RÅDET FOR DEN EUROPÆISKE UNION

Bruxelles, den 20. november 2008 (21.11) (OR. fr)

15899/08

Interinstitutionel sag: 2007/0248 (COD)

TELECOM 203
MI 460
COMPET 490
DATAPROTECT 94
CONSOM 182
CODEC 1582

RAPPORT

fra:	Coreper
til:	Rådet
Komm. forsl. nr.:	15387/07 TELECOM 151 MI 298 COMPET 392 DATAPROTECT 50 CONSOM 133 CODEC 1297 15422/08 TELECOM 186 MI 427 COMPET 456 DATAPROTECT 88 CONSOM 170 CODEC 1507
Tidl. dok. nr.:	15106/08 TELECOM 177 MI 415 COMPET 439 DATAPROTECT 81 CONSOM 165 CODEC 1471
Vedr.:	Revurdering af EU's regelsæt for elektroniske kommunikationsnet og -tjenester: Forslag til Europa-Parlamentets og Rådets direktiv om ændring af direktiv 2002/22/EF om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester, direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor og forordning (EF) nr. 2006/2004 om forbrugerbeskyttelsessamarbejde – Politisk enighed

I. INDLEDNING

1. Kommissionen vedtog den 13. november 2007 sine lovgivningsforslag, der består af to ændringsdirektiver og en forordning, vedrørende revurdering af EU's regelsæt for elektroniske kommunikationsnet og -tjenester. Denne rapport vedrører det direktiv, der er kendt som direktivet om borgernes rettigheder, og den del, der ændrer det nuværende direktiv 2002/58/EF om e-databeskyttelse. Den del, der ændrer direktiv 2002/22/EF om forsyningspligt, vil blive behandlet i en særskilt rapport (dok. 15896/08).

2. Et af de centrale mål for rammelovgivningen er at fremme EU-borgernes interesser, bl.a. ved at sikre effektiv beskyttelse af persondata og privatlivets fred og sikre, at de offentlige kommunikationsnets integritet og sikkerhed bevares. Det stigende antal nye elektroniske trusler i de senere år som f.eks. virus, spam, spyware og phishing har givet dette formål øget vægt.

   Kommissionens forslag til e-databeskyttelsesdirektiv behandler spørgsmål som sikkerhed for, at forbrugerne informeres, hvis deres persondata er blevet kompromitteret som følge af sikkerhedsbrud på nettene, øget ansvar til operatører og nationale sikkerhedsmyndigheder for alle elektroniske kommunikationsnets og -tjenesters sikkerhed og integritet, udvidelse af de kompetente myndigheders gennemførelses- og håndhævelsesbeføjelser til bl.a. at bekæmpe spam og tydeliggørelse af EU-reglernes anvendelse på dataindsamlings- og identifikationsudstyr, der benytter offentlige elektroniske kommunikationsnet.

3. Drøftelserne under de slovenske formandskab mundede ud i en statusrapport, som der blev udvekslet synspunkter om den 12. juni 2008. Forslaget er blevet drøftet mere indgående under de franske formandskab, bl.a. på baggrund af Europa-Parlamentets førstebehandlingsudtalelse, der blev vedtaget den 24. september 2008.

4. Kommissionen vedtog den 6. november 2008 sit ændrede forslag på baggrund af Europa-Parlamentets førstebehandling (15422/08).

5. Det Europæiske Økonomiske og Sociale Udvalg vedtog sin udtalelse den 29. maj 2008, og Regionsudvalget vedtog sin udtalelse den 19. juni 2008.

II. RESULTATET AF COREPERS DRØFTELSER

1. Teksten til formandskabets kompromisforslag vedrørende e-databeskyttelsesdirektivet findes i bilaget til dette dokument. Teksten er en konsolideret udgave af forslaget til ændringsdirektiv på grundlag af resultatet af drøftelserne i Coreper den 14. november 2008. Coreper er nået til bred konsensus om teksten.

2. Kun én delegation tager fortsat forbehold med hensyn til teksten til artikel 6, stk. 6a, vedrørende behandlingen af trafikdata (s. 14).

3. Samtlige delegationer tager sprogligt forbehold med hensyn til teksten, og Kommissionen har forbeholdt sig sin samlede stilling til formandskabets kompromisforslag.

III. RÅDETS OPGAVE

Rådet anmodes derfor om at behandle de fortsat udestående spørgsmål med henblik på at nå til politisk enighed. Teksten sendes til jurist-lingvisterne til gennemgang med henblik på vedtagelsen af Rådets fælles holdning.

FORMANDSKABETS KOMPROMISFORSLAG TIL

KONSOLIDERET UDGAVE AF FORSLAG TIL ÆNDRING AF DIREKTIV 2002/58/EF

(databeskyttelsesdirektivet)

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR -

under henvisning til traktaten om oprettelse af Det Europæiske Fællesskab, særlig artikel 95,

under henvisning til forslag fra Kommissionen,

under henvisning til udtalelse fra Det Økonomiske og Sociale Udvalg,

efter høring af Regionsudvalget,

i henhold til fremgangsmåden i traktatens artikel 251, og

ud fra følgende betragtninger:

[med hensyn til betragtninger, der er fælles for dette direktiv og forsyningspligtdirektivet, se forsyningspligtdirektivet]

(27) Liberaliseringen af markederne for elektroniske kommunikationsnet og -tjenester og den hurtige teknologiske udvikling har tilsammen sat skub i konkurrencen og den økonomiske vækst og har resulteret i en mangfoldighed af tjenester, som slutbrugerne kan få adgang til via offentlige elektroniske kommunikationsnet. Der er behov for at sikre, at forbrugerne og brugerne ydes samme grad af privatlivs- og persondatabeskyttelse, uanset hvilken teknologi der benyttes til at levere en given tjenesteydelse.

(30b) Ved gennemførelsen af foranstaltninger til gennemførelse af direktiv 2002/58/EF bør medlemsstaternes myndigheder og domstole ikke kun fortolke deres nationale lovgivning på en måde, der er forenelig med ovennævnte direktiv, men også sikre, at de ikke lægger en fortolkning af dette direktiv til grund, som er i strid med andre grundlæggende rettigheder eller almindelige fællesskabsretlige principper, såsom proportionalitetsprincippet.

[med hensyn til de øvrige betragtninger, se de relevante artikler]–

UDSTEDT FØLGENDE DIREKTIV:

Artikel 1

Anvendelsesområde og formål

1. Dette direktiv tager sigte på en harmonisering af medlemsstaternes bestemmelser, der er nødvendig for at sikre et ensartet niveau i beskyttelsen af de grundlæggende rettigheder og frihedsrettigheder og navnlig privatlivets fred i forbindelse med behandling af personoplysninger inden for den elektroniske kommunikationssektor, og for at sikre fri omsætning af sådanne oplysninger og af elektronisk kommunikationsudstyr og elektroniske kommunikationstjenester i Fællesskabet.

2. Med henblik på at nå de i stk. 1 omhandlede mål specificerer og supplerer dette direktivs bestemmelser direktiv 95/46/EF. Nærværende bestemmelser beskytter desuden legitime interesser hos abonnenter, der er juridiske personer.

3. Dette direktiv gælder ikke for aktiviteter, der ikke er omfattet af traktaten om oprettelse af Det Europæiske Fællesskab, som f.eks. de aktiviteter, der er omfattet af afsnit V og VI i traktaten om Den Europæiske Union, og under ingen omstændigheder for aktiviteter, der vedrører den offentlige sikkerhed, forsvaret, statens sikkerhed (herunder statens økonomiske interesser, når disse aktiviteter er forbundet med spørgsmål vedrørende statens sikkerhed) og statens aktiviteter på det strafferetlige område.

Artikel 2

Definitioner

Medmindre andet angives, gælder i dette direktiv de definitioner, der er fastsat i direktiv 95/46/EF og i direktiv 2002/21/EF **[…]** om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet).

I dette direktiv forstås endvidere ved:

a) "bruger": en fysisk person, som anvender en offentligt tilgængelig elektronisk kommunikationstjeneste i privat eller forretningsmæssigt øjemed, uden nødvendigvis at abonnere på den pågældende tjeneste

b) "trafikdata": data, som behandles med henblik på overføring af kommunikation i et elektronisk kommunikationsnet eller debitering heraf

c) "lokaliseringsdata": data, som behandles i et elektronisk kommunikationsnet **eller af en elektronisk kommunikationstjeneste** og angiver den geografiske placering af det terminaludstyr, som brugeren af en offentligt tilgængelig elektronisk kommunikationstjeneste anvender

d) "kommunikation": oplysninger, som udveksles eller overføres mellem et begrænset antal parter via en offentligt tilgængelig elektronisk kommunikationstjeneste. Dette omfatter ikke oplysninger, der overføres som del af en radio- og fjernsynstransmissionstjeneste til offentligheden via et elektronisk kommunikationsnet, medmindre oplysningerne kan kædes sammen med en identificerbar abonnent eller bruger, der modtager oplysningerne

e) flyttet til rammedirektivet

f) "samtykke": givet af bruger eller abonnent svarer til den registreredes samtykke i direktiv 95/46/EF

g) "værdiforøgende tjeneste": enhver form for tjeneste, der kræver behandling af trafik- eller lokaliseringsdata, bortset fra trafikdata, ud over hvad der er nødvendigt for overføring af en kommunikation eller debitering heraf

h) "elektronisk post": enhver meddelelse i form af tekst, stemmegengivelse, lyd eller billede, som sendes via et offentligt kommunikationsnet, og som kan lagres i nettet eller i modtagerens terminaludstyr, indtil meddelelsen hentes af modtageren

i) "brud på persondatasikkerheden": et sikkerhedsbrud, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, ubeføjet videregivelse af eller adgang til persondata, der sendes, lagres eller på anden måde behandles i forbindelse med udbuddet af offentligt tilgængelige kommunikationstjenester i Fællesskabet.

Artikel 3

Omfattede tjenester

Dette direktiv finder anvendelse på behandling af persondata i forbindelse med, at offentligt tilgængelige elektroniske kommunikationstjenester stilles til rådighed via offentlige kommunikationsnet i Fællesskabet, **herunder offentlige kommunikationsnet med dataindsamlings- og identifikationsudstyr**.

2. Udgår.

3. Udgår.

(27a ny) Dette direktiv fokuserer i tråd med målsætningen for EU's regelsæt for elektronisk kommunikation, proportionalitetsprincippet og subsidiaritetsprincippet og med henblik på retlig sikkerhed og effektivitet for såvel det europæiske erhvervsliv som de nationale tilsynsmyndigheder på offentligt tilgængelige elektroniske kommunikationsnet eller -tjenester, og det gælder ikke for lukkede brugergrupper og virksomhedsnet.

*(28) De teknologiske fremskridt gør det muligt at udvikle nye applikationer, som bygger på apparater til dataindsamling og identifikation, herunder kontaktfrie apparater, der fungerer ved hjælp af radiofrekvenser. Eksempelvis benyttes der i radiofrekvensbaseret identifikation (RFID) radiofrekvenser til at opfange data fra entydigt identitetsmærkede brikker, og disse data kan derpå overføres gennem de eksisterende kommunikationsnet. Hvis sådanne teknologier får stor udbredelse, kan de give et stort økonomisk og samfundsmæssigt udbytte og dermed yde et væsentligt bidrag til det indre marked, hvis borgerne kan acceptere, at de bruges. For at opnå en sådan accept er det nødvendigt at sørge for, at **alle** det enkelte menneskes grundlæggende rettigheder beskyttes, herunder[...] retten til privatlivets fred og til beskyttelse af persondata. Når sådanne anordninger forbindes med offentligt tilgængelige elektroniske kommunikationsnet eller indgår som grundlæggende infrastruktur i elektroniske kommunikationstjenester, bør de relevante bestemmelser i direktiv 2002/58/EF, herunder bestemmelserne om sikkerhed, trafikdata og lokaliseringsdata samt om kommunikationshemmelighed, finde anvendelse.*

Artikel 4

Sikkerhed i forbindelse med behandlingen

1. Udbyderen af en offentligt tilgængelig kommunikationstjeneste skal træffe passende tekniske og organisatoriske foranstaltninger for at beskytte sine tjenester, for netsikkerhedens vedkommende om nødvendigt sammen med udbyderen af det offentlige kommunikationsnet. Under hensyn til teknologiens stade og omkostningerne i forbindelse med gennemførelsen skal disse foranstaltninger garantere et sikkerhedsniveau, der står i forhold til risikoen.

2. Hvor der er særlig risiko for brud på netsikkerheden, skal udbyderen af en offentligt tilgængelig kommunikationstjeneste informere abonnenterne herom samt, hvis risikoen ligger uden for de foranstaltninger, der skal træffes af udbyderen, om, hvorledes sådanne brud i givet fald kan forebygges, herunder angive de omkostninger, der sandsynligvis vil være forbundet hermed.

3. Hvis der sker et brud på persondatasikkerheden […] […] skal den berørte udbyder af offentligt tilgængelige kommunikationstjenester [...] vurdere omfanget af bruddet på persondatasikkerheden, bedømme, hvor alvorligt det er, og overveje, om det er nødvendigt at underrette den kompetente nationale myndighed og den berørte abonnent om bruddet under hensyntagen til de relevante regler fastsat af den kompetente nationale myndighed i overensstemmelse med stk. 3a.

Når bruddet på persondatasikkerheden udgør en alvorlig risiko for privatlivets fred for abonnenten, underretter den berørte udbyder af offentligt tilgængelige kommunikationstjenester den kompetente nationale myndighed og den berørte abonnent om et sådant brud uden unødig forsinkelse.

Underretningen af abonnenten skal mindst indeholde en beskrivelse af karakteren af bruddet på persondatasikkerheden og omhandle de kontaktpunkter, hvor der kan indhentes flere oplysninger, og den skal indeholde anbefalinger af, hvordan de mulige negative virkninger af bruddet på persondatasikkerheden kan afbødes. Underretningen til den kompetente nationale [...]myndighed skal derudover beskrive følgerne af bruddet, og hvilke modforholdsregler udbyderen har foreslået eller truffet for at håndtere bruddet på persondatasikkerheden.

(28b) Udbyderen af en offentligt tilgængelig elektronisk kommunikationstjeneste bør træffe passende tekniske og organisatoriske foranstaltninger for at sikre beskyttelse af sine tjenester. Uden at dette berører direktiv 95/46/EF, bør sådanne foranstaltninger sikre, at kun autoriserede personer kan få adgang til personoplysninger til lovlige formål, og at såvel lagrede eller sendte personoplysninger som nettet og tjenesterne er beskyttede. Desuden bør der indføres en sikkerhedspolitik for behandling af personoplysninger med henblik på at identificere svage punkter i systemet og foretages regelmæssig overvågning samt træffes forebyggende, korrigerende og afbødende foranstaltninger.

(28c) De kompetente nationale myndigheder bør overvåge de trufne foranstaltninger og videreformidle bedste praksis blandt udbydere af offentligt tilgængelige elektroniske kommunikationstjenester.

(29) Brud på sikkerheden, der fører til tab eller beskadigelse af persondata om den enkelte abonnent kan medføre store økonomiske tab og sociale skader, herunder identitetsmisbrug, hvis ikke de afhjælpes hurtigt og på betryggende vis. ***Så snart udbyderen af en offentligt tilgængelig kommunikationstjeneste bliver opmærksom på, at der er sket et sådant sikkerhedsbrud, skal udbyderen*** *derfor* ***vurdere den risiko, der er forbundet hermed, f.eks. ved at fastslå, hvilken type data der er berørt af bruddet (herunder disse datas følsomhed, den nærmere sammenhæng og de trufne sikkerhedsforanstaltninger), årsagen til og omfanget af sikkerhedsbruddet, antallet af berørte abonnenter og mulige skader for abonnenterne på grund af bruddet (f.eks. identitetstyveri, økonomisk tab, tab af erhvervs- eller beskæftigelsesmuligheder, fysisk skade).*** *Abonnenter, der kommer ud for [...] sikkerhedshændelser,* ***der kan påføre dem en alvorlig risiko for privatlivets fred (f.eks. identitetstyveri eller identitetsmisbrug, fysisk skade, betydelig tort eller skade af omdømme)*** *bør straks underrettes* ***[...]****, så de kan træffe de nødvendige forholdsregler. Underretningen bør indeholde oplysninger om, hvilke foranstaltninger udbyderen har sat i værk for at afhjælpe bruddet på sikkerheden, og anbefalinger til de berørte brugere.* ***Underretning af en abonnent om et brud på sikkerheden bør ikke kræves, hvis udbyderen over for den kompetente myndighed har godtgjort, at den har implementeret passende teknologiske beskyttelsesforanstaltninger og disse foranstaltninger er blevet anvendt på de data, som sikkerhedsbruddet vedrørte. Sådanne teknologiske beskyttelsesforanstaltninger skal gøre dataene uforståelige for alle, der ikke må få adgang til disse data.***

(30) De nationale tilsynsmyndigheder bør bl.a. fremme EU-borgernes interesser ved at bidrage til sikringen af et højt beskyttelsesniveau for persondata og privatlivets fred. Det forudsætter, at de har de nødvendige ressourcer til at varetage deres opgaver, herunder at de råder over omfattende og pålidelige data om faktiske sikkerhedshændelser, der har medført beskadigelse af persondata om enkeltpersoner.

3a. Medlemsstaterne sikrer, at den kompetente nationale myndighed kan fastsætte nærmere regler for, og hvis det er nødvendigt, give instrukser om, under hvilke omstændigheder udbyderen af offentligt tilgængelige elektroniske kommunikationstjenester skal give underretning om brud på persondatasikkerheden, samt hvilke former og procedurer, der skal anvendes ved underretningen.

4. For at sikre en ensartet gennemførelse af de foranstaltninger, der er anført i stk. 1, 2, 3 og 3a, kan Kommissionen efter at have hørt [...] Det Europæiske Agentur for Net- og Informationssikkerhed, Artikel 29-Gruppen og den europæiske tilsynsførende for databeskyttelse vedtage […] anbefalinger om, bl.a. under hvilke omstændigheder informations- og underretningskravene i denne artikel gælder, samt hvilke former og procedurer der skal anvendes.

[...]

(31) Der bør gives hjemmel til ***[...]****,* ***at Kommissionen kan vedtage anbefalinger med hensyn til, hvorledes*** *der kan opnås fyldestgørende beskyttelse af privatlivet og af transmitterede eller behandlede persondata i forbindelse med brugen af elektroniske kommunikationsnet på det indre marked.*

(32) Når der fastsættes nærmere regler for, hvilket format og hvilke procedurer der skal anvendes ved underretningen om ***[...]*** *brud* ***på persondatasikkerheden****, bør der tages hensyn til omstændighederne omkring sikkerhedsbruddet, herunder til om de pågældende persondata var beskyttet ved kryptering eller på en anden måde, der effektivt begrænser sandsynligheden af identitetsmisbrug eller andre former for misbrug. Sådanne regler og procedurer bør desuden tage hensyn til de retshåndhævende myndigheders legitime interesser i tilfælde, hvor en åben redegørelse på et tidligt tidspunkt kunne udgøre en unødvendig hæmsko for efterforskningen af omstændighederne ved et sikkerhedsbrud.*

Betragtning 33 udgår.

Artikel 5

Kommunikationshemmelighed

1. Medlemsstaterne sikrer kommunikationshemmeligheden ved brug af offentlige kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester, både for så vidt angår selve kommunikationen og de dermed forbundne trafikdata, via nationale forskrifter. De forbyder især aflytning, registrering, lagring og andre måder, hvorpå samtaler kan opfanges eller overvåges af andre end brugerne, uden at de pågældende brugere har indvilget heri, bortset fra tilfælde, hvor det er tilladt ifølge lovgivningen, jf. artikel 15, stk. 1. Dette stykke er ikke til hinder for teknisk lagring, som er nødvendig for overføring af en kommunikation, forudsat at princippet om kommunikationshemmelighed ikke berøres heraf.

2. Stk. 1 vedrører ikke lovmedholdelig registrering af kommunikation og de dermed forbundne trafikdata, hvis den foretages som led i lovlig forretningspraksis med henblik på at kunne forelægge bevis for en handelstransaktion eller enhver anden forretningsmæssig kommunikation.

3. Medlemsstaterne sikrer, at […] **lagring af** oplysninger eller […] adgang til oplysninger, der **allerede** er lagret i en abonnents eller brugers terminaludstyr, kun er tilladt på betingelse af, at abonnenten eller brugeren får klare og fyldestgørende oplysninger, bl.a. om formålet med behandlingen i overensstemmelse med direktiv 95/46/EF og ret til at nægte den registeransvarlige en sådan behandling. Dette er ikke til hinder for teknisk lagring eller adgang til oplysninger, hvis det alene sker med det formål at overføre eller lette overføring af kommunikation via et elektronisk kommunikationsnet eller er absolut påkrævet for at levere en informationssamfundstjeneste, abonnenten eller brugeren udtrykkelig ønsker.

(34) Programmer, der til fordel for en tredjepart i det skjulte overvåger en brugers handlinger og/eller hindrer brugerens terminaludstyr i at fungere efter hensigten (såkaldt spionsoftware), udgør en alvorlig trussel mod privatlivets fred for brugerne. Det er nødvendigt at sikre et højt og ensartet beskyttelsesniveau for brugernes privatsfære, uanset om brugeren downloader de uønskede spionprogrammer via elektroniske kommunikationsnet uden at være klar over det, eller om de leveres og installeres skjult i programmer, der distribueres på andre eksterne datalagringsmedier som f.eks. cd'er, cd-rom'er eller usb-nøgler. ***Medlemsstaterne bør opfordre slutbrugerne til at træffe de fornødne foranstaltninger til at beskytte deres terminaludstyr mod virus og spyware.***

Artikel 6

Trafikdata

1. Trafikdata vedrørende abonnenter og brugere, som behandles og lagres af udbyderen af et offentligt kommunikationsnet eller en offentligt tilgængelig elektronisk kommunikationstjeneste, skal slettes eller gøres anonyme, når de ikke længere er nødvendige for fremføringen af kommunikationen, jf. dog stk. 2, 3, [...] 5 **og 6a**, samt artikel 15, stk.1.

2. Med henblik på debitering af abonnenten og afregning for samtrafik er det tilladt at behandle trafikdata. En sådan behandling er tilladt indtil udløbet af den lovbestemte forældelsesfrist for sådanne gældsforpligtelser eller fristen for anfægtelse af sådanne afregninger.

3. Med henblik på markedsføring af elektroniske kommunikationstjenester eller levering af værdiforøgende tjenester er det tilladt udbyderen af en offentligt tilgængelig elektronisk kommunikationstjeneste at behandle de i stk. 1 omtalte oplysninger i det omfang og tidsrum, som sådanne tjenester eller markedsføringen kræver, hvis den abonnent eller bruger, som oplysningerne vedrører, **forudgående** har givet sit samtykke hertil. Brugeren eller abonnenten skal på et hvilket som helst tidspunkt have mulighed for at trække sit samtykke til behandling af trafikdata tilbage.

4. Tjenesteudbyderen underretter abonnenten eller brugeren om, hvilke typer trafikdata der behandles med henblik på det i stk. 2 omhandlede formål og om behandlingens varighed; ved behandling med henblik på det i stk. 3 omhandlede formål skal underretning ske, inden samtykke indhentes.

5. Behandling af trafikdata i henhold til stk. 1, 2, 3 og 4 må kun foretages af personer, som handler efter bemyndigelse fra udbydere af de offentligt tilgængelige kommunikationsnet og -tjenester, og som er beskæftiget med debitering eller trafikstyring, kundeforespørgsler, afsløring af svig, markedsføring af elektroniske kommunikationstjenester eller levering af en værdiforøgende tjeneste, og skal begrænses til det for sådanne aktiviteter nødvendige.

6. Stk. 1, 2, 3 og 5 berører ikke de kompetente organers mulighed for i overensstemmelse med gældende lovgivning at indhente oplysninger om trafikdata med henblik på bilæggelse af tvister, navnlig vedrørende samtrafik eller debitering.

6a. [...] Trafikdata kan behandles, [...] i det omfang det er strengt nødvendigt for at [...] garantere net- og informationssikkerheden som defineret i artikel 4, litra c, i Europa-Parlamentets og Rådets forordning (EF) nr. 460/2004 af 10. marts 2004 om oprettelse af et europæisk agentur for net- og informationssikkerhed [...].[1]

(26a) Behandling af trafikdata vil, i det omfang det er strengt nødvendigt for at detektere, lokalisere og afhjælpe fejl og fejlfunktioner i netværket, og til informationssikkerhedsformål til sikring af tilgængeligheden, autenticiteten, integriteten og fortroligheden af lagrede og videresendte oplysninger [...] bidrage til at forhindre uautoriseret adgang og skadelig distribution af koder, [...] denial of service-angreb og beskadigelser af computere og elektroniske kommunikationssystemer. [...]

---

1 DE tager forbehold med hensyn til stk. 6a.

Artikel 7

Specificerede regninger

1. Abonnenter har ret til at modtage uspecificerede forbrugsopgørelser.

2. Medlemsstaterne skal anvende nationale retsforskrifter for at sikre, at der ikke er modstrid mellem abonnenternes ret til at modtage specificerede forbrugsopgørelser og kaldende brugeres og kaldte abonnenters ret til privatlivets fred, f.eks. ved at sikre, at brugere og abonnenter råder over tilstrækkelige alternative kommunikations- eller betalingsmuligheder, der styrker beskyttelsen af privatlivets fred.

Artikel 8

Visning af A-nummer og af tilsluttet nummer samt begrænsning heraf

1. Hvor der er adgang til visning af A-nummer, skal tjenesteudbyderen tilbyde den kaldende bruger mulighed for i forbindelse med hvert enkelt opkald ved hjælp af en simpel, gebyrfri anordning at forhindre, at hans abonnentsnummer fremsendes til A-nummervisning. Den kaldende abonnent skal have denne mulighed på hver enkelt linje.

2. Hvor der er adgang til visning af A-nummer, skal tjenesteudbyderen tilbyde den kaldte abonnent mulighed for ved hjælp af en simpel anordning, der er gebyrfri ved rimelig anvendelse heraf, at forhindre visning af A-nummeret ved ankommende opkald.

3. Hvor der er adgang til visning af A-nummer, og A-nummeret vises inden tilslutningen, skal tjenesteudbyderen tilbyde den kaldte abonnent mulighed for ved hjælp af en simpel anordning at afvise ankommende opkald, når den kaldende bruger eller abonnent har blokeret visningen af A-nummeret.

4. Hvor der er adgang til visning af tilsluttet nummer, skal tjenesteudbyderen tilbyde den kaldte abonnent mulighed for ved hjælp af en simpel, gebyrfri anordning at forhindre, at den kaldende bruger får vist det tilsluttede nummer.

5. Stk. 1 finder også anvendelse på opkald fra Fællesskabet til lande uden for dette. Stk. 2, 3 og 4 finder også anvendelse på ankommende opkald fra tredjelande.

6. Medlemsstaterne sikrer, at udbyderne af offentligt tilgængelige elektroniske kommunikationstjenester, når der er adgang til visning af A-nummer og/eller tilsluttet nummer, informerer offentligheden herom og om mulighederne i stk. 1, 2, 3 og 4.

Artikel 9

Lokaliseringsdata, bortset fra trafikdata

1. Hvis lokaliseringsdata, bortset fra trafikdata, vedrørende brugere af eller abonnenter på de offentlige kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester, kan behandles, må disse data kun behandles, når de er gjort anonyme, eller når brugeren eller abonnenten har givet sit samtykke hertil, og da kun i det omfang og i det tidsrum, som er nødvendigt for levering af en værdiforøgende tjeneste. Tjenesteudbyderen skal, inden brugernes eller abonnenternes samtykke indhentes, underrette dem om, hvilken type lokaliseringsdata, bortset fra trafikdata, der behandles, hvorfor og hvor længe de behandles, og om de videregives til en tredjemand med henblik på levering af den værdiforøgende tjeneste. Brugere eller abonnenter skal have mulighed for til enhver tid at trække deres samtykke til behandling af lokaliseringsdata, bortset fra trafikdata, tilbage.

2. Hvis brugeren eller abonnenten har givet sit samtykke til behandling af lokaliseringsdata, bortset fra trafikdata, skal brugeren eller abonnenten fortsat have mulighed for ved hjælp af en simpel, gebyrfri anordning midlertidigt at forhindre behandling af sådanne data ved hvert enkelt opkald til nettet eller ved hver enkelt fremføring af kommunikation.

3. Behandling af lokaliseringsdata, bortset fra trafikdata, i henhold til stk. 1 og 2 må kun foretages af personer, som handler efter bemyndigelse fra udbyderen af det offentlige kommunikationsnetværk eller den offentligt tilgængelige elektroniske kommunikationstjeneste eller fra den tredjemand, som leverer den værdiforøgende tjeneste, og skal begrænses til det for leveringen af den værdiforøgende tjeneste nødvendige.

Artikel 10

Undtagelsesbestemmelser

Medlemsstaterne sikrer, at der er gennemskuelige procedurer for den måde, hvorpå udbyderen af et offentligt kommunikationsnet og/eller en offentligt tilgængelig elektronisk kommunikationstjeneste kan:

a) suspendere blokeringen af A-nummervisningen midlertidigt, når en abonnent anmoder om at få chikaneopkald eller andre generende opkald eftersporet; i så tilfælde skal de data, hvorved den kaldende abonnent identificeres, i overensstemmelse med national lovgivning opbevares og stilles til rådighed af udbyderen af et offentligt kommunikationsnet og/eller en offentligt tilgængelig elektronisk kommunikationstjeneste

b) suspendere blokering af visningen af tilsluttet nummer eller se bort fra, at en abonnent eller bruger har nægtet eller ikke har givet sit samtykke til, at lokaliseringsdata behandles for specifikke linjer med henblik på at give organisationer, der tager sig af nødopkald og er godkendte som sådanne af en medlemsstat, herunder retshåndhævende myndigheder, ambulancetjenester og brandvæsener, mulighed for at reagere på sådanne opkald.

Artikel 11

Automatisk viderestilling

Medlemsstaterne sikrer, at enhver abonnent har mulighed for ved hjælp af en simpel, gebyrfri anordning at forhindre en tredjemand i at foretage automatisk viderestilling til abonnentens terminal.

Artikel 12

Abonnentfortegnelser

1. Medlemsstaterne sikrer, at abonnenterne gebyrfrit, og inden de medtages i fortegnelsen, underrettes om formålet med en trykt eller elektronisk abonnentfortegnelse, som er offentligt tilgængelig eller kan benyttes via oplysningstjenester, og hvori personoplysninger om abonnenterne kan medtages, og at de underrettes om andre anvendelsesmuligheder heraf på grundlag af søgefunktioner, som er indbygget i elektroniske udgaver af fortegnelsen.

2. Medlemsstaterne sikrer, at abonnenterne får mulighed for at bestemme, om deres personoplysninger skal medtages i en offentlig fortegnelse, og i så fald hvilke, for så vidt sådanne oplysninger er relevante for formålet med fortegnelsen som angivet af udbyderen af fortegnelsen, samt mulighed for at kontrollere, få rettet eller slettet sådanne oplysninger. Det skal være gebyrfrit ikke at være medtaget i en offentlig abonnentfortegnelse og at få kontrolleret, rettet, eller slettet personoplysninger i den.

3. Medlemsstaterne kan kræve, at abonnenter skal anmodes om supplerende samtykke til, at en offentlig fortegnelse anvendes til ethvert formål, der går ud over søgning efter adresseoplysninger om personer på grundlag af deres navn og eventuelt et minimum af andre identifikatorer.

4. Stk. 1 og 2 finder anvendelse på abonnenter, der er fysiske personer. Medlemsstaterne sikrer endvidere inden for rammerne af gældende fællesskabsret og national lovgivning, at de legitime interesser for abonnenter, der ikke er fysiske personer, nyder tilstrækkelig beskyttelse for så vidt angår deres optagelse i offentlige abonnentfortegnelser.

Artikel 13

Uanmodet kommunikation

1. Anvendelse af automatiserede opkaldsanordninger uden menneskelige indgreb (automatisk opkaldsmaskine), telefaxapparater (fax) eller elektronisk post **(herunder sms- og mms-tjenester)** med henblik på direkte markedsføring kan **kun** tillades over for abonnenter **eller brugere**, som forudgående har givet deres samtykke hertil.

2. Uanset stk. 1 kan en fysisk eller juridisk person, hvis denne fra sine kunder modtager deres egne elektroniske adresseoplysninger vedrørende elektronisk post i forbindelse med salg af et produkt eller en tjenesteydelse i overensstemmelse med direktiv 95/46/EF, anvende disse elektroniske adresseoplysninger til direkte markedsføring af sine egne tilsvarende produkter eller tjenesteydelser, såfremt kunderne klart og utvetydigt har mulighed for let og gebyrfrit, at afvise en sådan anvendelse af de elektroniske adresseoplysninger, […] **på det tidspunkt, hvor adresseoplysningerne indsamles**, og ved hver meddelelse, såfremt kunden ikke fra begyndelsen afviste denne anvendelse.

3. Medlemsstaterne træffer de fornødne foranstaltninger for at sikre […], at uanmodet kommunikation, hvis formål er direkte markedsføring i andre tilfælde end dem, der er nævnt i stk. 1 og 2, ikke er tilladt, hverken i forhold til abonnenter **eller brugere**, som ikke har givet deres samtykke til at modtage sådan kommunikation, eller i forhold til abonnenter **eller brugere**, som har frabedt sig at modtage sådan kommunikation. Det afgøres i national lovgivning hvilken af de to muligheder der skal gælde **under hensyntagen til, at begge muligheder skal være gebyrfrie for abonnenten.**

4. Udsendelse af elektronisk post som led i direkte markedsføring, hvorved identiteten af den afsender, på hvis vegne meddelelsen sendes, tilsløres eller holdes skjult, **eller i strid med artikel 6 i direktiv 2000/31/EF** eller uden en adresse, som modtageren kan henvende sig til for at få standset sådanne henvendelser, er under alle omstændigheder forbudt.

5. Stk. 1 og 3 finder anvendelse på abonnenter, der er fysiske personer. Medlemsstaterne sikrer endvidere inden for rammerne af gældende fællesskabsret og national lovgivning, at de legitime interesser for abonnenter, der ikke er fysiske personer, nyder tilstrækkelig beskyttelse for så vidt angår uanmodet kommunikation.

6. Uden at indskrænke en eventuel administrativ klageadgang, som blandt andet kan indføres i medfør af artikel 15a, stk. 2, sikrer medlemsstaterne, at fysiske og juridiske personer […], der krænkes af overtrædelser af nationale bestemmelser i medfør af denne artikel og derfor har en legitim interesse i, at sådanne overtrædelser bringes til ophør eller forbydes, herunder en udbyder af elektroniske kommunikationstjenester, der vil beskytte sine legitime forretningsinteresser […], kan indbringe sådanne overtrædelser for domstolene. Medlemsstaterne kan også fastsætte særlige bestemmelser om sanktioner over for udbydere af elektroniske kommunikationstjenester, der ved deres [...] uagtsomhed bidrager til overtrædelser af nationale bestemmelser, der vedtages i henhold til denne artikel.

*(35) Udbyderne af elektroniske kommunikationstjenester må foretage store investeringer for at bekæmpe uønskede reklamehenvendelser ("spam"). Desuden har de bedre forudsætninger end slutbrugerne, fordi de har den viden og de ressourcer, der skal til for at detektere og identificere spammere. Udbydere af mailtjenester og andre tjenesteudbydere bør derfor have mulighed for at anlægge sag mod spammere **for sådanne overtrædelser** og således forsvare deres kunders interesser **[...] og dermed** deres egne legitime erhvervsinteresser.*

Artikel 14

Tekniske funktioner og standardisering

1 Ved gennemførelsen af bestemmelserne i dette direktiv drager medlemsstaterne omsorg for, at der ikke stilles bindende krav om, at terminaludstyr eller andet elektronisk kommunikationsudstyr skal indeholde specifikke funktioner, hvorved markedsføring af udstyr og den frie bevægelighed for sådant udstyr i medlemsstaterne og mellem disse hindres, jf. dog stk. 2 og 3.

2. I tilfælde, hvor bestemmelser i dette direktiv kun kan gennemføres ved et krav om specifikke tekniske funktioner i elektroniske kommunikationsnet, underretter medlemsstaterne Kommissionen herom efter proceduren i Europa-Parlamentets og Rådets direktiv 98/34/EF af 22. juni 1998 om en informationsprocedure med hensyn til tekniske standarder og forskrifter samt forskrifter for informationssamfundets tjenester.

3. Hvor der er behov herfor, kan der vedtages foranstaltninger for at sikre, at terminaludstyr fremstilles på en måde, der er forenelig med brugernes ret til at beskytte og kontrollere anvendelsen af deres personoplysninger i overensstemmelse med direktiv 1999/5/EF og Rådets beslutning 87/95/EØF af 22. december 1986 om standardisering inden for informationsteknologi og telekommunikation.

Artikel 14a

Udvalg

Udgår.

Artikel 15

Anvendelsesområdet for visse bestemmelser i direktiv 95/46/EF

1. Medlemsstaterne kan vedtage retsforskrifter med henblik på at indskrænke rækkevidden af de rettigheder og forpligtelser, der omhandles i artikel 5, artikel 6, artikel 8, stk. 1, 2, 3 og 4, og artikel 9, hvis en sådan indskrænkning er nødvendig, passende og forholdsmæssig i et demokratisk samfund af hensyn til den nationale sikkerhed (dvs. statens sikkerhed), forsvaret, den offentlige sikkerhed, eller forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller uautoriseret brug af det elektroniske kommunikationssystem efter artikel 13, stk. 1, i direktiv 95/46/EF. Med henblik herpå kan medlemsstaterne bl.a. vedtage retsforskrifter om lagring af data i en begrænset periode, som kan begrundes i et af de hensyn, der er nævnt i dette stykke. Alle i dette stykke omhandlede forskrifter skal være i overensstemmelse med fællesskabsrettens generelle principper, herunder principperne i EU-traktatens artikel 6, stk. 1 og 2.

1a. Stk. 1 finder ikke anvendelse på data, der udtrykkelig kræves lagret i henhold til Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet til det formål, der er omhandlet i nævnte direktivs artikel 1, stk. 1.

2. Bestemmelserne i direktiv 95/46/EF, kapitel III, "retsmidler, ansvar og sanktioner", finder anvendelse på nationale bestemmelser, der vedtages til nærværende direktivs gennemførelse, og på individuelle rettigheder afledt af nærværende direktiv.

3. Den gruppe vedrørende beskyttelse af personer i forbindelse med behandling af personoplysninger, som blev nedsat ved artikel 29 i direktiv 95/46/EF, varetager også de opgaver, der er fastsat i artikel 30 i direktiv 95/46/EF med hensyn til de af dette direktiv omfattede forhold, dvs. beskyttelse af grundlæggende rettigheder og frihedsrettigheder samt legitime interesser i den elektroniske kommunikationssektor.

Artikel 15a

Gennemførelse og håndhævelse

1. Medlemsstaterne fastsætter bestemmelser om sanktioner for overtrædelse af de nationale bestemmelser, der er vedtaget i medfør af dette direktiv, og træffer alle nødvendige foranstaltninger til at sikre gennemførelsen heraf. De sanktioner, der pålægges, skal være effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning, og kan anvendes i en periode svarende til overtrædelsens varighed, også selv om overtrædelsen i mellemtiden er bragt til ophør. Medlemsstaterne giver senest den <tidsfrist for gennemførelse af ændringsretsakten> Kommissionen meddelelse om disse sanktionsbestemmelser og giver omgående meddelelse om senere ændringer af betydning for dem.

2. […] Medlemsstaterne sikrer, at den […] kompetente nationale myndighed og, hvor det er relevant, andre nationale organer har beføjelse til at beordre overtrædelser som omhandlet i stk.1 bragt til ophør.

3. Medlemsstaterne sikrer, at […] kompetente nationale myndigheder, og, hvor det er relevant, andre nationale organer, har alle nødvendige beføjelser og ressourcer til efterforskning, herunder mulighed for at skaffe sig relevante oplysninger, som de måtte have brug for under overvågningen og håndhævelsen af nationale bestemmelser, der er vedtaget i medfør af dette direktiv.

4. For at sikre et effektivt samarbejde hen over grænserne om at håndhæve de nationale love, der vedtages i medfør af dette direktiv, og for at tilvejebringe harmoniserede vilkår for udbuddet af tjenester, der medfører datastrømme hen over grænserne, kan Kommissionen vedtage […] anbefalinger efter at have hørt [...] Det Europæiske Agentur for Net- og Informationssikkerhed, Artikel 29-Gruppen og de relevante tilsynsmyndigheder.

[...]

(36) Behovet for at sikre en fyldestgørende beskyttelse af privatlivet og af transmitterede eller behandlede persondata i forbindelse med brugen af elektroniske kommunikationsnet i Fællesskabet gør det nødvendigt at sikre, at reglerne kan gennemføres og håndhæves effektivt, således at der bliver tilstrækkelige incitamenter til at overholde dem. De ***kompetente*** *nationale* ***[...]****myndigheder* ***og, hvor det er hensigtsmæssigt, andre relevante nationale organer*** *bør have tilstrækkelige beføjelser og ressourcer til at efterforske tilfælde af manglende overholdelse effektivt og herunder have mulighed for at indhente de relevante informationer, de har behov for med henblik på at afgøre klagesager og idømme bøder, når reglerne ikke overholdes.*

(36a) Gennemførelse og håndhævelse af bestemmelserne i dette direktiv nødvendiggør ofte et samarbejde mellem de nationale tilsynsmyndigheder i to eller flere medlemsstater, f.eks. om bekæmpelse af spam og spyware hen over grænserne. For at sikre et gnidningsløst og hurtigt samarbejde i sådanne tilfælde bør der i anbefalingerne fastlægges procedurer med hensyn til f.eks. omfanget og formatet af de oplysninger, der udveksles mellem myndighederne, eller de frister, der skal overholdes. Sådanne procedurer vil også give mulighed for at harmonisere de deraf følgende forpligtelser for markedsaktørerne og dermed bidrage til etablering af lige konkurrencevilkår i Fællesskabet.

Artikel 16

Overgangsordninger

1. Artikel 12 finder ikke anvendelse på udgaver af abonnentfortegnelser, som allerede er fremstillet eller markedsført i trykt form eller i offline elektronisk form, inden de nationale bestemmelser, der vedtages i henhold til dette direktiv, træder i kraft.

2. Hvis personoplysninger om abonnenter på faste eller mobile offentlige taletelefonitjeneste er medtaget i en offentlig abonnentfortegnelse i overensstemmelse med direktiv 95/46/EF og artikel 11 i direktiv 97/66/EF, inden de nationale bestemmelser, der vedtages i henhold til dette direktiv, træder i kraft, kan personoplysninger om sådanne abonnenter fortsat medtages i denne offentlige fortegnelse i dens trykte eller elektroniske udgave, herunder udgaver med mulighed for "omvendt" søgning, medmindre abonnenter frabeder sig dette efter at have modtaget fuldstændige oplysninger om formålet og valgmulighederne i overensstemmelse med artikel 12 i dette direktiv.

[Artikel 4

Gennemførelse

Artikel 5

Ikrafttræden

Artikel 6

Adressater]

_____