II

(Icke-lagstiftningsakter)

BESLUT

KOMMISSIONENS GENOMFÖRANDEBESLUT (EU) 2020/1023

av den 15 juli 2020

om ändring av genomförandebeslut (EU) 2019/1765 vad gäller det gränsöverskridande utbytet av uppgifter mellan nationella mobilapplikationer för kontaktspårning och varning i kampen mot covid-19-pandemin

(Text av betydelse för EES)

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård ([1]), särskilt artikel 14.3, och

av följande skäl:

(1) Enligt artikel 14 i direktiv 2011/24/EU ska unionen stödja och främja samarbete om och utbyte av information mellan medlemsstaterna inom ramen för ett frivilligt nätverk som kopplar ihop nationella myndigheter som är ansvariga för e-hälsa (nedan kallat *nätverket för e-hälsa*), utsedda av medlemsstaterna.

(2) I kommissionens genomförandebeslut (EU) 2019/1765 ([2]) fastslås regler för inrättande, förvaltning och drift av ett nätverk av nationella myndigheter med ansvar för e-hälsa. Genom artikel 4 i beslutet ges nätverket för e-hälsa i uppdrag att främja större interoperabilitet mellan de nationella informations- och kommunikationstekniksystemen och gränsöverskridande överförbarhet för elektroniska hälsouppgifter vid gränsöverskridande hälso- och sjukvård.

(3) Till följd av den folkhälsokris som orsakats av covid-19-pandemin har flera medlemsstater utvecklat mobilapplikationer för kontaktspårning, som innebär att användare av dessa applikationer kan få varningar och vidta lämpliga åtgärder, t.ex. testning eller självisolering, om de potentiellt har exponerats för viruset genom att de har varit i närheten av en annan användare av sådana applikationer, som har rapporterat att vederbörande har infekterats med sars-cov-2. I dessa applikationer används bluetooth-teknik för att upptäcka enheter i närheten. Sedan juni 2020 har man lättat på reserestriktionerna mellan medlemsstaterna och därför bör bättre interoperabilitet mellan nationella informations- och kommunikationstekniksystem uppnås mellan medlemsstaterna i nätverket för e-hälsa, genom införandet av en digital infrastruktur som möjliggör interoperabilitet mellan nationella mobilapplikationer som stöder kontaktspårning och varningar.

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

([2]) Kommissionens genomförandebeslut (EU) 2019/1765 av den 22 oktober 2019 om regler för inrättande, förvaltning och drift av ett nätverk av nationella myndigheter med ansvar för e-hälsa och om upphävande av genomförandebeslut 2011/890/EU (EUT L 270, 24.10.2019, s. 83).

(4) Kommissionen stöder medlemsstaterna vad gäller de ovan nämnda mobilapplikationerna. Den 8 april 2020 antog kommissionen en rekommendation om en unionsgemensam verktygslåda för användningen av teknik och data för att bekämpa och komma ut ur covid-19-krisen, särskilt när det gäller mobilapplikationer och användning av anonymiserade rörlighetsdata ([3]). Med stöd av kommissionen antog medlemsstaterna i nätverket för e-hälsa en unionsgemensam verktygslåda för medlemsstaterna avseende mobilapplikationer som stöd vid kontaktspårning ([4]) och interoperabilitetsriktlinjer för godkända mobilapplikationer för kontaktspårning i EU ([5]). I verktygslådan förklaras de nationella kraven på nationella mobilapplikationer för kontaktspårning och varning, särskilt att applikationerna bör vara frivilliga, godkända av behörig hälsomyndighet, integritetsbevarande och avvecklas så snart de inte längre behövs. Mot bakgrund av hur covid-19-krisen har utvecklats på senare tid har både kommissionen ([6]) och Europeiska dataskyddsstyrelsen ([7]) utfärdat vägledning om mobilapplikationer och kontaktspårningsverktyg med avseende på dataskydd. Utformningen av medlemsstaternas mobilapplikationer och av den digitala infrastruktur som möjliggör interoperabiliteten mellan dem utgår från den unionsgemensamma verktygslådan, ovan nämnda vägledning och de tekniska specifikationer som man enats om i nätverket för e-hälsa.

(5) De medlemsstater som ingår i nätverket för e-hälsa har beslutat att på frivillig grund öka samarbetet på detta område och har med stöd av kommissionen utvecklat en digital infrastruktur i form av ett it-verktyg för utbyte av uppgifter, i syfte att underlätta interoperabiliteten mellan nationella mobilapplikationer för kontaktspårning och varningar. Denna digitala infrastruktur kallas för den samordnade nätslussen.

(6) I detta beslut fastställs bestämmelser för de roller som de deltagande medlemsstaterna och kommissionen har vad gäller driften av den samordnade nätslussen för gränsöverskridande interoperabilitet mellan nationella mobilapplikationer för kontaktspårning och varning.

(7) Behandling av personuppgifter för användare av mobilapplikationer för kontaktspårning och varning, som utförs under ansvar av medlemsstaterna eller andra offentliga organisationer eller organ i medlemsstaterna, bör genomföras i enlighet med Europaparlamentets och rådets förordning (EU) 2016/679 ([8]) (nedan kallad *den allmänna dataskyddsförordningen*) och Europaparlamentets och rådets direktiv 2002/58/EG ([9]). Behandling av personuppgifter under kommissionens ansvar för förvaltning och säkerställande av den samordnade nätslussens säkerhet bör följa Europaparlamentets och rådets förordning (EU) 2018/1725 ([10]).

(8) Den samordnade nätslussen bör bestå av en säker it-infrastruktur som tillhandahåller ett gemensamt gränssnitt, där utsedda nationella myndigheter eller offentliga organ kan utbyta en minimiuppsättning uppgifter avseende kontakter med personer som har infekterats med sars-cov-2, i syfte att informera andra om att de potentiellt blivit exponerade för detta virus, samt främjar ett ändamålsenligt hälso- och sjukvårdssamarbete mellan medlemsstaterna genom att underlätta utbytet av relevant information.

(9) I detta beslut bör det därför fastställas villkor för det gränsöverskridande utbytet av uppgifter mellan utsedda nationella myndigheter eller offentliga organ genom den samordnade nätslussen inom EU.

([3]) Kommissionens rekommendation (EU) 2020/518 av den 8 april 2020 om en unionsgemensam verktygslåda för användningen av teknik och data för att bekämpa och komma ut ur covid-19-krisen, särskilt när det gäller mobilapplikationer och användning av anonymiserade rörlighetsdata (EUT L 114, 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]) Kommissionens meddelande *Vägledning om appar till stöd för kampen mot covid-19-pandemin med avseende på dataskydd* (EUT C 124 I, 17.4.2020, s. 1).

([7]) *Riktlinjer 4/2020 om användning av lokaliseringsuppgifter och kontaktspårningsverktyg i samband med covid-19-utbrottet* och Europeiska dataskyddsstyrelsens uttalande av den 16 juni 2020 om de konsekvenser som kontaktspårningsappars kompatibilitet innebär för dataskyddet, som båda finns tillgängliga på https://edpb.europa.eu

([8]) 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) (EUT L 119, 4.5.2016, s. 1).

([9]) Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37).

([10]) Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39).

(10) De deltagande medlemsstaterna, företrädda av de utsedda nationella myndigheterna eller offentliga organen, fastställer tillsammans syftet med och metoderna för behandling av personuppgifter genom den samordnade nätslussen och är därför gemensamt personuppgiftsansvariga. Enligt artikel 26 i den allmänna dataskyddsförordningen ska gemensamt personuppgiftsansvariga för behandling av personuppgifter under öppna former fastställa sitt respektive ansvar för att fullgöra skyldigheterna enligt den förordningen. Genom artikeln ges också möjlighet att få detta ansvar fastställt genom unionsrätten eller i medlemsstaternas nationella rätt som de personuppgiftsansvariga omfattas av. Var och en av de personuppgiftsansvariga bör säkerställa att det finns rättslig grund på nationell nivå för behandling i den samordnade nätslussen.

(11) I egenskap av tillhandahållare av tekniska och organisatoriska lösningar för den samordnade nätslussen behandlar kommissionen pseudonymiserade personuppgifter för de deltagande medlemsstaternas räkning i den samordnade nätslussen i deras egenskap av gemensamt personuppgiftsansvariga, och är därför ett personuppgiftsbiträde. I artikel 28 i den allmänna dataskyddsförordningen och i artikel 29 i förordning (EU) 2018/1725 fastställs att när uppgifter behandlas av ett personuppgiftsbiträde ska behandlingen regleras genom ett avtal eller en rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt som är bindande för personuppgiftsbiträdet med avseende på den personuppgiftsansvarige och som specificerar behandlingen. I detta beslut fastställs regler för kommissionens behandling i egenskap av personuppgiftsbiträde.

(12) Vid behandling av personuppgifter inom ramen för den samordnade nätslussen måste kommissionen följa kommissionens beslut (EU, Euratom) 2017/46 ([11]).

(13) Eftersom de syften för vilka personuppgiftsansvariga behandlar personuppgifter i de nationella mobilapplikationerna för kontaktspårning och varning inte nödvändigtvis kräver att den registrerade identifieras har de personuppgiftsansvariga kanske inte alltid möjlighet att säkerställa tillämpningen av de registrerades rättigheter. De rättigheter som avses i artiklarna 15–20 i den allmänna dataskyddsförordningen är därför möjligen inte tillämpliga när villkoren enligt artikel 11 i den förordningen är uppfyllda.

(14) Den nuvarande bilagan till genomförandebeslut (EU) 2019/1765 behöver numreras om på grund av att två nya bilagor har lagts till.

(15) Genomförandebeslut (EU) 2019/1765 bör därför ändras i enlighet med detta.

(16) Med tanke på den akuta situation som uppstått på grund av covid-19-pandemin bör detta beslut träda i kraft dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

(17) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i förordning (EU) 2018/1725 och avgav ett yttrande den 9 juli 2020.

(18) De åtgärder som föreskrivs i detta beslut är förenliga med yttrandet från den kommitté som inrättats genom artikel 16 i direktiv 2011/24/EU.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Genomförandebeslut (EU) 2019/1765 ska ändras på följande sätt:

1. I artikel 2.1 ska följande led läggas till som leden g, h, i, j, k, l, m, n och o:

”g) *applikationsanvändare*: person som innehar en smart enhet och som har laddat ned och använder en godkänd mobilapplikation för kontaktspårning och varning.

h) *kontaktspårning*: åtgärder för att spåra personer som exponerats för en källa till ett allvarligt gränsöverskridande hot mot människors hälsa enligt artikel 3 c i Europaparlamentets och rådets beslut nr 1082/2013/EU (*).

([11]) Kommissionens beslut (EU, Euratom) 2017/46 av den 10 januari 2017 om säkerheten i Europeiska kommissionens kommunikations- och informationssystem (EUT L 6, 11.1.2017, s. 40). Kommissionen offentliggör mer information om de säkerhetsstandarder som är tillämpliga på EU-kommissionens informationssystem på https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_en

i) *nationell mobilapplikation för kontaktspårning och varning*: programvaruapplikation som är godkänd på nationell nivå och används i smarta enheter, särskilt smarttelefoner, och som vanligen är avsedd för omfattande och riktad interaktion med webbresurser som behandlar närhetsdata och andra kontextuella data som samlas in av de många sensorer som finns i smarta enheter i syfte att spåra kontakter med personer som är infekterade med sars-cov-2 och varna personer som kan ha exponerats för sars-cov-2. Dessa mobilapplikationer kan upptäcka andra enheter genom bluetooth och utbyta uppgifter med backendservrar via internet.

j) *samordnad nätsluss*: nätverkssluss som drivs av kommissionen genom ett säkert it-verktyg, som tar emot, lagrar och tillhandahåller en minimiuppsättning personuppgifter mellan medlemsstaters backendservrar i syfte att säkerställa interoperabiliteten mellan nationella mobilapplikationer för kontaktspårning och varning.

k) *nyckel*: unik tillfällig identifierare avseende en applikationsanvändare som rapporterar att han eller hon har infekterats med sars-cov-2 eller som kan ha exponerats för sars-cov-2.

l) *verifiering av infektion*: metod som används för att bekräfta en infektion med sars-cov-2, dvs. om detta är självrapporterat av applikationsanvändaren eller om infektionen har bekräftats av en nationell hälso- och sjukvårdsmyndighet eller genom ett laboratorietest.

m) *länder av intresse*: den eller de medlemsstater där en applikationsanvändare har vistats under fjortondagarsperioden före datumet för uppladdning av nycklarna och där användaren har laddat ned den godkända nationella mobilapplikationen för kontaktspårning och varning och/eller där användaren har varit på resa.

n) *ursprungsland för nycklarna*: den medlemsstat där den backendserver som laddade upp nycklarna till den samordnade nätslussen är placerad.

o) *logguppgifter*: automatisk registrering av en aktivitet i samband med utbytet av, och tillgången till, uppgifter som behandlas genom den samordnade nätslussen, som framför allt visar typen av behandling, datum och tidpunkt för behandlingen och identifieraren för den person som behandlar uppgifterna.

_____

(*) Europaparlamentets och rådets beslut nr 1082/2013/EU av den 22 oktober 2013 om allvarliga gränsöverskridande hot mot människors hälsa och om upphävande av beslut nr 2119/98/EG (EUT L 293, 5.11.2013, s. 1).”

2. I artikel 4.1 ska följande led läggas till som led h:

”h) Ge vägledning till medlemsstaterna om gränsöverskridande utbyte av personuppgifter genom den samordnade nätslussen mellan nationella mobilapplikationer för kontaktspårning och varning.”

3. I artikel 6.1 ska följande led läggas till som leden f och g:

”f) utveckla, implementera och upprätthålla ändamålsenliga tekniska och organisatoriska åtgärder avseende säkerheten vid överföring av och värdtjänster för personuppgifter i den samordnade nätslussen i syfte att säkerställa interoperabiliteten mellan nationella mobilapplikationer för kontaktspårning och varning,

g) stödja nätverket för e-hälsa när det gäller att fastställa att de nationella myndigheterna tekniskt och organisatoriskt uppfyller kraven på gränsöverskridande utbyte av personuppgifter i den samordnade nätslussen genom att tillhandahålla och utföra nödvändiga test och revisioner. Experter från medlemsstaterna får bistå kommissionens revisorer.”

4. Artikel 7 ska ändras på följande sätt:

a) Rubriken ska ändras till ”Skydd av personuppgifter som behandlas genom infrastrukturen för digitala e-hälsotjänster”.

b) I punkt 2 ska ”bilagan” ersättas med ”bilaga I”.

5. Följande artikel ska läggas till som artikel 7a:

”*Artikel 7a*

Gränsöverskridande utbyte av uppgifter mellan nationella mobilapplikationer för kontaktspårning och varning genom den samordnade nätslussen

1. Vid utbyte av personuppgifter genom den samordnade nätslussen ska behandlingen vara begränsad till användning i syfte att underlätta interoperabiliteten mellan nationella mobilapplikationer för kontaktspårning och varning i den samordnade nätslussen och den fortsatta kontaktspårningen i ett gränsöverskridande sammanhang.

2. De personuppgifter som avses i punkt 3 ska överföras till den samordnade nätslussen i pseudonymiserad form.

3. Pseudonymiserade personuppgifter som utbyts genom och behandlas i den samordnade nätslussen ska endast bestå av följande information:

a) De nycklar som överförs av de nationella mobilapplikationerna för kontaktspårning och varning upp till 14 dagar före datumet för uppladdning av nycklarna.

b) Logguppgifter för nycklarna enligt det protokoll med tekniska specifikationer som används i ursprungslandet för nycklarna.

c) Verifiering av infektion.

d) Länder av intresse och ursprungsland för nycklarna.

4. De utsedda nationella myndigheter eller offentliga organ som behandlar personuppgifter i den samordnade nätslussen ska vara gemensamt personuppgiftsansvariga för de uppgifter som behandlas i den. De gemensamt personuppgiftsansvarigas respektive ansvarsområden ska fördelas i enlighet med bilaga II. Varje medlemsstat som vill delta i det gränsöverskridande utbytet av uppgifter mellan nationella mobilapplikationer för kontaktspårning och varning ska innan den går med i utbytet underrätta kommissionen om sina avsikter och ange den nationella myndighet eller det offentliga organ som har utsetts till personuppgiftsansvarig.

5. Kommissionen ska vara personuppgiftsbiträde för de personuppgifter som behandlas i den samordnade nätslussen. I egenskap av personuppgiftsbiträde ska kommissionen säkerställa säkerheten vid behandlingen av personuppgifter, vilket inbegriper överföring av och värdtjänster för personuppgifter, i den samordnade nätslussen och ska fullgöra sina skyldigheter som personuppgiftsbiträde i enlighet med bilaga III.

6. De tekniska och organisatoriska åtgärdernas ändamålsenlighet vad gäller att trygga säkerheten i behandlingen av personuppgifter i den samordnade nätslussen ska regelbundet testas, bedömas och utvärderas av kommissionen och de nationella myndigheter som har behörighet att ansluta till den samordnade nätslussen.

7. Utan att det påverkar de gemensamt personuppgiftsansvarigas beslut att avbryta behandlingen i den samordnade nätslussen ska driften av den samordnade nätslussen upphöra senast 14 dagar efter att alla anslutna nationella mobilapplikationer för kontaktspårning och varning har upphört att sända nycklar genom den samordnade nätslussen.”

6. Bilagan ska betecknas bilaga I.

7. Bilagorna II och III, enligt lydelsen i bilagan till detta beslut, ska läggas till.

Artikel 2

Detta beslut träder i kraft dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Utfärdat i Bryssel den 15 juli 2020.

På kommissionens vägnar
Ursula VON DER LEYEN
Ordförande

BILAGA

I genomförandebeslut (EU) 2019/1765 ska följande bilagor läggas till som bilagorna II och III:

"BILAGA II

DE DELTAGANDE MEDLEMSSTATERNAS ANSVAR I EGENSKAP AV GEMENSAMT PERSONUPPGIFTSANSVARIGA FÖR DEN SAMORDNADE NÄTSLUSSEN FÖR GRÄNSÖVERSKRIDANDE BEHANDLING MELLAN NATIONELLA MOBILAPPLIKATIONER FÖR KONTAKTSPÅRNING OCH VARNING

AVSNITT 1

Underavsnitt 1

Ansvarsfördelning

(1) De gemensamt personuppgiftsansvariga ska behandla personuppgifter via den samordnade nätslussen i enlighet med de tekniska specifikationer som fastställs av nätverket för e-hälsa ([1]).

(2) Varje personuppgiftsansvarig ska ansvara för behandlingen av personuppgifter i den samordnade nätslussen i enlighet med den allmänna dataskyddsförordningen och direktiv 2002/58/EG.

(3) Varje personuppgiftsansvarig ska inrätta en kontaktpunkt med en funktionsbrevlåda för kommunikationen mellan de gemensamt personuppgiftsansvariga och mellan de gemensamt personuppgiftsansvariga och personuppgiftsbiträdet.

(4) En tillfällig arbetsgrupp som inrättats av nätverket för e-hälsa i enlighet med artikel 5.4 ska ges i uppdrag att undersöka eventuella problem med interoperabiliteten mellan de nationella mobilapplikationerna för kontaktspårning och varning och med det gemensamma personuppgiftsansvaret för berörd behandling av personuppgifter samt att underlätta samordnade instruktioner till kommissionen i egenskap av personuppgiftsbiträde. Bland annat kan de personuppgiftsansvariga, inom ramen för den tillfälliga arbetsgruppen, arbeta för att komma fram till en gemensam strategi för lagring av uppgifter på nationella backendservrar, med beaktande av den lagringstid som anges i den samordnade nätslussen.

(5) Instruktioner till personuppgiftsbiträdet ska skickas genom någon av de gemensamt personuppgiftsansvarigas kontaktpunkt, i samförstånd med övriga gemensamt personuppgiftsansvariga i den arbetsgrupp som avses ovan.

(6) Endast personer som är behöriga enligt de utsedda nationella myndigheterna eller offentliga organen kan få tillgång till användares personuppgifter som utbyts i den samordnade nätslussen.

(7) Varje utsedd nationell myndighet eller utsett offentligt organ ska upphöra att vara gemensamt personuppgiftsansvarig från det datum myndigheten eller organet inte längre deltar i den samordnade nätslussen. Myndigheten eller organet ska dock ha fortsatt ansvar för den behandling i den samordnade nätslussen som utfördes innan deltagandet upphörde.

Underavsnitt 2

Ansvarsområden och roller vid hantering av förfrågningar från och information till registrerade

(1) Varje personuppgiftsansvarig ska ge användarna av dess nationella mobilapplikation för kontaktspårning och varning (nedan kallade *de registrerade*) information om behandlingen av deras personuppgifter i den samordnade nätslussen för gränsöverskridande interoperabilitet mellan de nationella mobilapplikationerna för kontaktspårning och varning, i enlighet med artiklarna 13 och 14 i den allmänna dataskyddsförordningen.

(2) Varje personuppgiftsansvarig ska fungera som kontaktpunkt för användarna av dess nationella mobilapplikation för kontaktspårning och varning och ska hantera förfrågningar rörande utnyttjandet av registrerades rättigheter i enlighet med den allmänna dataskyddsförordningen som inlämnas av dessa användare eller deras företrädare. Varje personuppgiftsansvarig ska utse en särskild kontaktpunkt för förfrågningar från registrerade. Om en gemensamt personuppgiftsansvarig får en förfrågan från en registrerad, som inte omfattas av dess ansvar, ska den gemensamt personuppgiftsansvariga omedelbart vidarebefordra denna förfrågan till den berörda gemensamt personuppgiftsansvariga parten. De gemensamt personuppgiftsansvariga ska på begäran bistå varandra i hanteringen av registrerades förfrågningar och ska svara varandra utan onödigt dröjsmål, senast inom 15 dagar från mottagandet av en begäran om bistånd.

([1]) I synnerhet interoperabilitetsspecifikationerna för gränsöverskridande överföringskedjor mellan godkända appar, av den 16 juni 2020, tillgängliga på https://ec.europa.eu/health/ehealth/key_documents_en#anchor0

(3) Varje personuppgiftsansvarig ska ge de registrerade tillgång till innehållet i denna bilaga, inbegripet de arrangemang som fastställs i punkterna 1 och 2.

AVSNITT 2

Hantering av säkerhetsincidenter, inbegripet personuppgiftsincidenter

(1) De gemensamt personuppgiftsansvariga ska bistå varandra i identifiering och hantering av alla säkerhetsincidenter, inbegripet personuppgiftsincidenter, som har koppling till behandlingen i den samordnade nätslussen.

(2) De gemensamt personuppgiftsansvariga ska särskilt underrätta varandra om följande:

a) Varje potentiell eller faktisk risk för tillgängligheten till samt sekretessen och/eller integriteten hos de personuppgifter som behandlas i den samordnade nätslussen.

b) Varje säkerhetsincident som har koppling till behandlingen i den samordnade nätslussen.

c) Varje personuppgiftsincident, de sannolika konsekvenserna av personuppgiftsincidenten och bedömningen av risken för fysiska personers rättigheter och friheter samt alla åtgärder som vidtagits för att åtgärda personuppgiftsincidenten och minska risken för fysiska personers rättigheter och friheter.

d) Varje överträdelse av tekniska och/eller organisatoriska skyddsåtgärder avseende behandlingen i den samordnade nätslussen.

(3) De gemensamt personuppgiftsansvariga ska anmäla alla personuppgiftsincidenter vad gäller behandlingen i den samordnade nätslussen till kommissionen, till behöriga tillsynsmyndigheter och, där så krävs, till registrerade, i enlighet med artiklarna 33 och 34 i förordning (EU) 2016/679 eller efter anmälan av kommissionen.

AVSNITT 3

Konsekvensbedömning avseende dataskydd

Om en personuppgiftsansvarig behöver information från en annan personuppgiftsansvarig, för att kunna uppfylla sina skyldigheter enligt artiklarna 35 och 36 i den allmänna dataskyddsförordningen, ska en särskild begäran skickas till den funktionsbrevlåda som avses i avsnitt 1 underavsnitt 1.3. Den andra personuppgiftsansvarige ska göra sitt yttersta för att tillhandahålla sådan information.

BILAGA III

KOMMISSIONENS ANSVAR I EGENSKAP AV PERSONUPPGIFTSBITRÄDE FÖR DEN SAMORDNADE NÄTSLUSSEN FÖR GRÄNSÖVERSKRIDANDE BEHANDLING MELLAN NATIONELLA MOBILAPPLIKATIONER FÖR KONTAKTSPÅRNING OCH VARNING

Kommissionen ska göra följande:

(1) Inrätta och säkerställa en säker och tillförlitlig kommunikationsinfrastruktur som kopplar samman nationella mobilapplikationer för kontaktspårning och varning i de medlemsstater som deltar i den samordnade nätslussen. För att fullgöra sina skyldigheter som personuppgiftsbiträde för den samordnade nätslussen får kommissionen anlita tredje parter som underleverantörer. Kommissionen ska informera de gemensamt personuppgiftsansvariga om eventuella avsiktliga förändringar rörande tillägg eller byte av underleverantörer och därmed ge de personuppgiftsansvariga möjlighet att gemensamt invända mot sådana förändringar enligt avsnitt 1 underavsnitt 1.4 i bilaga II. Kommissionen ska säkerställa att dataskyddsskyldigheterna i detta beslut även tillämpas på dessa underleverantörer.

(2) Endast behandla personuppgifter på grundval av dokumenterade instruktioner från de personuppgiftsansvariga, såvida inte denna behandling krävs enligt unionsrätten eller en medlemsstats nationella rätt; i sådant fall ska kommissionen informera de personuppgiftsansvariga om det rättsliga kravet innan uppgifterna behandlas, såvida det inte är förbjudet att lämna sådana uppgifter med hänvisning till ett viktigt allmänintresse enligt denna rätt.

(3) Kommissionens behandling omfattar följande:

a) Autentisering av nationella backendservrar, baserat på certifikat för nationella backendservrar.

b) Mottagande av de uppgifter som avses i artikel 7a.3 i genomförandebeslutet och som laddas upp av nationella backendservrar genom tillhandahållande av ett programmeringsgränssnitt som möjliggör att nationella backendservrar kan ladda upp de relevanta uppgifterna.

c) Lagring av uppgifterna i den samordnade nätslussen, när de tas emot från nationella backendservrar.

d) Göra uppgifterna tillgängliga för nedladdning av nationella backendservrar.

e) Radering av uppgifterna när alla deltagande backendservrar har laddat ned dem eller 14 dagar efter mottagandet, beroende på vad som inträffar först.

f) När tillhandahållandet av tjänsten har avslutats, radering av alla kvarvarande uppgifter såvida inte lagring av personuppgifterna krävs enligt unionsrätten eller medlemsstaternas nationella rätt.

Personuppgiftsbiträdet ska vidta de åtgärder som krävs för att bevara de behandlade uppgifternas integritet.

(4) Vidta alla förstklassiga organisatoriska, fysiska och logiska säkerhetsåtgärder som krävs för att upprätthålla den samordnade nätslussen. Kommissionen ska därför göra följande:

a) Utse en enhet som ansvarar för den samordnade nätslussens säkerhetsförvaltning, meddela de personuppgiftsansvariga enhetens kontaktuppgifter och säkerställa att den kan hantera säkerhetshot.

b) Ansvara för den samordnade nätslussens säkerhet.

c) Säkerställa att alla personer som beviljas tillgång till den samordnade nätslussen omfattas av avtalsenlig, yrkesmässig eller lagstadgad tystnadsplikt.

(5) Vidta alla nödvändiga säkerhetsåtgärder så att de nationella backendservrarna fungerar smidigt. Kommissionen ska därför införa särskilda förfaranden för anslutning från backendservrarna till den samordnade nätslussen. Detta omfattar följande:

a) Ett riskbedömningsförfarande, för att identifiera och utvärdera potentiella hot mot systemet.

b) Ett revisions- och granskningsförfarande för att

i) kontrollera sambandet mellan de genomförda säkerhetsåtgärderna och den tillämpliga säkerhetspolitiken,

ii) regelbundet kontrollera systemfilernas, säkerhetsparametrarnas och de beviljade tillståndens integritet,

iii) övervaka att säkerhetsöverträdelser och intrång upptäcks,

iv) genomföra ändringar för att minska befintliga säkerhetsbrister,

v) möjliggöra, även på begäran av personuppgiftsansvariga, och bidra till oberoende revisioner, inbegripet inspektioner, och översyner av säkerhetsåtgärder, på villkor som följer protokoll nr 7 till EUF-fördraget om Europeiska unionens immunitet och privilegier ([2]),

([2]) Protokoll nr 7 om Europeiska unionens immunitet och privilegier (EUT C 326, 26.10.2012, s. 266).

c) ändra kontrollförfarandet för att dokumentera och mäta effekten av en ändring innan den genomförs och hålla de personuppgiftsansvariga informerade om samtliga ändringar som kan påverka kommunikationen med och/eller säkerheten i deras infrastrukturer,

d) inrätta ett underhålls- och reparationsförfarande för att fastställa de regler och villkor som ska följas vid underhåll och/eller reparation av utrustning, och

e) inrätta ett förfarande för it-incidenter för att fastställa ett rapporterings- och eskaleringssystem, omedelbart informera de personuppgiftsansvariga samt Europeiska datatillsynsmannen om personuppgiftsincidenter och fastställa ett disciplinärt förfarande för att åtgärda dessa.

(6) Vidta förstklassiga fysiska och/eller logiska säkerhetsåtgärder för de anläggningar där utrustningen för den samordnade nätslussen finns och för kontroller av tillgången till logiska data och säkerhet. Kommissionen ska därför göra följande:

a) Införa fysiska säkerhetsåtgärder för att upprätta tydliga säkerhetsperimetrar och möjliggöra att överträdelser upptäcks.

b) Kontrollera tillträdet till anläggningar och upprätthålla ett besöksregister för spårning.

c) Säkerställa att externa personer som beviljas tillträde till lokaler åtföljs av vederbörligen bemyndigad personal.

d) Säkerställa att utrustning inte kan läggas till, ersättas eller avlägsnas utan förhandstillstånd från utsedda ansvariga organ.

e) Kontrollera åtkomst från och till de nationella backendservrarna till den samordnade nätslussen.

f) Säkerställa att personer som får tillgång till den samordnade nätslussen identifieras och autentiseras.

g) Se över de tillståndsrättigheter som gäller tillgång till den samordnade nätslussen vid säkerhetsöverträdelser som påverkar denna infrastruktur.

h) Bevara integriteten hos den information som överförs via den samordnade nätslussen.

i) Vidta tekniska och organisatoriska säkerhetsåtgärder för att förhindra obehörigt tillträde till personuppgifter.

j) Vid behov vidta åtgärder för att blockera obehörig tillgång till den samordnade nätslussen från de nationella myndigheternas domän (dvs. blockera en plats/en IP-adress).

(7) Vidta åtgärder för att skydda sin domän, inklusive genom frånkoppling, vid betydande avvikelser från principerna och koncepten för kvalitet eller säkerhet.

(8) Upprätthålla en riskhanteringsplan för sitt ansvarsområde.

(9) Övervaka – i realtid – prestandan för alla tjänstekomponenter i sina tjänster i den samordnade nätslussen, ta fram regelbunden statistik och upprätthålla register.

(10) Ge stöd för alla tjänster i den samordnade nätslussen dygnet runt och året runt på engelska via telefon, e-post eller webbportalen och godta samtal från godkända personer som ringer upp: samordnare vid den samordnade nätslussen och deras respektive helpdeskar, projektledare och utsedda personer från kommissionen.

(11) Bistå de personuppgiftsansvariga med lämpliga tekniska och organisatoriska åtgärder, när detta är möjligt, i syfte att fullgöra den personuppgiftsansvariges skyldigheter att besvara begäran om utövande av den registrerades rättigheter enligt kapitel III i den allmänna dataskyddsförordningen.

(12) Stödja de personuppgiftsansvariga genom att tillhandahålla information om den samordnade nätslussen, i syfte att fullgöra sina skyldigheter enligt artiklarna 32, 35 och 36 i den allmänna dataskyddsförordningen.

(13) Säkerställa att de uppgifter som behandlas i den samordnade nätslussen är oläsbara för personer som inte är behöriga att få tillgång till den.

(14) Vidta alla relevanta åtgärder för att förhindra att den samordnade nätslussens operatörer får obehörig tillgång till överförda uppgifter.

(15) Vidta åtgärder för att underlätta interoperabiliteten och kommunikationen mellan den samordnade nätslussens utsedda personuppgiftsansvariga.

(16) Föra ett register över behandling som utförts för de personuppgiftsansvarigas räkning i enlighet med artikel 31.2 i förordning (EU) 2018/1725.”