RÅDET FOR DEN EUROPÆISKE UNION

Bruxelles, den 28. april 2004 (06.05)
(OR. en)

8958/04

CRIMORG 36
TELECOM 82

FØLGESKRIVELSE

fra:	Den Franske Republik, Irland, Kongeriget Sverige og Det Forenede Kongerige
modtaget den:	28. april 2004
til:	Javier SOLANA, generalsekretær/højtstående repræsentant
Vedr.:	Udkast til rammeafgørelse om opbevaring af data, der behandles og lagres i forbindelse med levering af offentligt tilgængelige elektroniske kommunikationstjenester, og af data, der findes i offentlige kommunikationsnet, med henblik på at forebygge, efterforske, afsløre og strafforfølge kriminalitet og strafbare handlinger, herunder terrorisme

Hr. generalsekretær,

I medfør af artikel 31, stk. 1, litra c), og artikel 34, stk. 2, litra b), i traktaten om Den Europæiske Union fremsendes hermed et forslag fra Den Franske Republik, Irland, Kongeriget Sverige og Det Forenede Kongerige med henblik på Rådets vedtagelse af en rammeafgørelse om opbevaring af data, der behandles og lagres i forbindelse med levering af offentligt tilgængelige elektroniske kommunikationstjenester, og af data, der findes i offentlige kommunikationsnet, med henblik på at forebygge, efterforske, afsløre og strafforfølge kriminalitet og strafbare handlinger, herunder terrorisme.

Vi ville være Dem meget taknemmelig, hvis De i medfør af artikel 17 i Rådets forretningsorden vil sørge for, at dette initiativ offentliggøres i EU-Tidende og sendes til Europa-Parlamentet med henblik på udtalelse.

(Høflighedsformel).

Sign.:

Pierre SELLAL
Fast repræsentant
for Frankrig

Anne ANDERSON
Fast repræsentant
for Irland

Sven-Olof PETERSSON
Fast repræsentant
for Sverige

John GRANT
Fast repræsentant
for Det Forenede Kongerige

Udkast til rammeafgørelse

om opbevaring af data, der behandles og lagres i forbindelse med levering af offentligt tilgængelige elektroniske kommunikationstjenester, og af data, der findes i offentlige kommunikationsnet, med henblik på at forebygge, efterforske, afsløre og retsforfølge kriminalitet og strafbare handlinger, herunder terrorisme

RÅDET FOR DEN EUROPÆISKE UNION HAR -

under henvisning til traktaten om Den Europæiske Union, særlig artikel 31, stk. 1, litra c), og artikel 34, stk. 2, litra b),

under henvisning til initiativ fra Den Franske Republik, Irland, Kongeriget Sverige og Det Forenede Kongerige,

under henvisning til udtalelse fra Europa-Parlamentet, og

ud fra følgende betragtninger:

1. For at der kan ydes et højt beskyttelsesniveau i et område med frihed, sikkerhed og retfærdighed, må kriminalitet og strafbare handlinger forebygges, efterforskes, afsløres og strafforfølges på en hensigtsmæssig måde.

2. Rådets og Kommissionens handlingsplan for, hvorledes Amsterdam-traktatens bestemmelser om indførelse af et område med frihed, sikkerhed og retfærdighed bedst kan gennemføres, konklusionerne fra Det Europæiske Råds møde i Tammerfors den 15.-16. oktober 1999, konklusionerne fra Det Europæiske Råds møde i Santa Maria da Feira den 19.-20. juni 2000, Kommissionens resultattavle og Europa-Parlamentets beslutning af 19. maj 2000 efterlyser alle en indsats på området højteknologikriminalitet.

3. Rådets konklusioner af 20. september 2001 opfordrer til at drage omsorg for, at de retshåndhævende myndigheder har mulighed for at efterforske kriminelle handlinger, hvori der indgår anvendelse af elektroniske kommunikationssystemer, og træffe foranstaltninger mod gerningsmændene, samtidig med at balancen mellem beskyttelse af personoplysninger og de retshåndhævende myndigheders behov for adgang til oplysninger, der skal anvendes i kriminalefterforskningen, sikres. Rådet bemærker i sine konklusioner af 19. december 2002, at den betydelige vækst i de muligheder, der ligger i elektronisk kommunikation, har medført, at data vedrørende anvendelsen af elektronisk kommunikation i dag udgør et særdeles vigtigt og brugbart redskab i forebyggelse, efterforskning, afsløring og strafforfølgning af kriminalitet og strafbare handlinger, især organiseret kriminalitet og terrorisme.

4. Erklæringen om bekæmpelse af terrorisme, som Det Europæiske Råd vedtog den 25. marts 2004, pålægger Rådet at behandle foranstaltninger vedrørende opstilling af regler for tjenesteudbyderes lagring af kommunikationsdata med henblik på vedtagelse inden juni 2005.

5. Det er vigtigt at opbevare data i de offentlige kommunikationsnet, som frembringes i forbindelse med en kommunikation, i det følgende benævnt "data", med henblik på at forebygge, efterforske, afsløre og strafforfølge kriminalitet og strafbare handlinger, der involverer anvendelse af elektroniske kommunikationssystemer. Denne rammeafgørelse vedrører udelukkende data, der frembringes i forbindelse med en kommunikation, og vedrører ikke oplysninger, der udgør selve kommunikationens indhold. Det er navnlig nødvendigt at opbevare data for at kunne spore kilden til et ulovligt indhold såsom børnepornografi og racistisk og fremmedfjendsk materiale og kilden til angreb på informationssystemerne, og for at kunne finde frem til dem, der anvender de elektroniske kommunikationsnet til organiseret kriminalitet og terrorisme.

6. Det er for at tilgodese disse krav ikke tilstrækkeligt blot at gemme specifikke data vedrørende bestemte personer i konkrete tilfælde. I forbindelse med en efterforskning er det måske først muligt at se, hvilke data der er nødvendige, eller hvem der er involveret, mange måneder eller år efter den oprindelige kommunikation. Det er derfor nødvendigt at opbevare visse typer data, der allerede er behandlet og lagret med henblik på fakturering eller i kommercielt eller andet legitimt øjemed, i en vis yderligere periode for at tage højde for, at der kan blive brug for dem i en fremtidig kriminalefterforskning eller retssag. Denne rammeafgørelse vedrører derfor opbevaring af data og ikke gemning af data.

7. I erkendelse af, hvor vigtigt det er at opbevare data, åbner artikel 15 i direktiv 2002/58/EF mulighed for at vedtage retsforskrifter, der under visse omstændigheder tillader lagring af data med henblik på at forebygge, efterforske, afsløre og strafforfølge kriminalitet og strafbare handlinger. Denne rammeafgørelse vedrører ikke andre formål, der er omhandlet i nævnte direktivs artikel 15, og indeholder derfor ikke regler for opbevaring af data af hensyn til den nationale sikkerhed (dvs. statens sikkerhed), forsvaret, eller den offentlige sikkerhed. Den omfatter heller ikke uautoriseret brug af det elektroniske kommunikationssystem, når en sådan brug ikke udgør en strafbar handling.

8. Mange medlemsstater har vedtaget love om forhåndsopbevaring af data med henblik på forebyggelse, efterforskning, afsløring og strafforfølgning af kriminalitet og strafbare handlinger. I andre medlemsstater er der lovgivning undervejs på dette område. Indholdet af denne lovgivning varierer betydeligt fra medlemsstat til medlemsstat.

9. Forskellene mellem medlemsstaternes lovgivning hæmmer samarbejdet mellem de kompetente myndigheder om forebyggelse, efterforskning, afsløring og strafforfølgning af kriminalitet og strafbare handlinger. For at sikre et effektivt politisamarbejde og retligt samarbejde i kriminalsager er det derfor nødvendigt at sikre, at alle medlemsstater træffer de nødvendige foranstaltninger med henblik på opbevaring af visse typer data i en vis periode under iagttagelse af nærmere angivne parametre for at forebygge, efterforske, afsløre og strafforfølge kriminalitet og strafbare handlinger, herunder terrorisme. Disse data bør være tilgængelige for de øvrige medlemsstater i overensstemmelse med de instrumenter vedrørende retligt samarbejde i kriminalsager, der er vedtaget i henhold til afsnit VI i traktaten om Den Europæiske Union. Sidestillet med sådanne instrumenter bør være instrumenter, der ikke er vedtaget i henhold til nævnte afsnit, men som medlemsstaterne har tiltrådt, og som der henvises til i de instrumenter vedrørende retligt samarbejde i kriminalsager, der er vedtaget i henhold til afsnit VI i traktaten om Den Europæiske Union.

10. En sådan forhåndsopbevaring af data og adgangen til sådanne data vil kunne udgøre et indgreb i privatlivets fred. Et sådant indgreb krænker imidlertid ikke de internationale regler for retten til respekt for privatlivets fred og for behandling af personoplysninger, som findes i bl.a. den europæiske menneskerettighedskonvention af 4. november 1950, Europarådets konvention nr. 108 af 28. januar 1981 om beskyttelse af personer i forbindelse med automatiseret behandling af persondata og direktiverne 95/46/EF, 97/66/EF og 2002/58/EF, for så vidt indgrebet er hjemlet ved lov, og for så vidt det er passende, står i åbenbart rimeligt forhold til det mål, der forfølges, og er nødvendigt i et demokratisk samfund for at forebygge, efterforske, afsløre og strafforfølge kriminalitet og strafbare handlinger, herunder terrorisme, samt i øvrigt er omfattet af passende beskyttelsesordninger.

11. Der bør fastsættes parametre for forhåndsopbevaring af data, der tager hensyn til såvel behovet for at sikre, at data forhåndsopbevares på en effektiv og ensartet måde, som behovet for at give medlemsstaterne tilstrækkeligt råderum, så de kan foretage deres egne individuelle vurderinger i betragtning af forskellene mellem strafferetssystemerne.

12. Data kan forhåndsopbevares i perioder af forskellig længde afhængigt af type. Opbevaringstiden for de enkelte typer data vil være afhængig af, hvor nyttige dataene er i forbindelse med forebyggelse, efterforskning, afsløring og strafforfølgning af kriminalitet og strafbare handlinger, og hvor store omkostningerne forbundet med at opbevare dem er. Opbevaringstiden skal være rimelig ud fra en afvejning af behovet for sådanne data med henblik på forebyggelse, efterforskning, afsløring og strafforfølgning af kriminalitet og strafbare handlinger og det indgreb i privatlivets fred, som en sådan opbevaring vil indebære i forbindelse med videregivelse af de opbevarede data.

13. Ved opstillingen af eventuelle fortegnelser over de typer data, der skal opbevares, skal der være en passende balance mellem den nytteværdi for forebyggelsen, efterforskningen, afsløringen og strafforfølgningen af kriminalitet og strafbare handlinger, der er forbundet med at opbevare de enkelte typer data og omfanget af det indgreb i privatlivets fred, som opbevaringen vil medføre.

14. Denne rammeafgørelse finder ikke anvendelse på adgang til data på transmissionstidspunktet, dvs. i forbindelse med overvågning, aflytning eller optagelse af telekommunikation.

15. Medlemsstaterne skal sikre, at der ved adgangen til de opbevarede data tages hensyn til de regler for privatlivets fred, der er fastlagt i international lov om beskyttelse af personoplysninger.

16. Medlemsstaterne skal sikre, at denne rammeafgørelse gennemføres i relevant samråd med den berørte sektor -

VEDTAGET FØLGENDE RAMMEAFGØRELSE:

Artikel 1

Anvendelsesområde og formål

1. Denne rammeafgørelse har til formål at lette det retlige samarbejde i kriminalsager gennem en indbyrdes tilnærmelse af medlemsstaternes lovgivning om opbevaring af data, der behandles og lagres af leverandører af offentligt tilgængelige elektroniske kommunikationstjenester eller et offentligt kommunikationsnet, med henblik på at forebygge, efterforske, afsløre og strafforfølge kriminalitet og strafbare handlinger, herunder terrorisme.

2. Denne rammeafgørelse finder ikke anvendelse på selve indholdet af en kommunikation, herunder informationer, der søges gennem et elektronisk kommunikationsnet, for så vidt dette er fastsat i national lovgivning.

3. En medlemsstat kan beslutte ikke at anvende stk. 1, når formålet med at opbevare data, der behandles og lagres, er forebyggelse af kriminalitet og strafbare handlinger, såfremt den ikke finder dette formål acceptabelt efter nationale procedurer eller høringer. En medlemsstat, der på et givet tidspunkt beslutter at gøre brug af denne undtagelse, skal underrette Rådet og Kommissionen om sin beslutning.

4. Denne rammeafgørelse berører ikke:

   – regler, der finder anvendelse på retligt samarbejde i kriminalsager for så vidt angår aflytning og optagelse af telekommunikation

   – aktiviteter, der vedrører den offentlige sikkerhed, forsvaret eller den nationale sikkerhed (dvs. statens sikkerhed)

   – nationale regler for opbevaring af de typer data, som leverandørerne af kommunikationstjenester ikke lagrer i forretningsmæssigt øjemed.

Artikel 2

Definitioner

1. I denne rammeafgørelse forstås ved:

   a) "data": trafikdata og lokaliseringsdata som omhandlet i artikel 2 i direktiv 2002/58/EF samt de oplysninger om abonnenter og brugere, der er knyttet til sådanne data

   b) "brugeroplysninger": oplysninger om fysiske personer, som anvender en offentligt tilgængelig elektronisk kommunikationstjeneste i privat eller forretningsmæssigt øjemed uden nødvendigvis at abonnere på den pågældende tjeneste

   c) "abonnentsoplysninger": oplysninger om fysiske personer, som abonnerer på en offentligt tilgængelig elektronisk kommunikationstjeneste i privat eller forretningsmæssigt øjemed uden nødvendigvis at anvende den pågældende tjeneste.

2. Med henblik på anvendelsen af denne rammeafgørelse omfatter data:

   a) data, der er nødvendige for at spore og identificere en kommunikations oprindelse, herunder personoplysninger, adresseoplysninger og oplysninger, der viser, hvilke tjenester der abonneres på

   b) data, der er nødvendige for at fastslå en kommunikations rutning og bestemmelsessted

   c) data, der er nødvendige for at fastslå tidspunkt og dato for en kommunikation samt kommunikationens varighed

   d) data, der er nødvendige for at bestemme den berørte telekommunikation

e) data, der er nødvendige for at bestemme kommunikationsudstyret eller det, der fremtræder som værende udstyret

f) data, der er nødvendige for at foretage en lokalisering ved kommunikationens begyndelse og under hele dens varighed.

3. Disse data omfatter data, der frembringes af tjenester, der leveres inden for rammerne af følgende kommunikationsinfrastrukturer, -arkitekturer og -protokoller:

a) telefoni, dog ikke sms, elektroniske medietjenester og multimediemeddelelsestjenester

b) sms, elektroniske medietjenester og multimediemeddelelsestjenester, der leveres som led i en telefonitjeneste

c) internet-protokoller, herunder e-mail, voice over IP, WWW, FTP, NNTP, HTTP, voice over bredbånd samt undersæt af IP-numre - NAT-data.

4. Fremtidig teknologisk udvikling, der gør det lettere at overføre kommunikation, falder ind under denne rammeafgørelses anvendelsesområde.

Artikel 3

Opbevaring af data

Hver medlemsstat træffer de nødvendige foranstaltninger til at sikre, at data, der behandles og lagres af leverandører af et offentligt kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester, herunder abonnentsoplysninger og brugeroplysninger, der er knyttet til sådanne data opbevares i overensstemmelse med denne rammeafgørelse, med henblik på retligt samarbejde i kriminalsager.

Artikel 4

Dataopbevaringstid

1. Hver medlemsstat træffer de nødvendige foranstaltninger til at sikre, at data opbevares i mindst 12 måneder og højst 36 måneder efter frembringelsen. Medlemsstaterne kan fastsætte en længere dataopbevaringstid efter nationale kriterier, hvis en sådan opbevaring er nødvendig, passende og forholdsmæssig i et demokratisk samfund.

2. En medlemsstat kan beslutte at fravige stk. 1 for så vidt angår de i artikel 2, stk. 2, omhandlede typer data i forbindelse med de kommunikationsmetoder, der er nævnt i artikel 2, stk. 3, litra b) og c), såfremt den ikke finder de i stk. 1 fastsatte opbevaringstider acceptable efter nationale procedurer eller høringer. En medlemsstat, der på et givet tidspunkt beslutter at gøre brug af denne undtagelse, skal underrette Rådet og Kommissionen om sin beslutning og oplyse de alternative opbevaringstider, der fastsættes for de berørte typer data. Enhver sådan fravigelse tages op til revision hvert år.

Artikel 5

Adgang til data med henblik på retligt samarbejde i kriminalsager

Anmodninger fra en medlemsstat til en anden om adgang til de i artikel 2 omhandlede data fremsættes og besvares i overensstemmelse med de instrumenter vedrørende retligt samarbejde i kriminalsager, der er vedtaget i henhold til afsnit VI i traktaten om Den Europæiske Union. Den anmodede medlemsstat kan stille de samme betingelser for at give sit samtykke til en sådan anmodning om dataadgang, som den ville stille i en tilsvarende national sag.

Artikel 6

Databeskyttelse

Hver medlemsstat sikrer, at data, der opbevares i medfør af denne rammeafgørelse, som et minimum er underlagt nedennævnte databeskyttelsesprincipper, og sørger for adgang til retsmidler i overensstemmelse med kapitel III om retsmidler, ansvar og sanktioner i direktiv 95/46/EF:

a) der skal være adgang til dataene for kompetente myndigheder fra sag til sag til udtrykkeligt angivne legitime formål i overensstemmelse med national lovgivning, og dataene må ikke behandles videre på en måde, som er uforenelig med disse formål

b) dataene skal være hensigtsmæssige og relevante og må ikke være mere omfattende end krævet til opfyldelse af de formål, der begrunder adgangen til dem. Dataene skal behandles rimeligt og lovligt

c) data, som kompetente myndigheder får adgang til, skal opbevares på en måde, der ikke giver mulighed for at identificere de personer, dataene vedrører, længere end det er nødvendigt af hensyn til de formål, som lå til grund for indsamlingen af dataene, eller som ligger til grund for en videre behandling

d) dataenes fortrolighed og integritet skal sikres

e) data, der gives adgang til, skal være korrekte, og der skal tages ethvert rimeligt skridt til at sikre, at personoplysninger, der er urigtige i forhold til det formål, som lå til grund for indsamlingen af dataene, eller som ligger til grund for en videre behandling, slettes eller berigtiges.

Artikel 7

Datasikkerhed

Hver medlemsstat sikrer, at data, der opbevares i medfør af denne rammeafgørelse, som et minimum er underlagt nedennævnte datasikkerhedsprincipper, idet der tages hensyn til artikel 4 i direktiv 2002/58/EF:

a) de opbevarede data skal være af samme kvalitet som dem, der findes på nettet

b) dataene skal være omfattet af de fornødne tekniske og organisatoriske foranstaltninger, så de er beskyttet mod hændelig eller ulovlig tilintetgørelse eller mod hændeligt tab, mod forringelse, ubeføjet udbredelse eller ikke-autoriseret adgang samt mod enhver anden form for ulovlig behandling

c) samtlige data skal tilintetgøres ved udløbet af opbevaringstiden, bortset fra data, der har været givet adgang til, og som er blevet gemt

d) hver medlemsstat fastsætter i sin nationale lovgivning den fremgangsmåde, der skal følges for at få adgang til opbevarede data og for at gemme data, der har været givet adgang til.

Artikel 8

Gennemførelse

Medlemsstaterne træffer de nødvendige foranstaltninger til at efterkomme denne rammeafgørelse [inden den ... juni 2007] [senest to år efter vedtagelsesdatoen].

Medlemsstaterne meddeler inden samme dato Generalsekretariatet for Rådet og Kommissionen teksten til de retsforskrifter, som de udsteder for at gennemføre de forpligtelser, der følger af denne rammeafgørelse, i national ret. Generalsekretariatet for Rådet meddeler medlemsstaterne de oplysninger, det modtager i medfør af denne artikel.

Kommissionen forelægger inden [den ….1. januar 2008] Rådet en rapport, der undersøger, om medlemsstaterne har truffet de nødvendige foranstaltninger til at efterkomme denne rammeafgørelse.

Artikel 9

Ikrafttræden

Denne rammeafgørelse træder i kraft på tyvendedagen efter offentliggørelsen i Den Europæiske Unions Tidende.

Udfærdiget i Bruxelles,

_____