II

(Ikke-lovgivningsmæssige retsakter)

AFGØRELSER

KOMMISSIONENS GENNEMFØRELSESAFGØRELSE (EU) 2020/1023

af 15. juli 2020

om ændring af gennemførelsesafgørelse (EU) 2019/1765 for så vidt angår grænseoverskridende udveksling af data mellem nationale kontaktopsporings- og advarselsmobilapplikationer som led i bekæmpelsen af covid-19-pandemien

(EØS-relevant tekst)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets direktiv 2011/24/EU af 9. marts 2011 om patientrettigheder i forbindelse med grænseoverskridende sundhedsydelser ([1]), særlig artikel 14, stk. 3, og

ud fra følgende betragtninger:

(1) Ved artikel 14 i direktiv 2011/24/EU fik Unionen til opgave at støtte og lette samarbejdet og udvekslingen af oplysninger mellem medlemsstater, der arbejder inden for et frivilligt netværk mellem de nationale myndigheder, der er ansvarlige for e-sundhed (i det følgende benævnt »e-sundhedsnetværket«), og som er udpeget af medlemsstaterne.

(2) Kommissionens gennemførelsesafgørelse (EU) 2019/1765 ([2]) indeholder regler om etablering, forvaltning og drift af netværket af nationale myndigheder, der er ansvarlige for e-sundhed. Ved samme afgørelses artikel 4 får e-sundhedsnetværket til opgave at lette større interoperabilitet mellem de nationale informations- og kommunikationsteknologisystemer og grænseoverskridende overførsel af elektroniske sundhedsdata i grænseoverskridende sundhedsydelser.

(3) På baggrund af den folkesundhedskrise, covid-19-pandemien har forårsaget, har flere medlemsstater udviklet mobilapplikationer, der understøtter kontaktopsporing og gør det muligt at advare brugerne af applikationerne om behovet for at træffe passende foranstaltninger, såsom testning eller selvisolation, hvis de potentielt er blevet eksponeret for virusset, fordi de har været tæt på en anden bruger af den pågældende applikation, som har givet notifikation om en positiv diagnose. Disse applikationer er baseret på Bluetooth-teknologi til konstatering af nærhed mellem enheder. Med ophævelsen af restriktionerne for rejser mellem medlemsstaterne siden juni 2020 bør der sikres større interoperabilitet mellem de nationale informations- og kommunikationsteknologisystemer i medlemsstaterne i e-sundhedsnetværket gennem implementering af en digital infrastruktur, der muliggør interoperabilitet mellem nationale mobilapplikationer, der understøtter kontaktopsporing og advarsel.

([1]) EUT L 88 af 4.4.2011, s. 45.

([2]) Kommissionens gennemførelsesafgørelse (EU) 2019/1765 af 22. oktober 2019 om foranstaltninger til etablering, forvaltning og drift af netværket af nationale myndigheder, der er ansvarlige for e-sundhed, og om ophævelse af gennemførelsesafgørelse 2011/890/EU (EUT L 270 af 24.10.2019, s. 83).

(4) Kommissionen har støttet medlemsstaterne med hensyn til ovennævnte mobilapplikationer. Den 8. april 2020 vedtog Kommissionen en henstilling om en fælles EU-værktøjskasse med henblik på at udnytte teknik og data til at bekæmpe og overvinde covid-19-krisen, navnlig hvad angår mobilapplikationer og anvendelse af anonymiserede mobilitetsdata (»Kommissionens henstilling«) ([3]). Medlemsstaterne i e-sundhedsnetværket vedtog, med støtte fra Kommissionen, en fælles EU-værktøjskasse for medlemsstaterne vedrørende mobilapplikationer til støtte for kontaktopsporing ([4]) samt interoperabilitetsretningslinjer for godkendte kontaktopsporingsmobilapplikationer i EU ([5]). Værktøjskassen forklarer de nationale krav til nationale kontaktopsporings- og advarselsmobilapplikationer, og først og fremmest, at de skal være frivillige, godkendes af den nationale sundhedsmyndighed, sikre beskyttelse af privatlivets fred og afmonteres, så snart der ikke længere er behov for dem. Efter den seneste udvikling i covid-19-krisen har Kommissionen ([6]) og Det Europæiske Databeskyttelsesråd ([7]) hver især udstedt retningslinjer for mobilapplikationer og kontaktopsporingsredskaber i relation til databeskyttelse. Udformningen af medlemsstaternes mobilapplikationer og af den digitale infrastruktur, der muliggør deres interoperabilitet, bygger på den fælles EU-værktøjskasse, ovennævnte retningslinjer og de tekniske specifikationer, der er aftalt i e-sundhedsnetværket.

(5) For at fremme interoperabiliteten mellem nationale kontaktopsporings- og advarselsmobilapplikationer udviklede medlemsstaterne i e-sundhedsnetværket, som valgte at gå et skridt videre i deres samarbejde på dette område på frivillig basis, med støtte fra Kommissionen en digital infrastruktur som et IT-redskab til udveksling af data. Denne digitale infrastruktur kaldes »den fælles gateway-facilitet«.

(6) Ved denne afgørelse fastsættes der bestemmelser om de deltagende medlemsstaters og Kommissionens roller i driften af den fælles gateway-facilitet for grænseoverskridende interoperabilitet mellem nationale kontaktopsporings- og advarselsmobilapplikationer.

(7) Behandling af personoplysninger for brugere af kontaktopsporings- og advarselsmobilapplikationer, som foretages under ansvar af medlemsstaterne eller andre offentlige organisationer eller officielle organer i medlemsstaterne, bør ske i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2016/679 ([8]) (»den generelle forordning om databeskyttelse«) og Europa-Parlamentets og Rådets direktiv 2002/58/EF ([9]). Behandling af personoplysninger under Kommissionens ansvar med henblik på forvaltning og sikring af sikkerheden i den fælles gateway-facilitet bør ske i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([10]).

(8) Den fælles gateway-facilitet bør bestå af en sikker IT-infrastruktur, der udgør en fælles grænseflade, hvor udpegede nationale myndigheder eller officielle organer kan udveksle et minimumssæt af data vedrørende kontakter med personer, der er smittet med SARS-CoV-2, med det formål at informere andre om deres potentielle eksponering for denne smitte og fremme et effektivt samarbejde om sundhedsydelser medlemsstaterne imellem ved at lette udvekslingen af relevante oplysninger.

(9) Der bør derfor ved denne afgørelse fastlægges nærmere vilkår for grænseoverskridende udveksling af data mellem udpegede nationale myndigheder eller officielle organer via den fælles gateway-facilitet inden for EU.

([3]) Kommissionens henstilling (EU) 2020/518 af 8. april 2020 om en fælles EU-værktøjskasse med henblik på at udnytte teknik og data til at bekæmpe og overvinde covid-19-krisen, navnlig hvad angår mobilapplikationer og anvendelse af anonymiserede mobilitetsdata (EUT L 114 af 14.4.2020, s. 7).

([4]) https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

([5]) https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf.

([6]) Meddelelse fra Kommissionen — Vejledning om apps til støtte for bekæmpelse af covid-19-pandemien i forbindelse med databeskyttelse (EUT C 124I af 17.4.2020, s. 1).

([7]) Retningslinjer 04/2020 om brug af lokaliseringsdata og kontaktopsporingsredskaber i forbindelse med covid-19-udbruddet og udtalelse fra Det Europæiske Databeskyttelsesråd af 16. juni 2020 om virkningerne i databeskyttelseshenseende af interoperabilitet mellem kontaktopsporingsapps, som begge findes på: https://edpb.europa.eu

([8]) 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 (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

([9]) Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation) (EFT L 201 af 31.7.2002, s. 37).

([10]) Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39).

(10) De deltagende medlemsstater, repræsenteret ved de udpegede nationale myndigheder eller officielle organer, fastlægger i fællesskab formålet med og midlerne til behandling af personoplysninger via den fælles gateway-facilitet og er derfor fælles dataansvarlige. Artikel 26 i den generelle forordning om databeskyttelse forpligter fælles dataansvarlige for behandling af personoplysninger til på en gennemsigtig måde at fastlægge deres respektive ansvar for overholdelse af forpligtelserne i henhold til samme forordning. Ved nævnte artikel fastsættes også muligheden for, at disse ansvar kan fastlægges i EU-retten eller medlemsstaternes nationale ret, som de dataansvarlige er underlagt. De enkelte dataansvarlige bør sikre, at de har et retsgrundlag på nationalt plan for behandling af data i den fælles gateway-facilitet.

(11) Kommissionen behandler, som leverandør af tekniske og organisatoriske løsninger til den fælles gateway-facilitet, pseudonymiserede personoplysninger på vegne af de deltagende medlemsstater i den fælles gateway-facilitet som fælles dataansvarlige og er således databehandler. I henhold til artikel 28 i den generelle forordning om databeskyttelse og artikel 29 i forordning (EU) 2018/1725 skal en databehandlers behandling være reguleret af en kontrakt eller et andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, der er bindende for databehandleren med hensyn til den dataansvarlige, og som præciserer, hvad behandlingen omfatter. Ved denne afgørelse fastsættes der regler om Kommissionens behandlingsaktiviteter som databehandler.

(12) Kommissionen er i forbindelse med behandling af personoplysninger inden for rammerne af den fælles gateway-facilitet bundet af Kommissionens afgørelse (EU, Euratom) 2017/46 ([11]).

(13) I betragtning af at de formål, til hvilke dataansvarlige behandler personoplysninger i de nationale kontaktopsporings- og advarselsmobilapplikationer, ikke nødvendigvis kræver identifikation af en registreret, vil de dataansvarlige måske ikke altid være i stand til at sikre udøvelsen af registreredes rettigheder. De rettigheder, der er omhandlet i artikel 15-20 i den generelle forordning om databeskyttelse, vil derfor ikke nødvendigvis gælde, når betingelserne i samme forordnings artikel 11 er opfyldt.

(14) Det er nødvendigt at omnummerere det eksisterende bilag til gennemførelsesafgørelse (EU) 2019/1765, da der tilføjes to nye bilag.

(15) Gennemførelsesafgørelse (EU) 2019/1765 bør derfor ændres.

(16) På grund af situationens hastende karakter som følge af covid-19-pandemien bør denne afgørelse finde anvendelse fra dagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

(17) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i forordning (EU) 2018/1725 og afgav udtalelse den 9. juli 2020.

(18) Foranstaltningerne i denne afgørelse er i overensstemmelse med udtalelse fra det udvalg, der er nedsat i henhold til artikel 16 i direktiv 2011/24/EU —

VEDTAGET DENNE AFGØRELSE:

Artikel 1

I gennemførelsesafgørelse (EU) 2019/1765 foretages følgende ændringer:

1) I artikel 2, stk. 1, indsættes følgende som litra g), h), i), j), k), l), m), n) og o):

»g) »applikationsbruger«: en person, som er i besiddelse af en intelligent enhed, og som har downloadet og kører en godkendt kontaktopsporings- og advarselsmobilapplikation

h) »kontaktopsporing«: foranstaltninger, der gennemføres for at opspore personer, der har været udsat for en kilde til en alvorlig grænseoverskridende sundhedstrussel efter betydningen i artikel 3, litra c), i Europa-Parlamentets og Rådets afgørelse nr. 1082/2013/EU (*)

([11]) Kommissionens afgørelse (EU, Euratom) 2017/46 af 10. januar 2017 om kommunikations- og informationssystemernes sikkerhed i Europa-Kommissionen (EUT L 6 af 11.1.2017, s. 40). Kommissionen offentliggør yderligere oplysninger om sikkerhedsstandarder for alle Kommissionens informationssystemer på https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_da.

i) »national kontaktopsporings- og advarselsmobilapplikation«: en softwareapplikation godkendt på nationalt plan, som kører på intelligente enheder, navnlig smartphones, og som sædvanligvis er udviklet til omfattende og målrettet samspil med webressourcer og behandler nærhedsdata og andre kontekstafhængige oplysninger, der indsamles af flere sensorer i de intelligente enheder med det formål at opspore personkontakter, der er smittet med SARS-CoV-2, og advare personer, der kan være blevet eksponeret for SARS-CoV-2. Disse mobilapplikationer er i stand til at opdage andre enheder i nærheden, der anvender Bluetooth, og udveksle oplysninger med backend-servere over internettet

j) »fælles gateway-facilitet«: en netværksgateway, som drives af Kommissionen via et sikkert IT-værktøj, og som modtager, lagrer og giver adgang til et minimumssæt af personoplysninger medlemsstaternes backend-servere imellem med det formål at sikre interoperabilitet mellem nationale kontaktopsporings- og advarselsmobilapplikationer

k) »nøgle«: en unik, kortvarig identifikator knyttet til en applikationsbruger, der giver notifikation om at være blevet smittet med SARS-CoV-2, eller som kan være blevet eksponeret for SARS-CoV-2

l) »smitteverifikation«: metoden til bekræftelse af smitte med SARS-CoV-2, dvs. enten at applikationsbrugeren selv har foretaget smittenotifikation, eller at smitten er bekræftet af en national sundhedsmyndighed eller med en laboratorietest

m) »berørte lande«: den medlemsstat, eller de medlemsstater, hvor en applikationsbruger har opholdt sig i de sidste 14 dage, før nøglerne blev uploadet, og hvor vedkommende har downloadet den godkendte nationale kontaktopsporings- og advarselsmobilapplikation og/eller har rejst

n) »nøglernes oprindelsesland«: den medlemsstat, hvor den backend-server, der uploadede nøglerne til den fælles gateway-facilitet, er placeret

o) »logdata«: en automatisk registrering af en aktivitet vedrørende udveksling af, og adgang til, data, der behandles via den fælles gateway-facilitet, og som viser navnlig typen af behandlingsaktivitet, dato og klokkeslæt for behandlingsaktiviteten og identifikatoren for den person, der har behandlet dataene.

_____

(*) Europa-Parlamentets og Rådets afgørelse nr. 1082/2013/EU af 22. oktober 2013 om alvorlige grænseoverskridende sundhedstrusler og om ophævelse af beslutning nr. 2119/98/EF (EUT L 293 af 5.11.2013, s. 1).«

2) I artikel 4, stk. 1, indsættes følgende som litra h):

»h) yde vejledning til medlemsstaterne om grænseoverskridende udveksling af personoplysninger via den fælles gateway-facilitet mellem nationale kontaktopsporings- og advarselsmobilapplikationer.«

3) I artikel 6, stk. 1, indsættes følgende som litra f) og g):

»f) udvikle, gennemføre og opretholde passende tekniske og organisatoriske foranstaltninger vedrørende sikkerheden i forbindelse med overførsel og hosting af personoplysninger i den fælles gateway-facilitet med det formål at sikre interoperabilitet mellem nationale kontaktopsporings- og advarselsmobilapplikationer

g) støtte e-sundhedsnetværket ved konstatering af, at de nationale myndigheder i teknisk og organisatorisk forstand overholder kravene til grænseoverskridende udveksling af personoplysninger i den fælles gateway-facilitet, ved at foretage de nødvendige test og audit. Eksperter fra medlemsstaterne kan bistå Kommissionens auditører.«

4) I artikel 7 foretages følgende ændringer:

a) Titlen ændres til »Beskyttelse af personoplysninger, der behandles via digitaltjenesteinfrastrukturen for e-sundhed«.

b) I stk. 2 ændres ordet »bilaget« til »bilag I«.

5) Følgende indsættes som artikel 7a:

»*Artikel 7a*

Grænseoverskridende udveksling af data mellem nationale kontaktopsporings- og advarselsmobilapplikationer via den fælles gateway-facilitet

1. Ved udveksling af personoplysninger via den fælles gateway-facilitet begrænses behandlingen til formål, der vedrører fremme af interoperabiliteten mellem nationale kontaktopsporings- og advarselsmobilapplikationer inden for den fælles gateway-facilitet og kontinuiteten i kontaktopsporing på tværs af grænserne.

2. De i stk. 3 omhandlede personoplysninger overføres til den fælles gateway-facilitet i et pseudonymiseret format.

3. De pseudonymiserede personoplysninger, der udveksles gennem og behandles i den fælles gateway-facilitet, må kun omfatte følgende informationer:

a) de nøgler, som de nationale kontaktopsporings- og advarselsmobilapplikationer har sendt, op til 14 dage før nøglerne blev uploadet

b) logdata i tilknytning til nøglerne i overensstemmelse med den protokol for tekniske specifikationer, der anvendes i nøglernes oprindelsesland

c) smitteverifikationen

d) de berørte lande og nøglernes oprindelsesland.

4. De udpegede nationale myndigheder eller officielle organer, der behandler personoplysninger i den fælles gateway-facilitet, er fælles dataansvarlige for de data, der behandles i den fælles gateway-facilitet. De fælles dataansvarliges respektive ansvar er som angivet i bilag II. Hver medlemsstat, der ønsker at deltage i den grænseoverskridende udveksling af data mellem nationale kontaktopsporings- og advarselsmobilapplikationer, underretter, inden den tilslutter sig, Kommissionen om sin hensigt og oplyser, hvilken national myndighed eller hvilket officielt organ der er udpeget som dataansvarlig.

5. Kommissionen er databehandler for personoplysninger, der behandles inden for den fælles gateway-facilitet. Kommissionen sørger i sin egenskab af databehandler for sikkerheden i forbindelse med behandlingen, herunder overførsel og hosting, af personoplysninger inden for den fælles gateway-facilitet og opfylder de forpligtelser, der påhviler en databehandler, som fastsat i bilag III.

6. Kommissionen og de nationale myndigheder, der har tilladelse til at tilgå den fælles gateway-facilitet, afprøver, vurderer og evaluerer regelmæssigt effektiviteten af de tekniske og organisatoriske foranstaltninger, der skal garantere sikkerheden i forbindelse med behandling af personoplysninger inden for den fælles gateway-facilitet.

7. Uden at det berører de fælles dataansvarliges beslutning om at indstille behandlingen i den fælles gateway-facilitet, skal driften af den fælles gateway-facilitet deaktiveres, senest 14 dage efter at alle forbundne nationale kontaktopsporings- og advarselsmobilapplikationer ophører med at sende nøgler via den fælles gateway-facilitet.«

6) Bilaget bliver herefter bilag I.

(7) Der indsættes et bilag II og et bilag III, hvis tekst er angivet i bilaget til denne afgørelse.

Artikel 2

Denne afgørelse træder i kraft dagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Udfærdiget i Bruxelles, den 15. juli 2020.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand

BILAG

I gennemførelsesafgørelse (EU) 2019/1765 tilføjes følgende som bilag II og III:

»*BILAG II*

DE DELTAGENDE MEDLEMSSTATERS ANSVAR SOM FÆLLES DATAANSVARLIGE FOR DEN FÆLLES GATEWAY-FACILITET FOR GRÆNSEOVERSKRIDENDE BEHANDLING MELLEM NATIONALE KONTAKTOPSPORINGS- OG ADVARSELSMOBILAPPLIKATIONER

AFSNIT 1

Underafsnit 1

Ansvarsfordeling

1) De fælles dataansvarlige behandler personoplysninger via den fælles gateway-facilitet i overensstemmelse med de tekniske specifikationer, der er fastsat af e-sundhedsnetværket ([1]).

2) Hver dataansvarlig er ansvarlig for at behandle personoplysninger i den fælles gateway-facilitet i overensstemmelse med den generelle forordning om databeskyttelse og direktiv 2002/58/EF.

3) Hver dataansvarlig opretter et kontaktpunkt med en funktionel mailboks, som anvendes til kommunikation mellem de fælles dataansvarlige og mellem de fælles dataansvarlige og databehandleren.

4) En midlertidig undergruppe, som oprettes af e-sundhedsnetværket i overensstemmelse med artikel 5, stk. 4, skal have til opgave at undersøge alle spørgsmål, der opstår i relation til de nationale kontaktopsporings- og advarselsmobilapplikationers interoperabilitet og det fælles dataansvar for dertil knyttet behandling af personoplysninger, og at lette koordinerede instrukser til Kommissionen som databehandler. De dataansvarlige kan inden for rammerne af den midlertidige undergruppe blandt andet arbejde for en fælles tilgang til opbevaring af data på deres nationale backendservere under hensyntagen til den opbevaringsperiode, der er fastsat i den fælles gateway-facilitet.

5) Instrukser til databehandleren sendes af et af de fælles dataansvarliges kontaktpunkt efter aftale med de øvrige fælles dataansvarlige i ovennævnte undergruppe.

6) Kun personer med tilladelse fra de udpegede nationale myndigheder eller officielle organer må tilgå personoplysninger om brugere, der udveksles i den fælles gateway-facilitet.

7) Hver(t) udpeget national myndighed eller officielt organ ophører med at være fælles dataansvarlig fra datoen for dens/dets udtræden af den fælles gateway-facilitet. Den/det er dog fortsat ansvarlig(t) for behandlingsaktiviteter i den fælles gateway-facilitet, der fandt sted før den/dets udtræden.

Underafsnit 2

Ansvar og roller i forbindelse med behandling af anmodninger fra og information af registrerede

1) Hver dataansvarlig giver, i overensstemmelse med artikel 13 og 14 i den generelle forordning om databeskyttelse, brugerne af dens nationale kontaktopsporings- og advarselsmobilapplikation (»de registrerede«) oplysninger om behandlingen af deres personoplysninger i den fælles gateway-facilitet til formål vedrørende de nationale kontaktopsporings- og advarselsmobilapplikationers grænseoverskridende interoperabilitet.

2) Hver dataansvarlig fungerer som kontaktpunkt for brugerne af dens nationale kontaktopsporings- og advarselsmobilapplikation og behandler anmodninger vedrørende udøvelsen af registreredes rettigheder i overensstemmelse med den generelle forordning om databeskyttelse, som indgives af disse brugere eller deres repræsentanter. Hver dataansvarlig udpeger et særligt kontaktpunkt med ansvar for anmodninger fra registrerede. Hvis en fælles dataansvarlig modtager en anmodning fra en registreret, der ikke falder ind under dens ansvarsområde, videresender den straks anmodningen til den ansvarlige fælles dataansvarlige. De fælles dataansvarlige bistår efter anmodning hinanden med behandlingen af registreredes anmodninger, og de svarer hinanden hurtigst muligt og under alle omstændigheder senest 15 dage efter at have modtaget en anmodning om bistand.

([1]) Først og fremmest interoperabilitetsspecifikationerne for grænseoverskridende transmissionskæder mellem godkendte apps af 16. juni 2020, som findes på: https://ec.europa.eu/health/ehealth/key_documents_en#anchor0

3) Hver dataansvarlig stiller indholdet af dette bilag, herunder de ordninger, der er fastlagt i punkt 1 og 2, til rådighed for de registrerede.

AFSNIT 2

Håndtering af sikkerhedsrelaterede hændelser, herunder brud på persondatasikkerheden

1) De fælles dataansvarlige bistår hinanden med identifikation og håndtering af eventuelle sikkerhedsrelaterede hændelser, herunder brud på persondatasikkerheden, i forbindelse med behandlingen i den fælles gateway-facilitet.

2) De fælles dataansvarlige underretter især hinanden om følgende:

a) enhver potentiel eller reel risiko i forhold til adgangen til, fortroligheden for og/eller integriteten af de personoplysninger, der er genstand for behandling i den fælles gateway-facilitet

b) enhver sikkerhedsrelateret hændelse i forbindelse med behandlingsaktiviteterne i den fælles gateway-facilitet

c) ethvert brud på persondatasikkerheden, de sandsynlige konsekvenser af bruddet på persondatabeskyttelsen og en vurdering af risikoen for fysiske personers rettigheder og frihedsrettigheder samt alle foranstaltninger, der træffes for at håndtere bruddet på persondatasikkerheden og begrænse risikoen for fysiske personers rettigheder og frihedsrettigheder

d) enhver overtrædelse af de tekniske og/eller organisatoriske sikkerhedsforanstaltninger for behandlingsaktiviteterne i den fælles gateway-facilitet.

3) De fælles dataansvarlige anmelder, i overensstemmelse med artikel 33 og 34 i forordning (EU) 2016/679 eller efter anmeldelse fra Kommissionen, ethvert brud på persondatasikkerheden i forbindelse med behandlingsaktiviteterne i den fælles gateway-facilitet til Kommissionen, til de kompetente tilsynsmyndigheder og, for så vidt det er påkrævet, til de registrerede.

AFSNIT 3

Konsekvensanalyse vedrørende databeskyttelse

Hvis en dataansvarlig, for at overholde sine forpligtelser i henhold til artikel 35 og 36 i den generelle forordning om databeskyttelse, har brug for oplysninger fra en anden dataansvarlig, sender førstnævnte dataansvarlige en specifik anmodning til den funktionelle mailboks, der er omhandlet i afsnit 1, underafsnit 1, punkt 3). Sidstnævnte gør sit bedste for at tilvejebringe de pågældende oplysninger.

BILAG III

KOMMISSIONENS ANSVAR SOM DATABEHANDLER FOR DEN FÆLLES GATEWAY-FACILITET FOR GRÆNSEOVERSKRIDENDE BEHANDLING MELLEM NATIONALE KONTAKTOPSPORINGS- OG ADVARSELS-MOBILAPPLIKATIONER

Kommissionen skal:

1) sørge for og sikre en sikker og pålidelig kommunikationsinfrastruktur, der forbinder nationale kontaktopsporings- og advarselsmobilapplikationer i de medlemsstater, der deltager i den fælles gateway-facilitet. Kommission kan for at opfylde sine forpligtelser som databehandler for den fælles gateway-facilitet inddrage tredjeparter som underdatabehandlere; Kommissionen underretter de fælles dataansvarlige om alle påtænkte ændringer vedrørende tilføjelse eller udskiftning af andre underdatabehandlere, således at de dataansvarlige har mulighed for i fællesskab at gøre indsigelse mod de pågældende ændringer, jf. bilag II, afsnit 1, underafsnit 1, punkt 4). Kommissionen sikrer, at der gælder samme databeskyttelsesforpligtelser for disse underdatabehandlere som fastsat i denne afgørelse

2) behandle personoplysningerne udelukkende efter dokumenterede instrukser fra de dataansvarlige, medmindre det kræves i henhold til EU-retten eller medlemsstaternes nationale ret; i så fald underretter Kommissionen de dataansvarlige om dette retlige krav, inden oplysningerne behandles, medmindre den pågældende ret forbyder en sådan underretning af hensyn til væsentlige samfundsinteresser.

3) Kommissionens behandling indebærer følgende:

a) at autentificere nationale backend-servere på grundlag af nationale backend-servercertifikater

b) at modtage de data omhandlet i gennemførelsesafgørelsens artikel 7a, stk. 3, der uploades af de nationale backend-servere, ved at stille en applikationsprogrammeringsgrænseflade til rådighed, som gør det muligt for nationale backend-servere at uploade de relevante data

c) at lagre dataene i den fælles gateway-facilitet, når den modtager dem fra nationale backend-servere

d) at stille dataene til rådighed, så de kan downloades af de nationale backend-servere

e) at slette dataene, når alle de deltagende backend-servere har downloadet dem, dog senest 14 dage efter modtagelsen

f) at slette eventuelle resterende data, efter at tjenesterne er ophørt, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

Databehandleren træffer de nødvendige foranstaltninger til at beskytte de behandlede datas integritet

4) træffe alle avancerede organisatoriske, fysiske og logiske sikkerhedsforanstaltninger for at vedligeholde den fælles gateway-facilitet. Kommissionen skal med henblik herpå:

a) udpege en enhed, der er ansvarlig for sikkerhedsstyring på niveauet for den fælles gateway-facilitet, kommunikere enhedens kontaktoplysninger til de dataansvarlige og sikre, at enheden kan reagere på sikkerhedstrusler

b) påtage sig ansvaret for sikkerheden i den fælles gateway-facilitet

c) sikre, at alle, der får adgang til den fælles gateway-facilitet, er underlagt kontraktlig, professionel eller lovbestemt tavshedspligt

5) træffe alle nødvendige sikkerhedsforanstaltninger til at undgå at kompromittere driften af de nationale backend-servere. Kommissionen skal til dette formål fastlægge specifikke procedurer i tilknytning til forbindelsen fra backend-serverne til den fælles gateway-facilitet. Dette omfatter:

a) risikovurderingsprocedure — til identificering og vurdering af mulige trusler mod systemet

b) audit- og kontrolprocedure til:

   i. kontrol af overensstemmelse mellem de gennemførte sikkerhedsforanstaltninger og sikkerhedspolitik i anvendelse

   ii. regelmæssig kontrol af integriteten af systemfiler, sikkerhedsparametre og udstedte tilladelser

   iii. overvågning med henblik på afsløring af brud på sikkerheden og indtrængen

   iv. gennemførelse af ændringer for at begrænse eksisterende sikkerhedsproblemer

   v. sikring, herunder på anmodning fra dataansvarlige, af og bidrag til udførelsen af uafhængige audit, herunder inspektioner, og gennemgang af sikkerhedsforanstaltninger på vilkår, der er i overensstemmelse med protokol (nr. 7) til TEUF vedrørende Den Europæiske Unions privilegier og immuniteter ([2])

([2]) Protokol (nr. 7) vedrørende Den Europæiske Unions privilegier og immuniteter (EUT C 326 af 26.10.2012, s. 266).

c) ændring af kontrolproceduren til dokumentation og måling af virkningen af en ændring, før den gennemføres, og underretning af de dataansvarlige om ændringer, der kan påvirke kommunikationen med og/eller sikkerheden i deres infrastrukturer

d) fastlæggelse af en vedligeholdelses- og reparationsprocedure til præcisering af bestemmelser og betingelser, som skal overholdes ved vedligeholdelse og/eller reparation af udstyr

e) fastlæggelse af en procedure for sikkerhedsrelaterede hændelser til fastlæggelse af rapporterings- og eskaleringsordningen, omgående underretning af de dataansvarlige samt Den Europæiske Tilsynsførende for Databeskyttelse om brud på persondatasikkerheden og fastlæggelse af en disciplinær proces til håndtering af brud på sikkerheden.

6) træffe avancerede fysiske og/eller logiske sikkerhedsforanstaltninger for de faciliteter, som opbevarer udstyret til den fælles gateway-facilitet, og for kontrollen af adgangen til logiske data og sikkerhed. Kommissionen skal med henblik herpå:

a) håndhæve den fysiske sikkerhed for at oprette særlige sikkerhedsområder og muliggøre afsløring af brud

b) kontrollere adgang til faciliteterne og vedligeholde et besøgsregister med henblik på sporing

c) sikre, at eksterne personer med adgang til området ledsages af behørigt bemyndigede medarbejdere

d) sikre, at udstyr ikke kan tilføjes, erstattes eller fjernes uden forudgående godkendelse fra de udpegede ansvarlige organer

e) kontrollere adgang fra og til de nationale backend-servere til den fælles gateway-facilitet

f) sikre, at alle, der har adgang til den fælles gateway-facilitet, identificeres og autentificeres

g) gennemgå godkendelsesrettighederne i forbindelse med adgang til den fælles gateway-facilitet, i tilfælde af at et brud på sikkerheden har betydning for denne infrastruktur

h) fastholde integriteten i de oplysninger, der overføres via den fælles gateway-facilitet

i) gennemføre tekniske og organisatoriske sikkerhedsforanstaltninger for at forhindre uautoriseret adgang til personoplysninger

j) om nødvendigt gennemføre foranstaltninger for at blokere uautoriseret adgang til den fælles gateway-facilitet fra de nationale myndigheders domæne (dvs. blokere en lokation/IP-adresse)

7) træffe foranstaltninger til beskyttelse af sit domæne, herunder fjerne forbindelser, hvis der er væsentlig afvigelse fra principper og koncepter for kvalitet og sikkerhed

8) opstille en risikostyringsplan i forbindelse med sit ansvarsområde

9) overvåge — i realtid — udførelsen af alle servicekomponenter af sine tjenester i den fælles gateway-facilitet, udarbejde regelmæssige statistikker og føre registre

10) yde støtte til alle den fælles gateway-facilitets tjenester på engelsk 24/7 via telefon, e-mail eller webportal og modtage opkald fra autoriserede personer: koordinatorer af den fælles gateway-facilitet og deres respektive helpdeske, projektledere og udpegede personer fra Kommissionen

11) bistå de dataansvarlige, i den udstrækning det er muligt og ved hjælp af passende tekniske og organisatoriske foranstaltninger, med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder som fastlagt i kapitel III i den generelle forordning om databeskyttelse

12) yde støtte til de dataansvarlige ved at levere oplysninger vedrørende den fælles gateway-facilitet for at gennemføre forpligtelserne i henhold til artikel 32, 35 og 36 i den generelle forordning om databeskyttelse

13) sikre, at oplysninger, der behandles inden for den fælles gateway-facilitet, er uforståelige for alle, der ikke har tilladelse til at tilgå faciliteten

14) træffe alle relevante foranstaltninger for at forhindre, at operatører af den fælles gateway-facilitet har uautoriseret adgang til overførte oplysninger

15) træffe foranstaltninger for at fremme interoperabiliteten og kommunikationen mellem den fælles gateway-facilitets udpegede dataansvarlige

16) føre en fortegnelse over de behandlingsaktiviteter, der foretages på vegne af de dataansvarlige, i overensstemmelse med artikel 31, stk. 2, i forordning (EU) 2018/1725.«