den information som översänds av den centrala servern måste vara signerad för att autentisera ursprunget och integriteten.
SEC-10	Tillgång till alla uppgifter som lagras på den centrala servern och inte är tillgängliga för allmänheten ska begränsas till endast auktoriserade personer.

SEC-11	Apparatens tillståndsadministratör på operativsystemsnivå ska bara begära de tillstånd som är nödvändiga för att vid behov få tillgång till och använda kommunikationsmodulerna, lagra uppgifterna i terminalen och utbyta information med den centrala servern.

9. Skydd av fysiska personers personuppgifter och integritet

Påminnelse: följande riktlinjer gäller en app vars enda syfte är kontaktspårning.

PRIV-1	Vid uppgiftsutbytet måste användarnas integritet respekteras (och i synnerhet principen om uppgiftsminimering).
PRIV-2	Användning av appen får inte leda till att användarna direkt kan identifieras.
PRIV-3	Användning av appen får inte leda till att användares rörelser kan spåras.
PRIV-4	Användning av appen får inte leda till att användare kan få tillgång till uppgifter om andra användare (och särskilt inte uppgifter som visar huruvida de är virusbärare).
PRIV-5	Förtroendet för den centrala servern måste vara begränsat. Förvaltningen av den centrala servern måste ske enligt tydligt definierade styrningsregler och omfatta alla nödvändiga åtgärder för att garantera dess säkerhet. Den centrala servern bör vara lokaliserad någonstans där den behöriga tillsynsmyndigheten kan utöva faktisk tillsyn av den.
PRIV-6	En konsekvensbedömning av dataskyddet måste genomföras och offentliggöras.
PRIV-7	Det enda som appen bör visa användaren är om vederbörande har exponerats för viruset och, om detta är möjligt utan att samtidigt visa information om andra användare, hur många gånger och när exponeringen ägt rum.
PRIV-8	Användarna får inte utifrån de uppgifter som framgår av appen kunna identifiera de användare som är virusbärare eller deras rörelser.
PRIV-9	Hälsovårdsmyndigheterna får inte utifrån de uppgifter som framgår av appen kunna identifiera potentiellt exponerade användare utan deras samtycke.
PRIV-10	Begäranden som av appen riktats till den centrala servern får inte avslöja något om bäraren av viruset.
PRIV-11	Begäranden som av appen riktas till den centrala servern får inte i onödan avslöja någon information om användaren, förutom möjligen och endast när så är nödvändigt, användarens pseudonymiserade identifierare och dennes kontaktlista.
PRIV-12	Länkningsattacker får inte vara möjliga.
PRIV-13	Användarna måste kunna få sina rättigheter tillgodosedda genom appen.
PRIV-14	Radering av appen måste leda till att alla lokalt insamlade uppgifter raderas.
PRIV-15	Appen bör endast samla in uppgifter som överförts av instanser i appen eller driftskompatibla likvärdiga appar. Inga uppgifter om andra appar och/eller apparater som medger närkommunikation ska samlas in.
PRIV-16	För att undvika att den centrala servern utför avanonymiseringar bör proxyservrar inrättas. Syftet med dessa *servrar som inte fritt samverkar* är att blanda flera användares identifierare (både virusbärarnas och dem som skickas av begärarna) innan de delas med den centrala servern, så att den inte kan känna till användarnas identifierare (t.ex. IP-adresser).

PRIV-17	Appen och servern måste vara noggrant utvecklade och konfigurerade för att inte samla in onödiga uppgifter (t.ex. bör inga identifierare ingå i serverloggarna) och för att undvika användning av någon tredjeparts programutvecklingsverktyg som samlar in uppgifter för andra ändamål.

I de flesta kontaktspårningsappar som för närvarande diskuteras tillämpas i princip två metoder när en användare har förklarats smittad. Antingen kan den historik över närhetskontakter som apparna fått fram genom avsökning skickas till en server, eller så kan listan över de egna identifierare som sänts ut av apparna skickas. Följande principer delas i enlighet med dessa båda metoder: Visserligen diskuteras dessa metoder här, men det innebär inte att andra metoder inte kan tänkas eller vara bättre, t.ex. metoder som inbegriper någon form av E2E-kryptering eller bygger på annan teknik för att förbättra säkerheten eller integritetsskyddet.

9.1. Principer som gäller enbart **när en kontaktlista skickas till servern från appen:**

CON-1	Den centrala servern måste samla in kontakthistorik från användare som rapporterats som sars-cov-2-positiva som ett resultat av frivilligt agerande från deras sida.
CON-2	Den centrala servern får inte behålla eller sprida förteckningen över pseudonymiserade identifierare för användare som är bärare av viruset.
CON-3	Den kontakthistorik som lagras på den centrala servern måste raderas så snart användarna underrättats om att de befunnit sig i närheten av en person som testats positivt.
CON-4	Förutom när den användare som testats positivt delar sin kontakthistorik med den centrala servern, eller när användaren riktar en begäran till servern för att ta reda på sin potentiella exponering för viruset, får inga uppgifter lämna användarens utrustning.
CON-5	Varje identifierare som ingår i den lokala historiken måste raderas efter X dagar efter insamlingstillfället (X fastställs av hälso- och sjukvårdsmyndigheterna).
CON-6	Kontakthistoriken som lämnas in av en viss användare bör inte behandlas vidare, t.ex. korskopplas för att skapa globala närhetskartor.
CON-7	Uppgifter i serverloggar måste minimeras och uppfylla dataskyddskraven.

9.2. Principer som gäller enbart när en lista över de egna identifierarna skickas från appen till en server:

ID-1	Den centrala servern måste samla in de identifierare som sänts ut från appen om användare som rapporterats som sars-cov-2-positiva som ett resultat av frivilligt agerande från deras sida.
ID-2	Den centrala servern får inte behålla eller sprida kontakthistoriken från användare som bär på viruset.

ID-3	Identifierare lagrade på den centrala servern måste raderas så snart de spritts till övriga appar.
ID-4	När den användare som testats positivt delar sina identifierare med den centrala servern, får inga uppgifter lämna användarens utrustning. Inte heller när användaren riktar en begäran till servern för att ta reda på sin potentiella exponering för viruset, får några uppgifter lämna användarens utrustning.
ID-5	Uppgifter i serverloggar måste minimeras och uppfylla dataskyddskraven.