EUROPA-KOMMISSIONEN

Bruxelles, den 18.4.2011
KOM(2011) 225 endelig

# BERETNING FRA KOMMISSIONEN TIL RÅDET OG EUROPA-PARLAMENTET

## Evalueringsrapport om datalagringsdirektivet (direktiv 2006/24/EF)

# BERETNING FRA KOMMISSIONEN TIL RÅDET OG EUROPA-PARLAMENTET

## Evalueringsrapport om datalagringsdirektivet (direktiv 2006/24/EF)

## 1. INDLEDNING

Ifølge datalagringsdirektivet[1], i det følgende benævnt "direktivet", skal medlemsstaterne pålægge udbydere af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet, i det følgende benævnt "operatører", at lagre trafikdata og lokaliseringsdata i en periode på seks måneder til to år med henblik på efterforskning, afsløring og retsforfølgning af grov kriminalitet.

I denne rapport fra Kommissionen foretages i medfør af artikel 14 i direktivet en evaluering af medlemsstaternes anvendelse af direktivet og af dets virkning på økonomiske aktører og forbrugere under hensyntagen til den videre udvikling, der er sket inden for elektronisk kommunikationsteknologi, og de statistiske oplysninger, der er sendt til Kommissionen, med henblik på at fastslå, om det er nødvendigt at ændre direktivets bestemmelser, særlig hvad angår datadækning og lagringsperioder. Der ses i rapporten også på direktivets konsekvenser for grundlæggende rettigheder i lyset af den kritik, der generelt er blevet rejst i forbindelse med datalagring, og det undersøges, om der er behov for foranstaltninger for at afhjælpe de problemer, der er forbundet med brugen af anonyme SIM-kort til kriminelle formål[2].

Overordnet set har evalueringen vist, at datalagring er et nyttigt værktøj for de strafferetlige systemer og for retshåndhævelsen i EU. Direktivets bidrag til en harmonisering af datalagring har været begrænset med hensyn til f.eks. formålsbegrænsning og lagringsperioder samt godtgørelse af operatørernes udgifter, som ligger uden for dets anvendelsesområde. I betragtning af følgerne og risiciene for det indre marked og respekten for retten til privatlivets fred og beskyttelse af personoplysninger bør EU ved hjælp af fælles regler fortsat sikre, at der konsekvent stilles høje krav til lagring, dataudtræk og brug af trafikdata og lokaliseringsdata. I lyset af disse konklusioner er det Kommissionens hensigt at foreslå ændringer af direktivet på grundlag af en konsekvensanalyse.

## 2. BAGGRUND FOR EVALUERINGEN

Denne evalueringsrapport bygger på omfattende drøftelser med og bidrag fra medlemsstater, eksperter og involverede parter.

---

1 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 og om ændring af direktiv 2002/58/EF, EUT L 105 af 13.4.2006, s. 54-63.

2 Rådets konklusioner om bekæmpelse af kriminel misbrug og kriminel anonym anvendelse af elektronisk kommunikation, 2908. samling i Rådet (retlige og indre anliggender) - Bruxelles, den 27.-28. november 2008.

I maj 2009 afholdt Kommissionen en konference som optakt til evalueringen af datalagringsdirektivet (Towards the Evaluation of the Data Retention Directive) med deltagelse af datatilsynsmyndigheder, den private sektor, civilsamfundet og akademiske kredse. I september 2009 sendte Kommissionen et spørgeskema til de involverede parter fra disse grupper, og den modtog ca. 70 besvarelser[3]. Kommissionen afholdt anden konference i december 2010 om datalagringsdirektivet (Taking on the Data Retention Directive), hvor et lignende uddrag af involverede parter deltog for at udveksle de foreløbige vurderinger af direktivet og drøfte kommende udfordringer på området.

Fra oktober 2009 til marts 2010 mødtes Kommissionen med repræsentanter fra alle medlemsstater og associerede EØS-lande for at se nærmere på de problemer, der var blevet rejst i spørgeskemaet vedrørende direktivets anvendelse. Medlemsstaterne begyndte at anvende direktivet senere end forventet, navnlig med hensyn til internetdata. Forsinkelser i gennemførelsen betød, at ni medlemsstater var i stand til at give Kommissionen alle de statistikker for enten 2008 eller 2009, der kræves i henhold til artikel 10 i direktivet, mens i alt 19 medlemsstater gav nogle statistikker (se afsnit 4.7). Kommissionen skrev til medlemsstaterne i juli 2010 og bad om yderligere kvantitative og kvalitative oplysninger vedrørende nødvendigheden af dataudtræk for at opnå resultater med retshåndhævelsen. Ti medlemsstater gav nærmere oplysninger om bestemte sager, hvor dataene havde været nødvendige[4].

Denne rapport bygger på de oplæg, der er blevet vedtaget af ekspertgruppen "Platform for Lagring af Elektroniske Data med henblik på Efterforskning, Afsløring og Retsforfølgning af Grov Kriminalitet", siden dens oprettelse i 2008[5]. Kommissionen har taget hensyn til rapporterne fra artikel 29-gruppen, Gruppe vedrørende Beskyttelse af Personer i forbindelse med Behandling af Personoplysninger[6], navnlig rapporten om den anden håndhævelsesforanstaltning, dvs. dens vurdering af medlemsstaternes efterlevelse af kravene til databeskyttelse og datasikkerhed i direktivet[7].

---

3 Svarene er offentliggjort på Kommissionens websted (http://ec.europa.eu/home-affairs/news/consulting_public/consulting_0008_en.htm

4 Belgien, Tjekkiet, Cypern, Litauen, Ungarn, Nederlandene, Polen, Slovenien og Det Forenede Kongerige. Sverige meddelte adskillige tilfælde af grov kriminalitet, hvor historiske trafikdata, som var til rådighed på trods af, at der ikke var nogen datalagringsforpligtelse, havde været afgørende for domsfældelsen.

5 Denne ekspertgruppe blev oprettet ved Kommissionens afgørelse 2008/324/EF, EUT L 111 af 23.4.2008, s. 11-14. Kommissionen har regelmæssigt holdt møder med gruppen. Dens oplæg findes på http://ec.europa.eu/justice_home/doc_centre/police/doc_police_intro_en.htm

6 Gruppen vedrørende Beskyttelse af Personer i forbindelse med Behandling af Personoplysninger, der er nedsat ved artikel 29 i databeskyttelsesdirektivet (Europa-Parlamentets og Rådets direktiv 95/46/EF af 24.10.1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger) (EUT L 281 af 23.11.1995, s. 31).

7 En rapport om telekommunikations- og internetudbyderes efterlevelse af forpligtelserne i national lovgivning om lagring af trafikdata: "Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive" (WP 172), 13.7.2010, findes på http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm

## 3. DATALAGRING I DEN EUROPÆISKE UNION

### 3.1. Datalagring med henblik på strafferetlig retsforfølgning og retshåndhævelse

Udbydere af telenet eller -tjenester, i det følgende benævnt "operatører", behandler som led i deres aktiviteter personoplysninger med henblik på fremføring af kommunikation, debitering af abonnenten, afregning for samtrafik, markedsføring og visse andre tillægstjenester. Sådanne operationer involverer data, der angiver kilde, bestemmelsessted, dato, klokkeslæt, varighed, kommunikationstype, samt brugernes kommunikationsudstyr og i tilfælde af mobiltelefoni data om lokalisering af udstyret. Ifølge direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor, i det følgende benævnt "e-data-direktivet"[8], skal sådanne trafikdata, som genereres ved brugen af elektroniske kommunikationstjenester, i princippet slettes eller gøres anonyme, når disse data ikke længere er nødvendige for fremføringen af kommunikation, medmindre de er nødvendige i debiteringsøjemed, og da kun i det tidsrum, der nødvendigt, eller hvis abonnenten eller brugeren har givet sit samtykke. Lokaliseringsdata kan kun behandles, hvis de er gjort anonyme, eller hvis den pågældende bruger har givet sit samtykke, i det omfang og i det tidsrum, som er nødvendigt for levering af en tillægstjeneste.

Forud for direktivets ikrafttrædelse kunne de nationale myndigheder på visse betingelser anmode operatørerne om adgang til sådanne data for f.eks. at identificere abonnenter, der benyttede en IP-adresse, for at undersøge tidligere kommunikationsaktiviteter og for at lokalisere en mobiltelefon.

På EU-plan blev lagring og brug af data til retshåndhævelsesformål først behandlet i direktiv 97/66/EF om behandling af personoplysninger og beskyttelse af privatlivets fred inden for telesektoren. Direktivet gav i første omgang medlemsstaterne mulighed for at vedtage de retsforskrifter, der er nødvendige til beskyttelse af statens sikkerhed, forsvaret eller den offentlige sikkerhed, herunder statens økonomiske interesser, når disse aktiviteter er forbundet med spørgsmål vedrørende statens sikkerhed, og statens aktiviteter på det strafferetlige område[9].

Denne bestemmelse blev yderligere udvidet i e-data-direktivet, som giver medlemsstaterne mulighed for at vedtage retsforskrifter, der afviger fra princippet om kommunikationshemmelighed, herunder på visse betingelser om lagring af, adgang til og brug af data til retshåndhævelsesformål. Ifølge artikel 15, stk. 1, kan medlemsstaterne indskrænke både retten til privatlivets fred og forpligtelser, herunder ved lagring af data i en begrænset periode, "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".

---

8 Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktivet om databeskyttelse inden for elektronisk kommunikation) (EFT L 201 af 31.7.2002, s. 37-47).

9 Artikel 14, stk. 1, i Europa-Parlamentets og Rådets direktiv 97/66/EF af 15. december 1997 om behandling af personoplysninger og beskyttelse af privatlivets fred inden for telesektoren (EFT L 24 af 30.1.1998, s. 1-8).

Datalagringens betydning for de strafferetlige systemer og retshåndhævelsen uddybes i afsnit 5.

### 3.2. Datalagringsdirektivets formål og retsgrundlag

Som følge af bestemmelserne i direktiv 97/66/EF og e-data-direktivet, som gør det muligt for medlemsstaterne at vedtage lovgivning om datalagring, blev operatører i nogle medlemsstater pålagt at købe datalagringsudstyr og ansætte personale til at udtrække data på vegne af de retshåndhævende myndigheder, mens det samme ikke gjorde sig gældende for operatører i andre medlemsstater, hvilket førte til forvridninger på det indre marked. Endvidere betød udviklingen i forretningsmodeller og tjenesteudbud, såsom væksten i enhedstakster samt forudbetalte og gratis elektroniske kommunikationstjenester, at operatører gradvist holdt op med at lagre trafik- og lokaliseringsdata til debiteringsformål, hvorved disse data ikke længere var til rådighed i samme udstrækning til strafferetlig retsforfølgning og retshåndhævelsesformål. Terrorangrebene i Madrid i 2004 og i London i 2005 betød, at det blev endnu vigtigere at finde ud af, hvordan man skulle håndtere disse spørgsmål på EU-plan.

På denne baggrund blev medlemsstaterne ved datalagringsdirektivet pålagt at forpligte udbydere af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske netværk til at lagre kommunikationsdata med henblik på efterforskning, afsløring og retsforfølgning af grov kriminalitet som defineret af de enkelte medlemsstater i deres nationale lovgivning, og der blev tilstræbt en harmonisering af visse relaterede emner på EU-plan.

Direktivet ændrede artikel 15, stk. 1, i e-data-direktivet ved at indsætte et stykke, ifølge hvilket nævnte artikel 15, stk. 1, ikke finder anvendelse på data, der kræves lagret i henhold til datalagringsdirektivet[10]. Medlemsstaterne kan derfor (som anført i betragtning 12 i direktivet) fortsat afvige fra princippet om kommunikationshemmelighed. Datalagringsdirektivet regulerer kun lagring af data med henblik på det mere afgrænsede formål at efterforske, afsløre og retsforfølge grove forbrydelser.

Dette komplekse juridiske forhold mellem direktivet og e-data-direktivet i kombination med en manglende definition i direktiverne af begrebet "grov kriminalitet" gør det vanskeligt at skelne mellem på den ene side de foranstaltninger, medlemsstaterne har truffet for at gennemføre forpligtelserne i datalagringsdirektivet, og på den anden side den mere generelle datalagringspraksis i medlemsstaterne, som muliggøres ved artikel 15, stk. 1, i e-data-direktivet[11]. Dette drøftes nærmere i afsnit 4.

Direktivet bygger på artikel 95 i traktaten om Det Europæiske Fællesskab (erstattet af artikel 114 i traktaten om Den Europæiske Unions funktionsmåde) om det indre markeds

---

[10] Det hedder i direktivets artikel 11: I artikel 15 i direktiv 2002/58/EF indsættes følgende stykke: "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 de formål, der er omhandlet i nævnte direktivs artikel 1, stk. 1."

[11] Artikel 29-gruppen sætter spørgsmålstegn ved, om tanken med [datalagrings]direktivet var at afvige fra den generelle forpligtelse til at slette trafikdata efter afslutning af den elektroniske kommunikation eller at tillade lagring af alle de data, som udbydere allerede havde lov til at lagre til egen "forretningsmæssig brug".

gennemførelse og funktion. Efter vedtagelsen af direktivet blev retsgrundlaget anfægtet ved EU-Domstolen ud fra den antagelse, at hovedformålet var efterforskning, afsløring og retsforfølgning af alvorlige forbrydelser. Domstolen fastslog, at direktivet regulerer de transaktioner, som foretages uafhængigt af iværksættelsen af et eventuelt politisamarbejde og retligt samarbejde i kriminalsager, og at det hverken harmoniserer den adgang, som tilkommer de kompetente nationale myndigheder, eller adgangen for dem til at anvende og indbyrdes udveksle disse data. Det blev derfor konkluderet, at direktivet hovedsageligt var rettet mod operatørernes aktiviteter i den relevante sektor af det indre marked. Retsgrundlaget blev derfor fastholdt[12].

### 3.3. Hastesikring af data

Datalagring adskiller sig fra hastesikring af data ved, at operatørerne i tilfælde af hastesikring af data i medfør af en retskendelse får pålæg om at lagre data, som kun vedrører specifikke personer, der er mistænkt for forbrydelser fra datoen for retskendelsen. Hastesikring af data er et af de efterforskningsværktøjer, som de stater, der deltager i Europarådets konvention om internetkriminalitet[13], påtænker at anvende eller anvender. Næsten alle af deltagende stater har etableret et kontaktpunkt, som har til opgave at sikre øjeblikkelig bistand i efterforskningen eller retsforfølgningen af internetkriminalitet. Det er dog ikke alle parter i konventionen, der har indført hastesikring af data, og der er endnu ikke foretaget en evaluering af, hvor effektiv modellen har været til at tackle internetkriminalitet[14]. På det seneste er der blevet udviklet en ny type hastesikring af data. Denne type går videre end den almindelige hastesikring, idet en dommer også kan give adgang til hastesikring af data, som endnu ikke er blevet slettet af operatører. Der ville endvidere i medfør af lovgivning være en meget begrænset fritagelse fra forpligtelsen til at slette visse kommunikationsdata, som normalt ikke lagres, for en kort periode, såsom lokaliseringsdata, internetforbindelsesdata og dynamiske IP-adresser for brugere, som har et abonnement med fast pris, og hvor der ikke er nogen grund til at lagre data til debiteringsformål.

Fortalere for hastesikring af data mener, at den tilsidesætter retten til privatlivets fred i mindre grad end datalagring. Mange medlemsstater er dog ikke enige i, at eventuelle varianter af hastesikring af data reelt kan erstatte datalagring, idet de hævder, at datalagring giver adgang til historiske data, mens hastesikring af data ikke giver nogen garanti for, at der kan etableres beviser forud for retskendelsen om hastesikring af data, at der kan foretages efterforskning, hvis et mål er ukendt, og at der kan indsamles bevis for f.eks. ofres eller vidners færden[15].

## 4. GENNEMFØRELSE AF DATALAGRINGSDIREKIVET I NATIONAL LOVGIVNING

Medlemsstaterne skulle gennemføre direktivet senest den 15. september 2007 med mulighed for at udsætte gennemførelsen af lagringsforpligtelserne vedrørende internetadgang, e-mail og telefoni via internettet til den 15. marts 2009.

---

12 Domstolens dom, sag C-301/6, Irland mod Europa-Parlamentet og Rådet, Sml. [2009] I, s. 593.

13 Artikel 16 i konventionen om internetkriminalitet (http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm) .

14 Kilde: Europarådet.

15 Dette blev også anerkendt af den tyske forfatningsdomstol i dens dom om annullering af den tyske lovgivning, der skulle gennemføre direktivet (se afsnit 4.9) (Bundesverfassungsgericht, 1 BvR 256/08 af 2. marts 2010, § 208).

Den følgende analyse bygger på de meddelelser om gennemførelsen, som Kommissionen har fået fra 25 medlemsstater, herunder fra Belgien, som kun delvis har gennemført direktivet i national lovgivning[16]. Østrig og Sverige drøfter stadig udkast til lovgivning. I disse to medlemsstater er der ingen forpligtelse til at lagre data, men retshåndhævelsesmyndigheder kan anmode om trafikdata fra operatører, i det omfang dataene findes. Efter den første meddelelse om gennemførelse fra Tjekkiet, Tyskland og Rumænien har deres respektive forfatningsdomstole annulleret den nationale lovgivning, som gennemfører direktivet[17], og landene overvejer nu, hvordan de så skal gennemføre direktivet.

I dette afsnit ses nærmere på, hvordan medlemsstaterne har gennemført de relevante bestemmelser i direktivet. Det undersøges også, om medlemsstaterne har valgt at godtgøre de udgifter, operatørerne har i forbindelse med lagring og udtræk af data, hvilket ikke fastlægges i direktivet, samt hvilken relevans den tyske, den rumænske og tjekkiske forfatningsdomstols afgørelse har for direktivet.

### 4.1. Datalagringens formålet (artikel 1)

Direktivet pålægger medlemsstaterne at træffe foranstaltninger til at sikre, at data lagres og stilles til rådighed i forbindelse med efterforskning, afsløring og retsforfølgning af grov kriminalitet som defineret af den enkelte medlemsstat i national lovgivning. Der er imidlertid stadig forskel på, hvilket formål der er anført med lagringen og/eller adgangen til data i den nationale lovgivning i EU. Ti medlemsstater (Bulgarien, Estland, Irland, Grækenland, Spanien, Litauen, Luxembourg, Ungarn, Nederlandene og Finland) har defineret "grov kriminalitet" under henvisning til minimumsfængselsstraffen, til muligheden for frihedsstraf eller til en liste over forbrydelser defineret andetsteds i national lovgivning. Otte medlemsstater (Belgien, Danmark, Frankrig, Italien, Letland, Polen, Slovakiet og Slovenien) kræver, at data lagres ikke blot med henblik på efterforskning, afsløring og retsforfølgning i forbindelse med grov kriminalitet, men også i forbindelse med alle andre strafbare handlinger og med henblik på forebyggelse af kriminalitet eller generelt af hensyn til den nationale/statens sikkerhed og/eller den offentlige sikkerhed. Lovgivningen i fire medlemsstater (Cypern, Malta, Portugal og Det Forenede Kongerige) henviser til "grov kriminalitet" eller "alvorlige forbrydelser" uden at definere det nærmere. De nærmere oplysninger fremgår af tabel 1.

---

16 De 25 medlemsstater, der har underrettet Kommissionen om gennemførelsen af direktivet, er: Belgien, Bulgarien, Tjekkiet, Danmark, Tyskland, Grækenland, Estland, Irland, Spanien, Frankrig, Italien, Cypern, Letland, Litauen, Luxembourg, Ungarn, Malta, Nederlandene, Polen, Portugal, Rumænien, Slovenien, Slovakiet, Finland og Det Forenede Kongerige. Belgien meddelte Kommissionen, at udkast til lovgivning, som fuldender gennemførelsen, stadig behandles af Parlamentet.

17 Den rumænske forfatningsdomstols afgørelse nr. 1258 af 8. oktober 2009, rumænske statstidende nr. 789 af 23. november 2009; den tyske forfatningsdomstols dom 1 BvR 256/08 af 2. marts 2010, tyske statstidende af 1. april 2011 og forfatningsdomstolens dom af 22. marts om bestemmelserne i artikel 97, stk. 3 og 4 i lov nr. 127/2005 sml. om elektronisk kommunikation og om ændring af visse relaterede love, som ændret, og dekret nr. 485/2005 sml. om datalagring og dataudlevering til kompetente myndigheder.

| Tabel 1: Formålsbegrænsning for datalagring i national lovgivning | |
|---|---|
| Belgien | Til efterforskning og retsforfølgning af strafbare handlinger, retsforfølgning af misbrug af nødopkaldsnumre, efterforskning af skadeligt misbrug af elektroniske kommunikationsnet eller –tjenester og til efterretningsindsamlingsmissioner foretaget af efterretnings- og sikkerhedstjenester[18]. |
| Bulgarien | Til afsløring og efterforskning af grov kriminalitet, jf. artikel 319a-319f i straffeloven, samt til eftersøgning af personer[19]. |
| Tjekkiet | Ikke gennemført. |
| Danmark | Til efterforskning og retsforfølgning af strafbare forhold[20]. |
| Tyskland | Ikke gennemført. |
| Estland | Kan anvendes, hvis indhentning af beviser i medfør af andre processuelle regler er udelukket eller meget kompliceret, og genstanden for en straffesag er en strafbar handling [i første grad eller en forsætlig strafbar handling i anden grad med en strafferamme på mindst tre års fængsel][21]. |
| Irland | Til forebyggelse af grov kriminalitet [dvs. forbrydelser, der straffes med en fængselsstraf på fem år eller mere, eller en forbrydelse opført i bilaget til gennemførelsesloven], til sikring af statens sikkerhed og redning af menneskeliv[22]. |
| Grækenland | Til afsløring af særlig grove forbrydelser[23]. |
| Spanien | Til afsløring, efterforskning og retsforfølgning af grov kriminalitet, jf. straffeloven eller specielle straffelove[24]. |
| Frankrig | Til afsløring, efterforskning og retsforfølgning af strafbare handlinger og til det ene formål at give retsmyndigheder de fornødne oplysninger og til forebyggelse af terrorhandlinger og til beskyttelse af intellektuel ejendom[25]. |
| Italien | Til afsløring og bekæmpelse af strafbare handlinger[26]. |
| Cypern | Til efterforskning af grov kriminalitet[27]. |
| Letland | Til beskyttelse af staten og den offentlige sikkerhed eller til efterforskning af strafbare handlinger, retsforfølgning og straffesager[28]. |
| Litauen | Til efterforskning, afsløring og retsforfølgning af grov og meget grov kriminalitet som defineret i den litauiske straffelov[29]. |
| Luxembourg | Til afsløring, efterforskning og retsforfølgning af strafbare handlinger, som medfører en fængselsstraf på et år eller mere[30]. |

18 Artikel 126, stk. 1, i lov af 13. juni 2005 om elektronisk kommunikation.

19 Artikel 250a, stk. 2, i lov om elektronisk kommunikation (ændret) 2010.

20 Artikel 1 i logningsbekendtgørelsen.

21 Artikel 110, stk. 1, i strafferetsplejeloven.

22 Artikel 6 i kommunikationsloven (datalagring) af 2011.

23 Sådanne forbrydelser er defineret i artikel 4 i lov 2225/1994; artikel 1 i lov 3917/2011.

24 Artikel 1, stk. 1, i lov 25/2007.

25 De love, der regulerer brugen af lagrede data henholdsvis for strafbare handlinger, for terrorforebyggelse og for beskyttelse af intellektuel ejendomsret, er følgende: artikel L.34-1(II) i lov om elektronisk kommunikation (CPCE), lov nr. 2006-64 af 23. januar 2006 og lov nr. 2009-669 af 12. juni 2009.

26 Artikel 132, stk. 1, i databeskyttelsesloven.

27 Artikel 4, stk. 1, i lov 183(I)/2007.

28 Artikel 71, stk. 1, i lov om elektronisk kommunikation.

29 Artikel 65 i lov X-1835.

30 Artikel 1, stk. 1, i lov af 24. juli 2010.

| Tabel 1: Formålsbegrænsning for datalagring i national lovgivning | |
|---|---|
| Ungarn | Til at sætte efterforskningsorganer, den offentlige anklager, domstolene og nationale sikkerhedsagenturer i stand til at udføre deres opgaver, og til at sætte det nationale told- og skattekontor i stand til at efterforske forsætlige forbrydelser, der medfører en fængselsstraf på to år eller mere[31]. |
| Malta | Til efterforskning, afsløring eller retsforfølgning af grov kriminalitet[32]. |
| Nederlandene | Til efterforskning og retsforfølgning af grov kriminalitet, som kan medføre fængselsstraf[33]. |
| Østrig | Ikke gennemført. |
| Polen | Til forebyggelse eller afsløring af strafbare handlinger, til forebyggelse og afsløring af skattesvig, til brug for anklagere og domstole, hvis det er relevant for en verserende sag, og til brug for sikkerheds- og efterretningstjenester, det centrale korruptionsbekæmpelseskontor samt militærets kontraspionagetjeneste og efterretningstjeneste[34]. |
| Portugal | Til efterforskning, afsløring og retsforfølgning af grov kriminalitet[35]. |
| Rumænien | Ikke gennemført. |
| Slovenien | Til sikring af national sikkerhed, forfatningsmæssig regulering og statens sikkerhedsmæssige, politiske og økonomiske interesser samt det nationale forsvar[36]. |
| Slovakiet | Til forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger[37]. |
| Finland | Til efterforskning, afsløring og retsforfølgning af grov kriminalitet, jf. kapitel 5a, artikel 3, stk. 1, i loven om tvangsmidler[38]. |
| Sverige | Ikke gennemført. |
| Det Forenede Kongerige | Til efterforskning, afsløring og retsforfølgning af grov kriminalitet[39]. |

De fleste medlemsstater, som har gennemført direktivet, tillader i den nationale lovgivning adgang til og anvendelse af lagrede data til formål, som går videre end formålene i direktivet, herunder forebyggelse og bekæmpelse af strafbare handlinger generelt og risici for liv og legeme. Selv om dette er tilladt i henhold til e-data-direktivet, har EU-lovgivningen på området kun medført en begrænset grad af harmonisering. Forskelle i formålene med datalagringen vil sandsynligvis påvirke mængden og hyppigheden af anmodninger og dermed de udgifter, der er forbundet med at opfylde forpligtelserne i direktivet. Endvidere giver denne situation måske ikke tilstrækkelig forudsigelighed, hvilket er et krav til enhver lovgivningsmæssig foranstaltning, som indskrænker retten til privatlivets fred[40].

---

31 Datalagrings formål generelt: artikel 159/A i lov C/2003, som ændret ved lov CLXXIV/2007; Politiets adgang: artikel 68 i lov XXXIV/1994; og det nationale told- og skattekontors adgang: artikel 59 i lov CXXII/2010.

32 Artikel 20, stk. 1, i anordning 198/2008.

33 Artikel 126 i strafferetsplejeloven.

34 Artikel 180a, i telekommunikationsloven af 16. juli 2004, som ændret ved artikel 1, lov af 24. april 2009.

35 Artikel 1 og artikel 3, stk. 1, i lov 32/2008.

36 Artikel 170a, stk. 1, i lov om elektronisk kommunikation.

37 Artikel 59a, stk. 6, i lov om elektronisk kommunikation.

38 Artikel 14a, stk. 1, i lov om elektronisk kommunikation.

39 Datalagringsreglerne (EF-direktiv) af 2009 (2009 nr. 859).

40 EU-Domstolens dom af 20. maj 2003 i forenede sager C-465/00, C-138/01 og C-139/01 (anmodning om en præjudiciel afgørelse fra Verfassungsgerichtshof og Oberster Gerichtshof): Rechnungshof (sag C-465/00) mod Österreichischer Rundfunk og andre og mellem Christa Neukomm (C-138/01), Joseph

Kommissionen vil se på behovet og mulighederne for at opnå større harmonisering på området[41].

### 4.2. Operatører har pligt til at lagre data (artikel 1)

Direktivet gælder for "udbydere af offentligt tilgængelige elektroniske kommunikationstjenester eller af et offentligt kommunikationsnet" (artikel 1, stk. 1). To medlemsstater (Finland og Det Forenede Kongerige) pålægger ikke små operatører at lagre data, fordi de hævder, at udgifterne for både operatøren og staten overskygger fordelene for de strafferetlige systemer og retshåndhævelsen. Fire medlemsstater (Letland, Luxembourg, Nederlandene og Polen) har meddelt, at de har indført andre administrative ordninger). Store operatører, som er aktive i flere medlemsstater, har stordriftsfordele med hensyn til omkostninger, mens mindre operatører i nogle medlemsstater ofte etablerer joint venture-selskaber eller udliciterer til virksomheder, som er specialiserede i datalagring og dataudtræk for at mindske omkostningerne. En sådan outsourcing af tekniske funktioner ændrer ikke ved operatørernes forpligtelse til at føre behørigt tilsyn med databehandlingsoperationerne og til at sikre, at der er truffet de påkrævede sikkerhedsforanstaltninger, hvilket kan være vanskeligt, navnlig for mindre operatører. Kommissionen vil undersøge spørgsmålet om datasikkerhed og virkningen på små og mellemstore virksomheder, når den ser på mulighederne for at ændre reglerne for datalagring.

### 4.3. Adgang til data: myndigheder, procedurer og betingelser (artikel 4)

Medlemsstaterne sikrer, "at data, der lagres ... kun udleveres til de kompetente nationale myndigheder i særlige sager og i overensstemmelse med national lovgivning." Det er op til medlemsstaterne i deres nationale lovgivning at fastsætte "den procedure, der skal følges, og de betingelser, der skal være opfyldt for at få adgang til lagrede data i overensstemmelse med kravet om nødvendighed og proportionalitet, under hensyn til de relevante bestemmelser i EU-retten og folkeretten, herunder navnlig den europæiske menneskerettighedskonvention, således som den er fortolket af Den Europæiske Menneskerettighedsdomstol."

I alle medlemsstater kan det nationale politi og, med undtagelse af common law-systemer (Irland og Det Forenede Kongerige), anklagemyndigheden få adgang til lagrede data. Fjorten medlemsstater opfører sikkerheds- eller efterretningstjenester eller militæret blandt de kompetente myndigheder. Seks medlemsstater opfører skatte- og/eller toldmyndigheder, og tre opfører grænsemyndigheder. En medlemsstat tillader andre offentlige myndigheder at få adgang til dataene, hvis de i henhold til afledt ret har tilladelse til at få adgang til specifikke formål. I elleve medlemsstater skal der foreligge en retskendelse hver gang, der anmodes om adgang til lagrede data. I tre medlemsstater kræves der i de fleste tilfælde retskendelse. I fire andre medlemsstater kræves der tilladelse fra en overordnet myndighed, men ikke fra en dommer. I to medlemsstater ser den eneste betingelse ud til at være en skriftlig anmodning.

---

41 Lauermann (C-139/01) og Österreichischer Rundfunk (om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger – direktiv 95/46/EF – beskyttelse af privatlivets fred – offentliggørelse af indkomstoplysninger for ansatte i organer, der er underlagt Rechnungshofs revision). I forbindelse med direktivets vedtagelse offentliggjorde Kommissionen en erklæring, hvori den foreslog, at man overvejede at benytte listen over forbrydelser i den europæiske arrestordre. (Rådets rammeafgørelse 2002/584/RIA af 13. juni 2002 om den europæiske arrestordre og om procedurerne for overgivelse mellem medlemsstaterne).

| Tabel 2: Adgang til lagrede telekommunikationsdata | | |
|---|---|---|
| | *Kompetente nationale myndigheder* | *Procedurer og betingelser* |
| Belgien | Retslig koordineringsenhed, undersøgelsesdommere, den offentlige anklager og kriminalpolitiet. | Adgang forudsætter tilladelse fra en dommer eller anklager. På anmodning skal operatører straks give tidstro abonnentdata, trafikdata og lokaliseringsdata vedrørende de opkald, der er foretaget inden for den seneste måned.<br>Data vedrørende ældre opkald skal gives snarest muligt. |
| Bulgarien[42] | Specifikke direktorater og departementer i det statslige agentur for national sikkerhed, indenrigsministeriet, den militære informationstjeneste, militærpolititjenesten, forsvarsministeriet, det nationale efterforskningskontor, domstolene og forundersøgelsesmyndigheder på de givne betingelser. | Adgang forudsætter tilladelse fra retspræsidenten for en regional domstol. |
| Tjekkiet | Ikke gennemført. | |
| Danmark[43] | Politiet. | Adgang kræver retskendelse; retskendelser gives, hvis ansøgningen opfylder strenge kriterier om mistanke, nødvendighed og proportionalitet. |
| Tyskland | Ikke gennemført | |
| Estland[44] | Rigspolitiet, grænsepolitiet, sikkerhedspolitiet og med hensyn til genstande og elektronisk kommunikation told- og skattestyrelsen. | Adgang forudsætter retskendelse fra en undersøgelsesdommer.<br>Operatører skal i hastetilfælde give adgang til lagrede data inden for 10 timer og i andre tilfælde inden for 10 arbejdsdage regnet fra modtagelse af anmodningen. |
| Irland[45] | Medlemmer af Garda Síochána (politi) med rang af ledende politikommissær og derover, medlemmer af den permanente forsvarsstyrke med rang af oberst eller derover og medlemmer af skattevæsenet (Revenue Commissioners) med rang af ledende medarbejder eller derover. | Anmodninger indgives skriftligt. |
| Grækenland[46] | Retsmyndigheder, militære myndigheder eller politiet. | Adgang forudsætter en retskendelse, hvoraf det fremgår, at efterforskning ved hjælp af andre midler ikke er muligt eller meget vanskeligt. |
| Spanien[47] | Politi med ansvar for afsløring, efterforskning og retsforfølgning af grov kriminalitet, det nationale efterretningscenter og toldvæsenet. | De kompetente nationale myndigheders adgang til disse data kræver forudgående retskendelse. |
| Frankrig[48] | Den offentlige anklager og udpegede medlemmer af politistyrken (gendarmeri og | Politiet skal begrunde enhver anmodning om adgang til lagrede data og skal søge |

42 Artikel 250b, stk. 1, i lov om elektronisk kommunikation (ændret) 2010 (myndigheder); artikel 250b, stk. 2, og artikel 250c, stk. 1, i lov om elektronisk kommunikation (ændret) 2010 (adgang).

43 Kapitel 71 i retsplejeloven.

44 Artikel 112, stk. 2 og 3, i strafferetsplejeloven (om tilladelser og procedure), og artikel 111, stk. 9, (betingelser) i lov om elektronisk kommunikation.

45 Artikel 6 i kommunikationsloven (datalagring) af 2009.

46 Artikel 3 og 4 i lov 2225/94.

47 Artikel 6 og 7 i lov 25/2007.

| Tabel 2: Adgang til lagrede telekommunikationsdata | | |
|---|---|---|
| | *Kompetente nationale myndigheder* | *Procedurer og betingelser* |
| | politi). | tilladelse fra den person i indenrigsministeriet, der har fået bemyndigelse til at give tilladelse af den nationale kontrolmyndighed for sikkerhedsmæssig aflytning (Commission nationale de contrôle des interceptions de sécurité).<br>Anmodninger om adgang behandles af en udpeget administrator, der arbejder for operatøren. |
| Italien[49] | Den offentlige anklager, politiet og forsvarer for enten sagsøgte, eller den person, der efterforskes. | Adgang forudsætter en begrundet afgørelse fra den offentlige anklager. |
| Cypern[50] | Domstolene, den offentlige anklager og politiet. | Adgang skal godkendes af en anklager, hvis denne mener, at det kan give bevis for, at der er begået grov kriminalitet.<br>En dommer kan afsige kendelse, hvis der er begrundet mistanke om en alvorlig forbrydelse, og hvis dataene sandsynligvis vil vedrøre den. |
| Letland[51] | Bemyndigede administratorer i undersøgelsesinstitutioner, personer, der udfører efterforskningsarbejde, bemyndigede personer i statens sikkerhedsinstitutioner, den offentlige anklager og domstolene. | Bemyndigede administratorer, den offentlige anklager og domstolene skal vurdere, hvorvidt en anmodning er hensigtsmæssig og relevant, de skal registrere anmodningen og sikre beskyttelse af de indhentede data. Bemyndigede organer kan indgå aftale med en operatør om f.eks. kryptering af indhentede data. |
| Litauen[52] | Organer i forundersøgelsesfasen og efterforskningsorganer, anklageren, domstolene (dommere) og efterretningstjenesten. | Bemyndigede offentlige myndigheder skal skriftligt anmode om lagrede data.<br>Adgang i forundersøgelses- og efterforskningsfasen kræver retskendelse. |
| Luxembourg[53] | Retsmyndigheder (undersøgelsesdommere og anklagere), myndigheder med ansvar for statens sikkerhed, forsvaret, den offentlige sikkerhed og forebyggelse, efterforskning, afsløring og retsforfølgning af kriminalitet. | Adgang forudsætter retskendelse. |
| Ungarn[54] | Politiet, den nationale told- og skattemyndighed, den nationale sikkerhedstjeneste og den offentlige anklager. | Politiet og den nationale told- og skattemyndighed skal have anklagers tilladelse.<br>Den offentlige anklager og de nationale sikkerhedstjenester kan få adgang uden retskendelse. |

---

48 Artikel 60-1 og 60-2, i strafferetsplejeloven (myndigheder) og artikel L.31-1-1 (betingelser).

49 Artikel 132, stk. 3, i databeskyttelsesloven.

50 Artikel 4, stk. 2 og 4, i lov 183(I)/2007.

51 Artikel 71, stk. 1, i lov om elektronisk kommunikation (myndigheder) og bekendtgørelse nr. 820 (procedurer).

52 Artikel 77, stk. 1 og 2, i lov X-1835 og mundtlig beretning til Kommissionen.

53 Artikel 5-2, stk. 1, og artikel 9, stk. 2, i lov af 24. juli 2010 (myndigheder) og artikel 67-1, i strafferetsplejeloven (betingelser).

54 Artikel 68, stk. 1, og artikel 69, stk. 1, litra c) og d), i lov XXXIV 1994; artikel 9/A, stk. 1, i lov V 1972; artikel 71, stk. 1, 3 og 4, 178/A (4), artikel 200, artikel 201 og artikel 268, stk. 2, i lov XIX 1998; Artikel 40, stk. 1 og 2, artikel 53, stk. 1, og artikel 54, stk. 1, litra j), i lov CXXV 1995.

| Tabel 2: Adgang til lagrede telekommunikationsdata | | |
|---|---|---|
| | *Kompetente nationale myndigheder* | *Procedurer og betingelser* |
| Malta[55] | Politiet og sikkerhedstjenesten. | Anmodninger indgives skriftligt. |
| Nederlandene[56] | Politiets efterforskningstjeneste. | Adgang gives, såfremt der foreligger tilladelse fra anklager eller undersøgelsesdommeren. |
| Østrig | Ikke gennemført | |
| Polen[57] | Politiet, grænsevagter, skatteinspektører, den interne sikkerhedstjeneste, efterretningstjenesten, det centrale kontor for bekæmpelse af svig, militærets kontraspionagetjeneste, militærets efterretningstjeneste, domstolene og den offentlige anklager. | Anmodninger skal indgives skriftligt, og for så vidt gælder politi, grænsevagter, skatteinspektører skal der indhentes tilladelse fra en ledende administrator i organisationen. |
| Portugal[58] | Kriminalpolitiet, nationalgarden "Guarda Nacional Republicana", tjenesten for offentlig sikkerhed, det militære kriminalpoliti, ministeriet for indvandrere og grænsekontrol og det maritime politi. | Udlevering af data forudsætter retskendelse, hvoraf det fremgår, at adgangen er afgørende for at finde frem til sandheden, eller at det vil være umuligt eller meget vanskeligt at opnå bevismateriale på anden måde. Retskendelsen er underlagt kravene om nødvendighed og proportionalitet. |
| Rumænien | Ikke gennemført | |
| Slovenien[59] | Politi, efterretnings- og sikkerhedstjenesten, forsvarstjenesten med ansvar for spionage og kontraspionage og sikkerhedsmissioner. | Adgang forudsætter retskendelse. |
| Slovakiet[60] | Retshåndhævende myndigheder og domstole. | Anmodninger indgives skriftligt. |
| Finland[61] | Politi, grænsevagter, toldmyndigheder (for så vidt angår lagrede abonnentdata, trafikdata og lokaliseringsdata).<br>Beredskabscenter og center for redningsoperationer til søs (identifikations- og lokaliseringsdata i nødsituationer). | Alle kompetente myndigheder kan få adgang til abonnentdata uden retskendelse.<br>Andre data forudsætter retskendelse. |
| Sverige | Ikke gennemført | |
| Det Forenede Kongerige[62] | Politi, efterforskningstjeneste, told- og skattemyndigheder og andre offentlige myndigheder i medfør af afledt ret. | Der gives adgang, såfremt der foreligger en tilladelse fra en "udpeget person", og der er foretaget en nødvendigheds- og proportionalitetstest i specifikke tilfælde og under omstændigheder, hvor afsløring af data er tilladt eller påkrævet i henhold til lovgivning. Der er aftalt specifikke procedurer med operatørerne. |

55 Artikel 20, stk. 1, i anordning 198/2008.

56 Artikel 126 i strafferetsplejeloven.

57 Artikel 179, stk. 3, i telekommunikationsloven af 16. juli 2004, som ændret ved artikel 1 i lov af 24. april 2009.

58 Artikel 2, stk. 1, artikel 3, stk. 2, og artikel 9 i lov 32/2008.

59 Artikel 107c i lov om elektronisk kommunikation; artikel 149b i strafferetsplejeloven; artikel 24, litra b), i lov om sikkerhedstjenesten og artikel 32 i lov om forsvar.

60 Artikel 59a, stk. 8, i lov om elektronisk kommunikation.

61 Artikel 35, stk. 1, og artikel 36 i lov om elektronisk kommunikation, artikel 31-33 i lov om politi og artikel 41 i lov om grænsevagter.

62 Artikel 25 og bilag 1 i lov om efterforskningsbeføjelser 2000 og artikel 7 i datalagringsforordningen. Artikel 22, stk. 2, i RIPA fastlægger, til hvilke formål myndighederne kan anmode om data.

Kommissionen vil se nærmere på behovet og muligheden for i højere grad at opnå en harmonisering med hensyn til, hvilke myndigheder der har adgang, og hvilke procedurer der gælder for at få adgang til lagrede data. Dette kunne omfatte mere klart definerede lister over kompetente myndigheder, uafhængigt og/eller retlig tilsyn med anmodninger om data og minimumskrav til operatørers procedurer for at give kompetente myndigheder adgang.

### 4.4. Datalagringens anvendelsesområde og omfattede datakategorier (artikel 1, stk. 2, artikel 3, stk. 2, og artikel 5)

Direktivet finder anvendelse på fastnettelefoni, mobiltelefoni, internetadgang, e-mail og telefoni via internettet. Det specificeres (i artikel 5), hvilke kategorier af data der skal lagres, nemlig data, der er nødvendige for at identificere:

(a) kilden til en kommunikation

(b) kommunikationens bestemmelsessted

(c) kommunikationens dato, klokkeslæt og varighed

(d) kommunikationens type

(e) brugernes kommunikationsudstyr eller det, der fremstår som værende deres udstyr, og

(f) lokaliseringen af mobilt udstyr.

Det omfatter også (artikel 3, stk. 2) lagring af data i forbindelse med forgæves opkaldsforsøg, dvs. et telefonopkald, hvor der opnås forbindelse, men som ikke besvares, eller hvor netværkssystemet har grebet ind, og hvor data om disse forsøg genereres eller behandles og lagres af operatører. Data, der afslører indholdet af kommunikationen, kan ikke lagres i medfør af dette direktiv. Det er også efterfølgende blevet præciseret, at søgninger, dvs. serverlogfiler, der genereres i forbindelse med en søgemaskinetjeneste, også falder uden for direktivets anvendelsesområde, fordi de snarere betragtes som indhold end trafikdata[63].

21 medlemsstater giver mulighed for lagring af hver af disse datakategorier i deres nationale lovgivning til gennemførelse af direktivet. Belgien præciserer ikke, hvilke typer telefonidata der kan lagres, og har ingen bestemmelser for internetdata. De medlemsstater, der besvarede Kommissionens spørgeskema, fandt det ikke nødvendigt at ændre de datakategorier, der skal lagres, selv om Europa-Parlamentet har sendt Kommissionen en skriftlig erklæring, hvori det opfordrer til, at direktivet udvides til at omfatte søgemaskiner for "hurtigt og effektivt at kunne sætte ind over for børnepornografi og seksuelle overgreb på internettet"[64]. Artikel 29-gruppen hævdede i sin rapport om anden håndhævelsesforanstaltning, at datakategorierne i direktivet burde anses for udtømmende, og at operatørerne ikke burde pålægges ekstra datalagringsforpligtelser. Kommissionen vil se på nødvendigheden af alle disse datakategorier.

---

63 Artikel 29-gruppens udtalelse om databeskyttelse i forbindelse med søgemaskiner vedtaget den 4. april 2008.

64 Skriftlig erklæring, jf. forretningsordenens artikel 123 om oprettelse af en hurtig varslingsordning mod pædofili og personer, der begår seksuelle overgreb, 19.4.2010, 0029/2010.

## 4.5. Lagringsperioder (artikel 6 og 12)

Medlemsstaterne sørger for, at de i artikel 5 omhandlede datakategorier lagres i mindst seks måneder og højst to år. Den længste lagringsperiode kan forlænges af en medlemsstat, som står over for "særlige omstændigheder, som berettiger til en forlængelse af i en begrænset periode"; en sådan forlængelse skal straks meddeles Kommissionen, som inden for seks måneder fra meddelelsen kan beslutte at godkende eller afvise forlængelsen. Mens den længste lagringsperiode kan forlænges, er der ingen mulighed for at afkorte minimumsperiode til mindre end seks måneder. Alle medlemsstater, som har gennemført direktivet, med undtagelse af én, har en lagringsperiode eller lagringsperioder inden for disse grænser, og Kommissionen har ikke modtaget meddelelser om forlængelser. Der er dog ingen ensartet fremgangsmåde i EU.

Femten medlemsstater specificerer én periode for alle datakategorier: en medlemsstat (Polen) anfører en lagringsperiode på to år, en medlemsstat (Letland) anfører en lagringsperiode på halvandet år, ti medlemsstater (Bulgarien, Danmark, Estland, Grækenland, Spanien, Frankrig, Nederlandene, Portugal, Finland og Det Forenede Kongerige) anfører en lagringsperiode på et år og tre medlemsstater (Cypern, Luxembourg og Litauen) anfører en lagringsperiode på seks måneder. Fem medlemsstater har fastlagt forskellige lagringsperioder for forskellige datakategorier: to medlemsstater (Irland og Italien) anfører to år for fastnet- og mobiltelefonidata og et år for data vedrørende internetadgang, e-mail og telefoni via internettet; en medlemsstat (Slovenien) anfører fjorten måneder for telefonidata og otte måneder for internetdata; en medlemsstat (Slovakiet) anfører et år for fastnet- og mobiltelefonidata og seks måneder for internetdata; en medlemsstat (Malta) anfører et år for fastnet- og mobiltelefonidata og data vedrørende telefoni via internettet og seks måneder for data vedrørende internetadgang og e-mail. En medlemsstat (Ungarn) lagrer alle data i et år, med undtagelse af data for forgæves opkaldsforsøg, som kun lagres i seks måneder. En medlemsstat (Belgien) har ikke specificeret en datalagringsperiode for de datakategorier, der er anført i direktivet. Nærmere oplysninger fremgår af tabel 3.

| **Tabel 3: Lagringsperioder i national lovgivning** | |
|---|---|
| Belgien[65] | Mellem 1 år og 36 måneder for "offentligt tilgængelige" telefontjenester. Ingen bestemmelse vedrørende internetdata. |
| Bulgarien | 1 år. Data, som der er givet adgang til, kan på anmodning lagres i yderligere 6 måneder. |
| Tjekkiet | Ikke gennemført. |
| Danmark | 1 år |
| Tyskland | Ikke gennemført. |
| Estland | 1 år |
| Irland | 2 år for fastnet- og mobiltelefonidata og 1 år for data vedrørende internetadgang, e-mail og telefoni via internettet. |
| Grækenland | 1 år |
| Spanien | 1 år |
| Frankrig | 1 år |
| Italien | 2 år for fastnet- og mobiltelefonidata og 1 år for data vedrørende internetadgang, e-mail og telefoni via internettet. |
| Cypern | 6 måneder |
| Letland | 18 måneder |

[65] Artikel 126, stk. 2, i lov af 13. juni 2005 om elektronisk kommunikation.

| Tabel 3: Lagringsperioder i national lovgivning | |
|---|---|
| Litauen | 6 måneder |
| Luxembourg | 6 måneder |
| Ungarn | 6 måneder for forgæves opkald og 1 år for alle andre data. |
| Malta | 1 år for fastnet- og mobiltelefonidata og data vedrørende telefoni via internettet og 6 måneder for data vedrørende internetadgang og e-mail. |
| Nederlandene | 1 år |
| Østrig | Ikke gennemført. |
| Polen | 2 år |
| Portugal | 1 år |
| Rumænien | Ikke gennemført (6 måneder ifølge de tidligere, nu annullerede gennemførelsesbestemmelser). |
| Slovenien | 14 måneder for telefonidata og 8 måneder for internetdata. |
| Slovakiet | 1 år for fastnet- og mobiltelefonidata og 6 måneder for data vedrørende internetadgang, e-mail og telefoni via internettet. |
| Finland | 1 år |
| Sverige | Ikke gennemført. |
| Det Forenede Kongerige | 1 år |

Selv om disse forskelligheder er tilladt ifølge direktivet, er resultatet, at direktivet kun giver begrænset retssikkerhed og forudsigelighed i EU for operatører, som udbyder tjenester i mere end én medlemsstat, og for borgere, hvis kommunikationsdata måske lagres i forskellige medlemsstater. I betragtning af den stigende internationalisering af databehandling og udlicitering af datalagring bør muligheden for at harmonisere lagringsperioder i EU overvejes. Med henblik på at overholde proportionalitetsprincippet og i lyset af kvantitativ og kvalitativ dokumentation for værdien af lagrede data i medlemsstaterne samt udviklingen inden for kommunikation og teknologi og kriminalitet og terrorisme vil Kommissionen overveje at anvende forskellige perioder for forskellige datakategorier eller for forskellige kategorier af grov kriminalitet eller en kombination heraf[66]. Den kvantitative dokumentation fra medlemsstaterne vedrørende de lagrede datas alder tyder indtil videre på, at ca. 90 % af dataene er seks måneder gamle eller derunder, og at 70 % er tre måneder gamle eller derunder på det tidspunkt, hvor de retshåndhævende myndigheder fremsætter (første) anmodning om adgang (se afsnit 5.2).

### 4.6. Databeskyttelse, datasikkerhed og tilsynsmyndigheder (artikel 7 og 9)

Ifølge direktivet skal medlemsstaterne sikre, at operatører som minimum respekterer fire datasikkerhedsprincipper, nemlig at de lagrede data:

(a) skal være af samme kvalitet og være omfattet af den samme sikkerhed og beskyttelse som de data, der findes på nettet [for offentlig kommunikation]

(b) skal være omfattet af de fornødne tekniske og organisatoriske foranstaltninger, så de er beskyttet mod hændelig eller ulovlig tilintetgørelse eller hændeligt tab, mod forringelse, ubeføjet eller ulovlig lagring, behandling, adgang eller udbredelse

[66] I Kommissionens forslag til et direktiv om datalagring i 2005 anførtes en lagringsperiode på et år for telefonidata og seks måneder for internetdata.

(c) skal være omfattet af de fornødne tekniske og organisatoriske foranstaltninger, så det sikres, at kun særligt autoriserede personer får adgang til dataene, og

(d) skal tilintetgøres ved udløbet af lagringstiden, bortset fra data, der har været givet adgang til, og som er blevet gemt [med henblik på direktivets formål].

I lighed med databeskyttelsesdirektivet og e-data-direktivet må operatører ikke behandle data, der er lagret i medfør af direktivet, til andre formål, forudsat at dataene ellers ikke ville have været lagret[67]. Medlemsstaterne skal udpege en eller flere offentlige myndigheder, der i fuld uafhængighed har til opgave at påse, at disse principper overholdes, og disse myndighed kan være de samme myndigheder som dem, der er nævnt i databeskyttelsesdirektivet[68].

Femten medlemsstater har gennemført alle disse principper i den relevante lovgivning. Fire medlemsstater (Belgien, Estland, Spanien og Letland) har gennemført to eller tre af principperne, men sikrer ikke eksplicit tilintetgørelse af data ved lagringsperiodens udløb. To medlemsstater (Italien og Finland) sikrer, at dataene tilintetgøres. Det er ikke klart, hvilke specifikke tekniske og organisatoriske sikkerhedsforanstaltninger, såsom sikker autentificering og detaljeret logstyring[69], der er blevet anvendt. 22 medlemsstater har en tilsynsmyndighed, der er ansvarlig for at kontrollere, at principperne anvendes. I de fleste tilfælde er det datatilsynsmyndigheden. Nærmere oplysninger fremgår af tabel 4.

**Tabel 4: Databeskyttelse, datasikkerhed og tilsynsmyndigheder**

| *Medlemsstat* | *Bestemmelser om databeskyttelse og datasikkerhed i national lovgivning* | *Tilsynsmyndighed* |
|---|---|---|
| Belgien | Operatører skal sikre, at data ved udlevering ikke kan opsnappes af en tredjepart, og de skal overholde ETSI-standarder for telekommunikations-sikkerhed og lovlig aflytning[70].<br>Det ser ikke ud til, at der tages stilling til princippet om obligatorisk tilintetgørelse af data ved lagringsperiodens udløb. | Institut for posttjenester og telekommunikation |
| Bulgarien | Lovgivning til gennemførelse omfatter krav om at gennemføre de fire principper[71]. | Kommissionen for beskyttelse af personoplysninger fører tilsyn med behandling og lagring af data for at sikre, at forpligtelserne opfyldes, mens den parlamentariske kommission i nationalforsamlingen fører tilsyn med procedurerne for tilladelse og adgang til dataene. |
| Tjekkiet[72] | Ikke gennemført. | |

67 Artikel 13, stk. 1, i direktiv 95/46/EF.

68 Artikel 28 i direktiv 95/46/EF.

69 Sikker autentificering indebærer dobbelte autentificeringsmekanismer, såsom password og biometri eller password og token, for at sikre den fysiske tilstedeværelse af den person, der har ansvaret for at behandle trafikdata. Deltaljeret logstyring indebærer detaljeret sporing af adgangs- og behandlingsoperationer ved hjælp af lagring af logfiler med oplysninger om brugeridentitet, adgangstidspunkt og filer, der har været adgang til.

70 Artikel 6 i kongeligt dekret af 9. januar 2003.

71 Artikel 4, stk. 1, i lov om elektronisk kommunikation (ændret) 2010.

72 Artikel 87, stk. 3, og artikel 88 i lov 127/2005, som ændret ved lov 247/2008; artikel 2 i lov 336/2005; artikel 3, stk. 4, i lov 485/2005 og artikel 28, stk. 1, i lov 101/2000.

| Tabel 4: Databeskyttelse, datasikkerhed og tilsynsmyndigheder | | |
|---|---|---|
| *Medlemsstat* | *Bestemmelser om databeskyttelse og datasikkerhed i national lovgivning* | *Tilsynsmyndighed* |
| Danmark | Fire principper varetages[73]. | IT- og Telestyrelsen fører tilsyn med, at udbydere af elektroniske telekommunikationsnet og -tjenester overholder forpligtelsen til at sikre, at det tekniske udstyr og de tekniske systemer er indrettet således, at det efter anmodning fra politiet er muligt at få adgang til oplysninger om teletrafik. |
| Tyskland | Ikke gennemført. | |
| Estland | Der er bestemmelser, som dækker tre af de fire principper. Der er ingen specifik bestemmelse vedrørende det fjerde princip, selv om enhver person, hvis ret til privatlivets fred er blevet tilsidesat af overvågningsrelaterede aktiviteter, kan anmode om tilintetgørelse af data på grundlag af en retskendelse[74]. | Den tekniske tilsynsmyndighed er den ansvarlige myndighed. |
| Irland[75] | Lovgivning til gennemførelse af direktivet omfatter krav om at gennemføre de fire principper. | En udpeget dommer har beføjelse til at undersøge og rapportere om, hvorvidt de kompetente nationale myndigheder overholder bestemmelserne i den lovgivning, der gennemfører direktivet. |
| Grækenland[76] | Lovgivning til gennemførelse af direktivet omfatter krav om at gennemføre de fire principper med yderligere krav til operatører om at udarbejde og anvende en plan for at sikre overholdelse under ledelse af en udnævnt datatilsynsførende. | Tilsynsmyndighed for beskyttelse af personoplysninger og tilsynsmyndighed for beskyttelse af privatlivets fred i forbindelse med kommunikation. |
| Spanien[77] | Datasikkerhedsbestemmelser sikrer tre af de fire principper (de lagrede datas kvalitet og sikkerhed, autoriserede personers adgang og beskyttelse mod uautoriseret behandling). | Datatilsynsmyndigheden er den ansvarlige myndighed. |
| Frankrig[78] | Lovgivning til gennemførelse af direktivet omfatter krav om at gennemføre de fire principper. | Det nationale udvalg for informationsteknologi og -frihed fører tilsyn med, at forpligtelserne overholdes. |
| Italien | Der findes ingen udtrykkelige bestemmelser om sikkerhed i forbindelse med lagrede data, selv om der er et generelt krav om, at trafikdata tilintetgøres eller gøres anonyme, og om at abonnenten eller brugeren skal være indforstået med, at lokaliseringsdata behandles[79]. | Datatilsynsmyndigheden kontrollerer, at operatørerne overholder direktivet. |

73 Lov om behandling af personoplysninger og bekendtgørelse nr. 714 af 26. juni 2008 om udbud af elektroniske kommunikationsnet og -tjenester.

74 Artikel 111, stk. 9, i lov om elektronisk kommunikation, artikel 122, stk. 2, i strafferetsplejeloven.

75 Artikel 4, 11 og 12 i kommunikationsloven (datalagring) af 2009.

76 Artikel 6 i lov 3917/2011.

77 Artikel 8 i lov 25/2007 og artikel 38, stk. 3, i lov om telekommunikation. Loven (artikel 9) henviser til undtagelsen fra adgangs- og tilintetgørelsesrettighederne i forfatningslov 15/1999 om beskyttelse af personoplysninger (artikel 22 og 23).

78 Artikel D.98-5 i CPCE, artikel L-34-1(V) i CPCE, artikel 34 i lov nr. 78-17, artikel 34-1 i CPCE og artikel 11 i lov nr. 78-17 af 6. januar 1978.

79 Artikel 123 og 126 i databeskyttelsesloven.

| Tabel 4: Databeskyttelse, datasikkerhed og tilsynsmyndigheder | | |
|---|---|---|
| *Medlemsstat* | *Bestemmelser om databeskyttelse og datasikkerhed i national lovgivning* | *Tilsynsmyndighed* |
| Cypern[80] | Der er bestemmelser, som dækker de fire principper. | Tilsynsmyndigheden for beskyttelse af personoplysninger fører tilsyn med, at lovgivningen anvendes. |
| Letland[81] | Der er bestemmelser, som dækker to af principperne: fortrolighed og uautoriseret adgang til lagrede data samt tilintetgørelse af data ved lagringsperiodens udløb. | Statens datainspektorat fører tilsyn med beskyttelsen af personoplysninger i sektoren for elektronisk kommunikation, men ikke med adgang til og behandling af lagrede data. |
| Litauen[82] | Lovgivning til gennemførelse af direktivet dækker de fire principper. | Statens datatilsyn fører tilsyn med, at lovgivningen gennemføres, og har til opgave at forsyne Europa-Kommissionen med statistikker. |
| Luxembourg[83] | Lovgivning til gennemførelse af direktivet dækker de fire principper. | Datatilsynsmyndigheden. |
| Ungarn[84] | Lovgivning til gennemførelse af direktivet dækker de fire principper. | Den parlamentariske kommission for databeskyttelse og informationsfrihed. |
| Malta[85] | Lovgivning til gennemførelse af direktivet dækker de fire principper. | Datatilsynet. |
| Nederlandene[86] | Lovgivning til gennemførelse af direktivet dækker de fire principper. | Radiokommunikationsmyndigheden fører tilsyn med, at udbydere af telekommunikation og internetadgang overholder deres forpligtelser; datatilsynsmyndigheden fører tilsyn med den generelle behandling af personoplysninger og en protokol beskriver samarbejdet mellem de to myndigheder nærmere. |
| Østrig | Ikke gennemført. | |
| Polen | Lovgivning til gennemførelse af direktivet dækker de fire principper[87]. | Datatilsynsmyndigheden. |
| Portugal | Lovgivning til gennemførelse af direktivet dækker de fire principper[88]. | Datatilsynsmyndigheden. |
| Rumænien | Ikke gennemført. | |
| Slovenien[89] | Lovgivning til gennemførelse af direktivet dækker de fire principper. | Informationstilsynet. |
| Slovakiet[90] | Lovgivning til gennemførelse af direktivet dækker de fire principper. | Den nationale regulerings- og prissætningsmyndighed inden for elektronisk kommunikation fører tilsyn med beskyttelsen af personoplysninger. |

80 Artikel 14 og 15 i lov 183(I)/2007.

81 Artikel 4, stk. 4, og artikel 71, stk. 6-8, i lov om elektronisk kommunikation.

82 Artikel 12, stk. 5, og artikel 66, stk. 8 og 9, i lov om elektronisk kommunikation som ændret den 14. november 2009.

83 Artikel 1, stk. 5, i lov af 24. juli 2010.

84 Artikel 157 i lov C/2003, som ændret ved lov CLXXIV/2007, artikel 2 i dekret 226/2003 og lov LXIII/1992 om databeskyttelse.

85 Artikel 24 i anordning 198/2008 og artikel 40, litra b), i databeskyttelsesloven (Kap. 440).

86 Artikel 13, stk. 5, i telekommunikationsloven; den lange titel på samarbejdsprotokollen er "Samenwerkingsovereenkomst tussen Agentschap Telecom en het College bescherming persoonsgegevens met het oog op de wijzigingen in de Telecommunicatiewet naar aanleiding van de Wet bewaarplicht telecommunicatiegegevens".

87 Artikel 180a og 180e i telekommunikationsloven.

88 Artikel 7, stk. 1 og 5, og artikel 11 i lov 32/2008 samt artikel 53 og 54 i lov om beskyttelse af personoplysninger.

89 Artikel 170a, stk. 6, og artikel 107c i lov om elektronisk kommunikation.

90 Artikel 59a i loven om elektronisk kommunikation og artikel S33 i lov nr. 428/2002 om beskyttelse af personoplysninger.

| Tabel 4: Databeskyttelse, datasikkerhed og tilsynsmyndigheder | | |
|---|---|---|
| *Medlemsstat* | *Bestemmelser om databeskyttelse og datasikkerhed i national lovgivning* | *Tilsynsmyndighed* |
| Finland | Lovgivning til gennemførelse af direktivet stiller kun udtrykkeligt krav om tilintetgørelse af data ved lagringsperiodens udløb[91]. | Den finske kommunikationsreguleringsmyndighed fører tilsyn med, at operatørerne overholder datalagringsreglerne.<br>Datatilsynsombudsmanden fører tilsyn med den generelle lovlighed af behandlingen af personoplysninger. |
| Sverige | Ikke gennemført. | |
| Det Forenede Kongerige | Lovgivning til gennemførelse af direktivet dækker de fire principper[92]. | Datatilsynet fører tilsyn med lagring og/eller behandling af kommunikationsdata (og eventuelle andre personoplysninger) og foretager hensigtsmæssig kontrol af databeskyttelse.<br>Aflytningstilsynet (en fungerende eller pensioneret ledende dommer) fører tilsyn med offentlige myndigheders erhvervelse af kommunikationsdata i medfør af RIPA.<br>Domstolen for efterforskningsbeføjelser efterforsker klager om misbrug af data, hvis disse er erhvervet i medfør af RIPA. |

Gennemførelsen af artikel 7 er ikke konsekvent. Lagrede data kan være af meget personlig og følsom karakter, og der skal konsekvent og på en synlig måde anvendes høje standarder for databeskyttelse og datasikkerhed i hele processen for lagring, udtræk og anvendelse for at mindske risikoen for krænkelse af retten til privatlivets fred og for at opretholde borgernes tillid. Kommissionen vil overveje, hvilke muligheder der er for at styrke kravene til datasikkerhed og databeskyttelse, herunder for at indføre løsninger med indbygget beskyttelse af privatlivets fred, for at sikre, at disse krav opfyldes både i forbindelse med lagring og udlevering af data. Den vil også tage hensyn til de henstillinger til minimumskrav og tekniske og organisatoriske sikkerhedsforanstaltninger, der blev fremsat af artikel 29-gruppen i dens rapport om anden håndhævelsesforanstaltning[93].

## 4.7. Statistikker (artikel 10)

Medlemsstaterne sørger for, at der årligt tilsendes Kommissionen statistikker om lagring af data, herunder oplysninger om:

- de tilfælde, hvor der er sendt data til de kompetente myndigheder i overensstemmelse med gældende national ret

- tidsrummet mellem den dato, hvor dataene blev lagret, og den dato, hvor den kompetente myndighed anmodede om udlevering af dataene (dvs. dataenes alder) og

- de tilfælde, hvor anmodninger om data ikke kunne efterkommes.

I forbindelse med sin anmodning om statistikker i medfør af denne bestemmelse bad Kommissionen medlemsstaterne om at give nærmere oplysninger om de enkelte anmodninger om data. Ikke desto mindre var statistikkerne meget forskellige i omfang og i

---

91 Artikel 16, stk. 3, i lov om elektronisk kommunikation.

92 Artikel 6 i datalagringsbekendtgørelsen.

93 Artikel 29-gruppens udtalelse 3/2006 (WP119); Rapport 01/2010.

detaljeringsgrad: Nogle medlemsstater skelnede i deres svar mellem forskellige former for kommunikation, nogle angav dataenes alder på tidspunktet for anmodningen, mens andre kun gav årlige statistikker uden nogen form for nærmere opdeling. Nitten medlemsstater[94] gav statistikker over antallet af dataanmodninger for 2009 og/eller 2008; herunder Irland, Grækenland og Østrig, hvor der anmodes om data, selv om der ikke findes lovgivning til gennemførelse af direktivet, samt Tjekkiet og Tyskland, hvis lovgivning om datalagring blev annulleret. Syv medlemsstater, som har gennemført direktivet, gav ingen statistikker, selv om Belgien gav et skøn over mængden af årlige anmodninger om telefonidata (300 000).

Pålidelige kvantitative og kvalitative data er meget vigtige for at påvise nødvendigheden og værdien af sikkerhedsforanstaltninger såsom datalagring. Dette blev anerkendt i 2006-handlingsplanen om måling af kriminalitet og strafferetlig behandling deraf[95], som indeholdt et mål om at udvikle metoder for regelmæssig indsamling af data i overensstemmelse med direktivet og at medtage statistikkerne i Eurostats database (forudsat at de opfylder kvalitetskravene). Det har ikke været muligt at opfylde dette mål, eftersom de fleste medlemsstater først har gennemført direktivet fuldt ud inden for de seneste to år og har fortolket kilderne til statistikker forskelligt. Kommissionen vil i sit kommende forslag til revision af datalagringsreglerne, sideløbende med revisionen af handlingsplanen om statistikker, bestræbe sig på at udarbejde praktisk anvendelige måle- og rapporteringsmetoder, der giver en gennemsigtig og meningsfuld overvågning af datalagring, og som ikke pålægger de strafferetlige systemer og retshåndhævende myndigheder unødige administrative byrder.

### 4.8. Gennemførelse i EØS-landene

Der findes lovgivning om datalagring i Island, Liechtenstein og Norge[96].

### 4.9. Forfatningsdomstolenes afgørelse om lovgivning til gennemførelse af direktivet

Den rumænske forfatningsdomstol, den tyske forbundsstats forfatningsdomstol og den tjekkiske forfatningsdomstol annullerede henholdsvis i oktober 2009, marts 2010 og marts 2011 de love, der skulle gennemføre direktivet i deres respektive jurisdiktioner ud fra den betragtning, at de var forfatningsstridige. Den rumænske domstol[97] accepterede, at indgriben i grundlæggende rettigheder kan tillades, forudsat at visse regler respekteres, og at der træffes hensigtsmæssige og tilstrækkelige foranstaltninger til at beskytte mod potentiel vilkårlig indgriben fra statens side. På baggrund af Den Europæiske Menneskerettighedsdomstols[98] retspraksis fandt domstolen imidlertid, at lovgivningen til gennemførelse af direktivet var uklar med hensyn til anvendelsesområde og formål uden tilstrækkelige sikkerhedsforanstaltninger, og den hævdede, at en "konstant lovpligtig forpligtelse" til at lagre alle trafikdata i seks måneder var uforenelig med retten til privatlivets fred og ytringsfriheden i artikel 8 i den europæiske menneskerettighedskonvention.

---

94 Tjekkiet, Danmark, Tyskland, Estland, Irland, Grækenland, Spanien, Frankrig, Cypern, Letland, Litauen, Malta, Nederlandene, Østrig, Polen, Slovenien, Slovakiet, Finland og Det Forenede Kongerige.

95 Meddelelse fra Kommissionen (2006) 437, "En overordnet og sammenhængende EU-strategi for måling af kriminalitet og strafferetlig behandling deraf: En EU-handlingsplan 2006-2010".

96 Lovgivningen er gennemført i Island ved telekommunikationslov 81/2003 (som ændret i april 2005) og i Liechtenstein ved telekommunikationslov af 2006. I Norge blev der vedtaget en lov den 5. april 2011, som nu afventer kongens stadfæstelse.

97 Den rumænske forfatningsdomstols afgørelse nr. 1258 af 8. oktober 2009.

98 EMRK, Rotaru mod Rumænien 2000, Sunday Times mod Det Forenede Kongerige 1979 og Prins Hans-Adam af Liechtenstein mod Rumænien 2001.

Den tyske forfatningsdomstol[99] anførte, at datalagring resulterede i en følelse af overvågning, som kunne skade den frie udøvelse af grundlæggende rettigheder. Den anerkendte udtrykkeligt, at datalagring til helt begrænsede formål og med en tilstrækkelig høj beskyttelse af data ikke ville være i strid med den tyske grundlov. Domstolen understregede dog, at sådanne data udgjorde en alvorlig begrænsning i retten til privatlivets fred og derfor kun kunne tillades i særligt begrænsede tilfælde, og at en lagringsperiode på seks måneder var lige i overkanten af ("an der Obergrenze"), hvad der kunne siges at være rimeligt (§ 215). Der bør kun anmodes om data, hvor der allerede er en mistanke om grov kriminalitet eller bevis på en fare for den offentlige sikkerhed, og dataudtræk bør forbydes for visse privilegerede kommunikationer (dvs. vedrørende følelsesmæssige eller sociale behov), som beror på fortrolighed. Data bør også indkodes med et gennemsigtig tilsyn med brugen af dem.

Den tjekkiske forfatningsdomstol[100] annullerede lovgivningen til direktivets gennemførelse med den begrundelse, at den som en foranstaltning, der gjorde indgreb i de grundlæggende rettigheder, ikke var tilstrækkelig præcist og klart formuleret. Domstolen anførte, at formålsbegrænsningen ikke var tilstrækkelig snæver i betragtning af datalagringskravets omfang. Den hævdede, at gennemførelseslovgivningen ikke indeholdt en tilstrækkelig klar definition af, hvilke myndigheder der har kompetence til at få adgang til og kunne anvende dataene eller af, hvilke procedurer der gælder for adgang til og anvendelse af dataene, til at sikre dataenes integritet og fortrolighed. Den enkelte borger har derfor ikke tilstrækkelig garanti for, at der ikke sker misbrug fra de offentlige myndigheders side. Domstolen kritiserede ikke selve direktivet og anførte, at det gav Tjekkiet tilstrækkelig frihed til at gennemføre det i national lovgivning i overensstemmelse med forfatningen. Domstolen rejste dog i en bibemærkning tvivl om, hvorvidt det var nødvendigt, effektivt og hensigtsmæssigt at lagre trafikdata i betragtning af nye kriminelle metoder, såsom brugen af anonyme SIM-kort.

Disse tre medlemsstater overvejer nu, hvordan direktivet så skal gennemføres. Der er også indbragt sager om datalagring for forfatningsdomstolen i Bulgarien, som førte til en revision af lovgivningen, i Cypern, hvor retskendelserne, der var afgivet i henhold til den pågældende lovgivning, blev erklæret forfatningsstridige, og i Ungarn, hvor der kører en sag om den manglende angivelse af det retlige formål med databehandling i lovgivningen til gennemførelse af direktivet[101].

Kommissionen vil tage de problemer, der er påpeget i national retspraksis, i betragtning i sit kommende forslag til en revision af datalagringsdirektivet.

### 4.10. Håndhævelse af direktivet

Kommissionen forventer, at de medlemsstater, som endnu ikke har gennemført direktivet fuldt ud i national lovgivning, eller som endnu ikke har vedtaget lovgivning til erstatning for den lovgivning, der er annulleret af de nationale domstole, vil få det gjort hurtigst muligt. I modsat fald forbeholder Kommissionen sig ret til at udøve sine beføjelser i medfør af EU-traktaterne. På nuværende tidspunkt har Domstolen konstateret, at to medlemsstater (Østrig og

---

99 Bundesverfassungsgericht, 1 BvR 256/08, § 1–345.

100 Den tjekkiske forfatningsdomstols dom af 22. marts vedrørende lov nr. 127/2005 og dekret nr. 485/2005, se især § 45-48, § 50-51 og § 56.

101 Bulgariens øverste administrative domstols afgørelse nr. 13627 af 11. december 2008, Cyperns øverste domstols afgørelse i appelsag nr. 65/2009, 78/2009, 82/2009 og 15/2010-22/2010 af 1. februar 2011 og klage indgivet af Ungarns forening for borgerlige rettigheder til den ungarske forfatningsdomstol den 2. juni 2008.

Sverige), som ikke har gennemført direktivet, har misligholdt deres forpligtelser i henhold til EU-retten[102]. I april 2011 besluttede Kommissionen at indbringe Sverige for domstolen for anden gang for manglende efterlevelse af dommen i sag C-185/09 og anmodede om, at der blev pålagt en tvangsbøde i medfør af artikel 260 i TEUF, efter at det svenske parlament besluttede at udskyde vedtagelsen af lovgivningen i 12 måneder. Kommissionen følger fortsat udviklingen nøje i Østrig, som har forelagt en plan for den nært forestående vedtagelse af lovgivning til gennemførelse af direktivet.

## 5. HVILKEN ROLLE SPILLER LAGREDE DATA FOR DEN STRAFFERETLIGE RETSFORFØLGNING OG FOR RETSHÅNDHÆVELSEN?

I dette afsnit beskrives kort den funktion, som de lagrede data har ifølge medlemsstaternes bidrag til evalueringen.

### 5.1. Hvor mange lagrede data har de kompetente nationale myndigheder haft adgang til?

Mængden af både telekommunikationstrafik og anmodninger om adgang til trafikdata er stigende. Statistikker fra 19 medlemsstater for enten 2008 og/eller 2009 viser, at i hele EU blev der indgivet over 2 millioner anmodninger om data hvert år. Der er dog stor forskel på medlemsstaterne, idet der i nogle var mindre end 100 pr. år (Cypern) og i andre over 1 million pr. år (Polen). Ifølge oplysninger for 2008 eller 2009 fra 12 medlemsstater, om hvilke typer data der blev anmodet om, blev der oftest anmodet om data vedrørende mobiltelefoni (se tabel 5, 8 og 12). Det præcise formål med den enkelte anmodning fremgår ikke af statistikkerne. Tjekkiet, Letland og Polen anførte, at med hensyn til mobiltelefonidata var de kompetente myndigheder nødt til at indgive samme anmodning til hver enkelt af de største mobiltelefonioperatører, og at det reelle antal anmodninger pr. sag derfor var væsentligt lavere end det antal, der var angivet i statistikkerne.

Der er ingen indlysende forklaring på disse forskelle, selv om forskelle på indbyggertal, hyppigt forekommende forbrydelser, formålsbegrænsninger og betingelser for adgang, samt udgifter til erhvervelse af data alle er relevante faktorer.

### 5.2. Hvor gamle er de lagrede data, der er givet adgang til?

På baggrund af en statistisk opdeling for 2008 fra 9 medlemsstater[103] (se resumé i tabel 5 og nærmere oplysninger i bilaget) var ca. 90 % af de data, som de kompetente myndigheder havde adgang til, seks måneder gamle eller derunder, og ca. 70 % var tre måneder gamle eller derunder, da den første anmodning om adgang blev fremsat.

**Tabel 5: Oversigt over alderen af de data, som der er givet adgang til i ni medlemsstater, som gav oplysninger for 2008 efter datatype**

| *Alder* | *Fastnettelefoni* | *Mobiltelefoni* | *Internetdata* | *Sammenlagt* |
|---|---|---|---|---|
| Under 3 måneder | 61 % | 70 % | 56 % | 67 % |
| 3-6 måneder | 28 % | 18 % | 19 % | 19 % |

[102] Henholdsvis sag C-189/09 og sag C-185/09.

[103] Tjekkiet, Danmark, Estland, Irland, Spanien, Cypern, Letland, Malta og Det Forenede Kongerige.

| Tabel 5: Oversigt over alderen af de data, som der er givet adgang til i ni medlemsstater, som gav oplysninger for 2008 efter datatype | | | | |
|---|---|---|---|---|
| *Alder* | *Fastnettelefoni* | *Mobiltelefoni* | *Internetdata* | *Sammenlagt* |
| 6-12 måneder | 8 % | 11 % | 18 % | 12 % |
| Over 1 år | 3 % | 1 % | 7 % | 2 % |

Ifølge de fleste medlemsstater er brugen af lagrede data, der er over tre eller seks måneder gamle, mindre almindelig, men den kan have afgørende betydning og opdeles ofte i tre kategorier. For det første er der en tendens til, at der anmodes om internetdata senere end andre former for beviser i løbet af efterforskningen af en straffesag. Analyser af fastnettelefonidata og mobiltelefonidata giver ofte ledetråde, som dernæst fører til yderligere anmodninger om ældre data. Hvis efterforskningsholdet f.eks. finder et navn i løbet af efterforskningen på grundlag af fastnettelefonidata eller mobiltelefonidata, ønsker det måske at identificere, hvilken IP-adresse den pågældende person har benyttet, og det ønsker måske at finde ud af, hvem den pågældende har været i kontakt med i løbet af en periode ved hjælp af denne IP-adresse. I så tilfælde vil efterforskningsgruppen formodentlig anmode om data, der kan spore kommunikation med andre IP-adresser samt fastslå identiteten på de personer, der har anvendt de pågældende IP-adresser.

For det andet er efterforskningen af særlig grov kriminalitet, en række forbrydelser, organiseret kriminalitet og terroristangreb ofte afhængig af ældre lagrede data, som afspejler længden af den tid, det har taget at planlægge disse forbrydelser, idet disse data kan afsløre mønstre i den kriminelle adfærd og forbindelser mellem medskyldige i en forbrydelse og fastslå den kriminelle hensigt. Aktiviteter i forbindelse med komplekse økonomiske forbrydelser afsløres ofte først efter adskillige måneder. For det tredje og undtagelsesvist har medlemsstater anmodet om trafikdata fra en anden medlemsstat, som normalt kun kan frigive disse data med en retlig tilladelse som svar på en retsanmodning fra en dommer i den anmodende medlemsstat. Denne form for gensidig retsbistand kan være en langvarig proces, hvilket forklarer hvorfor nogle af dataene var over seks måneder gamle.

### 5.3. Anmodninger om lagrede data på tværs af grænser

Efterforskning af straffesager og retsforfølgninger kan indebære bevismateriale eller vidner fra flere medlemsstater eller hændelser, som fandt sted i flere medlemsstater. Ifølge medlemsstaternes statistikker vedrørte mindre end 1 % af alle dataanmodninger data, der var lagret i en anden medlemsstat. De retshåndhævende myndigheder anførte, at de foretrækker at anmode om data fra nationale operatører, som kan have lagret de ønskede data, snarere end at iværksætte en procedure for gensidig retsbistand, som kan være tidskrævende uden at give nogen garanti for, at der gives dataadgang. Rammeafgørelse 2006/960/RIA om forenkling af udvekslingen af oplysninger og efterretninger mellem medlemsstaternes retshåndhævende myndigheder[104], som fastsætter frister for videregivelse af oplysninger på en anden medlemsstats anmodning, finder ikke anvendelse, fordi lagrede data anses for at være oplysninger, der er opnået ved hjælp af tvangsindgreb, hvilket falder uden for instrumentets anvendelsesområde. Ikke desto mindre har ingen medlemsstater eller retshåndhævende myndigheder opfordret til, at udvekslingen på tværs af grænser gøres lettere.

---

104 Rådets rammeafgørelse 2006/960/RIA af 18. december 2006 om forenkling af udvekslingen af oplysninger og efterretninger mellem medlemsstaternes retshåndhævende myndigheder, EUT L 386 af 29.12.2006, s. 89-100 og EUT L 200 af 1.8.2007, s. 637-648.

## 5.4. Værdien af lagrede data for efterforskning og retsforfølgning af straffesager

Selv om det absolutte antal dataanmodninger ikke nødvendigvis afspejler dataenes værdi for de enkelte efterforskningssager, har medlemsstaterne generelt meddelt, at datalagring som minimum er nyttig og i nogle tilfælde uundværlig[105] for at forhindre og bekæmpe kriminalitet, herunder for at beskytte ofre og frikende uskyldige i straffesager. Domsfældelser bygger på tilståelser, vidneserklæringer eller retsteknisk bevismateriale. Nogle medlemsstater anfører, at lagrede trafikdata har vist sig nødvendige for at kontakte vidner, som ellers ikke ville være blevet identificeret, og for at skaffe bevis på eller spor af meddelagtighed i en forbrydelse. Visse medlemsstater[106] har endvidere hævdet, at brugen af lagrede data har bidraget til at frifinde personer, som var mistænkt for en forbrydelse, uden at skulle benytte andre overvågningsmetoder, såsom aflytning og husransagelse, som kunne anses for at være mere indgribende.

Der findes ingen generel definition af "grov kriminalitet" i EU, og der er derfor ingen EU-statistikker om tilfælde af grov kriminalitet eller om efterforskning og retsforfølgning af grov kriminalitet, selv om der jævnligt offentliggøres data om kriminalitet og straffesager. Den samlede mængde anmodninger om lagrede data blev af 19 medlemsstater, som indsendte nogle data for 2009 og/eller 2008, anslået til ca. 2,6 millioner. Ud fra de seneste statistikker over kriminalitet og straffesager, som findes for disse 19 medlemsstater, og som henviser til alle anmeldte forbrydelser og ikke kun til alvorlige forbrydelser, var der lige over to anmodninger pr. politibetjent pr. år eller 11 anmodninger pr. 100 anmeldte forbrydelser[107].

På grundlag af de foreliggende statistikker og illustrative eksempler, som knytter anvendelsen af lagrede historiske kommunikationsdata til antallet af domme, frifindelser, frafaldne sager og forhindrede forbrydelser, kan der drages en række konklusioner med hensyn til den rolle og værdi, lagrede data har for efterforskningen af straffesager.

*Etablering af beviser*

For det første bidrager lagrede data til at etablere spor af beviser forud for en forbrydelse. De bruges til at af- eller bekræfte andre former for bevis på aktiviteter og relationer mellem mistænkte. Særlig lokaliseringsdata er blevet anvendt både af retshåndhævende myndigheder og af forsvarere til at udelukke mistænkte fra forbrydelser og til at bekræfte alibier. Denne form for bevis kan derfor udelukke personer fra efterforskningen af straffesager og dermed fjerne behovet for mere forstyrrende undersøgelser, eller de kan fører til frifindelse. Belgien nævner den dom, der blev afsagt af retten i Antwerpen i 2008 over forbryderne bag tiger-kidnapningen af en ansat, hvor lokaliseringsdataene knyttede en forbindelse mellem

---

105 Tjekkiet fandt, at datalagring var ganske uundværlig i en lang række sager; Ungarn anførte, at den var uundværlig for de retshåndhævende myndigheders løbende arbejde; Slovenien anførte, at manglen på lagrede data ville lamme de retshåndhævende myndigheders arbejde og en politimyndighed i Det Forenede Kongerige anførte, at trafikdata var absolut nødvendig for efterforskningen af terrortrusler og grov kriminalitet.

106 Tyskland, Polen, Slovenien og Det Forenede Kongerige.

107 I 2007 var der 1,7 millioner politifolk i EU-27, hvoraf 1,2 millioner hørte til i de 19 medlemsstater, som indsendte statistikker om anmodninger om lagrede data; i 2007 registrerede politiet i EU 29,2 millioner forbrydelser, hvoraf 24 millioner blev registreret i de 19 medlemsstater, der indsendte statistikker (kilde: Eurostat 2009).

forbrydernes aktiviteter i tre forskellige byer og var afgørende for, at juryen blev overbevist om deres skyld. I et andet eksempel vedrørende et mord i 2007 i forbindelse med en motorcykelbande viste lokaliseringsdata fra forbrydernes mobiltelefoner, at de befandt sig i området, da mordet fandt sted, og det førte til en delvis tilståelse[108]. Ifølge Belgien, Irland og Det Forenede Kongerige kan visse former for kriminalitet, som involverer kommunikation via internettet, *kun* efterforskes ved hjælp af lagrede data: trusler om vold, som fremsættes i chat rooms, efterlader f.eks. intet andet spor end trafikdata på internettet. En lignende situation gælder i tilfælde af forbrydelser, der udføres over telefonen. Ungarn og Polen nævner en sag om svig mod ældre personer i slutningen af 2009/starten af 2010, som blev udført ved hjælp af telefonopringninger, hvor forbryderen foregav at være et familiemedlem, der havde brug for et lån, og som kun kunne identificeres ved hjælp af lagrede telefonidata.

*Indledning af efterforskningen i straffesager*

For det andet har der været efterforskningssager, som i mangel af retsteknisk bevis eller øjenvidner kun kunne indledes ved at konsultere lagrede data. Tyskland nævner som eksempel et mord på en politimand, hvor overfaldsmanden flygtede i offerets bil, som han dernæst efterlod. Det var muligt at fastlægge, at han dernæst ringede for at skaffe et alternativt transportmiddel. Der var intet retsteknisk bevis og ingen øjenvidner, der kunne identificere morderen, og myndighederne var derfor afhængige af trafikdataene for at komme videre med efterforskningen. I tilfælde af internetrelateret seksuelt misbrug af børn har datalagring været afgørende for efterforskningsresultatet. Sammen med andre efterforskningsteknikker gør lagrede data det muligt at identificere forbrugere af indhold vedrørende børnemisbrug[109], og de bidrager til at få børneofrene identificeret og reddet. Tjekkiet anførte, at uden adgang til lagrede internetdata ville det ikke have været muligt at indlede efterforskningen som led i "Operation Vilma" af et netværk af brugere og formidlere af børnepornografi. På EU-niveau har den manglende gennemførelse af bestemmelserne om datalagring hindret visse medlemsstater i at efterforske medlemmer af et omfattende internationalt pædofilinetværk ved brug af IP-adresser, som kan være op til et år gammelt, og det har stået i vejen for, at "Operation Rescue" (som får bistand af Europol) effektivt har kunnet beskytte børn mod misbrug.

Ved efterforskningen af internetkriminalitet er en IP-adresse ofte første spor. Retshåndhævelsesmyndigheder kan ved udtræk af trafikdata identificere abonnenten bag IP-adressen, før de afgør, om efterforskningen af en straffesag kan indledes. Det giver også politiet mulighed for at give potentielle ofre for internetangreb et forvarsel: hvis politiet får beslaglagt en command-and-control server, der benyttes af botnet-operatører, kan de kun se de IP-adresser, der er knyttet til den pågældende server, men ved at få adgang til lagrede data kan politiet identificere og advare potentielle ofre, som ejer de pågældende IP-adresser.

*Lagrede data er en integreret del af efterforskningen i straffesager*

---

108 Publikation fra National Policing Improvement Agency (UK), "*The Journal of Homicide and Major Incident Investigation*", Volume 5, Nr. 1, Forår 2009, s. 39-51.

109 Projektet om måling og analyse af peer-to-peer-aktivitet med fokus på pædofilt indhold ("Measurement and analysis of p2p activity against paedophile content"), som får støtte af Safer internet-programmet, gav nøjagtige oplysninger om pædofile aktiviteter i p2p-systemet eDonkey, og gjorde det muligt at identificere 178 000 brugere (ud af 89 millioner screenede brugere), som anmodede om pædofilt indhold.

For det tredje er lagrede data en integreret del af efterforskningen og retsforfølgningen af straffesager i EU, selv om retshåndhævende myndigheder og domstole i de fleste medlemsstater ikke fører statistikker over, hvilken form for bevis der var afgørende for dommen eller frifindelsen. Visse medlemsstater anførte, at virkningen af de lagrede data for efterforskningen og retsforfølgningen af straffesager ikke altid kan vurderes isoleret, fordi domstolene tager al bevismateriale i betragtning og sjældent finder, at ét bestemt bevis er afgørende[110]. Nederlandene meddelte, at fra januar til juli 2010 var historiske trafikdata en afgørende faktor i 24 domme. Finland anførte, at ud af 3 405 anmodninger viste de lagrede data i 56 % af tilfældene sig at være vigtige eller afgørende for afsløringen og/eller retsforfølgningen af en straffesag. Det Forenede Kongerige indsendte data, som skulle kvantificere virkningen af datalagring på strafferetlige retsforfølgninger; det fremgik, at for tre af de retshåndhævende myndigheders vedkommende var lagrede data nødvendige i om ikke alle så næsten alle tilfælde af efterforskning af straffesager, som førte til retsforfølgning eller domsfældelse.

## 5.5. Teknologisk udvikling og brugen af forudbetalte SIM-kort

Retshåndhævelsen skal holde trit med den teknologiske udvikling, som benyttes til at begå eller bidrage til kriminalitet. Datalagring er et af de efterforskningsværktøjer, der er nødvendigt, hvis de retshåndhævende myndigheder skal kunne tackle nutidens mangeartede forbrydelser og den hastighed, hvormed de begås. En række stadig mere almindelige former for kommunikation ligger uden for direktivets anvendelsesområde. Virtuelle private netværk (VPN) på f.eks. universiteter eller i store virksomhedskoncerner giver adskillige brugere mulighed for at få adgang til internettet ved hjælp af én fælles gateway ved brug af samme IP-adresse. Nyt teknologi, som gør det muligt at give adresser til de enkelte VPN-brugere, er dog ved at blive indført.

Andelen af mobiltelefonbrugere, som benytter forudbetalte tjenester, varierer i EU. Nogle medlemsstater har hævdet, at anonyme forudbetalte SIM-kort, især hvis de købes i en anden medlemsstat, også kan anvendes af dem, der er involveret i kriminalitet, som et middel til at undgå at blive identificeret som følge af efterforskning af en straffesag[111]. Seks medlemsstater (Danmark, Spanien, Italien, Grækenland, Slovakiet og Bulgarien) har vedtaget foranstaltninger, der kræver registrering af forudbetalte SIM-kort. Disse og andre medlemsstater (Polen, Cypern og Litauen) er fortalere for en EU-omspændende foranstaltning om obligatorisk registrering af brugerne af forudbetalte tjenester. Der foreligger endnu ingen dokumentation for, hvor effektive disse nationale foranstaltninger er. Der er påpeget potentielle begrænsninger, f.eks. i tilfælde af identitetstyveri eller hvis et SIM-kort er købt af en tredjepart, eller hvis en bruger roamer med et kort, der er købt i et tredjeland. Alt i alt er Kommissionen ikke overbevist om, at der på nuværende tidspunkt er behov for foranstaltninger på EU-plan på dette område.

---

110 Belgien, Tjekkiet og Litauen.

111 Rådets konklusioner om bekæmpelse af kriminel misbrug og kriminel anonym anvendelse af elektronisk kommunikation.

## 6. VIRKNINGEN AF DATALAGRING PÅ OPERATØRER OG FORBRUGERE

### 6.1. Operatører og forbrugere

I en fælles erklæring til Kommissionen anførte fem større brancheforeninger, at den økonomiske virkning af direktivet var "betydelig" eller "enorm" for mindre operatører, fordi direktivet giver stor manøvrefrihed[112]. Otte operatører indgav meget forskellige skøn over de udgifter, der i form af anlægs- og driftsudgifter er forbundet med efterlevelsen af direktivet. Dette kan bekræftes af oplysninger om godtgørelse af operatørernes udgifter fra fire medlemsstater (se tabel 6).

I en undersøgelse, som blev foretaget før direktivets gennemførelse i de fleste medlemsstater, blev udgifterne til etablering af et system til datalagring for en internetudbyder med en halv million kunder anslået til 375 240 EUR i det første år og til 9 870 EUR i driftsudgifter pr. måned derefter[113], og udgifterne til etablering af et system til dataudtræk blev anslået til 131 190 EUR med driftsudgifter på 28 960 EUR pr. måned. Den tyske forfatningsdomstol fandt imidlertid i sin dom af 2. marts 2010, at indførelsen af en lagringspligt hverken var speciel byrdefuld for den pågældende tjenesteudbyder, eller at den udgjorde en urimelig finansiel byrde for virksomheden[114]. Udgifterne pr. lagret dataenhed er omvendt proportional med operatørernes størrelse og den grad af standardisering, der er i medlemsstaternes samarbejde med operatører[115].

De fleste operatører kunne i deres svar på Kommissionens spørgeskema ikke kvantificere direktivets indvirkning på konkurrencen, forbrugerpriserne eller investeringer i ny infrastruktur og nye tjenester.

Der er ikke noget, der tyder på, at direktivet har en målelig eller væsentlig indvirkning på forbrugerpriserne på elektroniske kommunikationstjenester; der var ingen bidrag fra forbrugerorganisationer til den offentlige høring i 2009. Det fremgik af en undersøgelse, som blev foretaget i Tyskland på vegne af en civilsamfundsorganisation, at forbrugerne havde til hensigt at ændre deres kommunikationsmønster og undgå elektroniske kommunikationstjenester under visse omstændigheder, men der er intet, der bekræfter, at der er sket en adfærdsændring hverken i enkelte medlemsstater eller i EU generelt[116].

Kommissionen vil vurdere virkningen af fremtidige ændringer af direktivet på branchen og forbrugerne, eventuelt ved en specifik Eurobarometer-undersøgelse, for at danne sig et indtryk af offentlighedens opfattelse.

### 6.2. Godtgørelse af udgifter

Direktivet regulerer ikke godtgørelsen af de udgifter, operatørerne har som følge af kravene om datalagring. Ved disse udgifter forstås:

---

112 http://www.gsmeurope.org/documents/Joint_Industry_Statement_on_DRD.PDF

113 En undersøgelse foretaget af Wilfried Gansterer & Michael Ilger: "Data retention – The EU Directive 2006/24/EC from a Technological Perspective", Wien: Verlag Medien und Recht, 2008.

114 Bundesverfassungsgericht, 1 BvR 256/08 af 2. marts 2010, § 299.

115 http://www.etsi.org/website/technologies/lawfulinterception.aspx

116 Undersøgelsen blev foretaget af Forsa på foranledning af AK Vorratsdatenspeicherung. http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf

(a) *driftsudgifter*, dvs. driftsudgifter eller faste udgifter, som vedrører driften af virksomheden, en anordning, en komponent, udstyr eller faciliteter og

(b) *anlægsudgifter,* dvs. udgifter, der skaber fremtidige fordele, eller udgifter til udvikling eller tilvejebringelse af ikke-forbrugelige dele til produktet eller systemet, hvilket kan omfatte personaleomkostninger og udgifter til faciliteter, såsom leje og forsyningsydelser.

Alle medlemsstater sikrer en vis form for godtgørelse, når der anmodes om data i forbindelse med en strafferetlig retssag. To medlemsstater har anført, at de godtgør både driftsudgifter og anlægsudgifter. Seks medlemsstater godtgør kun driftsudgifter. Der er ikke anmeldt nogen anden godtgørelsesordning til Kommissionen. Nærmere oplysninger fremgår af tabel 6.

**Tabel 6: Medlemsstater, som godtgør udgifter**

| **Medlemsstat** | **Driftsudgifter** | **Anlægsudgifter** | **Årlige godtgørelsesudgifter (mio. EUR)** |
|---|---|---|---|
| Belgien | Ja | Nej | 22 (2008) |
| Bulgarien | Nej | Nej | - |
| Tjekkiet | Ikke gennemført[117]. | | |
| Danmark | Ja | Nej | - |
| Tyskland | Ikke gennemført. | | |
| Estland | Ja | Nej | - |
| Irland | Nej | Nej | - |
| Grækenland | Nej | Nej | - |
| Spanien | Nej | Nej | - |
| Frankrig | Ja | Nej | - |
| Italien | - | - | - |
| Cypern | Nej | Nej | - |
| Letland | Nej | Nej | - |
| Litauen | Ja, mod begrundet anmodning. | Nej | - |
| Luxembourg | Nej | Nej | - |
| Ungarn | Nej | Nej | - |
| Malta | Nej | Nej | - |
| Nederlandene | Ja | Nej | - |
| Østrig | Ikke gennemført. | | |
| Polen | Nej | Nej | - |
| Portugal | Nej | Nej | - |
| Rumænien | Ikke gennemført. | | |
| Slovenien | Nej | Nej | - |
| Slovakiet | Nej | Nej | - |
| Finland | Ja | Ja | 1 |
| Sverige | Ikke gennemført. | | |
| Det Forenede Kongerige | Ja | Ja | 55 (for udgifter, der er påløbet i løbet af tre år) |

På baggrund af ovenstående kan det konkluderes, at målet med direktivet om at skabe lige vilkår for operatører i EU ikke er nået fuldt ud. Kommissionen vil undersøge mulighederne

[117] Før annulleringen af gennemførelseslovgivningen godtgjorde Tjekkiet både drifts- og anlægsudgifter til et beløb af 6,8 mio. EUR i 2009.

for at mindske hindringerne for det indre markeds funktion ved at sikre, at operatørerne mere konsekvent får godtgjort de udgifter, de har til efterlevelse af datalagringskravene, særlig små og mellemstore operatører.

## 7. DATALAGRINGENS KONSEKVENSER FOR DE GRUNDLÆGGENDE RETTIGHEDER

### 7.1. Den grundlæggende ret til privatlivets fred og beskyttelse af personoplysninger

Datalagring er en begrænsning af retten til privatlivets fred og beskyttelse af personoplysninger, som er grundlæggende rettigheder i EU[118]. En sådan begrænsning skal ifølge artikel 52, stk. 1, i chartret om grundlæggende rettigheder "være fastlagt i lovgivningen og skal respektere disse rettigheders og friheders væsentligste indhold. Under iagttagelse af proportionalitetsprincippet kan der kun indføres begrænsninger, såfremt disse er nødvendige og faktisk svarer til mål af almen interesse, der er anerkendt af Unionen, eller et behov for beskyttelse af andres rettigheder og friheder". I praksis betyder det, at enhver begrænsning[119]:

(a) skal være formuleret tydeligt og forudsigeligt

(b) skal være nødvendig for at opfylde et mål af almen interesse eller for at beskytte andres rettigheder og friheder

(c) skal være proportionel i forhold til det forfulgte mål og

(d) skal være forenelig med hovedindholdet i de pågældende grundlæggende rettigheder.

Ifølge artikel 8, stk. 2, i Den Europæiske Menneskerettighedskonvention kan en offentlig myndighed gøre indgreb i udøvelsen af en persons ret til privatlivets fred, såfremt det sker af hensyn til den nationale sikkerhed, den offentlige tryghed eller for at forebygge en forbrydelse[120]. Artikel 15, stk. 1, i e-data-direktivet og betragtningerne i datalagringsdirektivet bekræfter disse principper, som understøtter EU's tilgang til datalagring.

EU-Domstolen og Den Europæiske Menneskerettighedsdomstol har gennem retspraksis fastlagt betingelser, som enhver begrænsning i retten til privatlivets fred skal opfylde. Disse domme har betydning for, om direktivet bør ændres, navnlig med hensyn til betingelserne for adgang til og brug af lagrede data.

*Enhver begrænsning af retten til privatliv skal være formuleret tydeligt og forudsigeligt*

---

118 Artikel 7 og 8 i Den Europæiske Unions charter om grundlæggende rettigheder (EUT C 83 af 30.3.2010, s. 389) garanterer alle "ret til beskyttelse af personoplysninger, der vedrører den pågældende." Artikel 16 i traktaten om Den Europæiske Unions funktionsmåde (EUT C 83 af 30.3.2010, s. 1) garanterer ligeledes "ret til beskyttelse af personoplysninger om vedkommende selv."

119 Se Kommissionens tjekliste for grundlæggende rettigheder for alle lovgivningsmæssige forslag i Kommissionens meddelelse KOM(2010) 573/4 "Strategi for Den Europæiske Unions effektive gennemførelse af chartret om grundlæggende rettigheder".

120 Artikel 8 i konvention til Beskyttelse af Menneskerettigheder og Grundlæggende Frihedsrettigheder (ETS nr. 5), Europarådet, 4.11.1950.

I sagen om *Österreichischer Rundfunk* fastslog EU-Domstolen, at enhver lovgivningsmæssig indgriben i retten til privatliv skal være "affattet tilstrækkeligt præcist til, at lovens adressater kan tilpasse deres adfærd, ... [således at den] opfylder kravet om forudsigelighed".

*Enhver begrænsning i retten til privatliv skal være nødvendig og have et minimum af garantier*

I sagen "Copland v. the United Kingdom", som vedrørte statens overvågning af en persons telefonopkald, e-mail og brug af internettet, fastslog Den Europæiske Menneskerettighedsdomstol, at en sådan begrænsning i retten til privatlivets fred kun kunne anses for at være nødvendig, hvis den var baseret på relevant national lovgivning[121]. Sagen "S. and Marper v. the United Kingdom", som vedrørte lagring af DNA-profiler eller fingeraftryk fra en person, der er dømt for en forbrydelse, eller hvis sag frafaldes inden dom, fastslog domstolen, at en sådan begrænsning i retten til privatliv kun kan retfærdiggøres, hvis den opfylder et vigtigt socialt behov, hvis den er proportionel med det forfulgte mål, og hvis de grunde, den offentlige myndighed havde fremsat, er relevante og tilstrækkelige[122]. Ifølge databeskyttelses vigtigste principper skal datalagringen være proportionel med formålet med dataindsamlingen, og lagringsperioden skal være begrænset[123]. Med hensyn til telefonaflytning, hemmelig overvågning og skjult efterretningsindsamling er det essentielt at have klare, detaljerede regler for foranstaltningernes anvendelsesområde, samt et minimum af sikkerhedsgarantier vedrørende bl.a. varighed, lagring, anvendelse, tredjeparts adgang, procedurer til sikring af dataenes integritet og fortrolighed samt procedurer for dataenes tilintetgørelse, og derved i tilstrækkelig grad sikre dataene mod risikoen for misbrug og vilkårlighed.

*Enhver begrænsning af retten til privatlivets fred skal være proportionel med mål af almen interesse*

EU-Domstolen fastslog ligeledes i sin dom om Schecke og Eifert vedrørende offentliggørelse på internettet af oplysninger om modtagerne af landbrugsmidler[124], at det ikke så ud til, at EU-lovgiverne havde truffet de fornødne foranstaltninger til at foretage en afvejning af respekten for retten til privatlivets fred og mål af almen interesse (åbenhed) som anerkendt af EU. Domstolen fandt navnlig, at lovgiverne ikke havde taget andre fremgangsmåder i betragtning, som kunne have været forenelige med formålet og samtidig være mindre indgribende i støttemodtagernes ret til respekt for privatlivets fred og beskyttelse af personoplysninger. Domstolen hævdede derfor, at lovgiverne havde overskredet proportionalitetsgrænserne, da "begrænsninger af beskyttelsen af personoplysninger skal holdes inden for det strengt nødvendige".

---

121 Copland v. the United Kingdom, dom afsagt af Den Europæiske Menneskerettighedsdomstol, Strasbourg 3.4.2007, s. 9.

122 Marper v the United Kingdom, dom afsagt af Den Europæiske Menneskerettighedsdomstol, Strasbourg 4.12.2008, s. 31.

123 Marper, s. 30.

124 C-92/09, Volker und Markus Schecke GbR mod Land Hessen, og C-93/09, Eifert mod Land Hessen og Bundesanstalt für Landwirtschaft und Ernährung, 9.11.10.

## 7.2. Kritik af princippet om datalagring

Mange civilsamfundsorganisationer har skrevet til Kommissionen og hævdet, at datalagring i princippet er en uberettiget og unødvendig indskrænkning af privatpersoners ret til privatliv. De betragter den omfattende og vilkårlige lagring af trafikdata, lokaliseringsdata og abonnentdata i forbindelse med personers telekommunikation, som finder sted uden samtykke, som en ulovlig indskrænkning af de grundlæggende rettigheder. Efter en sag, som er indbragt for domstolen i en medlemsstat (Irland) af en borgerrettighedsgruppe, forventes spørgsmålet om direktivets lovlighed at blive forelagt for EU-Domstolen[125]. Den europæiske tilsynsførende for databeskyttelse udtrykte ligeledes tvivl om, hvorvidt foranstaltningen var nødvendig.

## 7.3. Der opfordres til større datasikkerhed og bedre databeskyttelsesregler

Artikel 29-gruppen anførte i sin rapport om anden håndhævelsesforanstaltning, at risikoen for, at kommunikationsfortroligheden og ytringsfriheden krænkes, er uløseligt forbundet med lagringen af trafikdata. Den kritiserede visse aspekter af den nationale gennemførelse, navnlig datalogging, lagringsperioder, typen af lagrede data og datasikkerhedsforanstaltninger. Arbejdsgruppen rapporterede om sager, hvor detaljer af *indholdet* i internetkommunikation, som falder uden for direktivets anvendelsesområde, blev lagret, herunder IP-modtageradresser, websteders URL, e-mailhovedet og listen over modtagere i "cc" feltet. Den anmodede derfor om, at det præciseres, at kategorierne er udtømmende, og at operatørerne ikke bør pålægges yderligere forpligtelser til datalagring.

Den Europæiske Tilsynsførende for Databeskyttelse har vurderet, at direktivet ikke har formået at harmonisere den nationale lovgivning, og at brugen af lagrede data ikke er strengt begrænset til bekæmpelsen af grov kriminalitet[126]. Han har anført, at et EU-instrument, der indeholder regler om obligatorisk datalagring, også såfremt det viser sig nødvendigt, bør indeholde regler om de retshåndhævende myndigheders adgang til og videre anvendelse af data. Han opfordrede EU til at vedtage omfattende retsregler, som ikke kun pålægger operatørerne en forpligtelse til at lagre data, men også fastlægger, hvordan medlemsstaterne skal anvende dataene til retshåndhævelsesformål, for derved at give borgerne den fornødne retssikkerhed.

Datatilsynsmyndighederne har generelt hævdet, at datalagring i sig selv indebærer en risiko for krænkelse af privatlivets fred, hvilket ikke reguleres på EU-plan af direktivet, som i stedet pålægger medlemsstaterne at sikre, at de nationale databeskyttelsesregler overholdes. Selv om der ikke er nogen konkrete eksempler på alvorlige krænkelser af privatlivets fred, er der alligevel en risiko for, at datasikkerheden krænkes, og den vil muligvis stige med udviklingen inden for teknologi og kommunikationsformer, hvad enten data lagres af kommercielle eller sikkerhedsmæssige hensyn, både i og uden for EU, medmindre der træffes yderligere sikkerhedsforanstaltninger.

---

125 Den 5. maj 2010 efterkom højesteretten i Irland Digital Rights Ireland Limiteds begæring om at få sagen forelagt for EU-Domstolen i medfør af artikel 267 i TEUF.

126 Tale ved Peter Hustinx på konferencen "Taking on the Data Retention Directive" af 3. december 2010.

## 8. KONKLUSION OG ANBEFALINGER

I denne rapport påpeges en række fordele ved det nuværende datalagringssystem i EU samt nogle områder, hvor det kan forbedres. EU vedtog direktivet på et tidspunkt, hvor alarmberedskabet over for trusler om terrorangreb var højt. Den konsekvensanalyse, som Kommissionen har til hensigt at foretage, er en mulighed for at vurdere datalagringen i EU og efterprøve, om den opfylder kravene om nødvendighed og proportionalitet under hensyn til den interne sikkerhed, et velfungerende indre marked og en øget respekt for privatlivets fred og den grundlæggende ret til beskyttelse af personoplysninger. Kommissionens forslag til en revision af datalagringsreglerne bør bygge på følgende konklusioner og anbefalinger.

### 8.1. EU bør støtte og regulere datalagring som en sikkerhedsforanstaltning

De fleste medlemsstater er af den opfattelse, at EU-regler om datalagring er nødvendige som et værktøj til retshåndhævelse og beskyttelse af ofre og de strafferetlige systemer. Medlemsstaternes dokumentation, som består af statistikker og eksempler, er begrænset på nogle områder, men vidner ikke desto mindre om, at datalagring spiller en vigtig rolle for efterforskningen af straffesager. Dataene udgør vigtige spor og bevis i arbejdet med at forebygge og retsforfølge kriminalitet og sikre retfærdig rettergang i straffesager. De har resulteret i domsfældelser for forbrydelser, som uden datalagring måske aldrig ville være blevet opklaret. De har også betydet, at uskyldige er blevet frifundet. Harmoniserede regler på området bør sikre, at datalagring er et effektivt værktøj til bekæmpelse af kriminalitet, at sektoren har retssikkerhed i et velfungerende indre marked, og at respekten for privatlivets fred og beskyttelsen af personoplysninger er høj over alt i EU.

### 8.2. Gennemførelsen har været uens

22 medlemsstater har gennemført direktivet i national lovgivning. Det er meget vanskeligt at vurdere datalagringsdirektivet grundet det forholdsvis store spillerum, medlemsstaterne har til at vedtage datalagringsforanstaltninger i medfør af artikel 15, stk. 1, i e-data-direktivet. Der er betydelige forskelle i de nationale gennemførelsesbestemmelser med hensyn til formålsbegrænsning, adgang til data, lagringsperioder, databeskyttelse, datasikkerhed og statistikker. Tre medlemsstater har misligholdt direktivet, siden gennemførelsen i national lovgivning blev annulleret af deres respektive forfatningsdomstole. To medlemsstater mangler stadig at gennemføre direktivet i national lovgivning. Kommissionen vil fortsat arbejde sammen med alle medlemsstater for at sikre en effektiv implementering af direktivet. Den vil også fortsat holde øje med, at EU-retten håndhæves, og om nødvendigt indlede traktatbrudssager.

### 8.3. Direktivet har ikke fuldt ud harmoniseret datalagring og har ikke skabt lige vilkår for operatørerne

Direktivet har sikret, at data nu lagres i de fleste medlemsstater. Direktivet giver ikke i sig selv nogen garanti for, at lagrede data lagres, udtrækkes eller anvendes i fuld overensstemmelse med retten til privatlivets fred og beskyttelse af personlige oplysninger. Ansvaret for at sikre, at disse rettigheder respekteres, ligger hos medlemsstaterne. Direktivet tilstræber kun en delvis harmonisering af datalagring: derfor er det ingen overraskelse, at der ikke findes en fælles tilgang, hvad enten det drejer sig om specifikke bestemmelser i direktivet, såsom formålsbegrænsning eller lagringsperioder, eller om aspekter uden for direktivets anvendelsesområde, såsom godtgørelse af udgifter. Ud over de

variationsmuligheder, direktivet giver, har forskelle i den nationale anvendelse af datalagring imidlertid skabt betydelige vanskeligheder for operatører.

### 8.4. Operatører bør konsekvent få godtgjort deres udgifter

Retssikkerheden er stadig utilstrækkelig for sektoren. Forpligtelsen til at lagre og udtrække data udgør en væsentlig udgift for operatører, navnlig mindre operatører, og operatører i forskellige medlemsstater påvirkes forskelligt og får godtgjort deres udgifter i forskellig grad, selv om det ikke er påvist, at telekommunikationssektoren overordnet set er blevet påvirket negativt af direktivet. Kommissionen vil overveje, hvordan man kan sikre en mere ensartet godtgørelse af operatørernes udgifter.

### 8.5. Proportionalitetsprincippet skal respekteres i hele forløbet for lagring, udtræk og anvendelse af data

Kommissionen vil sikre, at et kommende forslag om datalagring respekterer proportionalitetsprincippet, at det er egnet til formålet om at bekæmpe grov kriminalitet og terrorisme, og at det ikke er mere vidtrækkende end nødvendigt. Den anerkender, at eventuelle undtagelser eller begrænsninger i forbindelse med beskyttelsen af personlige oplysninger kun bør gælde, hvis de er nødvendige. Den vil se nøje på, hvilken indflydelse en mere stringent regulering af lagringen af, adgangen til og anvendelsen af trafikdata har på, hvor effektiv retshåndhævelsen og det strafferetlige system er, samt på retten til privatliv og den offentlige administrations og operatørernes udgifter. Følgende områder bør især undersøges i konsekvensanalysen:

(1)Konsekvens i formålsbegrænsningen for datalagring og i de former for forbrydelser, som giver adgang til og ret til at anvende lagrede data

(2)Større harmonisering og om muligt afkortning af de obligatoriske datalagringsperioder

(3)Uafhængigt tilsyn med dataanmodninger og det generelle datalagringssystem i alle medlemsstater

(4)Begrænsning af de myndigheder, der har bemyndigelse til at få dataadgang

(5)Reduktion af de datakategorier, der kan lagres

(6)Vejledning i tekniske og organisatoriske sikkerhedsforanstaltninger for dataadgang, herunder afleveringsprocedurer

(7)Vejledning i brugen af data, herunder data mining og

(8)Udvikling af praktisk anvendelige målingsmetoder og rapporteringsprocedurer for at gøre det lettere at sammenligne anvendelsen og evalueringen af fremtidige regler.

Kommissionen vil også overveje, om og i givet fald hvordan en EU-tilgang til hastesikring af data kunne supplere datalagring.

Med henvisning til tjeklisten for grundlæggende rettigheder og tilgangen til informationsstyring på området frihed, sikkerhed og retfærdighed[127] vil Kommissionen se på hvert af disse områder i overensstemmelse med proportionalitetsprincippet og kravet om forudsigelighed. Den vil også sikre overensstemmelse med den igangværende revision af EU's databeskyttelsesregler[128].

### 8.6. Næste skridt

I lyset af denne evaluering vil Kommissionen foreslå en revision af de nuværende datalagringsregler. Den vil finde frem til en række løsningsmuligheder i samråd med retshåndhævende myndigheder, dommerstanden, erhvervssektoren, forbrugergrupper, datatilsynsmyndigheder og civilsamfundsorganisationer. Den vil undersøge offentlighedens opfattelse af datalagring, og datalagringens indflydelse på adfærden. Resultaterne heraf vil indgå i en konsekvensanalyse af den valgte løsningsmodel, som vil danne grundlag for Kommissionens forslag.

---

127 Se ovenstående henvisning til meddelelse om gennemførelsen af chartret for grundlæggende rettigheder og "Oversigt over informationsstyring på området frihed, sikkerhed og retfærdighed", KOM(2010) 385 af 20.7.2010.

128 KOM(2010) 609 af 4.11.2010.

## Bilag: Yderligere statistikker om lagring af trafikdata

Bemærkninger til bilag:

1. Ved dataenes alder forstås tidsrummet mellem den dato, hvor dataene lagres, og den dato, hvor den kompetente myndighed anmoder om udlevering af dataene.

2. Ved internetdata forstås data vedrørende internetadgang, e-mail og telefoni via internettet.

3. Statistikkerne for Tjekkiet, Letland og Polen bør tages med et vist forbehold (jf. afsnit 5.1)

### Medlemsstaternes statistikker for 2008

**Tabel 7: Anmodninger om lagrede data efter alder i 2008**

| **Dataenes alder (i måneder) pr. medlemsstat** | **0-3** | **3-6** | **6-9** | **9-12** | **12-15** | **15-18** | **18-21** | **21-24** | **I alt** |
|---|---|---|---|---|---|---|---|---|---|
| Belgien | Ikke oplyst | | | | | | | | |
| Bulgarien | Ikke oplyst | | | | | | | | |
| Tjekkiet | 102691 | 18440 | 10110 | 319 | 0 | 0 | 0 | 0 | 131560 |
| Danmark | 2669 | 672 | 185 | 37 | 23 | 2 | 7 | 4 | 3599 |
| Tyskland | 9363 | 2336 | 985 | 0 | 0 | 0 | 0 | 0 | 12684 |
| Estland | 2773 | 733 | 157 | 827 | 0 | 0 | 0 | 0 | 4490 |
| Irland | 8981 | 2016 | 936 | 1855 | 90 | 85 | 78 | 54 | 14095 |
| Grækenland | Opdeling efter alder ikke oplyst | | | | | | | | 584 |
| Spanien | 22629 | 15868 | 10298 | 4783 | 0 | 0 | 0 | 0 | 53578 |
| Frankrig | Opdeling efter alder ikke oplyst | | | | | | | | **503437** |
| Italien | Ikke oplyst | | | | | | | | |
| Cypern | 30 | 4 | 0 | 0 | 0 | 0 | 0 | 0 | 34 |
| Letland | 10539 | 2739 | 1368 | 1211 | 597 | 438 | 0 | 0 | 16892 |
| Litauen | 55735 | 23817 | 5251 | 512 | 0 | 0 | 0 | 0 | 85315 |
| Luxembourg | Ikke oplyst | | | | | | | | |
| Ungarn | Ikke oplyst | | | | | | | | |
| Malta | 810 | 59 | 0 | 0 | 0 | 0 | 0 | 0 | 869 |
| Nederlandene | Opdeling efter alder ikke oplyst | | | | | | | | 85000 |
| Østrig | Opdeling efter alder ikke oplyst | | | | | | | | 3093 |
| Polen | Ikke oplyst | | | | | | | | |
| Portugal | Ikke oplyst | | | | | | | | |
| Rumænien | Ikke oplyst | | | | | | | | |
| Slovenien | Opdeling efter alder ikke oplyst | | | | | | | | 2821 |
| Slovakiet | Ikke oplyst | | | | | | | | |
| Finland | 9134 | 1144 | 448 | 214 | 268 | | | | 4008 |
| Sverige | Ikke oplyst | | | | | | | | |
| Det Forenede Kongerige | 315350 | 88339 | 34665 | 19398 | 6385 | 2973 | 1536 | 1576 | 470222 |
| **I alt** | **533504** | **156167** | **64403** | **29156** | **7095*** | **3230*** | **1353*** | **1366*** | **1392281** |

* Finland eksklusiv.

| Tabel 8: Anmodninger om lagrede trafikdata efter datatype i 2008<br>(hvor dette er oplyst, angiver tallet i parentes antallet af anmodninger om data, der ikke kunne efterkommes) | | | | |
|---|---|---|---|---|
| **Datatype<br>Medlemsstat** | **Fastnettelefoni** | **Mobiltelefoni** | **Internetdata** | **I alt** |
| Belgien | Ikke oplyst | | | |
| Bulgarien | Ikke oplyst | | | |
| Tjekkiet | **4983 (131)** | **125040 (2276)** | **1537 (83)** | **131560 (2490)** |
| Danmark | **192 (0)** | **3273 (5)** | **134 (0)** | **3599 (5)** |
| Tyskland | Opdeling efter. datatype ikke oplyst | | | **12684 (931)** |
| Estland | **4114 (1519)** | **376 (7)** | **Ikke oplyst** | **4490 (1526)** |
| Irland | **5317 (16)** | **5873 (48)** | **2905 (33)** | **14095 (97)** |
| Grækenland | Opdeling efter datatype ikke oplyst | | | **584** |
| Spanien | **4448 (0)** | **40013 (0)** | **9117 (0)** | **53578 (0)** |
| Frankrig | Opdeling efter datatype ikke oplyst | | | **503437** |
| Italien | Ikke oplyst | | | |
| Cypern | **3 (0)** | **31 (5)** | **0 (0)** | **34 (5)** |
| Letland | **1602 (90)** | **14238 (530)** | **1052 (76)** | **16892 (696)** |
| Litauen | **765 (72)** | **84550 (5657)** | **Ikke oplyst** | **85315 (5729)** |
| Luxembourg | Ikke oplyst | | | |
| Ungarn | Ikke oplyst | | | |
| Malta | **29 (0)** | **748 (120)** | **92 (13)** | **869 (133)** |
| Nederlandene | Opdeling efter datatype ikke oplyst | | | **85000** |
| Østrig | Opdeling efter datatype ikke oplyst | | | **3093** |
| Polen | Ikke oplyst | | | |
| Portugal | Ikke oplyst | | | |
| Rumænien | Ikke oplyst | | | |
| Slovenien | Opdeling efter datatype ikke oplyst | | | **2821** |
| Slovakiet | Ikke oplyst | | | |
| Finland | Opdeling efter datatype ikke oplyst | | | **4008** |
| Sverige | Ikke oplyst | | | |
| Det Forenede Kongerige | **90747 (0)** | **329421 (0)** | **50054 (0)** | **470222 (0)** |
| **I alt** | | | | **1392281** |

| Tabel 9: Anmodninger, som blev efterkommet i 2008, om lagrede trafikdata vedrørende fastnettelefoni efter alder | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Dataenes alder (i måneder) pr. medlemsstat** | **0-3** | **3-6** | **6-9** | **9-12** | **12-15** | **15-18** | **18-21** | **21-24** | **I alt** |
| Belgien | Ikke oplyst | | | | | | | | |
| Bulgarien | Ikke oplyst | | | | | | | | |
| Tjekkiet | 3669 | 916 | 143 | 124 | 0 | 0 | 0 | 0 | 4852 |
| Danmark | 133 | 28 | 31 | 0 | 0 | 0 | 0 | 0 | 192 |
| Tyskland | Ikke oplyst | | | | | | | | |
| Estland | 1876 | 161 | 74 | 484 | 0 | 0 | 0 | 0 | 2595 |
| Irland | 4118 | 712 | 197 | 182 | 32 | 21 | 23 | 16 | 5301 |
| Grækenland | Ikke oplyst | | | | | | | | |
| Spanien | 1948 | 1431 | 741 | 328 | 0 | 0 | 0 | 0 | 4448 |
| Frankrig | Ikke oplyst | | | | | | | | |
| Italien | Ikke oplyst | | | | | | | | |
| Cypern | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 |
| Letland | 698 | 213 | 167 | 193 | 104 | 137 | 0 | 0 | 1512 |
| Litauen | 251 | 442 | 0 | 0 | 0 | 0 | 0 | 0 | 693 |
| Luxembourg | Ikke oplyst | | | | | | | | |
| Ungarn | Ikke oplyst | | | | | | | | |
| Malta | 28 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 29 |
| Nederlandene | Ikke oplyst | | | | | | | | |
| Østrig | Ikke oplyst | | | | | | | | |
| Polen | Ikke oplyst | | | | | | | | |
| Portugal | Ikke oplyst | | | | | | | | |
| Rumænien | Ikke oplyst | | | | | | | | |
| Slovenien | Ikke oplyst | | | | | | | | |
| Slovakiet | Ikke oplyst | | | | | | | | |
| Finland | Ikke oplyst | | | | | | | | |
| Sverige | Ikke oplyst | | | | | | | | |
| Det Forenede Kongerige | 54805 | 27052 | 5340 | 753 | 1135 | 437 | 1050 | 175 | 90747 |
| **I alt** | **67529** | **30956** | **6693** | **2064** | **1271** | **595** | **1073** | **191** | **110372** |

| Tabel 10: Anmodninger, som blev efterkommet i 2008, om lagrede trafikdata vedrørende mobiltelefoni efter alder | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Dataenes alder (i måneder) pr. medlemsstat** | **0-3** | **3-6** | **6-9** | **9-12** | **12-15** | **15-18** | **18-21** | **21-24** | **I alt** |
| Belgien | Ikke oplyst | | | | | | | | |
| Bulgarien | Ikke oplyst | | | | | | | | |
| Tjekkiet | 98232 | 17013 | 7518 | 1 | 0 | 0 | 0 | 0 | 122764 |
| Danmark | 2433 | 628 | 143 | 33 | 20 | 1 | 7 | 3 | 3268 |
| Tyskland | Ikke oplyst | | | | | | | | |
| Estland | 248 | 58 | 35 | 28 | 0 | 0 | 0 | 0 | 369 |
| Irland | 4326 | 820 | 230 | 240 | 57 | 63 | 52 | 37 | 5825 |
| Grækenland | Ikke oplyst | | | | | | | | |
| Spanien | 17403 | 12114 | 7444 | 3052 | 0 | 0 | 0 | 0 | 40013 |
| Frankrig | Ikke oplyst | | | | | | | | |
| Italien | Ikke oplyst | | | | | | | | |
| Cypern | 23 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 26 |
| Letland | 8928 | 2298 | 1085 | 746 | 394 | 257 | 0 | 0 | 13708 |
| Litauen | 55484 | 23375 | 14 | 20 | 0 | 0 | 0 | 0 | 78893 |
| Luxembourg | Ikke oplyst | | | | | | | | |
| Ungarn | Ikke oplyst | | | | | | | | |
| Malta | 575 | 53 | 0 | 0 | 0 | 0 | 0 | 0 | 628 |
| Nederlandene | Ikke oplyst | | | | | | | | |
| Østrig | Ikke oplyst | | | | | | | | |
| Polen | Ikke oplyst | | | | | | | | |
| Portugal | Ikke oplyst | | | | | | | | |
| Rumænien | Ikke oplyst | | | | | | | | |
| Slovenien | Ikke oplyst | | | | | | | | |
| Slovakiet | Ikke oplyst | | | | | | | | |
| Finland | Ikke oplyst | | | | | | | | |
| Sverige | Ikke oplyst | | | | | | | | |
| Det Forenede Kongerige | 229375 | 52241 | 26228 | 16040 | 3333 | 521 | 339 | 1344 | 329421 |
| **I alt** | **417027** | **108603** | **42697** | **20160** | **3804** | **842** | **398** | **1384** | **594915** |

| Tabel 11: Anmodninger, som blev efterkommet i 2008, om lagrede trafikdata vedrørende internet efter alder | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Dataenes alder (i måneder) pr. medlemsstat** | **0-3** | **3-6** | **6-9** | **9-12** | **12-15** | **15-18** | **18-21** | **21-24** | **I alt** |
| Belgien | Ikke oplyst | | | | | | | | |
| Bulgarien | Ikke oplyst | | | | | | | | |
| Tjekkiet | 737 | 412 | 137 | 168 | 0 | 0 | 0 | 0 | 1454 |
| Danmark | 102 | 14 | 11 | 2 | 3 | 1 | 0 | 1 | 134 |
| Tyskland | Ikke oplyst | | | | | | | | |
| Estland | Ikke oplyst | | | | | | | | |
| Irland | 492 | 460 | 498 | 1422 | 0 | 0 | 0 | 0 | 2872 |
| Grækenland | Ikke oplyst | | | | | | | | |
| Spanien | 3278 | 2323 | 2113 | 1403 | 0 | 0 | 0 | 0 | 9117 |
| Frankrig | Ikke oplyst | | | | | | | | |
| Italien | Ikke oplyst | | | | | | | | |
| Cypern | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Letland | 424 | 150 | 75 | 219 | 74 | 34 | 0 | 0 | 976 |
| Litauen | Ikke oplyst | | | | | | | | |
| Luxembourg | Ikke oplyst | | | | | | | | |
| Ungarn | Ikke oplyst | | | | | | | | |
| Malta | 76 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 79 |
| Nederlandene | Ikke oplyst | | | | | | | | |
| Østrig | Ikke oplyst | | | | | | | | |
| Polen | Ikke oplyst | | | | | | | | |
| Portugal | Ikke oplyst | | | | | | | | |
| Rumænien | Ikke oplyst | | | | | | | | |
| Slovenien | Ikke oplyst | | | | | | | | |
| Slovakiet | Ikke oplyst | | | | | | | | |
| Finland | Ikke oplyst | | | | | | | | |
| Sverige | Ikke oplyst | | | | | | | | |
| Det Forenede Kongerige | 31170 | 9046 | 3097 | 2605 | 1917 | 2015 | 147 | 57 | 50054 |
| **I alt** | **36279** | **12408** | **5931** | **5819** | **1994** | **2050** | **147** | **58** | **64686** |

## Medlemsstaternes statistikker for 2009

| Tabel 12: Anmodninger om lagrede data efter alder i 2009 | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Dataenes alder (i måneder) pr. medlemsstat** | **0-3** | **3-6** | **6-9** | **9-12** | **12-15** | **15-18** | **18-21** | **21-24** | **I alt** |
| Belgien | Ikke oplyst | | | | | | | | |
| Bulgarien | Ikke oplyst | | | | | | | | |
| Tjekkiet | 210975 | 56623 | 11620 | 1053 | 0 | 0 | 0 | 0 | 280271 |
| Danmark | 2980 | 685 | 179 | 104 | 54 | 38 | 12 | 14 | 4066 |
| Tyskland | Ingen bestemmelser | | | | | | | | |
| Estland | 4299 | 1836 | 1210 | 1065 | 0 | 0 | 0 | 0 | 8410 |
| Irland | 8117 | 1652 | 805 | 297 | 168 | 134 | 69 | 41 | 11283 |
| Grækenland | Ikke oplyst | | | | | | | | |
| Spanien | 29775 | 19346 | 13999 | 6970 | 0 | 0 | 0 | 0 | 70090 |
| Frankrig | Opdeling efter alder ikke oplyst | | | | | | | | 514813 |
| Italien | Ikke oplyst | | | | | | | | |
| Cypern | 31 | 8 | 1 | 0 | 0 | 0 | 0 | 0 | 40 |
| Letland | 20758 | 2414 | 1088 | 796 | 565 | 475 | 0 | 0 | 26096 |
| Litauen | 30247 | 35456 | 5886 | 884 | 0 | 0 | 0 | 0 | 72473 |
| Luxembourg | Ikke oplyst | | | | | | | | |
| Ungarn | Ikke oplyst | | | | | | | | |
| Malta | 3336 | 362 | 151 | 174 | 0 | 0 | 0 | 0 | 4023 |
| Nederlandene | Ikke oplyst | | | | | | | | |
| Østrig | Ikke oplyst | | | | | | | | |
| Portugal | Ikke oplyst | | | | | | | | |
| Rumænien | Ikke oplyst | | | | | | | | |
| Polen | 642327 | 178306 | 75525 | 52526 | 27098 | 23924 | 13984 | 34628 | 1048318 |
| Slovenien | Opdeling efter alder ikke oplyst | | | | | | | | 1918 |
| Slovakiet | Opdeling efter alder ikke oplyst | | | | | | | | 5214 |
| Finland | 2000 | 1310 | 532 | 152 | 76 | 0 | 0 | 0 | 4070 |
| Sverige | Ikke oplyst | | | | | | | | |
| Det Forenede Kongerige | Ikke oplyst | | | | | | | | |
| **I alt** | **954845** | **297998** | **110996** | **64021** | **27961** | **24571** | **14065** | **34683** | **2051085** |

| **Tabel 13: Anmodninger om lagrede data efter datatype i 2009 (hvor dette er oplyst, angiver tallet i parentes antallet af anmodninger om data, der ikke kunne efterkommes)** | | | | |
|---|---|---|---|---|
| **Datatype Medlemsstat** | **Fastnettelefoni** | **Mobiltelefoni** | **Internetdata** | **I alt** |
| Belgien | Ikke oplyst | | | |
| Bulgarien | Ikke oplyst | | | |
| Tjekkiet | 13843 (934) | 256074 (9141) | 10354 (371) | 280271 (10446) |
| Danmark | 133 (0) | 3771 (10) | 162 (1) | 4066 (11) |
| Tyskland | Ikke oplyst | | | |
| Estland | 6422 (2279) | 902 (21) | 1086 (468) | 8410 (2768) |
| Irland | 4542 (16) | 5239 (20) | 1502 (56) | 11283 (92) |
| Grækenland | Ikke oplyst | | | |
| Spanien | 5055 (0) | 56133 (0) | 8902 (0) | 70090 (0) |
| Frankrig | Opdeling efter datatype ikke oplyst | | | **514813** |
| Italien | Ikke oplyst | | | |
| Cypern | 0 (0) | 23 (3) | 14 (0) | 40 (3) |
| Letland | 1672 (218) | 22796 (102) | 1628 (240) | 26096 (560) |
| Litauen | 1321 (0) | 51573 (6237) | 19579 (343) | 72473 (6580) |
| Luxembourg | Ikke oplyst | | | |
| Ungarn | Ikke oplyst | | | |
| Malta | 156 (10) | 3693 (882) | 174 (10) | 4023 (902) |
| Nederlandene | Ikke oplyst | | | |
| Østrig | Ikke oplyst | | | |
| Polen | Opdeling efter datatype ikke oplyst | | | **1048318** |
| Portugal | Ikke oplyst | | | |
| Rumænien | Ikke oplyst | | | |
| Slovenien | Opdeling efter datatype ikke oplyst | | | **1918 (48)** |
| Slovakiet | Opdeling efter datatype ikke oplyst | | | **5214 (157)** |
| Finland | Opdeling efter datatype ikke oplyst | | | **4070** |
| Sverige | Ikke oplyst | | | |
| Det Forenede Kongerige | Ikke oplyst | | | |
| **I alt** | | | | **2051082 (1069885)** |

| Tabel 14: Anmodninger, som blev efterkommet i 2009, om lagrede fastnettelefonidata efter alder | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Dataenes alder (i måneder) pr. medlemsstat** | **0-3** | **3-6** | **6-9** | **9-12** | **12-15** | **15-18** | **18-21** | **21-24** | **I alt** |
| Belgien | Ikke oplyst | | | | | | | | |
| Bulgarien | Ikke oplyst | | | | | | | | |
| Tjekkiet | 9919 | 2907 | 47 | 36 | 0 | 0 | 0 | 0 | 12909 |
| Danmark | 105 | 19 | 7 | 2 | 0 | 0 | 0 | 0 | 133 |
| Tyskland | Ikke oplyst | | | | | | | | |
| Estland | 2254 | 866 | 599 | 424 | 0 | 0 | 0 | 0 | 4143 |
| Irland | 3934 | 337 | 69 | 70 | 50 | 39 | 16 | 11 | 4526 |
| Grækenland | Ikke oplyst | | | | | | | | |
| Spanien | 2371 | 1492 | 844 | 348 | 0 | 0 | 0 | 0 | 5055 |
| Frankrig | Ikke oplyst | | | | | | | | |
| Italien | Ikke oplyst | | | | | | | | |
| Cypern | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Letland | 744 | 253 | 157 | 143 | 68 | 89 | 0 | 0 | 1454 |
| Litauen | 469 | 773 | 73 | 6 | 0 | 0 | 0 | 0 | 1321 |
| Luxembourg | Ikke oplyst | | | | | | | | |
| Ungarn | Ikke oplyst | | | | | | | | |
| Malta | 83 | 25 | 18 | 20 | 0 | 0 | 0 | 0 | 146 |
| Nederlandene | Ikke oplyst | | | | | | | | |
| Østrig | Ikke oplyst | | | | | | | | |
| Polen | Ikke oplyst | | | | | | | | |
| Portugal | Ikke oplyst | | | | | | | | |
| Rumænien | Ikke oplyst | | | | | | | | |
| Slovenien | Ikke oplyst | | | | | | | | |
| Slovakiet | Ikke oplyst | | | | | | | | |
| Finland | Ikke oplyst | | | | | | | | |
| Sverige | Ikke oplyst | | | | | | | | |
| Det Forenede Kongerige | Ikke oplyst | | | | | | | | |
| **I alt** | **19879** | **6672** | **1814** | **1049** | **118** | **128** | **16** | **11** | **29687** |

| Tabel 15: Anmodninger, som blev efterkommet i 2009, om lagrede mobiltelefonidata efter alder | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Dataenes alder (i måneder) pr. medlemsstat** | **0-3** | **3-6** | **6-9** | **9-12** | **12-15** | **15-18** | **18-21** | **21-24** | **I alt** |
| Belgien | Ikke oplyst | | | | | | | | |
| Bulgarien | Ikke oplyst | | | | | | | | |
| Tjekkiet | 197620 | 48841 | 472 | 0 | 0 | 0 | 0 | 0 | 246933 |
| Danmark | 2777 | 639 | 162 | 98 | 47 | 19 | 12 | 7 | 3761 |
| Tyskland | Ikke oplyst | | | | | | | | |
| Estland | 318 | 397 | 96 | 70 | 0 | 0 | 0 | 0 | 881 |
| Irland | 3669 | 835 | 220 | 210 | 115 | 92 | 50 | 28 | 5219 |
| Grækenland | Ikke oplyst | | | | | | | | |
| Spanien | 24065 | 15648 | 11147 | 5273 | 0 | 0 | 0 | 0 | 56133 |
| Frankrig | Ikke oplyst | | | | | | | | |
| Italien | Ikke oplyst | | | | | | | | |
| Cypern | 17 | 16 | 0 | 0 | 0 | 0 | 0 | 0 | 23 |
| Letland | 18832 | 1912 | 778 | 515 | 394 | 263 | 0 | 0 | 22694 |
| Litauen | 25713 | 19595 | 28 | 0 | 0 | 0 | 0 | 0 | 45336 |
| Luxembourg | Ikke oplyst | | | | | | | | |
| Ungarn | Ikke oplyst | | | | | | | | |
| Malta | 2332 | 246 | 111 | 122 | 0 | 0 | 0 | 0 | 2811 |
| Nederlandene | Ikke oplyst | | | | | | | | |
| Østrig | Ikke oplyst | | | | | | | | |
| Polen | Ikke oplyst | | | | | | | | |
| Portugal | Ikke oplyst | | | | | | | | |
| Rumænien | Ikke oplyst | | | | | | | | |
| Slovenien | Ikke oplyst | | | | | | | | |
| Slovakiet | Ikke oplyst | | | | | | | | |
| Finland | Ikke oplyst | | | | | | | | |
| Sverige | Ikke oplyst | | | | | | | | |
| Det Forenede Kongerige | Ikke oplyst | | | | | | | | |
| **I alt** | **275343** | **88119** | **13014** | **6288** | **556** | **374** | **62** | **35** | **383791** |

| Tabel 16: Anmodninger, som blev efterkommet i 2009, om lagrede internetdata efter alder | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Dataenes alder (i måneder) pr. medlemsstat** | **0-3** | **3-6** | **6-9** | **9-12** | **12-15[1]** | **15-18** | **18-21** | **21-24** | **I alt** |
| Belgien | Ikke oplyst | | | | | | | | |
| Bulgarien | Ikke oplyst | | | | | | | | |
| Tjekkiet | 3369 | 4811 | 861 | 942 | 0 | 0 | 0 | 0 | 9983 |
| Danmark | 98 | 27 | 10 | 4 | 4 | 7 | 0 | 1 | 151 |
| Tyskland | Ikke oplyst | | | | | | | | |
| Estland | 315 | 145 | 56 | 102 | 0 | 0 | 0 | 0 | 618 |
| Irland | 489 | 455 | 502 | 0 | 0 | 0 | 0 | 0 | 1446 |
| Grækenland | Ikke oplyst | | | | | | | | |
| Spanien | 3339 | 2206 | 2008 | 1349 | 0 | 0 | 0 | 0 | 8902 |
| Frankrig | Ikke oplyst | | | | | | | | |
| Italien | Ikke oplyst | | | | | | | | |
| Cypern | 12 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 14 |
| Letland | 852 | 198 | 74 | 90 | 88 | 86 | 0 | 0 | 1388 |
| Litauen | 4060 | 15087 | 1 | 88 | 0 | 0 | 0 | 0 | 19236 |
| Luxembourg | Ikke oplyst | | | | | | | | |
| Ungarn | Ikke oplyst | | | | | | | | |
| Malta | 150 | 14 | 0 | 0 | 0 | 0 | 0 | 0 | 164 |
| Nederlandene | Ikke oplyst | | | | | | | | |
| Østrig | Ikke oplyst | | | | | | | | |
| Polen | Ikke oplyst | | | | | | | | |
| Portugal | Ikke oplyst | | | | | | | | |
| Rumænien | Ikke oplyst | | | | | | | | |
| Slovenien | Ikke oplyst | | | | | | | | |
| Slovakiet | Ikke oplyst | | | | | | | | |
| Finland | Ikke oplyst | | | | | | | | |
| Sverige | Ikke oplyst | | | | | | | | |
| Det Forenede Kongerige | Ikke oplyst | | | | | | | | |
| **I alt** | **12684** | **22945** | **3512** | **2575** | **92** | **93** | **0** | **1** | **41902** |