Retningslinjer 04/2020 om brug af lokaliseringsdata og kontaktopsporingsredskaber i forbindelse med covid-19-udbruddet

Vedtaget den 21. april 2020

Versionshistorik

Version 1.1	5. maj 2020	Mindre rettelser
Version 1.0	21. april 2020	Vedtagelse af retningslinjerne

Indhold

Det Europæiske Databeskyttelsesråd har —

under henvisning til artikel 70, stk. 1, litra e), i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (i det følgende benævnt "databeskyttelsesforordningen"),

under henvisning til EØS-aftalen, særlig bilag XI og protokol 37 som ændret ved Det Blandede EØS-Udvalgs afgørelse nr. 154/2018 af 6. juli 2018[1],

under henvisning til sin forretningsordens artikel 12 og 22 —

VEDTAGET FØLGENDE RETNINGSLINJER:

1 INDLEDNING OG BAGGRUND

1 Regeringer og private aktører bevæger sig i retning af brug af datadrevne løsninger som led i indsatsen over for covid-19-pandemien, hvilket rejser adskillige spørgsmål i relation til beskyttelsen af privatlivets fred.

2 Det Europæiske Databeskyttelsesråd (i det følgende benævnt "Databeskyttelsesrådet") understreger, at lovrammen for databeskyttelse blev udformet med henblik på fleksibilitet, og at den i kraft heraf gør det muligt både at sikre en effektiv indsats for at begrænse pandemien og at beskytte de grundlæggende menneskerettigheder og frihedsrettigheder.

3 Databeskyttelsesrådet er af den faste overbevisning, at databeskyttelse — når behandling af personoplysninger er påkrævet for at håndtere covid-19-pandemien — er en afgørende forudsætning for at opbygge tillid, skabe de fornødne betingelser for befolkningens accept af de relevante løsninger og dermed sikre de pågældende foranstaltningers effektivitet. Da virusset ikke kender til grænser, forekommer det hensigtsmæssigt at udvikle en fælles europæisk tilgang til at tackle den nuværende krise, eller i det mindste indføre en interoperabel ramme.

4 Databeskyttelsesrådet finder generelt, at data og teknologi, der bruges i kampen mod covid-19, bør anvendes til at styrke, snarere end at kontrollere, stigmatisere eller undertrykke de enkelte borgere. Dertil kommer, at data og teknologi — om end de kan være vigtige værktøjer — har iboende begrænsninger og udelukkende kan fungere som løftestang for andre folkesundhedsforanstaltningers effektivitet. De almindelige principper for effektivitet, nødvendighed og proportionalitet skal være retningsgivende for enhver foranstaltning fra medlemsstaternes eller EU-institutionernes side, der indebærer behandling af personoplysninger som led i kampen mod covid-19.

5 Med disse retningslinjer præciseres betingelserne og principperne for anvendelse af lokaliseringsdata og kontaktopsporingsredskaber i overensstemmelse med proportionalitetsprincippet med to specifikke formål for øje:

- brug af lokaliseringsdata til støtte for indsatsen over for pandemien ved hjælp af modelberegninger af virussets spredning, idet formålet er at vurdere effektiviteten af isolationsforanstaltninger samlet set

1 Henvisninger til "medlemsstater" i dette dokument skal forstås som henvisninger til "EØS-medlemsstater".

- kontaktopsporing, der har til formål at underrette personer om, at de har befundet sig tæt på en person, om hvem det efterfølgende bekræftes, at vedkommende var bærer af virusset, med det formål at bryde smittekæderne så tidligt som muligt.

6 Hvor effektivt kontaktopsporingsapplikationer bidrager til at holde pandemien under kontrol, afhænger af mange faktorer (f.eks. den procentvise andel af personer, der ville skulle installere den pågældende applikation, definitionen af "kontakt" med hensyn til nærhed og varighed). Det er desuden nødvendigt, at sådanne applikationer indgår i en samlet folkesundhedsstrategi for bekæmpelse af pandemien, som omfatter bl.a. testning og efterfølgende manuel kontaktopsporing med henblik på at fjerne tvivl. Udrulningen af dem bør ledsages af støtteforanstaltninger, der sikrer, at de oplysninger, brugerne får, sættes ind i den rette sammenhæng, og at det offentlige sundhedssystem kan drage nytte af advarslerne. Uden sådanne foranstaltninger risikerer man, at applikationerne ikke får den optimale effekt.

7 Databeskyttelsesrådet understreger, at databeskyttelsesforordningen og direktiv 2002/58/EF (i det følgende benævnt "direktivet") begge indeholder regler, der specifikt giver mulighed for at anvende anonymiserede oplysninger eller personoplysninger som støtte for offentlige myndigheder og andre aktører på nationalt plan og på EU-plan i deres indsats for at overvåge og dæmme op for spredningen af SARS-CoV-2-virusset[2].

8 I denne forbindelse har Databeskyttelsesrådet allerede indtaget den holdning, at brug af kontaktopsporingsapplikationer bør være frivillig og ikke baseres på sporing af individers færden, men snarere på nærhedsinformation om brugerne[3].

[2] Jf. Databeskyttelsesrådets tidligere erklæring om covid-19-udbruddet.
[3] [3]https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf.

2 BRUG AF LOKALISERINGSDATA

2.1 Kilder til lokaliseringsdata

9 Der findes to hovedkilder til lokaliseringsdata, som kan bruges til modelberegning af virussets spredning og effektiviteten af isolationsforanstaltninger samlet set:

- lokaliseringsdata, der indsamles af udbydere af elektroniske kommunikationstjenester (f.eks. mobiloperatører) i forbindelse med leveringen af deres tjenester, og
- lokaliseringsdata, der indsamles via informationssamfundstjenesteudbyderes applikationer, hvis funktionalitet kræver anvendelse af sådanne data (f.eks. navigation, transporttjenester osv.).

10 Databeskyttelsesrådet minder om, at lokaliseringsdata[4], der indsamles fra udbydere af elektroniske kommunikationstjenester, kun må behandles inden for rammerne af direktivets artikel 6 og 9. Det betyder, at disse data kun må overføres til myndigheder eller andre tredjeparter, hvis udbyderen har anonymiseret dem, eller — hvis der er tale om data, der angiver den geografiske placering af en brugers terminaludstyr og ikke er trafikdata — efter brugernes forudgående samtykke[5].

11 For så vidt angår oplysninger, herunder lokaliseringsdata, der indsamles direkte fra terminaludstyret, finder direktivets artikel 5, stk. 3, anvendelse. Det er således kun tilladt at lagre oplysninger på brugerens enhed eller at tilgå de oplysninger, der allerede er lagret, hvis i) brugeren har givet sit samtykke hertil[6], eller ii) lagringen og/eller adgangen er absolut påkrævet for en informationssamfundstjeneste, som brugeren udtrykkelig har anmodet om.

12 Direktivets artikel 15 giver dog mulighed for undtagelser fra de rettigheder og forpligtelser, der følger af samme direktiv, hvis de af bestemte hensyn er nødvendige, passende og forholdsmæssige i et demokratisk samfund[7].

13 For så vidt angår genanvendelse af lokaliseringsdata indsamlet af en udbyder af informationssamfundstjenester til modelberegningsformål (f.eks. via operativsystemet eller en tidligere installeret applikation), skal visse yderligere betingelser være opfyldt. Når data er indsamlet i overensstemmelse med direktivets artikel 5, stk. 3, kan de således kun behandles yderligere, hvis den registrerede igen giver sit samtykke, eller på grundlag af EU-ret eller medlemsstaters nationale ret, som udgør en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund for at sikre de formål, der er omhandlet i databeskyttelsesforordningens artikel 23, stk. 1[8].

2.2 Fokus på brug af anonymiserede lokaliseringsdata

14 Databeskyttelsesrådet understreger, at behandling af anonymiserede data frem for personoplysninger altid vil være at anbefale i forbindelse med brug af lokaliseringsdata.

15 Ved anonymisering forstås anvendelse af en kombination af teknikker med det formål at sikre, at det ikke er muligt — med en "rimelig" indsats — at henføre data til en identificeret eller identificerbar fysisk person. Der skal med "rimelighedstesten" tages hensyn til både objektive aspekter (tid, tekniske midler) og kontekstuelle elementer, som kan variere fra sag til sag (hvor sjældent et fænomen er under hensyntagen til f.eks. befolkningstæthed og dataenes art og

---

[4] Jf. direktivets artikel 2, litra c).
[5] Jf. direktivets artikel 6 og 9.
[6] Begrebet samtykke i direktivet dækker det samme som begrebet samtykke i databeskyttelsesforordningen og skal opfylde alle kravene vedrørende samtykke i databeskyttelsesforordningens artikel 4, nr. 11), og artikel 7.
[7] Vedrørende fortolkningen af direktivets artikel 15 henvises også til Domstolens dom af 29. januar 2008, sag C-275/06, Productores de Música de España (Promusicae) mod Telefónica de España SAU.
[8] Jf. punkt 1.5.3 i retningslinjer 1/2020 vedrørende behandling af personoplysninger i forbindelse med opkoblede køretøjer.

mængde). Hvis de pågældende data ikke består denne test, er de ikke blevet anonymiseret og er dermed fortsat omfattet af databeskyttelsesforordningen.

16 Evaluering af anonymiseringsrobustheden baseres på tre kriterier: i) udskillelse (isolering af et individ inden for en større gruppe på grundlag af de pågældende data), ii) sammenkædelighed (sammenkædning af to poster vedrørende det samme individ) og iii) inferens (hvor der udledes ikke allerede kendte oplysninger om et individ (med en væsentlig sandsynlighed)).

17 Begrebet anonymisering kan let misforstås og forveksles ofte med pseudonymisering. Mens anonymisering giver mulighed for at anvende dataene uden begrænsninger, er pseudonymiserede data stadig omfattet af databeskyttelsesforordningen.

18 Der findes mange muligheder for effektiv anonymisering[9], dog med et forbehold. Individuelle data kan ikke anonymiseres, hvilket betyder, at kun hele datasæt kan gøres anonyme. I denne forstand kan enhver indgriben i et enkelt datamønster (ved hjælp af kryptering eller enhver anden form for matematisk transformation) i bedste fald betragtes som pseudonymisering.

19 Anonymiseringsprocesser og genidentificeringsangreb er aktive forskningsområder. Det er altafgørende for enhver dataansvarlig, der implementerer anonymiseringsløsninger, at følge den seneste udvikling på dette område, navnlig med hensyn til lokaliseringsdata (fra telekommunikationsoperatører og/eller informationssamfundstjenester), som vides at være notorisk vanskelige at anonymisere.

20 Omfattende forskning har vist[10], at *lokaliseringsdata, som man troede var anonymiserede*, ikke nødvendigvis har været det. Individers bevægelsesspor er i sagens natur indbyrdes nært forbundet og unikke. De kan derfor under visse omstændigheder være sårbare over for genidentificeringsforsøg.

21 Et enkelt datamønster, der bruges til at spore et individs færden over en længere periode, kan ikke anonymiseres fuldstændigt. Dette kan også være tilfældet, hvis præcisionen i de registrerede geografiske koordinater ikke nedsættes tilstrækkeligt, eller hvis nærmere oplysninger om brugerens spor/bevægelser fjernes, og selv hvis kun de steder, hvor den registrerede opholder sig i længere tid, gemmes. Dette gælder også for lokaliseringsdata, der er ikke er aggregeret ordentligt.

22 For at sikre anonymisering skal lokaliseringsdata behandles omhyggeligt, for at de kan bestå rimelighedstesten. I den henseende omfatter denne proces vurdering af lokaliseringsdatasæt som en helhed samt behandling af data fra et sæt (af en rimelig størrelse) af individer ved hjælp af eksisterende robuste anonymiseringsteknikker, forudsat at de implementeres korrekt og effektivt.

23 Endelig tilskyndes der, fordi anonymiseringsprocesserne er komplekse, på det kraftigste til gennemsigtighed for så vidt angår anonymiseringsmetoden.

---

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

3 KONTAKTOPSPORINGSAPPLIKATIONER

3.1 Generel juridisk analyse

24 Systematisk og omfattende overvågning af, hvor fysiske personer befinder sig, og hvem de kommer i kontakt med, er en alvorlig krænkelse af privatlivets fred. Den kan kun legitimeres ved brugernes frivillighed for hvert af de pågældende formål. Dette indebærer først og fremmest, at individer, der beslutter sig for ikke at gøre brug af eller ikke *kan* gøre brug af de pågældende applikationer, ikke på nogen måde bør stilles ringere.

25 For at sikre ansvarlighed bør det for enhver kontaktopsporingsapplikation være klart defineret, hvem den dataansvarlige er. Databeskyttelsesrådet mener, at de nationale sundhedsmyndigheder kunne være dataansvarlige[11] for en sådan applikation; også andre dataansvarlige kunne komme på tale. I alle tilfælde bør det, hvis udrulningen af en kontaktopsporingsapplikation involverer flere forskellige aktører, fra starten klart defineres og forklares for brugerne, hvilke roller og ansvarsområder disse aktører har.

26 Jf. princippet om formålsbegrænsning skal formålene desuden være tilstrækkeligt specifikke til at udelukke yderligere behandling til formål, der ikke vedrører håndteringen af covid-19-sundhedskrisen (f.eks. kommercielle formål eller retshåndhævelse). Når formålet er klart defineret, vil det være nødvendigt at sikre, at anvendelsen af personoplysninger er relevant, nødvendig og forholdsmæssig.

27 I relation til en kontaktopsporingsapplikation bør der tages nøje hensyn til princippet om dataminimering og databeskyttelse gennem design og gennem standardindstillinger:

- Kontaktopsporingsapplikationer nødvendiggør ikke sporing af individuelle brugeres færden. I stedet bør der anvendes nærhedsdata.
- Da kontaktopsporingsapplikationer kan fungere uden direkte identificering af individer, bør der træffes passende foranstaltninger til at forhindre genidentificering.
- De indsamlede oplysninger bør befinde sig på brugerens terminaludstyr, og kun de relevante oplysninger bør indsamles, i det omfang det er strengt nødvendigt.

28 For så vidt angår lovligheden af behandlingen bemærker Databeskyttelsesrådet, at kontaktopsporingsapplikationer indebærer lagring af og/eller adgang til oplysninger, der allerede er lagret i terminalen, og som er omfattet af direktivets artikel 5, stk. 3. Hvis disse handlinger er absolut påkrævede for at sætte udbyderen af applikationen i stand til at levere en tjeneste, som brugeren udtrykkelig har anmodet om, vil behandlingen ikke kræve hans eller hendes samtykke. For handlinger, der ikke er absolut påkrævede, vil udbyderen skulle indhente brugerens samtykke.

29 Databeskyttelsesrådet bemærker endvidere, at det, at brug af kontaktopsporingsapplikationer sker på frivillig basis, ikke i sig selv betyder, at behandlingen af personoplysninger nødvendigvis vil være baseret på samtykke. For offentlige myndigheder, der leverer en tjeneste på grundlag af en hjemmel, der er fastsat ved og i overensstemmelse med lovkrav, forekommer nødvendighed af hensyn til udførelse af en opgave i samfundets interesse, dvs. databeskyttelsesforordningens artikel 6, stk. 1, litra e), at være det mest relevante retsgrundlag for behandlingen.

30 I databeskyttelsesforordningens artikel 6, stk. 3, præciseres det, at grundlaget for behandling som omhandlet i artikel 6, stk. 1, litra e), skal fremgå af EU-retten eller medlemsstaternes nationale ret, som den dataansvarlige er underlagt. Formålet med behandlingen skal være fastlagt i dette retsgrundlag eller, for så vidt angår den behandling, der er omhandlet i stk. 1,

[11] Jf. også Europa-Kommissionens "Vejledning om apps til støtte for bekæmpelse af covid-19-pandemien i forbindelse med databeskyttelse", Bruxelles, 16.4.2020 (C(2020) 2523 final).

litra e), være nødvendig for udførelsen af en opgave i samfundets interesse eller en opgave, som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt[12].

31 Retsgrundlaget eller den lovgivningsmæssige foranstaltning, der rent juridisk hjemler brugen af en kontaktopsporingsapplikation, bør dog omfatte garantier, der giver mening, herunder en henvisning til, at det er frivilligt, om man vil bruge applikationen. Der bør tillige klart angives formål og udtrykkelige begrænsninger med hensyn til den videre brug af personoplysninger, ligesom det tydeligt bør angives, hvem der er dataansvarlig(e). Desuden skal det oplyses, hvilke datakategorier der er tale om, samt hvilke enheder (og hvilke formål) personoplysningerne vil kunne blive videregivet til. Afhængigt af interferensniveauet bør der indlejres yderligere garantier under hensyntagen til behandlingens art, omfang og formål. Endelig anbefaler Databeskyttelsesrådet også, at der, så hurtigt som praktisk muligt, inkluderes kriterier for beslutningen om, hvornår applikationen skal afmonteres, og for, hvilken enhed der skal træffe og stå til ansvar for denne beslutning.

32 Er databehandlingen imidlertid baseret på et andet retsgrundlag, såsom samtykke (artikel 6, stk. 1, litra a)[13], vil den dataansvarlige skulle sikre, at de strenge krav til det pågældende retsgrundlag er opfyldt.

33 Anvendelsen af en applikation til bekæmpelse af covid-19-pandemien kan også føre til indsamling af helbredsoplysninger (f.eks. en smittet persons status). Behandling af sådanne oplysninger er tilladt, hvis den er nødvendig af hensyn til samfundsinteresser på folkesundhedsområdet, jf. betingelserne i databeskyttelsesforordningens artikel 9, stk. 2, litra i)[14], eller til sundhedsformål som beskrevet i databeskyttelsesforordningens artikel 9, stk. 2, litra h)[15]. Afhængigt af retsgrundlaget kan den også være baseret på udtrykkeligt samtykke (databeskyttelsesforordningens artikel 9, stk. 2, litra a)).

34 I overensstemmelse med det oprindelige formål er det i henhold databeskyttelsesforordningens artikel 9, stk. 2, litra j), desuden tilladt at behandle helbredsoplysninger, når det er nødvendigt til videnskabelige forskningsformål eller statistiske formål.

35 Den nuværende sundhedskrise bør ikke udnyttes som en mulighed for at indføre urimelige dataopbevaringsbemyndigelser. Der bør med lagringsbegrænsning tages hensyn til de reelle behov og den medicinske relevans (dette kan omfatte hensyntagen til epidemiologiske aspekter som inkubationstiden osv.), og personoplysninger bør kun opbevares, så længe covid-19-krisen står på. Derefter bør alle personoplysninger slettes eller anonymiseres som en generel regel.

36 Det er Databeskyttelsesrådets opfattelse, at sådanne applikationer ikke kan erstatte, men kun understøtte, manuel kontaktopsporing, som udføres af kvalificeret personale i den offentlige sundhedssektor, som kan vurdere, om det er sandsynligt, at tætte kontakter vil resultere i overførsel af virus eller ej (f.eks. når de interagerer med personer, der af beskyttet af passende udstyr — butiksassistenter osv. — eller ikke er beskyttet af sådant udstyr). Databeskyttelsesrådet understreger, at de procedurer og processer, herunder de relevante algoritmer, der anvendes af kontaktopsporingsapplikationerne, bør være under nøje tilsyn af kvalificeret personale, så omfanget af falsk positive og falsk negative resultater begrænses. Især bør opgaven med at yde rådgivning om de næste skridt ikke udelukkende være baseret på automatisk behandling.

37 For at sikre fairness og ansvarlighed i forbindelse med algoritmer, samt at de mere overordnet overholder lovgivningen, bør de være kontrollerbare og underlagt uafhængige eksperters

---

[12] Jf. betragtning 41.

[13] Dataansvarlige (især offentlige myndigheder) skal være særligt opmærksomme på, at samtykke ikke bør betragtes som givet frit, hvis individet ikke reelt har mulighed for at nægte at give sit samtykke eller at trække det tilbage, uden at det er til skade for den pågældende.

[14] Behandlingen skal være baseret på EU-ret eller medlemsstaters nationale ret, som indeholder passende og specifikke foranstaltninger, der garanterer den registreredes rettigheder og frihedsrettigheder, navnlig mht. tavshedspligt.

[15] Jf. databeskyttelsesforordningens artikel 9, stk. 2, litra h).

regelmæssige revision. Applikationens kildekode bør gøres offentligt tilgængelig med henblik på en så omfattende kontrol som muligt.

38 Der vil altid i et vist omfang forekomme falsk positive resultater. Da det er sandsynligt, at identifikation af en smitterisiko vil have stor indvirkning på et individ, f.eks. ved at den pågældende holder sig isoleret, indtil han eller hun er testet negativ, er det nødvendigt at kunne korrigere data og/eller efterfølgende analyseresultater. Dette bør naturligvis kun gælde for scenarier og implementeringer, hvor data behandles og/eller lagres på en måde, hvor sådanne korrektioner er teknisk mulige, og hvor det er sandsynligt, at de ovenfor nævnte skadelige virkninger vil indtræffe.

39 Endelig mener Databeskyttelsesrådet, at der bør gennemføres en konsekvensanalyse vedrørende databeskyttelse, før et sådant værktøj tages i brug, da det vurderes at være sandsynligt, at behandlingen vil indebære en høj risiko (helbredsoplysninger, forventet indførelse i stor skala, systematisk overvågning, brug af ny teknologisk løsning)[16]. Databeskyttelsesrådet anbefaler på det kraftigste, at konsekvensanalyser vedrørende databeskyttelse offentliggøres.

3.2 Anbefalinger og funktionelle krav

40 I henhold til princippet om dataminimering bør — blandt andre foranstaltninger til databeskyttelse gennem design og gennem standardindstillinger[17] — de data, der behandles, reduceres til et absolut minimum. Applikationen bør ikke indsamle ikke-relaterede eller ikke-nødvendige oplysninger, f.eks. om civilstand, kommunikationsidentifikatorer, udstyrsmappeemner, meddelelser, opkaldslogger, lokaliseringsdata, udstyrsidentifikatorer osv.

41 Data, der udsendes via applikationer, må kun indeholde visse unikke og pseudonymiserede identifikatorer, der er genereret af og specifikke for den pågældende applikation. Disse identifikatorer skal fornyes regelmæssigt og med en hyppighed, der er i overensstemmelse med målsætningen om at inddæmme virussets spredning og tilstrækkelig til at begrænse risikoen for identificering og fysisk sporing af individer.

42 Implementering af løsninger til kontaktopsporing kan ske i overensstemmelse med enten en central eller en decentral tilgang[18]. Begge tilgange bør anses for at være brugbare, forudsat at der er truffet passende sikkerhedsforanstaltninger, idet der er både fordele og ulemper ved dem begge. Derfor bør begge disse begreber altid overvejes grundigt i den konceptuelle fase af udviklingen af en applikation, med en nøje afvejning af de to tilganges respektive virkninger for databeskyttelsen/privatlivets fred og mulige konsekvenser for individers rettigheder.

43 Servere i kontaktopsporingssystemet må kun indsamle kontakthistorik eller pseudonymiserede identifikatorer for en bruger, der er diagnosticeret som smittet på grundlag af en korrekt vurdering foretaget af sundhedsmyndighederne, og som resultat af en frivillig handling fra brugerens side. Alternativt må der på serveren kun føres en liste over pseudonymiserede identifikatorer for smittede brugere eller deres kontakthistorik, så længe det er nødvendigt for at underrette potentielt smittede brugere om deres eksponering, og uden at det forsøges at identificere potentielt smittede brugere.

44 Indførelsen af en global kontaktopsporingsmetode, som omfatter både applikationer og manuel sporing, vil i nogle tilfælde kunne nødvendiggøre behandling af yderligere oplysninger. I forbindelse hermed bør de pågældende yderligere oplysninger forblive på brugerterminalen

---

[16] Jf. Artikel 29-gruppens retningslinjer (vedtaget af Databeskyttelsesrådet) for konsekvensanalyser vedrørende databeskyttelse og bestemmelse af, om behandlingen "sandsynligvis vil indebære en høj risiko" i henhold til forordning (EU) 2016/679.

[17] Jf. Databeskyttelsesrådets retningslinjer 4/2019 vedrørende databeskyttelse i henhold til artikel 25 gennem design og gennem standardindstillinger

[18] Den decentrale løsning er generelt mest i overensstemmelse med minimeringsprincippet.

og kun behandles, hvis det er absolut påkrævet, og med brugerens forudgående og specifikke samtykke.

45 Der skal implementeres avancerede kryptografiske teknikker med henblik på at sikre de data, der lagres på/i servere og applikationer, udvekslinger mellem applikationer og fjernserveren. Der skal også udføres gensidig godkendelse mellem applikation og server.

46 Indberetning i applikationen af brugere som smittet med SARS-CoV-2 skal være betinget af behørig godkendelse, f.eks. ved anvendelse af en engangskode, der knytter sig til et smittet individs pseudonymiserede identitet og er kædet til en teststation eller en sundhedsprofessionel. Hvis bekræftelse ikke kan opnås på sikker vis, bør der ikke foretages nogen databehandling, der forudsætter gyldig brugerstatus.

47 Den dataansvarlige skal, i samarbejde med de offentlige myndigheder, klart og udtrykkeligt oplyse om linket til at downloade den officielle nationale kontaktopsporingsapplikation for at mindske risikoen for, at individer anvender en tredjeparts app.

4 KONKLUSION

48 Verden står over for en alvorlig folkesundhedskrise, som nødvendiggør en robust indsats, der vil få konsekvenser også efter denne nødsituation. Automatiseret databehandling og digitale teknologier kan være nøgleelementer i kampen mod covid-19. Vi må imidlertid være på vagt over for "bordet fanger". Det er vores ansvar at sikre, at alle foranstaltninger, der træffes under disse usædvanlige omstændigheder, er nødvendige og tidsbegrænsede og begrænses til et nødvendigt minimum, og at de regelmæssigt gøres til genstand for en reel revurdering samt videnskabelig evaluering.

49 Databeskyttelsesrådet understreger, at vi ikke bør skulle vælge mellem en effektiv indsats over for den nuværende krise og beskyttelse af vores grundlæggende rettigheder: Vi kan opnå begge dele, og databeskyttelsesprincipper kan desuden spille en meget vigtig rolle i kampen mod virusset. Den europæiske databeskyttelseslovgivning tillader ansvarlig brug af personoplysninger til sundhedsforvaltningsformål og sikrer samtidig, at individuelle rettigheder og frihedsfriheder ikke undermineres i processen.

På vegne af Det Europæiske Databeskyttelsesråd

(Andrea Jelinek)

Formand

BILAG — KONTAKTOPSPORINGSAPPLIKATIONER ANALYSEVEJLEDNING

0. Ansvarsfraskrivelse

Nedenstående retningslinjer er hverken normative eller udtømmende, og de er udelukkende ment som en generel vejledning til dem, der udvikler og implementerer kontaktopsporingsapplikationer. Andre løsninger end dem, der beskrives her, vil kunne anvendes og være lovlige, så længe de er i overensstemmelse med den relevante lovramme (dvs. databeskyttelsesforordningen og direktivet).

Det skal også bemærkes, at denne vejledning er af generel karakter. De anbefalinger og forpligtelser, der er omhandlet i dette dokument, skal derfor ikke betragtes som udtømmende. Enhver vurdering vil skulle foretages fra sag til sag, og nogle applikationer vil kunne nødvendiggøre yderligere foranstaltninger, som ikke er omfattet af denne vejledning.

1. Sammenfatning

I mange medlemsstater overvejer interessenter at bruge *kontaktopsporingsapplikationer* til at hjælpe borgerne med at finde ud af, om de har været i kontakt med en person, der er smittet med SARS-CoV-2.

Det er endnu ikke fastlagt, under hvilke betingelser sådanne applikationer ville bidrage effektivt til håndteringen af pandemien. Og det er nødvendigt, at disse betingelser fastlægges inden en eventuel implementering af en sådan app. Det er imidlertid relevant at udstikke retningslinjer, der giver udviklingsteams i tidligere led relevante oplysninger, som gør det muligt at garantere beskyttelsen af personoplysninger allerede i den tidlige udviklingsfase.

Det skal bemærkes, at denne vejledning er af generel karakter. De anbefalinger og forpligtelser, der er omhandlet i dette dokument, skal derfor ikke betragtes som udtømmende. Enhver vurdering vil skulle foretages fra sag til sag, og nogle applikationer vil kunne nødvendiggøre yderligere foranstaltninger, som ikke er omfattet af denne vejledning. Denne vejledning er udelukkende ment som en generel vejledning til dem, der udvikler og implementerer kontaktopsporingsapplikationer.

Visse kriterier går muligvis videre end de strenge krav, der følger af databeskyttelseslovgivningen. De har til formål at sikre størst mulig gennemsigtighed for at øge sandsynligheden for, at befolkningen tager sådanne kontaktopsporingsapplikationer til sig.

I dette øjemed bør udgivere af kontaktopsporingsapplikationer tage hensyn til følgende kriterier:

- Brug af en sådan applikation skal være helt frivillig. Den må ikke på nogen måde være begrænsende for adgangen til lovsikrede rettigheder. Individer skal til enhver tid have fuld kontrol over deres data, og de bør frit kunne vælge, om de vil bruge applikationen.
- Det er sandsynligt, at kontaktopsporingsapplikationer vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder og gøre det nødvendigt at foretage en konsekvensanalyse vedrørende databeskyttelse forud for udrulningen af dem.
- Oplysninger om kort afstand mellem brugere af applikationen kan tilvejebringes, uden at brugerne lokaliseres. Denne type applikation kræver ikke — og bør derfor heller ikke omfatte — anvendelse af lokaliseringsdata.

- Når en bruger er diagnosticeret som smittet med SARS-CoV-2, er det kun de personer, som brugeren har været i tæt kontakt med i den epidemiologisk relevante periode, for hvilken kontaktopsporingsoplysningerne gemmes, der bør underrettes.
- Anvendelse af denne type applikation kan, afhængigt af den valgte arkitektur, nødvendiggøre brug af en central server. I sådanne tilfælde og i overensstemmelse med principperne om dataminimering og databeskyttelse gennem design bør de data, der behandles af den centrale server, begrænses til et absolut minimum:
    - Når en bruger diagnosticeres som smittet, må oplysninger om brugerens tidligere tætte kontakter eller de identifikatorer, der udsendes af brugerens applikation, kun indsamles efter samtykke fra brugeren. Der må fastlægges en kontrolmetode, som gør det muligt at fastslå, at en person rent faktisk er smittet, uden at brugeren identificeres. Teknisk set vil dette kunne sikres, ved at kontakter kun advares, når en sundhedsprofessionel har været involveret, f.eks. ved anvendelse af en særlig engangskode.
    - De oplysninger, der lagres på den centrale server, bør hverken gøre det muligt for den dataansvarlige at identificere brugere, der er diagnosticeret som smittet eller har været i kontakt med sådanne brugere, eller at udlede kontaktmønstre, der ikke er nødvendige for at kunne identificere de relevante kontakter.
- Anvendelse af denne type applikation kræver, at der udsendes data, som læses af andre brugeres enheder, og at de udsendte data registreres:
    - Det er tilstrækkeligt at udveksle pseudonymiserede identifikatorer mellem brugernes mobile udstyr (computere, tablets, smarture osv.), f.eks. ved at udsende dem (f.eks. vha. Bluetooth Low Energy-teknologi).
    - Identifikatorer skal genereres ved brug af avancerede kryptografiske processer.
    - Identifikatorer skal fornyes regelmæssigt for at mindske risikoen for fysisk sporing og sammenkædningsangreb ("linkage").
- Denne type applikation skal sikres for at garantere en sikker teknisk proces. Især følgende er vigtigt:
    - Applikationen bør ikke give brugerne oplysninger, der gør det muligt for dem at udlede andres identitet eller diagnose. Den centrale server må hverken identificere brugerne eller udlede oplysninger om dem.

Ansvarsfraskrivelse: Ovenstående principper vedrører det erklærede formål med *kontaktopsporingsapplikationer*, og udelukkende dette formål, idet det eneste sigte med disse applikationer er automatisk at underrette personer, der potentielt kan være blevet eksponeret for virusset (uden at det er nødvendigt at identificere dem). Operatørerne af applikationen og dennes infrastruktur kan kontrolleres af den kompetente tilsynsmyndighed. At følge alle eller dele af disse retningslinjer er ikke nødvendigvis tilstrækkeligt til at sikre, at databeskyttelseslovgivningen overholdes til punkt og prikke.

2. Definitioner

Kontakt	For en kontaktopsporingsapplikation er en kontakt en bruger, der har været en del af interaktion med en bruger, om hvem det er blevet bekræftet, at vedkommende er bærer af virusset, og hvor varigheden og afstanden ved kontakten har været sådan, at der er risiko for betydelig eksponering for virusinfektionen. Parametrene for eksponeringsvarighed og afstand mellem mennesker skal vurderes af sundhedsmyndighederne og kan fastsættes i applikationen.
Lokaliseringsdata	Hermed forstås alle data, der behandles i et elektronisk kommunikationsnet eller af en elektronisk kommunikationstjeneste og angiver den geografiske placering af det terminaludstyr, som anvendes af brugeren af en offentligt tilgængelig elektronisk kommunikationstjeneste (som defineret i direktivet), samt data fra andre potentielle kilder vedrørende: - bredde, længde og højde for terminaludstyret - retningen, brugerne bevæger sig i, eller - tidspunktet for registrering af lokaliseringsoplysningerne.
Interaktion	I relation til kontaktopsporingsapplikationen forstås ved interaktion udveksling af oplysninger mellem to enheder, der befinder sig tæt på hinanden (i tid og rum), inden for spektret af den kommunikationsteknologi, der anvendes (f.eks. Bluetooth). Denne definition udelukker lokalisering af de to brugere af interaktionen.
Virusbærer	I dette dokument forstås ved virusbærere brugere, der er testet positive for virusset, og som har fået en officiel diagnose af læger eller sundhedscentre.
Kontaktopsporing	Personer, der har været i tæt kontakt (ifølge kriterier, der skal fastlægges af epidemiologer) med et individ, der er smittet med virusset, har en betydelig risiko for også at blive smittet og for at smitte andre. Kontaktopsporing er en sygdomsbekæmpelsesmetode, hvor alle personer, der har været tæt på en bærer af virusset, registreres på en liste med henblik på at kontrollere, om de er i fare for at være blevet smittet, og træffe passende sundhedsforanstaltninger for dem.

3. Generelt

GEN-1	Applikationen skal være et redskab, der supplerer traditionelle kontaktopsporingsteknikker (navnlig samtaler med smittede personer), dvs. indgå som en del af et bredere folkesundhedsprogram. Den må kun anvendes, indtil det bliver muligt at håndtere mængden af nye smittetilfælde alene ved hjælp af manuelle kontaktopsporingsteknikker.

GEN-2	Senest når de kompetente offentlige myndigheder træffer beslutning om "tilbagevenden til normale tilstande", skal der indføres en procedure for at standse indsamlingen af identifikatorer (global deaktivering af applikationen, instrukser vedrørende afinstallation af applikationen, automatisk afinstallation osv.) og for at aktivere sletning af alle indsamlede data fra alle databaser (mobile applikationer og servere).
GEN-3	Kildekoden til applikationen og til dens backend skal være åben, og de tekniske specifikationer offentliggøres, så enhver berørt part kan kontrollere koden og — hvis det er relevant — bidrage til at forbedre koden, rette eventuelle fejl og sikre gennemsigtighed i behandlingen af personoplysninger.
GEN-4	Applikationens udrulningsfaser skal gøre det muligt gradvist at validere applikationens effektivitet ud fra et folkesundhedsmæssigt synspunkt. En evalueringsprotokol med angivelse af indikatorer, der gør det muligt at måle applikationens effektivitet, skal defineres i tidligere led med dette formål.

4. Formål

PUR-1	Applikationen skal udelukkende have til formål at spore kontakter, således at personer, der potentielt kan være blevet eksponeret for SARS-CoV-2, kan advares og blive taget hånd om. Den må ikke bruges til andre formål.
PUR-2	Applikationens primære anvendelsesformål må ikke "fordrejes", så den i stedet anvendes til overvågning af, at regler vedrørende karantæne eller indeslutning og/eller holden afstand overholdes.
PUR-3	Applikationen må ikke bruges til at drage konklusioner om, hvor brugerne befinder sig, på grundlag af deres interaktion og/eller andre metoder.

5. Funktionelle hensyn

FUNC-1	Applikationen skal indeholde en funktionalitet, der gør det muligt for brugerne at blive underrettet om, at de potentielt kan være blevet eksponeret for virusset, idet disse oplysninger baseres på nærhed til en smittet bruger inden for et vindue på X dage før den positive screeningtest (X-værdien fastsættes af sundhedsmyndighederne).
FUNC-2	Applikationen bør give anbefalinger til brugere, der er identificeret som potentielt værende blevet eksponeret for virusset. Den bør videreformidle instrukser vedrørende de foranstaltninger, de bør træffe, og bør give brugeren mulighed for at anmode om rådgivning. I sådanne tilfælde vil menneskelig indgriben være obligatorisk.
FUNC-3	Den algoritme, der måler smitterisikoen under hensyntagen til afstands- og tidsfaktorer og dermed afgør, hvornår en kontakt skal registreres på

	kontaktopsporingslisten, skal kunne justeres på sikker vis i overensstemmelse med den nyeste viden om virussets spredning.
FUNC-4	**Brugere skal underrettes, hvis de er blevet eksponeret for virusset**, eller skal regelmæssigt have oplysninger om, hvorvidt de er blevet eksponeret for virusset inden for dettes inkubationstid.
FUNC-5	Applikationen bør være interoperabel med andre applikationer udviklet i medlemsstater, således at brugere, der rejser mellem forskellige medlemsstater, kan underrettes på effektiv vis.

6. Data

DATA-1	Applikationen skal kunne udsende og modtage data via nærhedskommunikationsteknologier såsom Bluetooth Low Energy, således at kontaktopsporing er mulig.
DATA-2	Disse udsendte data skal indeholde kryptografisk stærke pseudo-vilkårlige identifikatorer, der er genereret af og specifikke for den pågældende applikation.
DATA-3	Risikoen for kollision mellem pseudo-vilkårlige identifikatorer bør være tilstrækkeligt lav.
DATA-4	Pseudo-vilkårlige identifikatorer skal fornyes regelmæssigt og med en hyppighed, der er tilstrækkelig til at begrænse risikoen for genidentificering, fysisk sporing eller sammenkædning ("linkage") af individer foretaget af andre, herunder operatører af centrale servere, andre brugere af applikationen eller ondsindede tredjeparter. Disse identifikatorer skal genereres af brugerens applikation, eventuelt baseret på en basisfil leveret af den centrale server.
DATA-5	I henhold til princippet om dataminimering må applikationen ikke indsamle andre data end dem, der er absolut påkrævede med henblik på kontaktopsporing.
DATA-6	Applikationen må ikke indsamle lokaliseringsdata med henblik på kontaktopsporing. Lokaliseringsdata må kun behandles med det formål at gøre det muligt for applikationen at interagere med lignende applikationer i andre lande, og de må ikke være mere præcise, end hvad der er absolut påkrævet med dette ene formål for øje.
DATA-7	Applikationen bør ikke indsamle helbredsoplysninger ud over dem, der er absolut påkrævede for anvendelsen af appen, undtagen på frivillig basis og udelukkende med det formål at bidrage til beslutningstagningen i forbindelse med underretning af brugeren.
DATA-8	Brugerne skal informeres om, nøjagtigt hvilke personoplysninger der vil blive indsamlet. Disse oplysninger bør kun indsamles efter tilladelse fra brugeren.

7. Tekniske egenskaber

TECH-1	Applikationen bør anvende tilgængelige teknologier såsom nærhedskommunikationsteknologi (f.eks. Bluetooth Low Energy) til at opdage brugere i nærheden af den enhed, applikationen kører på.
TECH-2	Applikationen bør opbevare brugerens kontakthistorik i udstyret i en på forhånd fastsat begrænset periode.
TECH-3	Nogle af applikationens funktioner vil kunne implementeres via en central server.
TECH-4	Applikationen skal være baseret på en arkitektur, der i videst mulig udstrækning gør brug af brugernes enheder.
TECH-5	På initiativ fra brugere, der er indberettet som værende smittet med virusset, og efter at deres status er blevet bekræftet af en behørigt certificeret sundhedsprofessionel, bør brugernes kontakthistorik eller deres egne identifikatorer overføres til den centrale server.

8. Sikkerhed

SEC-1	Der skal være en mekanisme, der kontrollerer statussen for brugere, der indberettes som SARS-CoV-2-positive i applikationen, f.eks. ved tildeling af en engangskode, der knytter sig til en teststation eller en sundhedsprofessionel. Hvis bekræftelsen ikke kan ske på sikker vis, må oplysningerne ikke behandles.
SEC-2	De data, der sendes til den centrale server, skal overføres via en sikker kanal. Brug af beskedtjenester, der leveres af OS-platformsleverandører, bør overvejes nøje og bør ikke føre til videregivelse af oplysninger til tredjeparter.
SEC-3	Anmodninger må ikke være sårbare over for manipulation fra ondsindede brugere.
SEC-4	Der skal anvendes avancerede kryptografiske teknikker for at garantere sikker udveksling mellem applikation og server samt mellem applikationerne indbyrdes og som en generel regel med henblik på at beskytte de oplysninger, der lagres i applikationerne og på serveren. Anvendelige teknikker er f.eks.: symmetrisk og asymmetrisk kryptering, hash-funktioner, Private Membership Test, Private Set Intersection, Bloom-filtre, Private Information Retrieval, homomorf kryptering osv.
SEC-5	Der må ikke bibeholdes nettilslutningsidentifikatorer (f.eks. IP-adresser) på den centrale server for nogen bruger, heller ikke brugere, der har fået stillet en positiv diagnose, og som har overført deres kontakthistorik eller deres egne identifikatorer.
SEC-6	For at undgå identitetstyveri eller oprettelse af falske brugere skal serveren godkende applikationen.
SEC-7	Applikationen skal godkende den centrale server.
SEC-8	Serverfunktionerne bør beskyttes mod replayangreb.

SEC-9	De oplysninger, der overføres af den centrale server, skal underskrives til bekræftelse af deres oprindelse og integritet.
SEC-10	Kun autoriserede personer skal have adgang til data, der er lagret på den centrale server og ikke er offentligt tilgængelige.
SEC-11	Enhedens rettighedsforvalter på operativsystemniveau skal kun anmode om de rettigheder, der er nødvendige for at tilgå og anvende kommunikationsmodulerne, i det omfang det er nødvendigt, at lagre dataene i terminalen og at udveksle oplysninger med den centrale server.

9. Beskyttelse af personoplysninger og privatlivets fred for fysiske personer

Påmindelse: Følgende retningslinjer vedrører en applikation, hvis eneste formål er kontaktopsporing.

PRIV-1	Ved udveksling af data skal brugernes privatliv respekteres (først og fremmest skal princippet om dataminimering overholdes).
PRIV-2	Applikationen må ikke gøre det muligt direkte at identificere brugere, når de anvender applikationen.
PRIV-3	Applikationen må ikke gøre det muligt at spore brugernes færden.
PRIV-4	Brug af applikationen bør ikke gøre det muligt for brugerne at finde ud af noget om andre brugere (især ikke, om de er virusbærere eller ej).
PRIV-5	Tilliden til den centrale server skal begrænses. Forvaltningen af den centrale server skal varetages i overensstemmelse med klart definerede forvaltningsregler og omfatte alle nødvendige foranstaltninger til at garantere dens sikkerhed. Den centrale server bør være placeret et sted, hvor det er muligt for den kompetente tilsynsmyndigheds at føre effektivt tilsyn.
PRIV-6	Der skal gennemføres en konsekvensanalyse vedrørende databeskyttelse, og analysen bør offentliggøres.
PRIV-7	Applikationen bør kun give brugeren viden om, hvorvidt han eller hun er blevet eksponeret for virusset, og — så vidt muligt uden at afsløre noget om andre brugere — hvor mange gange og på hvilke datoer han eller hun er blevet eksponeret.
PRIV-8	De oplysninger, applikationen giver, må ikke gøre det muligt for brugerne at identificere brugere, der er bærere af virusset, eller deres færden.
PRIV-9	De oplysninger, applikationen giver, må ikke gøre det muligt for sundhedsmyndighederne at identificere potentielt eksponerede brugere uden disses samtykke.
PRIV-10	Anmodninger fra applikationen til den centrale server må ikke afsløre noget om virusbæreren.
PRIV-11	Anmodninger fra applikationen til den centrale server må ikke indebære videregivelse af unødvendige oplysninger om brugeren, undtagen — eventuelt og kun hvis det er nødvendigt — til brug for brugerens pseudonymiserede identifikatorer og kontaktliste.
PRIV-12	Sammenkædningsangreb ("linkage") må ikke være mulige.
PRIV-13	Brugere skal kunne udøve deres rettigheder via applikationen.
PRIV-14	Sletning af applikationen skal resultere i, at alle lokalt indsamlede data slettes.
PRIV-15	Applikationen bør kun indsamle data, der er overført af instanser af applikationen eller af interoperable tilsvarende applikationer. Der må ikke indsamles data om andre applikationer og/eller andre enheder til nærhedskommunikation.
PRIV-16	For at undgå genidentificering foretaget af den centrale server bør der etableres proxyservere. Formålet med sådanne, *ikke-ondsindede servere* er at blande identifikatorerne for flere forskellige brugere (både virusbæreres identifikatorer

	og identifikatorer sendt af anmodere), før de deles med den centrale server, så det undgås, at den centrale server kender brugernes identifikatorer (såsom IP-adresser).
PRIV-17	Applikation og server skal udvikles og konfigureres omhyggeligt med henblik på at undgå indsamling af unødvendige data (f.eks. bør serverlogfilerne ikke indeholde identifikatorer) og for at undgå anvendelse af tredjeparts-SDK'er, der indsamler data til andre formål.

Med de fleste af de kontaktopsporingsapplikationer, der drøftes i øjeblikket, følges grundlæggende en af to tilgange, når en bruger erklæres for smittet: De kan enten sende nærkontakthistorikken, som de har tilvejebragt ved scanning, til en server, eller de kan sende listen over deres egne identifikatorer, som blev udsendt. Nedenstående principper er inddelt efter disse to tilgange. Det, at det er disse tilgange, der drøftes her, er ikke ensbetydende med, at andre tilgange ikke er mulige eller endda kan være at foretrække, f.eks. tilgange, der indebærer anvendelse af en eller anden form for E2E-kryptering eller andre teknologier til sikkerhedsforøgelse eller beskyttelse af privatlivets fred.

9.1. Principper, der kun gælder, når applikationen sender en kontaktliste til serveren:

CON-1	Den centrale server skal indsamle kontakthistorikken for brugere, der er indberettet som værende SARS-CoV-2-positive, som resultat af en frivillig handling fra brugernes side.
CON-2	Der må ikke på/via den centrale server bevares eller rundsendes en liste over pseudonymiserede identifikatorer for de brugere, der er bærere af virusset.
CON-3	Kontakthistorik, der lagres på den centrale server, skal slettes, så snart brugerne er blevet underrettet om, at de har været i nærheden af en person, der har fået stillet en positiv diagnose.
CON-4	Medmindre brugeren, der er blevet registreret som positiv, deler sin kontakthistorik med den centrale server, eller medmindre brugeren anmoder serveren om at finde ud af, hvilken eksponering for virusset han eller hun kan være blevet udsat for, må ingen data forlade brugerens udstyr.
CON-5	Alle identifikatorer, der indgår i den lokale historik, skal slettes X dage efter indsamlingen af dem (X-værdien fastsættes af sundhedsmyndighederne).
CON-6	Kontakthistorikker, der indsendes af forskellige brugere, bør ikke behandles yderligere, f.eks. ved krydskorrelation med henblik på opstilling af globale nærhedskort.
CON-7	Data i serverlogfiler skal begrænses til et minimum og skal overholde databeskyttelseskravene.

9.2. Principper, der kun gælder, når applikationen sender en liste over sine egne identifikatorer til en server:

ID-1	Den centrale server skal indsamle identifikatorerne, der udsendes af applikationen, for brugere, der er indberettet som værende SARS-CoV-2-positive, som resultat af en frivillig handling fra brugernes side.
ID-2	Kontakthistorikken for brugere, der er bærere af virusset, må ikke bevares på eller rundsendes via den centrale server.
ID-3	Identifikatorer, der lagres på den centrale server, skal slettes, så snart de er blevet distribueret til de øvrige applikationer.
ID-4	Medmindre brugeren, der er blevet registreret som positiv, deler sin kontakthistorik med den centrale server, eller medmindre brugeren anmoder serveren om at finde ud af, hvilken eksponering for virusset han eller hun kan være blevet udsat for, må ingen data forlade brugerens udstyr.
ID-5	Data i serverlogfiler skal begrænses til et minimum og skal overholde databeskyttelseskravene.