



17/DA

WP 247

**Udtalelse nr. 01/2017 om  
forslaget til e-databeskyttelsesforordning (2002/58/EF)**

**Vedtaget den 4. april 2017**

Artikel 29-Gruppen er nedsat ved artikel 29 i direktiv 95/46/EF. Gruppen er et uafhængigt EU-rådgivningsorgan vedrørende databeskyttelse og beskyttelse af privatlivets fred. Dens opgaver er beskrevet i artikel 30 i direktiv 95/46/EF og artikel 15 i direktiv 2002/58/EF.

Sekretariatet varetages af Direktorat C (Grundlæggende rettigheder og retsstatsprincippet) i Europa-Kommissionen, Generaldirektoratet for Retlige Anliggender og Forbrugere, B-1049 Bruxelles, Belgien, kontor nr. MO-59 05/035.

Websted: [http://ec.europa.eu/justice/data-protection/index\\_en.htm](http://ec.europa.eu/justice/data-protection/index_en.htm)

**GRUPPEN VEDRØRENDE BESKYTTELSE AF PERSONER I FORBINDELSE MED BEHANDLING  
AF PERSONOPLYSNINGER,**

som er nedsat ved Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995,

som henviser til artikel 29 og 30 i ovennævnte direktiv, og

som henviser til gruppens forretningsorden,

**HAR VEDTAGET FØLGENDE UDTALELSE:**

## RESUMÉ

Artikel 29-Gruppen glæder sig over Europa-Kommissionens forslag af 10. januar 2017 til en e-databeskyttelsesforordning. Det glæder Artikel 29-Gruppen, at der er **valgt en forordning** som retsakt. Dette sikrer, at reglerne er ensartede i hele Unionen, og sikrer klarhed for både tilsynsmyndigheder og organisationer. Det hjælper også med at sikre overensstemmelse med den generelle forordning om databeskyttelse. En sådan overensstemmelse understøttes yderligere af beslutningen om at gøre **den myndighed, som også er ansvarlig for tilsynet med overholdelsen af den generelle forordning om databeskyttelse**, ansvarlig for håndhævelsen af e-databeskyttelsesreglerne.

Samtidig bifaldes valget af (fastholdelsen af) en **supplerende retsakt**. Beskyttelsen af fortroligt kommunikations- og terminaludstyr omfatter særlige elementer, som ikke er omhandlet i den generelle forordning om databeskyttelse. Der er derfor behov for supplerende bestemmelser vedrørende sådanne tjenester for at sikre tilstrækkelig beskyttelse af den grundlæggende ret til privatlivets fred og kommunikationshemmelighed, herunder fortroligheden af terminaludstyr. I denne henseende går Artikel 29-Gruppen meget stærkt ind for den **principbaserede tilgang**, der er valgt i forordningsforslaget, med **brede forbud og snævre undtagelser** og **den målrettede anvendelse af samtykkebegrebet**.

Artikel 29-Gruppen bifalder udvidelsen af forordningsforslagets anvendelsesområde til at **omfatte leverandører af over the top-tjenester** (OTT-tjenester), som funktionelt svarer til mere traditionelle kommunikationsmidler, og som derfor potentielt kan påvirke privatlivets fred og retten til kommunikationshemmelighed for Unionens borgere. Det er også positivt, at forordningsforslaget klart omhandler **indhold og tilknyttede metadata**, og det anerkendes, at **metadata kan åbenbare yderst følsomme data**.

Artikel 29-Gruppen har imidlertid også fire **alvorlige betænkeligheder**. Med hensyn til **sporing af terminaludstyrs placering, betingelserne for at analysere indhold og metadata, standardindstillingerne på terminaludstyr og software og tracking walls** vil den foreslåede forordning sænke det beskyttelsesniveau, der er fastsat i den generelle forordning om databeskyttelse. I denne udtalelse fremkommer Artikel 29-Gruppen med forslag, som kan sikre, at e-databeskyttelsesforordningen vil garantere samme eller et højere beskyttelsesniveau, som er hensigtsmæssigt i lyset af den følsomme karakter af kommunikationsdata (både indhold og metadata).

I henhold til den generelle forordning om databeskyttelse er **WiFi-sporing**, afhængigt af omstændighederne og formålet med dataindsamlingen, sandsynligvis omfattet af et krav om samtykke eller kan kun foretages, hvis de tilvejebragte personoplysninger anonymiseres. I sidstnævnte tilfælde skal følgende fire betingelser opfyldes: Formålet med dataindsamlingen fra terminaludstyr skal være begrænset til ren statistisk optælling, sporingen skal i tid og omfang være begrænset til det, der er strengt nødvendigt til dette formål, oplysningerne skal slettes eller anonymiseres straks derefter, og der skal forefindes effektive fravalgsmuligheder. Kommissionen opfordres til at fremme en teknisk standard for mobilapparater, som automatisk signalerer en indvending mod en sådan sporing.

Med hensyn til **analysen af indhold og metadata** bør udgangspunktet være, at det er forbudt at behandle kommunikationsdata uden samtykke fra alle slutbrugere (afsendere og

modtagere). For at give leverandører mulighed for at levere tjenester, som brugeren udtrykkeligt anmoder om, f.eks. søge- og indekseringsfunktioner, eller tekst-til-tale-tjenester, bør der være en begrænset undtagelse for behandling af indhold og metadata alene til brugerens egne personlige formål.

Med hensyn til **samtykke til sporing** bør der efter Artikel 29-Gruppens opfattelse vedtages et udtrykkeligt forbud mod tracking walls, dvs. take it or leave it-spørgsmål, som tvinger brugerne til at give samtykke til sporing, hvis de ønsker at have adgang til tjenesten.

Sidst, men ikke mindst anbefaler Artikel 29-Gruppen, at terminaludstyr og software **som standard skal have privatlivsindstillinger** og skal give brugerne klare muligheder for at bekræfte eller ændre disse standardindstillinger i forbindelse med installationen. Indstillingerne skal være lettilgængelige, når udstyret anvendes. Brugerne skal kunne give deres specifikke samtykke ved hjælp af deres browserindstillinger. Foretrukne privatlivsindstillinger bør ikke være begrænset til tredjeparters indgreb eller være begrænset til cookies. Artikel 29-Gruppen anbefaler på det kraftigste, at overholdelse af do not track-standarden gøres obligatorisk.

Artikel 29-Gruppen har også udpeget andre forhold, der giver anledning til betænkeligheder, f.eks. anvendelsesområdet, beskyttelsen af terminaludstyr og direkte markedsføring. Sidst, men ikke mindst har Artikel 29-Gruppen udpeget forhold, som bør afklares for at sikre slutbrugerne bedre beskyttelse og for at styrke retssikkerheden for alle involverede interessenter.

## INDHOLDSFORTEGNELSE

<b>1. INDLEDNING .....</b>	<b>6</b>
<b>2. POSITIVE ASPEKTER VED DEN FORESLÅEDE FORORDNING .....</b>	<b>6</b>
<i>Harmonisering i hele Unionen, tilpasning af bøder og eksklusive håndhævelsesbeføjelser til datatilsynsmyndigheder .....</i>	<i>6</i>
<i>Udvidelse af anvendelsesområdet sammenlignet med e-datadirektivet .....</i>	<i>8</i>
<i>Målrettet anvendelse af begrebet samtykke .....</i>	<i>11</i>
<b>3. ALVORLIGE BETÆNKELIGHEDER.....</b>	<b>11</b>
<i>Beskyttelsen efter den generelle forordning om databeskyttelse svækkes af den foreslåede forordning .....</i>	<i>11</i>
<b>4. ANDRE BETÆNKELIGHEDER .....</b>	<b>18</b>
<i>Det territoriale og materielle anvendelsesområde skal udvides .....</i>	<i>18</i>
<i>Beskyttelsen af terminaludstyr skal styrkes.....</i>	<i>19</i>
<i>Direkte markedsføring .....</i>	<i>23</i>
<i>Tidsplan .....</i>	<i>26</i>
<i>Andre betænkeligheder .....</i>	<i>26</i>
<b>5. FORSLAG TIL PRÆCISERING AF HENSYN TIL RETSSIKKERHEDEN .....</b>	<b>29</b>
<i>Klarere anvendelsesområde .....</i>	<i>29</i>
<i>Afklaringer af begrebet og anvendelse af samtykke.....</i>	<i>32</i>
<i>Præciseringer vedrørende lokaliseringsdata og andre metadata.....</i>	<i>33</i>
<i>Præciseringer vedrørende uanmodet kommunikation .....</i>	<i>35</i>
<i>Præciseringer vedrørende anvendelsen af retsakter til beskyttelse af grundlæggende rettigheder .....</i>	<i>36</i>
<i>Andre præciseringer .....</i>	<i>37</i>

## 1. INDLEDNING

1. Artikel 29-Gruppen vedrørende Databeskyttelse (Artikel 29-Gruppen) glæder sig over Kommissionens forslag til e-databeskyttelsesforordning (den foreslåede forordning, forordningsforslaget eller e-databeskyttelsesforordningen)<sup>1</sup>, som har til formål at erstatte e-datadirektivet<sup>2</sup>.
2. Der er mange positive aspekter ved den foreslåede forordning, og Kommissionen har taget et vigtigt skridt med fremlæggelsen af dette forslag. Den foreslåede forordning kan imidlertid forbedres yderligere. Dette ville ikke kun sikre slutbrugerne bedre beskyttelse, men ville også styrke retssikkerheden for alle involverede interessenter.
3. Artikel 29-Gruppen har derfor en række betænkeligheder og anbefalinger til præcisering, som Parlamentet og Rådet bør behandle i deres forhandlinger om den foreslåede forordning. I denne udtalelse behandles først de positive aspekter ved den foreslåede forordning, og derefter fremhæves de områder, der giver anledning til betænkeligheder, og dem, der bør afklares.

## 2. POSITIVE ASPEKTER VED DEN FORESLÅEDE FORORDNING

*HARMONISERING I HELE UNIONEN, TILPASNING AF BØDER OG EKSKLUSIVE HÅNDHÆVELSESBEFØJELSER TIL DATATILSYNSMYNDIGHEDER*

4. Det glæder Artikel 29-Gruppen, at der er **valgt en forordning** som retsakt. Dette sikrer, at reglerne bliver de samme i hele Unionen (med visse undtagelser, som er omhandlet nedenfor). Dette skaber klarhed for både tilsynsmyndigheder og organisationer. I lyset af den centrale rolle, som den generelle forordning om databeskyttelse<sup>3</sup> spiller i den foreslåede forordning, medvirker dette til at sikre konsekvens mellem de to retsakter. Samtidig bifaldes valget af (fastholdelsen af) en **supplerende retsakt**. Beskyttelsen af fortroligt kommunikations- og terminaludstyr omfatter særlige elementer, som ikke er omhandlet i den generelle forordning om databeskyttelse. Der er derfor behov for supplerende bestemmelser vedrørende sådanne tjenester for at sikre tilstrækkelig beskyttelse af denne grundlæggende ret. I

---

<sup>1</sup> Forslag til Europa-Parlamentets og Rådets forordning om respekt for privatliv og beskyttelse af personoplysninger i forbindelse med elektroniske kommunikation og om ophævelse af direktiv 2002/58/EF (forordning om databeskyttelse inden for elektronisk kommunikation), 2017/0003 (COD), webadresse: [http://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=41241](http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241).

<sup>2</sup> 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 privatlivets fred og elektronisk kommunikation), EFT L 201 af 31.7.2002, s. 37-47, webadresse: <http://eur-lex.europa.eu/legal-content/DA/TXT/?uri=celex:32002L0058>.

<sup>3</sup> Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse), EUT L 119 af 4.5.2016, s. 1-88, webadresse: <http://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX%3A32016R0679>.

denne sammenhæng støtter Artikel 29-Gruppen også **den principbaserede tilgang, der er valgt i den foreslåede forordning, med brede forbud og snævre undtagelser**, og mener, at indførelsen af åbne undtagelser i stil med artikel 6 i den generelle forordning om databeskyttelse, særligt artikel 6, litra f), i den generelle forordning om databeskyttelse (legitim interesse), bør undgås.

5. Det forhold, at **disse regler skal håndhæves af den myndighed, som også er ansvarlig for at føre tilsyn med overholdelsen af den generelle forordning om databeskyttelse**, vil yderligere understøtte sammenhængen mellem de to retsakter. Da der er en sammenhæng mellem beskyttelsen af personoplysninger og beskyttelsen af fortroligt kommunikations- og terminaludstyr, er det en fordel, at håndhævelsen af bestemmelserne i den foreslåede forordning overlades til den tilsynsmyndighed, som også håndhæver den generelle forordning om databeskyttelse (forordningsforslagets betragtning 38 og artikel 18). EU-Domstolens praksis<sup>4</sup> bekræfter desuden, at det er afgørende, at tilsynsmyndigheden er uafhængig som fastsat i chartrets artikel 7. I praksis vil dette imidlertid medføre betydeligt ekstraarbejde for datatilsynsmyndighederne, som ikke kan garanteres udført, hvis der ikke bevilges ekstra midler. Datatilsynsmyndighederne glæder sig derfor over forordningsforslagets betragtning 38, hvori det fremhæves, at hver tilsynsmyndighed bør tildeles de nødvendige supplerende finansielle og menneskelige ressourcer samt lokaler og infrastruktur til effektivt at kunne udføre sine opgaver efter denne forordning. Det er også glædeligt, at artikel 18, stk. 2, udgør retsgrundlaget for samarbejdet mellem tilsynsmyndighederne i den foreslåede forordning og de nationale tilsynsmyndigheder, der er udpeget i henhold til det foreslåede direktiv om en europæisk kodeks for elektronisk kommunikation ("kodeksen for elektronisk kommunikation")<sup>5</sup>.
6. I lyset af det tætte forhold mellem den foreslåede forordning og den generelle forordning om databeskyttelse bifaldes også **tilpasningen af bøder under den foreslåede forordning med den generelle forordning om databeskyttelse**. De aktiviteter, som er omfattet af anvendelsesområdet for den foreslåede forordning, er ganske følsomme og omfatter bl.a. indgreb i fortroligt kommunikations- og terminaludstyr. Størrelsen af bøder bør afspejle denne følsomme sammenhæng. Denne sammenhæng er også grunden til, at harmonisering på tværs af EU-landene er vigtig, så der sikres det samme høje beskyttelsesniveau i hele Unionen. I forordningsforslagets artikel 23 er der fastsat effektive bøder for overtrædelse af forordningen, som svarer til de bøder, der er fastsat for overtrædelse af bestemmelserne i den generelle forordning om databeskyttelse, bortset fra på enkelte punkter (se bemærkning 38).

---

<sup>4</sup> Se f.eks. dom af 6.10.2015, C-362/14 (Safe Harbour), præmis 41, og dom af 21.12.2016, C-203/15 og C-698/15 (Tele2/Watson), præmis 123.

<sup>5</sup> Forslag til Europa-Parlamentets og Rådets direktiv om en europæisk kodeks for elektronisk kommunikation (Omarbejdning), 2016/0288 (COD), 12.10.2016, webadresse: [http://eur-lex.europa.eu/legal-content/DA/ALL/?uri=comnat:COM\\_2016\\_0590\\_FIN](http://eur-lex.europa.eu/legal-content/DA/ALL/?uri=comnat:COM_2016_0590_FIN).

7. **Fjernelsen af specifikke regler om anmeldelse af brud på datasikkerheden** fra denne retsakt er også glædelig, idet det kan forhindre unødvendig overlappning med bestemmelserne om brud på datasikkerheden i den generelle forordning om databeskyttelse.
8. Det glæder Artikel 29-Gruppen, **at der nu fokuseres på at sikre alle slutbrugere samme beskyttelsesniveau**, idet der i den foreslåede forordning ikke skelnes mellem "abonnenter" og andre brugere af elektroniske kommunikationstjenester.

#### *UDVIDELSE AF ANVENDELSESOMRÅDET SAMMENLIGNET MED E-DATADIREKTIVET*

9. Artikel 29-Gruppen glæder sig over **udvidelsen af forordningsforslagets anvendelsesområde til at omfatte leverandører af over the top-tjenester (OTT-tjenester)**, som funktionelt svarer til mere traditionelle kommunikationsmidler, og som derfor potentielt kan påvirke privatlivets fred og retten til kommunikationshemmelighed for EU-borgere. Det glæder navnlig Artikel 29-Gruppen, at alle OTT-kategorier (OTT0, OTT1 og nogle OTT2)<sup>6</sup> nu er omfattet af forordningens anvendelsesområde, da den ikke kun omhandler traditionelle kommunikationsmidler (OTT0), men også funktionelt tilsvarende tjenester (OTT1) som nævnt i forordningsforslagets artikel 8, stk. 1, litra c). Det er også positivt, at visse OTT2'er – i tillæg til definitionerne i kodeksen for elektronisk kommunikation – er medtaget, når de leverer interpersonelle og interaktive kommunikationstjenester som en ledsagende funktion, der er uløseligt forbundet med deres tjeneste, f.eks. i spil, i dating-apps eller på anmeldelseswebsteder (forordningsforslagets artikel 4, stk. 2). **Præciseringen af, at beskyttelsen også omfatter interaktion mellem maskiner**, hilses også velkommen. I betragtning 12 præciseres det, at apparater, som kommunikerer med hinanden, er omfattet af den beskyttelse, der sikres ved den foreslåede forordning. Dette er ønskværdigt, da sådan kommunikation ofte indeholder oplysninger, der er omfattet af retten til privatlivets fred. Anvendelsesområdet bør dog præciseres (se bemærkning 40h).
10. Det er endvidere positivt, at **den foreslåede forordning klart omfatter indhold og tilhørende metadata**. I betragtning 14 præciseres det, at det er meningen med definitionen i artikel 4, stk. 3, litra a), af "elektroniske kommunikationsdata", at den skal være så tilstrækkeligt omfattende, at *alle* former for indhold samt tilhørende metadata er omfattet, uanset hvordan signalerne f.eks. overføres. Artikel 29-Gruppen er imidlertid, som nævnt i bemærkning 39, betænkelig ved, at denne nugældende definition af "elektroniske kommunikationsdata" stadig er genstand for drøftelser. På linje med denne udvidelse af anvendelsesområdet finder Artikel 29-Gruppen, at **anerkendelsen af, at metadata kan åbenbare meget følsomme data** (se begrundelsens afsnit 2.2 og betragtning 2), er en vigtig tilføjelse. Det glæder

---

<sup>6</sup> For en nærmere forklaring af disse udtryk henvises der til Report on OTT Services, BoR (16) 35, 29.1.2016, s. 15 og 16, webadresse: [http://berec.europa.eu/eng/document\\_register/subject\\_matter/berec/reports/5751-berec-report-on-ott-services](http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services). Bemærk også bemærkningen i rapporten om, at kategorierne er tænkt som begreber, der skal anvendes i debatten om revisionen, ikke som juridiske begreber.



Artikel 29-Gruppen, at Kommissionen derved tager hensyn til EU-Domstolens bemærkninger i sagen *Digital Rights Ireland* og *Tele2/Watson*. Artikel 29-Gruppen glæder sig også over **anerkendelsen af, at indholdsanalyse udgør en højrisikobehandling**. I betragtning 19 og artikel 6, stk. 3, litra b), gives der udtryk for den logiske retlige formodning, at skanning af indhold er højrisikobehandling som omhandlet i artikel 35 i den generelle forordning om databeskyttelse, som altid – tilsyneladende uanset eksistensen af en resterende høj risiko – kræver forudgående høring af den ledende datatilsynsmyndighed. Samtidig er Artikel 29-Gruppen betænkelig ved anvendelsesområdet for definitionen af "metadata" og det forhold, at analysen af metadata ikke er omfattet af det samme obligatoriske krav om en konsekvensanalyse af databeskyttelsen (se bemærkning 33 og 46).

11. Den fortsatte **anerkendelse af betydningen af anonymisering** er også glædelig. Allerede i e-datadirektivet medvirkede anonymiseringsforanstaltninger til at sikre forenelighed (f.eks. e-datadirektivets artikel 6, stk. 1, hvorefter trafikdata skal slettes eller gøres anonyme, når de ikke længere er nødvendige for fremføringen af kommunikationen). Ifølge forordningsforslagets artikel 6, stk. 2, litra c), og artikel 6, stk. 3, litra b), gælder der en undtagelse til behandlingen af metadata og indhold, når der foreligger et samtykke, *"forudsat at det eller disse formål ikke kunne opnås ved at behandle anonymiserede oplysninger"*. Kravet om sådanne foranstaltninger til beskyttelse af privatlivet beskytter sammen med kravet om brugernes samtykke brugerne mod uønsket behandling. Artikel 29-Gruppen finder det imidlertid meget betænkeligt, at anvendelsen af sådanne anonymiseringsteknikker ikke kræves, når brugernes placering spores gennem deres mobiludstyr (se bemærkning 17). Selv når anonymiseringsforanstaltninger skal anvendes, bør leverandører altid gennemføre en konsekvensanalyse vedrørende databeskyttelse (se bemærkning 33 og 46), og der bør efter Artikel 29-Gruppens opfattelse indføres et yderligere krav om, at det oplyses, hvordan oplysningerne gøres anonyme og samles (se bemærkning 42b).
12. Et andet positivt punkt er den **brede formulering af beskyttelsen af terminaludstyr**. Ifølge betragtning 20 og artikel 8 er de teknologier, der anvendes til at få adgang til terminaludstyr, ikke relevante: Ethvert indgreb i terminaludstyr, herunder brugen af dets behandlingskapacitet, kræver slutbrugerens samtykke (med visse undtagelser). Kommissionen har nu ganske nyttigt bekræftet, at "device fingerprinting" er omfattet af denne bestemmelse. Det glæder desuden Artikel 29-Gruppen, at en tredjeparts manglende overholdelse af de præferencer, der er anført i en brugers **browserindstillinger, kan retsforfølges** som beskrevet i betragtning 22. Dette er nyttigt i situationer, hvor en tredjepart (f.eks. et annoncenetværk) ikke respekterer disse indstillinger. Det bør dog også fastsættes i en relevant bestemmelse i forordningsforslaget.
13. Endelig hilses den fortsatte **medtagelse af juridiske personer i forordningsforslagets anvendelsesområde** velkommen (se begrundelsens afsnit 2.2 og forordningsforslagets betragtning 3, 33 og 42 samt artikel 1, 15 og 16, stk. 5). Dette er allerede fastsat i e-datadirektivet, men det bør særligt fremhæves, da datatilsynsmyndighederne får til opgave at håndhæve de nye regler. Dette giver datatilsynsmyndighederne mulighed for at gribe ind, hvis juridiske personer udsættes for en overtrædelse, f.eks. hvis selskaber modtager spam eller deres kommunikation

hemmeligt overvåges. Artikel 29-Gruppen finder det imidlertid også betænkeligt, at anvendelsen af samtykke for juridiske personer ikke er klar (se bemærkning 41a), og at det ikke er klart, hvad der menes med juridiske personers "legitime interesser" i forbindelse med direkte markedsføring (se bemærkning 43c).

14. Artikel 29-Gruppen glæder sig over en anden kategori af forbedringer vedrørende anvendelsen og fortolkningen af begrebet samtykke. Artikel 29-Gruppen bifalder for det første **præciseringen af, at internetadgang og (mobil)telefoni er grundlæggende tjenester, og at leverandører af disse tjenester ikke kan "tvinge" deres kunder til at give deres samtykke til databehandling, som ikke er nødvendig for at levere selve den grundlæggende tjeneste.** I betragtning 18 bemærkes det navnlig, at basal bredbåndadgang til internettjenester og talekommunikationstjenester skal anses for at være grundlæggende tjenester. Henset til den omstændighed, at folk er afhængige af at have adgang til disse tjenester, betyder det, at et samtykke til behandling af kommunikationsdata til sådanne yderligere formål (f.eks. behandling med henblik på annoncering eller markedsføring) er ugyldigt. En anden betænkelighed for Artikel 29-Gruppen er, at denne præcisering er for begrænset. Tjenester fra visse OTT-leverandører kan også anses for grundlæggende tjenester, og e-databeskyttelsesforordningen bør også specifikt forbyde take it or leave it-valg i andre situationer (se bemærkning 20).
15. Det er desuden positivt, at **kravet om samtykke til opføring af fysiske personers personoplysninger i fortegnelser harmoniseres.** I henhold til forordningsforslagets artikel 15 er behandling af personoplysninger i offentligt tilgængelige fortegnelser kun tilladt med fysiske personers samtykke, og såfremt de har mulighed for at gøre indsigelse. Dette uddybes i betragtning 31, hvor det bemærkes, at dette samtykke specifikt skal gælde for hver af de kategorier af personoplysninger, der inkluderes i fortegnelsen. Artikel 29-Gruppen er imidlertid af den opfattelse, at det i den foreslåede forordning mere klart kunne anføres, at der kræves et specifikt særskilt samtykke til søgninger og omvendte søgninger (se bemærkning 37).
16. **Den nye målrettede undtagelse for terminaludstyr vedrørende fremgangsmåder, der ikke griber ind i privatlivets fred,** er også glædelig. Det er efter Artikel 29-Gruppens opfattelse nyttigt, at det i den foreslåede forordning præciseres, at forbuddet ikke finder anvendelse på måling af webstedstrafik (med den snævre undtagelse, at en sådan måling foretages af leverandøren af en informationssamfundstjeneste, som slutbrugeren har bestilt, jf. forordningsforslagets artikel 8, stk. 1, litra d)). Se også betragtning 21. Artikel 29-Gruppen foreslår imidlertid, at der anvendes en mere teknologineutral definition, og at anvendelsen af denne undtagelse præciseres (se bemærkning 25).

### 3. ALVORLIGE BETÆNKELIGHEDER

#### *BESKYTTELSEN EFTER DEN GENERELLE FORORDNING OM DATABESKYTTELSE SVÆKKES AF DEN FORESLÅEDE FORORDNING*

Som nævnt ovenfor indeholder den foreslåede forordning en række centrale forbedringer. Artikel 29-Gruppen nærer dog også en række betænkeligheder af varierende alvor. I dette afsnit behandler Artikel 29-Gruppen fire forhold, som den er **særdeles betænkelig** ved. Der er tale om bestemmelser, som **svækker den beskyttelse, der sikres ved den generelle forordning om databeskyttelse:**



17. **Forordningens krav om sporing af terminaludstyrs placering bør opfylde kravene om databeskyttelse i den generelle forordning om databeskyttelse.** I henhold til forordningsforslagets artikel 8, stk. 2, litra b), skal der blot vises en meddelelse og træffes visse sikkerhedsforanstaltninger for at indsamle oplysninger, der udsendes af terminaludstyr. I artikel 8, stk. 2, litra b), fastsættes det yderligere, at den ansvarlige for indsamlingen skal oplyse om foranstaltninger, som slutbrugerne kan træffe med henblik på at stoppe eller minimere indsamlingen. Med artikel 8, stk. 2, litra b), gives der dermed det indtryk, at organisationer kan indsamle oplysninger, der udsendes af terminaludstyr, med henblik på at spore personers fysiske bevægelser (f.eks. "WiFi-sporing" eller "Bluetooth-sporing") uden den pågældende persons samtykke. Den part, der indsamler disse oplysninger, kan tilsyneladende overholde bestemmelserne ved at vise brugerne en meddelelse om, at de skal slukke for deres apparater, hvis de ikke ønsker at blive sporet. En sådan tilgang er i strid med det grundlæggende mål med Kommissionens telekommunikationspolitik, nemlig at levere mobil internetkonnektivitet med høj hastighed og effektiv privatlivsbeskyttelse med lave omkostninger til alle europæere på tværs af grænser.

I den foreslåede forordning fastlægges der endvidere ikke klare begrænsninger med hensyn til omfanget af dataindsamlingen eller de efterfølgende behandlingsaktiviteter. I denne sammenhæng bør det bemærkes, at disse MAC-adresser er personoplysninger, selv efter gennemførelsen af sikkerhedsforanstaltninger som f.eks. hashing. Ved ikke at indføre yderligere krav eller begrænsninger er beskyttelsesniveauet for disse personoplysninger efter den foreslåede forordning betydeligt lavere end efter den generelle forordning om databeskyttelse, som bestemmer, at sådan sporing skal være lovlig og rimelig samt gennemsigtig. I betragtning 25 bemærkes det nytteløst, at nogle WiFi-sporingsfunktioner ikke medfører store private risici, mens andre – f.eks. sporing af personer over tid – gør. Mens Artikel 29-Gruppen sætter pris på anerkendelsen af, at sidstnævnte medfører store private risici, giver det ikke mening på forhånd at fastslå, at visse andre funktioner ikke medfører sådanne risici, uden en yderligere vurdering af omstændighederne og behandlingens proportionalitet. En sådan vurdering bør gennemføres under hensyntagen til følgende betingelser, for så vidt angår ikkeanonymiseret wi-fi-sporing.

Ifølge den generelle forordning om databeskyttelse er sådan sporing, afhængigt af omstændighederne og formålet med dataindsamlingen, sandsynligvis underlagt et krav om samtykke eller kan kun foretages, hvis de indsamlede personoplysninger anonymiseres. Denne anonymisering skal helst foretages umiddelbart efter indsamling. Hvis omgående anonymisering ikke er mulig som følge af formålet med dataindsamlingen, kan disse oplysninger behandles i en periode uden at være blevet anonymiseret, såfremt følgende betingelser er opfyldt: i) Formålet med dataindsamlingen fra terminaludstyr skal være begrænset til ren statistisk optælling (se eksemplerne nedenfor), ii) sporingen skal i tid og omfang være begrænset til det, der er strengt nødvendigt til dette formål, iii) oplysningerne skal slettes eller anonymiseres straks bagefter, og iv) der skal forefindes effektive fravalgsmuligheder. Dataansvarlige skal naturligvis under alle omstændigheder opfylde kravet om at fremlægge tilstrækkelige oplysninger.

Et potentielt tilbud om individuelt fravalg for hver organisation, der indsamler disse oplysninger, kan efter Artikel 29-Gruppens opfattelse pålægge borgerne en uacceptabel byrde som følge af den øgede anvendelse af sådanne sporingsteknologier hos både private og offentlige organisationer. Artikel 29-Gruppen opfordrer derfor EU-lovgiver til at fremme udviklingen af tekniske standarder for apparater, som automatisk signalerer en indvending mod en sådan sporing, og sikre, at overholdelsen af et sådant signal kan håndhæves.

Ifølge den generelle forordning om databeskyttelse kræves der sandsynligvis et samtykke, hvis en dataansvarlig indsamler og lagrer apparaters indirekte identificerbare (WiFi- eller Bluetooth-) MAC-adresser og beregner brugerens placering for at spore den pågældende brugers placering gennem længere tid, f.eks. på tværs af flere forretninger. Dette gælder navnlig, hvis sådan sporing finder sted i offentlige områder, hvor brugerne har en berettiget forventning om, at de ikke kan identificeres eller spores, men hvor forbipasserendes MAC-adresser indsamles. Et sådant samtykke kan f.eks. indhentes ved brug af en app, der opfordrer brugerne til at tillade sporing af deres placering inden for bestemte områder til gengæld for kommercielle tilbud, eller ved at tilbyde indtjekning på bestemte steder eller gennem et samtykkemodul på WiFi-hotspots.

Kun under særlige omstændigheder kan det tillades, at de dataansvarlige behandler de oplysninger, der udsendes af terminaludstyr, med henblik på at spore personers fysiske bevægelser uden de pågældende personers samtykke. Dette kan f.eks. være tilfældet ved en optælling af antallet af kunder på et bestemt sted eller ved indsamling af udsendte oplysninger på begge sider af et sikkerhedskontrolpunkt for at vise ventetiden. I begge eksempler skal oplysningerne slettes eller anonymiseres, så snart det statistiske formål er opfyldt. Det betyder, at MAC-adresserne på besøgendes apparater på et bestemt sted, f.eks. en forretning, skal anonymiseres straks efter indsamlingen uden permanent lagring af MAC-adresserne på en sådan måde, at det ikke er teknisk muligt at identificere dem igen. I eksemplet med beregning af ventetiden skal MAC-adresserne slettes eller anonymiseres, så snart oplysningerne ikke længere er relevante for at beregne ventetiden (f.eks. fordi den besøgende er nået om på den anden side af sikkerhedskontrollen, eller fordi han eller hun har forladt køen).

Den dataansvarlige skal desuden overholde kravene om dataminimering (f.eks. ikke at spore døgnet rundt, når formålet er begrænset til forretningens åbningstider og/eller udtagning af stikprøver med mellemrum). De dataansvarlige skal desuden også træffe andre afbødende foranstaltninger for at sikre, at brugernes privatlivsrettigheder ikke påvirkes eller kun påvirkes i meget begrænset omfang, f.eks. for at beskytte privatlivet for personer, der bor ved siden af et indsamlingspunkt.

Valget i forordningsforslagets artikel 8, stk. 2, af et rent meddelelseskrav er endnu mere bemærkelsesværdigt set i lyset af betragtning 20, hvor det konkluderes, at oplysninger vedrørende slutbrugernes apparater også kan fjernindsamles med henblik på identificering og sporing, og at sådan behandling – ifølge den foreslåede forordning – kan udgøre en alvorlig trussel for slutbrugernes privatliv. Dette krav går desuden ikke videre end det informationskrav, der allerede er fastsat i artikel 13 og

14 i den generelle forordning om databeskyttelse. Den alvorlige privatlivstrussel fra sporing forstærkes af andres mulighed for at få adgang til de indsamlede oplysninger, f.eks. muligheden for, at politiet kan identificere slutbrugere på grundlag af de lagrede MAC-adresser, som deres mobilapparater udsender.

#### 18. Betingelserne for at analysere indhold og metadata skal uddybes.

I forordningsforslagets artikel 6 tildeles metadata og indhold forskellige beskyttelsesniveauer. Artikel 29-Gruppen støtter ikke denne sondring: Begge kategorier af oplysninger er særdeles følsomme. Metadata og indhold bør derfor tillægges det samme høje beskyttelsesniveau. Udgangspunktet bør derfor være, at det er forbudt at behandle metadata og indhold uden samtykke fra alle slutbrugere (dvs. afsender og modtager).

Afhængigt af formålene kan visse former for behandling dog tillades uden samtykke, hvis det er strengt nødvendigt til disse formål:

- Leverandører kan behandle elektroniske kommunikationsdata til de formål, der er nævnt i forordningsforslagets artikel 6, stk. 1, litra a) og b), artikel 6, stk. 2, litra a) og b)<sup>7</sup>.
- Det bør præciseres, at visse teknikker til opdagelse/filtrering af spam og afbødning af botnet kan anses for strengt nødvendige for at opdage og stoppe misbrug af elektroniske kommunikationstjenester (artikel 6, stk. 2, litra b)). Med hensyn til filtrering af spam bør brugere, som modtager spam, tilbydes specifikke fravalgsmuligheder, hvis det er teknisk muligt.
- Det bør præciseres, at analysen af elektroniske kommunikationsdata med henblik på kundeservice også kan være omfattet af undtagelsen vedrørende "det er nødvendigt for at fakturere" (se artikel 6, stk. 2, litra b)). De relevante metadata kan opbevares indtil udgangen af den periode, inden for hvilken der gyldigt kan gøres indsigelse mod en faktura eller betalingen kan anfægtes efter national ret. De relevante data (f.eks. webadresser) må kun opbevares efter slutbrugerens anmodning og da kun i den periode, der er strengt nødvendig for at afgøre en tvist vedrørende en faktura (artikel 7, stk. 3, bør følgelig ændres i overensstemmelse hermed).
- Det bør være muligt at behandle elektroniske kommunikationsdata med henblik på at levere tjenester, som en slutbruger udtrykkeligt har anmodet om, f.eks. en funktion til søgeordsindeksering, virtuelle vejledninger, tekst-til-tale-tjenester og oversættelsestjenester. Dette kræver, at der indføres en undtagelse vedrørende analyse af sådanne data til rent individuel (privat)

---

<sup>7</sup> Med hensyn til det, der er nødvendigt for at leve op til de obligatoriske krav til tjenestekvalitet som omhandlet i forordningsforslagets artikel 6, stk. 2, litra a), bør leverandører tage hensyn til de betingelser, der er angivet i forordning (EU) 2015/2120 (den europæiske kodeks for elektronisk kommunikation), særligt artikel 3 og betragtning 10 samt 13-15. Med hjemmel i denne bestemmelse kan det kræves, at leverandører behandler kommunikationsdata for at opdage og filtrere malware og spyware, og det kan tillades, at de komprimerer data.

brug og vedrørende individuelle arbejdsrelaterede formål<sup>8</sup>. Dette vil således være muligt uden samtykke fra alle slutbrugere, men må kun finde sted med samtykke fra den slutbruger, der anmoder om tjenesten. Et sådant specifikt samtykke vil også hindre leverandøren i at bruge disse oplysninger til andre formål.

Det betyder, at analysen af indhold og/eller metadata til alle andre formål, f.eks. analyser, profilering, adfærdsbetinget reklamerings eller andre formål, som er til (kommerciel) fordel for leverandøren, kræver samtykke fra alle slutbrugere, hvis data behandles. Med hensyn til disse situationer bør det i den foreslåede forordning forklares, at selve afsendelsen af en e-mail eller en anden form for personlig kommunikation fra en anden tjeneste til en slutbruger, som personligt har givet samtykke til behandlingen af vedkommendes indhold og metadata (f.eks. i forbindelse med tilmeldingen til en mailservice), ikke udgør et gyldigt samtykke fra afsenderen.

Endelig bør det præciseres, at behandlingen af andre personers data end de involverede slutbrugeres (f.eks. en tredjemands billede eller beskrivelse i en udveksling mellem to personer) også skal overholde alle de relevante bestemmelser i den generelle forordning om databeskyttelse

19. **Terminaludstyr og software skal *som standard* modvirke, forebygge og forbyde ulovlig indgreb deri og give oplysninger om valgmulighederne.** Selv om leverandører af software, som muliggør elektronisk kommunikation, ved den foreslåede forordning forpligtes til at "give mulighed" for at forhindre begrænsede former for indgreb i terminaludstyr, og softwareleverandører efter installation forpligtes til at kræve, at slutbrugerne giver deres samtykke til en indstilling (artikel 10, stk. 1 og 2), er en sådan valgmulighed ikke det samme som *privatlivsbeskyttelse ved hjælp af standardindstillinger*. Muligheden for at forhindre visse former for indgreb findes desuden allerede, og indtil videre har det ikke ført til en tilstrækkelig løsning af problemet med uønsket sporing. Dette er netop årsagen til, at man i den generelle forordning om databeskyttelse bevidst har valgt at indføre principperne om databeskyttelse og beskyttelse af privatlivet ved hjælp af design og standardindstillinger (artikel 25 i den generelle forordning om databeskyttelse). Den foreslåede forordning undergraver disse principper for så vidt angår kommunikations- og apparatdata. Direktivet om radioudstyr 2014/53/EU<sup>9</sup> (der er nævnt i betragtning 10) indeholder kun et meget begrænset sikkerhedskrav, hvorefter radioudstyr skal være "i stand til at sikre, at personoplysninger om brugeren og abonnenten og disses privatliv beskyttes" (artikel 3, stk. 3, litra e)). Dette kan ikke erstatte specifik privatlivsbeskyttelse gennem standardindstillinger i den foreslåede forordning. Det bør i denne forbindelse også bemærkes, at Eurobarometer-undersøgelsen om

---

<sup>8</sup> Mens det i forordningsforslagets betragtning 13 udtrykkeligt er anført, at virksomhedsnet er udelukket fra forordningens anvendelsesområde, bør denne nye individuelle undtagelse også omhandle medarbejders brug af cloudtjenester til arbejdsrelaterede formål, f.eks. søgning i deres e-mail.

<sup>9</sup> Direktiv 2014/53/EU om radioudstyr.



databeskyttelse inden for elektronisk kommunikation, som blev offentliggjort i december 2016, viste, at "næsten syv ud af ti (69 %) er helt enige i, at standardindstillingerne i deres browser bør hindre, at deres oplysninger deles"<sup>10</sup>. Artikel 29-Gruppen har en særskilt betænkelighed vedrørende browserindstillinger og definitionen af "tredjeparter". Se bemærkning 24. Det bør endvidere erindres, at denne bestemmelse ikke kun vedrører browsere, der bruges på computere, men også omfatter andre typer software, som muliggør kommunikation (herunder operativsystemer, apps og softwaregrænseflader til internet of things-tilsluttede apparater). Terminaludstyr og software skal således *som standard* tilbyde privatlivsbeskyttende indstillinger og vejlede brugerne ved hjælp af konfigurationsmenuer, hvis de vil fravige disse standardindstillinger efter installationen. Disse konfigurationsmenuer bør altid være lettilgængelige under brug. Artikel 29-Gruppen opfordrer EU- lovgiver til at præcisere anvendelsesområdet for artikel 10 i dette øjemed.

20. **E-databeskyttelsesforordningen bør udtrykkeligt forbyde tracking walls**, dvs. den fremgangsmåde, hvorved adgang til et websted eller en tjeneste nægtes, medmindre brugerne accepterer at blive sporet på andre websteder eller tjenester. Som Artikel 29-Gruppen allerede har bemærket i tidligere udtalelser om e-datadirektivet<sup>11</sup>, er sådanne "take it or leave it"-fremgangsmåder sjældent berettigede<sup>12</sup>. Når brugen af terminaludstyrs behandlings- og lagringskapacitet eller indsamlingen af oplysninger fra slutbrugernes terminaludstyr muliggør sporing af brugernes aktiviteter i længere tid eller på tværs af forskellige tjenester (f.eks. forskellige websteder eller apps), kan en sådan databehandling i betydeligt omfang krænke disse brugeres privatliv. Henset til internettets grundlæggende betydning for udøvelsen af den grundlæggende ytringsfrihed, herunder retten til adgang til information, bør enkeltpersoners mulighed for at få adgang til onlineindhold ikke afhænge af, at de accepterer sporing af aktiviteter på tværs af apparater og websteder/apps. Det bør i den kommende e-databeskyttelsesforordning derfor præciseres, at adgang til indhold på f.eks. websteder og i apps ikke kan gøres betinget af accepten af en sådan indgribende databehandling, uanset den anvendte sporingsteknologi, f.eks. cookies, device fingerprinting, overførsel af unikke identifikatorer eller andre overvågningsteknikker. Nødvendigheden af dette forbud understreges af den seneste Eurobarometerundersøgelse om databeskyttelse inden for elektronisk kommunikation, hvor det bemærkes, at "næsten to tredjedele af respondenterne udtaler, at de ikke kan acceptere, at deres onlineaktiviteter overvåges til gengæld for ubegrænset adgang til et bestemt websted (64 %)".
21. Med hensyn til de fire ovennævnte punkter **bør den foreslåede forordning leve op til sin målsætning om at sikre det samme eller et højere beskyttelsesniveau end den generelle forordning om databeskyttelse**. I betragtning 5 konstateres det, at den

---

<sup>10</sup> Se Flash Eurobarometer 443, Report e-Privacy (offentliggjort december 2016), s. 5.

<sup>11</sup> Se f.eks. WP240 (ePrivacy review), s. 16, og WP208 (fritagelse for samtykke til cookies), s. 5.

<sup>12</sup> Dette gælder uanset artikel 7, stk. 4, i den generelle forordning om databeskyttelse, som også kan være til hinder for "take it or leave it"-valg i andre situationer, hvor det er hensigtsmæssigt.

foreslåede forordning ikke sænker beskyttelsesniveauet i forhold til den generelle forordning om databeskyttelse. Som den foreslåede forordning aktuelt foreligger, er dette imidlertid ikke korrekt, navnlig med hensyn til sporingen af apparater (bemærkning 17), den manglende overholdelse af princippet om privatlivsbeskyttelse gennem standardindstillinger (bemærkning 19) og samtykke (bemærkning 18). Dette er i særlig grad relevant, eftersom det i den samme betragtning anføres, at den foreslåede forordning udgør "særlovgivning i forhold til den generelle forordning om databeskyttelse og vil præcisere og supplere denne for så vidt angår elektronisk kommunikation, der betragtes som personoplysninger". Artikel 29-Gruppen foreslår, at det i e-databeskyttelsesforordningen som minimum præciseres, at

i) forbuddene i e-databeskyttelsesforordningen har forrang for tilladelserne i den generelle forordning om databeskyttelse (forbuddet mod indgreb i artikel 5 i e-databeskyttelsesforordningen har f.eks. forrang for elektroniske tjenesteleverandørers rettigheder til viderebehandling af personoplysninger i henhold til artikel 5, stk. 1, litra b), og artikel 6, stk. 4, i den generelle forordning om databeskyttelse)

ii) behandling af personoplysninger, når den er tilladt i kraft af en undtagelse (herunder samtykke) til e-databeskyttelsesforordningens forbud, stadig skal overholde alle relevante bestemmelser i den generelle forordning om databeskyttelse

iii) når behandlingen er tilladt i kraft af en undtagelse til e-databeskyttelsesforordningens forbud, er enhver anden behandling efter den generelle forordning om databeskyttelse, herunder behandling til andre formål i medfør af artikel 6, stk. 4, i den generelle forordning om databeskyttelse, forbudt. Dette bør ikke være til hinder for, at dataansvarlige anmoder om yderligere samtykke til nye behandlingsaktiviteter. Det bør heller ikke være til hinder for, at lovgiver fastlægger yderligere, begrænsede og specifikke undtagelser i e-databeskyttelsesforordningen, f.eks. med henblik på at tillade behandling til videnskabelige eller statistiske formål i henhold til artikel 89 i den generelle forordning om databeskyttelse eller for at beskytte en persons "vitale interesser" i henhold til artikel 6, litra d), i den generelle forordning om databeskyttelse.

E-databeskyttelsesforordningen bør desuden fortolkes således, at den sikrer mindst det samme beskyttelsesniveau som den generelle forordning om databeskyttelse og i relevante tilfælde et højere beskyttelsesniveau.

#### 4. ANDRE BETÆNKELIGHEDER

Ud over ovennævnte forhold er Artikel 29-Gruppen **betænkelig** ved følgende.

##### *DET TERRITORIALE OG MATERIELLE ANVENDELSESOMRÅDE SKAL UDVIDES*

22. **Udtrykket "metadata" er defineret for snævert.** I artikel 4, litra c), defineres dette udtryk på nuværende tidspunkt som "data behandlet i et elektronisk kommunikationsnet med henblik på at videresende, distribuere eller udveksle elektronisk kommunikationsindhold" (fremhævelse tilføjet). Anvendelsen af ordet "net" viser tilsyneladende, at kun data, der er genereret under leveringen af tjenester i

det "nederste" lag af nettet, anses for "metadata". Dette kan betyde, at data, der genereres under leveringen af en OTT-tjeneste, er udelukket fra dette anvendelsesområde. Dette er ikke ønskværdigt og er sandsynligvis ikke bevidst, da det netop er hensigten at udvide forordningsforslagets anvendelsesområde til OTT-tjenesteleverandører. For at afhjælpe dette bør definitionen af "elektroniske kommunikationsmetadata" ændres til at omfatte alle data, der behandles med henblik på at videresende, distribuere eller muliggøre udveksling af elektronisk kommunikationsindhold.

23. Det er desuden betænkeligt, at **den foreslåede forordnings territoriale anvendelsesområde med hensyn til organisationer, som ikke er etableret i Unionen, kun omhandler leverandører af elektroniske kommunikationstjenester**. I henhold til den foreslåede forordning skal leverandøren af en elektronisk kommunikationstjeneste, som ikke er etableret i Unionen, skriftligt udpege en repræsentant i Unionen (artikel 3, stk. 2). I betragtning 9 nævnes det også, at forordningen bør finde anvendelse på behandling, der foretages af leverandører af elektroniske kommunikationstjenester, uanset hvor behandlingen finder sted. Artikel 29-Gruppen glæder sig over denne præcisering. Da ordlyden er begrænset til leverandører af elektroniske kommunikationstjenester, er det imidlertid uvist, i hvilket omfang dette territoriale anvendelsesområde gælder for andre typer parter (f.eks. parter, der griber ind i eller indsamler oplysninger, der udsendes af slutbrugeres terminaludstyr, i henhold til artikel 3, stk. 1, litra c), sammenholdt med artikel 8 i den foreslåede forordning). Artikel 29-Gruppen foreslår derfor, at artikel 3, stk. 2 og 5, ændres med henblik på at medtage leverandører af offentligt tilgængelige fortegnelser, leverandører af software, som muliggør elektronisk kommunikation, og personer, der sender kommercielle direkte markedsføringsmeddelelser eller indsamler (andre) oplysninger om eller lagret på slutbrugers terminaludstyr, når deres aktiviteter er målrettet mod brugere i Unionen (jf. forordningsforslagets betragtning 8)<sup>13</sup>.

#### BESKYTTELSEN AF TERMINALUDSTYR SKAL STYRKES

En anden kategori af betænkeligheder omhandler den utilstrækkelige beskyttelse af terminaludstyr i den foreslåede forordning.

24. For det første **anføres det ukorrekt i den foreslåede forordning, at gyldigt samtykke kan gives gennem ikkespecifikke browserindstillinger**. Artikel 29-Gruppen anerkender, at slutbrugerne i dag bliver overbebyrdet med anmodninger om samtykke (betragtning 22). Browserindstillinger (og tilsvarende softwareindstillinger)

---

<sup>13</sup> Se artikel 3, stk. 2, i den generelle forordning om databeskyttelse: "Denne forordning finder anvendelse på behandling af personoplysninger om registrerede, der er i Unionen, og som foretages af en dataansvarlig eller databehandler, der ikke er etableret i Unionen, hvis behandlingsaktiviteterne vedrører: a) udbud af varer eller tjenester til sådanne registrerede i Unionen, uanset om betaling fra den registrerede er påkrævet, eller b) overvågning af sådanne registreredes adfærd, for så vidt deres adfærd finder sted i Unionen." Denne forpligtelse bør også omfatte undtagelser i overensstemmelse med artikel 27, stk. 2, i den generelle forordning om databeskyttelse.

kan medvirke til at løse dette problem. Da generelle browserindstillinger ikke er udviklet til at gælde for anvendelsen af en sporingsteknologi i et enkelt tilfælde, er de ikke egnede til at give samtykke i henhold til artikel 7 i og betragtning 32 til den generelle forordning om databeskyttelse (da samtykket ikke er informeret og tilstrækkeligt specifikt).

Slutbrugeren skal kunne give særskilt samtykke for hvert websted eller hver app til sporing til forskellige formål (f.eks. deling på sociale medier eller reklamer). En dataansvarlig, som er ansvarlig for flere websteder eller apps, kan også anmode om samtykke for alle andre websteder eller apps, som er under hans kontrol, såfremt denne anmodning om samtykke vises særskilt.

Den dataansvarlige skal desuden overholde alle andre forpligtelser vedrørende samtykke, herunder forpligtelsen til at give brugerne tilstrækkelige oplysninger. For både browsere og dataansvarlige betyder dette, at det vil være ugyldigt, hvis de kun giver mulighed for at "acceptere alle cookies", da dette ikke giver brugerne mulighed for at give det krævede specifikke samtykke. Browsere bør dog have mulighed for at tillade, at brugere træffer et informeret og bevidst valg om at acceptere alle cookies og dermed undgå specifikke anmodninger om samtykke fra websteder, som de besøger.

Artikel 29-Gruppen anbefaler på det kraftigste, at det i e-databeskyttelsesforordningen kræves, at browsere implementerer tekniske funktioner, som f.eks. do not track-standarden, for at sikre, at brugerne gives reelle valgmuligheder og reel kontrol over indgreb i deres apparater<sup>14</sup>.

Endnu mere vigtigt bør e-databeskyttelsesforordningen sikre, at både valget med hensyn til lagring af oplysninger på apparatet og et DNT-signal fra en browser accepteres som en retligt bindende tilkendegivelse eller afvisning af samtykke af alle dataansvarlige. Dette gælder uanset yderligere retningslinjer fra Artikel 29-Gruppen om overholdelse af DNT-standarden, herunder princippet om formålsbegrænsning, når standarden foreligger (planlagt til udgangen af 2017).

Underforståede typer "samtykke", f.eks. klik på et websted eller scrolling på siden, kan ikke tilsidesætte valg med hensyn til lagring og DNT-signalet. En vigtig fordel ved brugen af denne standard er, at den ikke er begrænset til cookie-sporingsteknologien, men også omhandler andre typer sporing, f.eks. fingerprinting.

Hvis overholdelse af denne standard blive obligatorisk, vil det også løse et andet problem i forbindelse med den nuværende anvendelse af udtrykket "tredjeparter" i artikel 10. En webside eller app indeholder generelt mange elementer, både fra selve webstedet og eksterne elementer. Ekstern kode kan også køres inden for rammerne af det besøgte websted, når det rapporterer tilbage til en tredjepartsserver. En sporingscookie lagres f.eks. af en førstepart, når en bruger besøger et socialt netværkswebsted. Dette sociale netværkswebsted kan være en tredjepart, når denne bruger besøger et andet websted, som indeholder interaktion med det pågældende sociale netværkswebsted. I alle disse tilfælde, uanset om der er tale om "adgang til" eller "lagring af oplysninger" på slutbrugerens apparat, udgør dette et indgreb i apparatet, som kræver brugerens samtykke (medmindre en af undtagelserne finder

---

<sup>14</sup> Se webadressen: <https://www.w3.org/TR/tracking-compliance/>. I afsnit 7 forklares undtagelsesmodellen og sondringen mellem webstedsspecifikke undtagelser og undtagelser for hele internettet. Afsnit 6 indeholder de maskinlæsbare oplysninger, som dataansvarlige kan give for at opfylde informationskravet i forbindelse med indhentning af samtykke.

anvendelse). Efter DNT-standarden behandles dette med brugen af udtrykkene "site-wide" og "internet-wide". For at øge retssikkerheden for alle interessenter bør henvisningen i e-databeskyttelsesforordningen til "tredjeparter" derfor omformuleres til at dække alle enheder, med hvilke et apparat interagerer (fordi de lagrer eller får adgang til oplysninger på apparatet).

For at gøre do not track-standarden forenelig med det høje niveau for beskyttelse af kommunikationshemmelighed og data, der sikres ved chartret, bør det i e-databeskyttelsesforordningen anføres, at anmodninger om "internet-wide" sporing i modsætning til "site-wide" sporing skal vises separat, og at brugerne frit skal kunne acceptere eller afvise sådanne anmodninger. For at beskytte brugerne mod hyppige anmodninger om samtykke bør det ved e-databeskyttelsesforordningen sikres, at en afvisning af accept af internet-wide sporing fra en specifik organisation (via do not track-standarden eller via en særskilt sortliste) forhindrer denne organisation i at fremsætte fremtidige anmodninger om samtykke i mindst seks måneder. Denne er ikke til hinder for, at denne organisation, når den besøges direkte af brugeren (dvs. som førstepart), anmoder om samtykke på dens eget websted (dvs. en anmodning om site-wide samtykke). I praksis betyder dette, at eksempelvis et videostreaming-websted, som lagrer sporingscookies, må anmode om samtykke, når brugeren besøger videostreaming-webstedet, men ikke må anmode om samtykke igen i en periode på seks måneder, når brugeren har afvist at give sit samtykke og besøger andre websteder, som indeholder videoer, der hentes fra streaming-webstedet.

25. **Undtagelsen vedrørende "måling af internetbesøgende" er desuden formuleret upræcist.** Forordningsforslagets artikel 8, stk. 1, litra d), omhandler en undtagelse vedrørende måling af internetbesøgende. Den første betænkelighed er, at udtrykket ikke er defineret og kan forveksles med brugerprofilering. Det bør i definitionen præciseres, at denne undtagelse ikke kan anvendes til profilering. Undtagelsen bør kun finde anvendelse på de brugsanalyser, der skal udføres for at analysere ydelsen af den tjeneste, brugeren har anmodet om, men ikke til brugeranalyser (dvs. analyse af identificerbare brugeres adfærd på et websted, i en app eller på et apparat). Undtagelsen må derfor ikke anvendes i tilfælde, hvor data kan kædes sammen med identificerbare brugerdata, som behandles af leverandøren eller andre dataansvarlige. Dens beskrivelse antyder desuden en meget teknologispecifik anvendelse. Udtrykket "måling af internetbesøgende" bør derfor omdefineres på en teknologineutral måde, så det også kommer til at omfatte lignende analytiske oplysninger om brug hentet fra apps, wearables og internet of things-apparater.

Artikel 29-Gruppen foreslår, at der hentes inspiration fra den nederlandske undtagelse, som gælder, hvis det er strengt nødvendigt, med henblik på at indhente oplysninger om den tekniske kvalitet eller effektivitet af en leveret informationssamfundstjeneste, og hvis det ikke har nogen eller kun begrænset indvirkning på abonnentens eller slutbrugerens privatliv (se artikel 11.7a, stk. 3, litra b), i den nederlandske telekommunikationslov). Med denne undtagelse tages der højde for, at de fleste data, der indsamles via web- eller app-analyser, er personoplysninger. Det betyder, at behandlingen af disse data også er underlagt den generelle forordning om databeskyttelse. Det indebærer f.eks., at brugsanalyser bør udføres af en ekstern organisation, men kun såfremt:

- i) denne organisation handler som databehandler
- ii) der er indgået en behandlingsaftale, som er i overensstemmelse med den generelle forordning om databeskyttelse
- iii) den anvendte analyseteknologi forhindrer genkendelse, herunder bl.a. anonymisering af brugernes IP-adresser
- iv) de specifikke cookies eller andre data, der bruges til analyse, kun kan bruges i forbindelse med det specifikke websted, den specifikke app eller den specifikke wearable og ikke kan kædes sammen med andre identificerbare data
- v) brugere har ret til fravalg (se også denne bemærkning 17 og 50 i denne udtalelse).

Selv om der ikke kræves samtykke, hvis disse betingelser er opfyldt, skal dataansvarlige stadig give tilstrækkelige oplysninger til brugerne, f.eks. gennem felterne for sporingssstatus i do not track-standard<sup>15</sup>.

26. E-databeskyttelsesforordningen **bør sikre snævre og præcist formulerede undtagelser til krav om samtykke**. Ordlyden af undtagelsen til kravet om samtykke til indgreb i apparater i artikel 8, stk. 1, litra c), er næsten identisk med den nuværende ordlyd af e-datadirektivets artikel 5, stk. 3, "*absolut påkrævet for at levere en informationssamfundstjeneste, abonnenten eller brugeren udtrykkelig ønsker*", men det vigtige ord "absolut" er udeladt uden forklaring. Dette giver anledning til bekymring af to grunde. Bestemmelsen i e-datadirektivet har for det første allerede ført til omfattende diskussioner om dens anvendelsesområde mellem tilsynsmyndigheder og organisationer, og fjernelsen af ordet "absolut" vil sikre endnu mindre retssikkerhed. Dette vækker også bekymring, fordi Artikel 29-Gruppen allerede har udtalt sig om fortolkningen af udtrykket "absolut" i denne sammenhæng. Artikel 29-Gruppen foreslog følgende præcisering i sin udtalelse om undtagelser fra kravet om, at der skal gives samtykke til cookies (WP 194):

*"En cookie er nødvendig for at stille en specifik funktionalitet til rådighed for brugeren(eller abonnenten). Hvis cookieerne er blokeret, vil denne funktionalitet ikke være til rådighed. Brugeren (eller abonnenten) har udtrykkeligt anmodet om denne funktionalitet som en del af en informationssamfundstjeneste."*<sup>16</sup>

Artikel 29-Gruppen præciserede desuden, at:

*"'tredjepartcookies' ikke altid [er] 'strengt nødvendige' for en bruger, der besøger et websted, da disse cookies sædvanligvis er knyttet til en anden tjeneste end den, brugeren 'udtrykkeligt har anmodet om'"*<sup>17</sup>.

Artikel 29-Gruppen tilføjede, at brugen af sociale plug-ins målrettet mod ikkemedlemmer af en platform eller et websted ligeledes ikke bør anses for strengt nødvendige.

<sup>15</sup> Se: Tracking Preference Expression (DNT), Editor's draft, 7.3.2016.

<sup>16</sup> Artikel 29-Gruppen, WP 194, udtalelse 04/2012 om undtagelser fra kravet om, at der skal gives samtykke til cookies, vedtaget den 7.6.2012, webadresse: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194\\_da.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_da.pdf).

<sup>17</sup> Ibid.

Mens forordningsforslagets artikel 6, stk. 1, litra b), tillader behandling af elektroniske kommunikationsdata, hvis det er "nødvendigt" af sikkerhedshensyn, kræves det i betragtning 49 i den generelle forordning om databeskyttelse, at denne er strengt nødvendig. Udeladelsen af ordet "strengt" er muligvis ikke bevidst, da det i forordningsforslagets betragtning 21 netop nævnes, at der ikke bør anmodes om samtykke til indgreb, som er "strengt" nødvendige. Den foreslåede forordning er imidlertid en anledning til yderligere at præcisere, at nødvendighedstesten i forbindelse med denne forordning bør fortolkes snævert for så vidt angår alle undtagelser. Med hensyn til alle undtagelser i forordningsforslagets artikel 6 og artikel 8, stk. 1, foreslår Artikel 29-Gruppen derfor, at ordet "strengt" indsættes foran "nødvendigt".

E-databeskyttelsesforordningen bør på den anden side udtrykkeligt tillade indgreb i udstyr, der har til formål at installere sikkerhedsopdateringer. Overførsel af sikkerhedsopdateringer via internettet er den foretrukne metode til installation af sikkerhedsopdateringer på de fleste slutbrugerapparater. Installation af opdateringer anses for et indgreb i terminaludstyr. Der er en legitim interesse i at sikre, at disse apparaters sikkerhed altid er ajourført. En leverandør af sikkerhedsforbedringer (patches) bør derfor generelt altid kunne installere de strengt nødvendige sikkerhedsopdateringer uden slutbrugerens samtykke. Det er imidlertid uvist, om dette indgreb kan være omfattet af undtagelsen til forbuddet mod indgreb vedrørende "informationssamfundet" (artikel 8, stk. 1, litra c)). Det bør præciseres, at installationen af sikkerhedsopdateringer er tilladt efter denne undtagelse, men kun for så vidt som i) sikkerhedsopdateringerne er pakket diskret og ikke på nogen måde ændrer softwarens funktionalitet på udstyret (herunder dens interaktion med anden software eller andre indstillinger, brugeren har valgt), ii) slutbrugeren på forhånd underrettes, hver gang en opdatering installeres, og iii) slutbrugeren har mulighed for at slå den automatiske installation af disse opdateringer fra.

## *DIREKTE MARKEDSFØRING*

En anden kategori af betænkeligheder vedrører den utilstrækkelige beskyttelse mod direkte markedsføring.

27. Det er for det første betænkeligt, at **anvendelsesområdet for direkte markedsføring er for begrænset**. I forordningsforslagets artikel 4, stk. 3, litra f), defineres "direkte markedsføringsmeddelelse" som "enhver form for reklame, uanset om den er skreven eller talt, som er sendt til en eller flere identificerede eller identificerbare slutbrugere af elektroniske kommunikationstjenester". Brugen af ordet "sendt" indebærer brugen af teknologiske kommunikationsmidler, der nødvendigvis involverer overføring af en meddelelse, mens størstedelen af annoncering på internettet (via sociale medieplatforme eller på websteder) ikke involverer egentlig "afsendelse" af reklamer. Dette understreges af de efterfølgende eksempler i definitionen (e-mail, sms osv.) og i betragtning 33. Disse henviser alle til ganske traditionelle former for markedsføringsmeddelelser, og selv brugen af – ganske traditionelle – opkaldssystemer er ikke omfattet af anvendelsesområdet. Artiklen og betragtningen bør ændres til at omfatte enhver form for reklame, som er *sendt, dirigeret eller vist* til

en eller flere identificerede eller identificerbare slutbrugere. Det bør endvidere sikres, at adfærdsbaserede reklamer (baseret på slutbrugernes profiler) også anses for direkte markedsføringsmeddelelser, der er dirigeret til "en eller flere identificerede eller identificerbare slutbrugere" (da sådanne reklamer er målrettet mod specifikke, identificerbare brugere).

Efter det foreslåede anvendelsesområde for "direkte markedsføringsmeddelelser" vil beskyttelsen i henhold til artikel 16, stk. 1, være begrænset til meddelelser, der indeholder reklamemateriale, og vil ikke beskytte personer mod andre meddelelser, der sendes, dirigeres eller vises til markedsføringsformål (f.eks. som lead generation-meddelelser, der har til formål at opnå samtykke, fremme af politiske holdninger eller afstemningspræferencer, fremme af velgørende eller andre non-profit-organisationer eller generel branding af en organisation). Faxmaskiner bruges desuden stadig i forbindelse med direkte markedsføring, selv om de ikke nævnes i definitionen. Artikel 4, stk. 3, litra f), bør derfor omfatte enhver form for reklame, opsøgende aktiviteter eller promovering, også for non-profit-organisationer, og bør udtrykkeligt omfatte faxmaskiner sammen med e-mail og sms (se også forslaget til præcisering i bemærkning 43, litra a). Endelig anføres det i betragtning 32, at direkte markedsføring omfatter meddelelser afsendt af politiske partier for at fremme deres partier. Denne betragtning bør opdateres til at omfatte politikere og kandidater til valg, som fremmer deres kandidatur.

28. **Tilbagetrækning af samtykke til direkte markedsføring er for det andet ikke gratis eller lige så let som at give samtykke.** Muligheden for at tilbagetrække samtykke i henhold til den foreslåede forordning skal præciseres for at sikre sammenhæng og forbedre beskyttelsen af modtagere. I henhold til forordningsforslagets nuværende artikel 16, stk. 6, skal modtagere af direkte markedsføring gives "de nødvendige oplysninger til at gøre brug af deres ret til på en nem måde at trække deres samtykke til at modtage flere markedsføringsmeddelelser tilbage" (fremhævelse tilføjet). Dette bekræftes i betragtning 34. Det følger imidlertid af betragtning 70 til den generelle forordning om databeskyttelse, at registrerede i henhold til den generelle forordning om databeskyttelse til enhver tid bør have ret til "gratis" at gøre indsigelse mod behandling med henblik på direkte markedsføring. Dette udtryk bruges også i forordningsforslagets artikel 16, stk. 2, men kun med hensyn til fravalg af direkte markedsføring på grundlag af kontaktoplysninger indhentet i forbindelse med et salg.

I henhold til artikel 7, stk. 3, i den generelle forordning om databeskyttelse skal det være lige så let at trække sit samtykke tilbage som at give det, og den registrerede har til enhver tid ret til at trække sit samtykke tilbage. I sin udtalelse 04/2010 om FEDMA (WP 174) anerkendte Artikel 29-Gruppen betydningen af at tilbyde "en enkel, effektiv, direkte og nem måde at afmelde kommercielle meddelelser vederlagsfrit"<sup>18</sup>. Denne standard for tilbagetrækning af samtykke bør indarbejdes i

---

18 Udtalelse nr. 4/2010 om FEDMA's europæiske adfærdskodeks for brug af personoplysninger i forbindelse med direkte markedsføring, vedtaget den 13.7.2010, webadresse: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174\\_da.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174_da.pdf).



reglerne om direkte markedsføring i den foreslåede forordning. Det samme gælder kravet i artikel 7, stk. 3, i den generelle forordning om databeskyttelse om, at det til enhver tid bør være lige så let at trække sit samtykke tilbage som at give det.

29. I sammenhæng hermed **bør det præciseres, hvordan samtykke tilbagetrækkes, eller direkte markedsføringsopkald fravælges.** På grundlag af forordningsforslagets artikel 16, stk. 4, kan medlemsstaterne vælge et system til fravalg af markedsføringsopkald. E-databeskyttelsesforordningen bør angive ordningerne for tilbagetrækning af samtykke og fravalg af markedsføringsopkald. I betragtning 36 angives det, at medlemsstaterne *bør kunne* indføre og/eller bevare nationale fravalgssystemer. På grundlag af denne bestemmelse kan medlemsstaterne endda tillade en situation, hvor en bruger skal foretage fravalg hos individuelle afsendere af meddelelser. En sådan gennemførelse beskytter ikke brugerne mod generne ved uønskede henvendelser<sup>19</sup> og tilvejebringer ikke et system til nemt og til enhver tid at tilbagetrække deres samtykke, som er i overensstemmelse med den generelle forordning om databeskyttelse. Det bør derfor i forordningen angives, at hver medlemsstat *skal* etablere et nationalt register over personer, der ikke ønsker markedsføringsopkald. Det bør desuden i forordningen angives, at modtagere af opkald bør have to muligheder for at trække deres samtykke tilbage: for fremtidige opkald fra denne virksomhed eller organisation og mulighed for under et opkald at registrere sig i det nationale register over personer, der ikke ønsker markedsføringsopkald.
30. En anden betænkelighed er, at **brugen af falske identiteter ved afsendelse af direkte markedsføringsmeddelelser ikke forbydes udtrykkeligt.** Det bemærkes i betragtning 34, at det er "nødvendigt at forbyde maskering af identiteter og brug af falske identiteter, falske afsenderadresser eller -numre, når der sendes uanmodede kommercielle direkte markedsføringsmeddelelser". I artikel 16, stk. 6, anføres det imidlertid blot, at slutbrugere skal informeres om "identiteten af den fysiske eller juridiske person på hvis vegne meddelelsen fremsendes". Denne forpligtelse til at informere modtagere om identiteten bør suppleres af et klart forbud mod anvendelsen af maskerede eller falske kontaktadresser i forbindelse med direkte markedsføring.
31. Dette punkt hænger sammen med en anden betænkelighed: **Kravet om et præfiks ved direkte markedsføringsopkald præsenteres som et alternativ til kravet om visning af et kontaktnummer.** I henhold til artikel 16, stk. 3, er direkte markedsføringsopkald tilladt, hvis opkalderen enten i) viser et nummer, hvorpå den fysiske eller juridiske person, der foretager opkaldet, kan kontaktes (artikel 16, stk. 3, litra a), eller ii) viser en specifik kode/eller et præfiks, der afspejler det forhold, at der er tale om et markedsføringsopkald (artikel 16, stk. 3, litra b)). Selv om Artikel 29-Gruppen glæder sig over forpligtelsen i artikel 16, stk. 3, litra b), til at vise et præfiks, finder den, at dette krav ikke omhandler det samme problem som forpligtelsen til at vise et kontaktnummer i artikel 16, stk. 3, litra a). Mens kravet om et præfiks har til formål at sætte modtageren i stand til på forhånd at genkende et opkald som et

---

<sup>19</sup> I det Forenede Kongerige registrerede telekommunikationsselskabet BT f.eks. 31 mio. generende opkald på én uge. Se: <http://www.bbc.com/news/business-38635921>.

markedsføringsopkald (og til at træffe foranstaltninger for at blokere disse opkald), har kravet om et kontaktnummer til formål at give modtageren (og tilsynsmyndighederne) mulighed for at identificere og kontakte den, der har iværksat markedsføringen. Dette er især relevant i forbindelse med automatiske opkald, hvor der er en kraftig ubalance mellem markedsføringsvirksomhedens mulighed for at foretage generende opkald og modtagerens mulighed for at undgå disse opkald. Kravene må derfor ikke være alternativer, men skal supplere hinanden.

#### *TIDSPLAN*

32. Artikel 29-Gruppen anbefaler Kommissionen at anerkende, at den foreslåede forordning bør træde i kraft sammen med den generelle forordning om databeskyttelse i maj 2018 for at undgå manglende overensstemmelse mellem de to retsakter. Denne ambitiøse tidsplan vækker imidlertid stadig bekymring, idet den også kræver, at udkastet til kodeksen for elektronisk kommunikation færdiggøres. Artikel 29-Gruppen anmoder derfor alle interessenter i lovgivningsprocessen om at forpligte sig til at overholde fristen i maj 2018.

#### *ANDRE BETÆNKELIGHEDER*

I dette afsnit behandles en række yderligere betænkeligheder.

33. Artikel 29-Gruppen er for det første betænkelig ved **forslaget om, at ikkemålrettet dataopbevaring kan accepteres**. I begrundelsen bemærkes det, at medlemsstaterne efter den foreslåede forordning frit kan bevare eller etablere nationale rammer for dataopbevaring bevare, der bl.a. indeholder bestemmelser om målrettet dataopbevaring (afsnit 1.3). Efter afgørelsen i *Tele2/Watson-sagen*<sup>20</sup> er det klart, at rammer for dataopbevaring, som omhandler andet end målrettet opbevaring, ikke er tilladt i henhold til chartret (og selv da er genstand for vigtige betingelser som f.eks. tilsyn), og at generel adgang til metadata må anses for en overtrædelse af artikel 7 på samme måde som generel adgang til indholdet af elektroniske kommunikationsmeddelelser (jf. Domstolens dom, Schrems, og betragtning 94). Formuleringen af dette punktum giver medlemsstaterne et vist råderum med hensyn til dataopbevaringsforanstaltninger, som ikke findes. I denne forbindelse **tildeles metadata ikke et tilstrækkeligt beskyttelsesniveau** i den foreslåede forordning. Som nævnt i bemærkning 10 glæder Artikel 29-Gruppen sig over anerkendelsen af, at metadata kan åbenbare meget følsomme data. I den foreslåede forordning sikres metadata dog ikke den beskyttelse, der bør følge af en sådan anerkendelse. I lyset af metadataes følsomhed, navnlig inden en analyse i henhold til artikel 6, stk. 2, litra c), bør der gennemføres en konsekvensanalyse vedrørende databeskyttelse (se også bemærkning 46).

---

<sup>20</sup> ECLI:EU:C:2016:970, webadresse: <http://curia.europa.eu/juris/celex.jsf?celex=62015CJ0203>.

34. **Den foreslåede forordning vil for det andet udvide mulighederne for at opbevare data i uønsket grad.** I forordningsforslagets artikel 11 henvises der til artikel 23, stk. 1, litra a)-e), i den generelle forordning om databeskyttelse ved beskrivelsen af de formål, til hvilke medlemsstaterne kan begrænse de forpligtelser og rettigheder, der er fastsat i forordningens artikel 5-8. Den generelle forordning om databeskyttelse omhandler ikke sådanne begrænsninger med hensyn til særlige datakategorier i medfør af de høje risici for registrerede. Mens en tilsvarende begrænsning er tilladt i henhold til det nuværende e-datadirektivs artikel 15, er formålene mere begrænset. I det nye forordningsforslag tillades nye begrænsninger med henblik på "fuldbyrdelse af strafferetlige sanktioner, herunder beskyttelse mod og forebyggelse af trusler mod den offentlige sikkerhed" (artikel 23, stk. 1, litra d), i den generelle forordning om databeskyttelse) og "andre vigtige målsætninger i forbindelse med beskyttelse af Unionens eller en medlemsstats generelle samfundsinteresser, navnlig Unionens eller en medlemsstats væsentlige økonomiske eller finansielle interesser, herunder valuta-, budget- og skatteanliggender, folkesundhed og social sikkerhed" (artikel 23, stk. 1, litra e), i den generelle forordning om databeskyttelse). Disse formål er ikke kun nye i forhold til e-datadirektivet, det sidste formål i artikel 23, stk. 1, litra d), og hele formålet i artikel 23, stk. 1, litra e), er formuleret særdeles bredt. Det foreslås derfor, at henvisningen til artikel 23, stk. 1, litra a)-e), i den generelle forordning om databeskyttelse slettes, og at kun de formål, der i øjeblikket er nævnt i e-datadirektivets artikel 15, i stedet nævnes.

35. **Forpligtelsen til at informere brugere om sikkerhedstrusler har et minimalistisk anvendelsesområde.** Artikel 29-Gruppen bifalder, at leverandører af tjenester skal informere brugere om sikkerhedstrusler og foranstaltninger til at imødegå disse trusler, f.eks. kryptering (artikel 17 og betragtning 37). Bestemmelsens overskrift er imidlertid: "Oplysning om konstaterede sikkerhedstrusler". Det forhold, at der i overskriften tales om konstaterede trusler, viser, at denne bestemmelse kun vedrører (potentielle) brud på sikkerheden, mens bestemmelsens og betragtningens ordlyd nærmere peger mod mere generel uddannelse af slutbrugere. Hvis en tjenesteleverandør f.eks. konstaterer, at en brugers apparat er inficeret med malware og er blevet en del af et botnet, er leverandøren i henhold til denne bestemmelse øjensynligt forpligtet til at oplyse brugeren om de deraf følgende trusler. Anvendelsesområdet for denne bestemmelse kan imidlertid præciseres og bør ikke være begrænset til dette specifikke scenario. Bestemmelsen bør i det mindste dække konstaterede sikkerhedstrusler i alt udstyr, som leveres til slutbrugeren af leverandøren som en del af abonnementet, f.eks. routere og mobilapparater, og omfatte oplysning om de risici, der er forbundet med ændring af privatlivsindstillinger, der er foretaget i overensstemmelse med princippet om databeskyttelse gennem design.

Artikel 29-Gruppen anbefaler, at anvendelsesområdet udvides til at omfatte softwareleverandører, som tillader elektroniske kommunikationstjenester (se betragtning 8), og muligvis også til en ny kategori: leverandører af teknologi, som er nødvendig for at sikre kommunikation, som ikke er leverandører af tjenester (f.eks. leverandører af krypteringsteknologi). I tilfælde af sidstnævnte udvidelse bør det

omhyggeligt sikres, at denne forpligtelse ikke overlapper forpligtelserne til underretning om sikkerhedsbrister i andre retsakter, f.eks. NIS-direktivet<sup>21</sup> og andre retsakter vedrørende certifikatleverandører. Da sidstnævnte kategori af teknologileverandører sædvanligvis ikke har direkte kontakt med slutbrugere, skal det også forklares, hvordan de kan overholde deres oplysningsforpligtelse efter denne bestemmelse.

36. Artikel 29-Gruppen glæder sig over bestemmelserne i artikel 2 og 13, som anvendes på nummerbaserede interpersonelle kommunikationstjenester. Det er imidlertid ikke umiddelbart klart, hvorfor **et lignende niveau af privatlivsbeskyttelse ikke gøres tilgængeligt for funktionelt tilsvarende OTT-opkaldstjenester.**
37. Artikel 29-Gruppen er også bekymret over **den manglende klarhed af det specifikke samtykke til omvendt søgning i fortegnelser.** I henhold til forordningsforslagets artikel 15, stk. 2, skal leverandører indhente slutbrugernes samtykke, inden de muliggør søgefunktioner vedrørende personoplysninger (se også betragtning 31). Artikel 29-Gruppen glæder sig over harmoniseringen af kravene til samtykke til optagelse i fortegnelser, men beklager den manglede detaljeringsgrad med hensyn til forskellige former for søgninger. I henhold til det nuværende e-datadirektiv kan medlemsstaterne kræve et særskilt krav om samtykke ved omvendte søgninger på grundlag af artikel 12, stk. 3. I henhold til denne artikel kan medlemsstaterne *"kræve, at abonnenter skal anmodes om supplerende samtykke til, at en offentlig fortegnelse anvendes til ethvert formål, der går ud over søgning efter adresseoplysninger om personer på grundlag af deres navn og eventuelt et minimum af andre identifikatorer"*. På grundlag af denne bestemmelse kræves der i mange medlemsstater et særskilt samtykke til omvendte søgninger, som tager hensyn til de forskellige niveauer af identifikationsmuligheder og dermed de to funktioners indgribende karakter.
38. Mere formelt **er bødernes størrelse ikke harmoniseret for alle overtrædelser af forordningen.** I henhold til den foreslåede forordning skal medlemsstaterne imidlertid fastsætte reglerne for, hvilke sanktioner der er for overtrædelse af artikel 23, stk. 4 og 6, og artikel 24 i den foreslåede forordning. Det er mere konsekvent, hvis dette også er omhandlet i selve e-databeskyttelsesforordningen.
39. Endelig **anvendes definitioner, som kan blive "bevægelige mål",** i forordningsforslaget. I forbindelse med flere centrale begreber henvises der i den foreslåede forordning til en anden retsakt, som aktuelt foreligger som et udkast: den foreslåede kodeks for elektronisk kommunikation (se f.eks. artikel 4, stk. 1, litra b)). To vigtige eksempler på dette er definitionen af "slutbruger", som aktuelt omfatter fysiske og juridiske personer, og definitionerne af "elektroniske kommunikationstjenester" og "interpersonelle kommunikationstjenester", som er anført i forordningsforslagets artikel 4, stk. 1, litra b), og som for sidstnævntes

---

<sup>21</sup> Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen, EUT L 194 af 19.7.2016, s. 1-30, webadresse: [http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_.2016.194.01.0001.01.ENG](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG).

vedkommende uddybes i artikel 4, stk. 2, til at omfatte tjenester, der specifikt er udelukket i kodeksen for elektronisk kommunikation<sup>22</sup>. Denne udtalelse er baseret på definitionerne, som de aktuelt foreligger. Den foreslåede kodeks for elektronisk kommunikation og/eller dens centrale begreber vil dog med sandsynlighed blive ændret. Dette vil også have direkte indvirkning på e-databeskyttelsesforordningen. Ideelt bør alle udtryk, der er afledt af kodeksen for elektronisk kommunikation, defineres uafhængigt i e-databeskyttelsesforordningen. Som minimum bør den foreslåede forordning ellers omfatte en præcisering, når der er tale om udtryk, hvis definitioner afviger fra definitionerne i kodeksen for elektronisk kommunikation (f.eks. førnævnte medtagelse af "ledsagende tjenester" i definitionen af "interpersonel kommunikationstjeneste"). Hvis dette ikke er muligt, foreslår Artikel 29-Gruppen, at alle parter, der er involveret i lovgivningsprocessen, sikrer, at både den foreslåede forordning og kodeksen for elektronisk kommunikation drøftes og sættes til afstemning samtidig, så interessenterne får mulighed for korrekt at vurdere de nye retsakters anvendelsesområde og konsekvenser.

## **5. FORSLAG TIL PRÆCISERING AF HENSYN TIL RETSSIKKERHEDEN**

Ud over ovennævnte punkter ønsker Artikel 29-Gruppen også at fremhæve forskellige bestemmelser i den foreslåede forordning, som med fordel kunne præciseres. Sådanne præciseringer anses for nødvendige af hensyn til retssikkerheden for alle interessenter, så der sikres en ensartet forståelse og anvendelse af e-databeskyttelsesforordningen i hele Unionen.

### *KLARERE ANVENDELSESOMRÅDE*

40. Med hensyn til forordningsforslagets anvendelsesområde foreslår Artikel 29-Gruppen følgende præciseringer:

- a. **Udtrykket "slutbruger" bør omfatte alle individuelle brugere.** I artikel 2, stk. 14, i kodeksen for elektronisk kommunikation defineres "slutbruger" som en bruger, der ikke udbyder offentlige kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester. Det bør præciseres, at personer, der bidrager til netværk – f.eks. til mesh-net med deres wi-fi-router – ikke er udelukket fra beskyttelse inden for rammerne af den foreslåede forordning.
- b. **Det bør præciseres, at det territoriale anvendelsesområde omfatter alle slutbrugere i Unionen.** I henhold til artikel 3, stk. 1, litra a), finder den foreslåede forordning anvendelse på levering af elektroniske

---

<sup>22</sup> I forordningsforslagets artikel 4, stk. 2, anføres det eksempelvis, at en interpersonel kommunikationstjeneste omfatter "tjenester, der muliggør interpersonel og interaktiv kommunikation som en mindre ledsagende funktion, der er uløseligt forbundet med en anden tjeneste", mens sådanne tjenester specifikt er udelukket fra denne definition i artikel 2, stk. 5, i kodeksen for elektronisk kommunikation. (I artikel 2, stk. 4, i kodeksen for elektronisk kommunikation er "interpersonelle kommunikationstjenester" medtaget i den bredere kategori "elektronisk kommunikationstjenester").

kommunikationstjenester til slutbrugere "i Unionen", mens den i henhold til artikel 3, stk. 1, litra c), finder anvendelse på beskyttelse af oplysninger vedrørende terminaludstyr tilhørende slutbrugere, "der befinder sig i Unionen" (fremhævelse tilføjet). Dette varierer i de forskellige oversættelser. Den tyske oversættelse indeholder ikke denne sondring, men det f.eks. den franske, spanske og nederlandske oversættelse. Det fremgår klart af betragtning 9, at det territoriale anvendelsesområde skal være bredt, uanset om tjenesterne leveres fra steder uden for Unionen, eller om behandlingen finder sted i Unionen. Det foreslås derfor, at udtrykket "der befinder sig" slettes i artikel 3, stk. 1, litra c), for at understrege dette brede anvendelsesområde.

- c. **Den foreslåede forordning beskytter øjensynligt kun fortrolige kommunikationsmeddelelser i transit, ikke når de er lagret.** På nuværende tidspunkt fokuseres der i den foreslåede forordning på beskyttelsen af overføringen af kommunikationsmeddelelser. Se f.eks. betragtning 15, hvor det anføres, at forbuddet mod at opfange kommunikationsdata bør finde anvendelse under overføringen af disse, dvs. indtil den modtager, som den elektroniske kommunikation er rettet til, har modtaget den. Omfanget af denne beskyttelse er baseret på en begrebsmæssig kommunikationsramme, som er forældet. De fleste kommunikationsdata er stadig lagret hos tjenesteleverandører, også efter deres modtagelse. Det bør sikres, at disse datas fortrolighed stadig er beskyttet. Kommunikation mellem de samme cloudbaserede tjenesters abonnenter (f.eks. webmail-leverandører) medfører ofte kun meget begrænsede overføringer: Afsendelsen af en e-mail betyder oftest, at den spejles i leverandørens database, snarere end, at der rent faktisk sendes en meddelelse mellem to parter. Argumentet om, at dette allerede er omhandlet i den generelle forordning om databeskyttelse, er ikke overbevisende: Hele formålet med den foreslåede forordning er at beskytte alle former for fortrolig kommunikation, uanset de tekniske midler, der benyttes til sådan kommunikation. Der er muligvis kun tale om en skrivefejl, da forbuddet i artikel 5 vedrører "lagring" og behandling".
- d. **Alle offentlige trådløse internethotspots bør være omfattet af anvendelsesområdet.** Da det er almindeligt at anvende trådløse hotspots, er det kun logisk, at der ikke må være tvivl med hensyn til, om fortroligheden af kommunikationsmeddelelser, der overføres via sådanne hotspots, er beskyttet. Forsøget i forordningen på at afklare dette er imidlertid mislykket, da anvendelsesområdet kun omfatter kommunikationsnet, der tilbydes til en "udefineret gruppe af slutbrugere" (betragtning 13). Udtrykkene "udefineret gruppe af slutbrugere" og "lukkede grupper af slutbrugere" bør defineres. Det bør navnlig præciseres, at sikre trådløse net (dvs. med en adgangskode) også er omfattet af anvendelsesområdet, hvis denne adgangskode gives til en teoretisk åben gruppe af brugere, hvis identitet ikke kan fastsættes på forhånd (f.eks. kunder i en cafe eller rejsende i en lufthavn). Det princip, der ligger til grund for dette, er i overensstemmelse med Artikel 29-Gruppens tidligere udtalelse om revisionen af e-datadirektivet, at "*kun tjenester, der ydes i en officiel eller ansættelsesmæssig situation alene til arbejdsrelaterede eller officielle formål, eller tekniske kommunikationsmeddelelser mellem*

*ikkeoffentlige organer eller offentlige organer alene med henblik på at kontrollere arbejds- eller forretningsformål samt anvendelsen af tjenester alene til hjemlige formål, kan fritages for e-databeskyttelsesretsakten."* (s. 8).

- e. **Data indsamlet i forbindelse med udbud af digitale spredningstjenester bør være omfattet af den foreslåede forordning.** I medfør af den følsomme karakter af seernes adfærd, da den åbenbarer deres personlige interesser og karakteristika, bør det i e-databeskyttelsesforordningen (eventuelt i en betragtning) anføres, at udelukkelsen af tjenester, der leverer "indhold overført ved brug af elektroniske kommunikationsnet" fra definitionen af "elektronisk kommunikationstjeneste", ikke betyder, at tjenesteleverandører, der tilbyder både elektroniske kommunikationstjenester og indholdstjenester, ikke er omfattet af anvendelsesområdet for e-databeskyttelsesforordningens bestemmelser, der er målrettet mod leverandører af elektroniske kommunikationstjenester. Dette er især relevant, da leveringen af tjenester, som leverer "indhold overført ved brug af elektroniske kommunikationsnet", er udelukket fra definitionen af "elektronisk kommunikationstjeneste" i den foreslåede kodeks for elektronisk kommunikation (artikel 2, stk. 4).
- f. **Kommunikationsdata er generelt personoplysninger.** Det bemærkes i betragtning 4, at kommunikationsdata kan omfatte personoplysninger. De fleste kommunikationsdata er imidlertid personoplysninger<sup>23</sup>, og for en stor dels vedkommende er der tale om oplysninger af en intim og følsom karakter. Dette bør derfor ændres, så det angives, at disse generelt er personoplysninger.
- g. **Fortrolig kommunikation omfatter beskeder på en platform.** I betragtning 1 forklares det, at fortrolighedsprincippet omfatter alle "nuværende og fremtidige kommunikationsmidler". Denne betragtning fortsætter derefter med en liste over eksempler på sådanne midler, herunder "private beskeder sendt gennem sociale medier". Dette har sandsynligvis til formål at medtage private beskeder mellem brugere af et socialt netværk (f.eks. Facebook eller Twitter) eller opslag på en tidslinje, som er tilgængelige for en lukket gruppe personer, men ordlyden er ikke tilstrækkeligt klar.
- h. **Anvendelsen af e-databeskyttelsesforordningen på interaktion mellem maskiner.** Som nævnt i afsnit 9 glæder Artikel 29-Gruppen sig over udvidelsen af beskyttelsen til at omfatte interaktion mellem maskiner. Dette nævnes imidlertid kun i betragtning 12 og ikke i en tilsvarende artikel. Denne beskyttelse er ønskelig, da sådan kommunikation ofte indeholder oplysninger, der er omfattet af retten til privatlivets fred. En snæver kategori af kommunikation udelukkende mellem maskiner bør være fritaget, hvis den ikke har indvirkning på privatlivet eller kommunikationsmeddelelsers fortrolighed, f.eks. de tilfælde, hvor sådan kommunikation gennemføres i forbindelse med udførelsen af en transmissionsprotokol mellem

---

<sup>23</sup> Se f.eks. Domstolens dom af 6.11.2003, C-101/01, præmis 24 (med hensyn til et telefonnummer), Domstolens dom af 19.10.2016, C-582/14 (Breyer), præmis 49 (med hensyn til dynamiske IP-adresser) og Domstolens dom af 8.4.2014, C-239/12 og C-594/12 (Digital Rights Ireland), præmis 26-27 (med hensyn til følsomheden af metadata).

netværkselementer (f.eks. servere eller switches), som meddeler aktuel aktivitetsstatus til hinanden.

Et særligt område, hvor e-databeskyttelsesforordningens anvendelse bør afklares, er området for intelligente transportsystemer. Det forventes, at køretøjer løbende vil overføre data, som indeholder en unik identifikator, via radio. Uden e-databeskyttelsesforordningens yderligere beskyttelse vedrørende kommunikationsdata kan dette føre til løbende sporing af føreres kørevaner, rejsemål og hastighed. Artikel 2, stk. 1, i den europæiske kodeks for elektronisk kommunikation indeholder imidlertid en ny og udvidet definition af kommunikationsnet. De omfatter transmissionssystemer, der ikke har en centraliseret forvaltningskapacitet, og som gør det muligt at overføre signaler via radio. I betragtning 14 til e-databeskyttelsesforordningen anføres det, at sådanne data er elektroniske kommunikationsdata. På grundlag af forordningsforslagets artikel 5 er enhver form for opfangning, overvågning eller lagring af sådanne kommunikationsdata forbudt, medmindre en af disse undtagelser finder anvendelse. Der er imidlertid interesse for at behandle sådanne data, som vil sætte genstande, f.eks. selvkørende biler og apparater, i stand til at advare hinanden om deres nærhed eller andre risici. Spørgsmålet er da, hvilken undtagelse der finder anvendelse i dette tilfælde. Samtykke fra slutbrugere er ikke en brugbar undtagelse, da det kan blive nødvendigt altid at være i stand til at behandle disse data. Leverandører bør derfor kunne henholde sig til en bestemt undtagelse, som sætter genstande, f.eks. selvkørende biler og apparater, i stand til at advare hinanden om deres nærhed eller andre risici.

#### *AFKLARINGER AF BEGREBET OG ANVENDELSE AF SAMTYKKE*

41. Med hensyn til begrebet og anvendelsen af samtykke i det nuværende forordningsforslag foreslår Artikel 29-Gruppen følgende præciseringer:

- a. **Sådan bør begrebet anvendes på juridiske personer.** I betragtning 3 bemærkes det, at forordningen bør sikre, at bestemmelserne i den generelle forordning om databeskyttelse også finder anvendelse på slutbrugere, som er juridiske personer. Dette omfatter ifølge betragtningen definitionen af samtykke i den generelle forordning om databeskyttelse (se også betragtning 18). Som nævnt i bemærkning 13 bifalder Artikel 29-Gruppen den udtrykkelige medtagelse af juridiske personer i forordningens anvendelsesområde. Den praktiske anvendelse heraf er imidlertid ikke klar. I den generelle forordning om databeskyttelse defineres samtykke som en "informeret" viljestilkendegivelse fra den registrerede "ved erklæring eller klar bekræftelse" (artikel 4, stk. 11, i den generelle forordning om databeskyttelse). Det skal præciseres, hvornår en juridisk person faktisk kan anses for "informeret", og hvornår der er tale om en sådan viljestilkendegivelse fra en juridisk person.
- b. I denne sammenhæng bør det bemærkes, at en arbejdsgiver under de fleste omstændigheder ikke kan give samtykke på vegne af sine medarbejdere, fordi et sådant samtykke, når en arbejdsgiver kræver et samtykke fra en medarbejder, og der i medfør af den skæve magtbalance er en reel eller



potentielt relevant risiko, hvis samtykket ikke gives, ikke er gyldigt, fordi det ikke er givet frivilligt<sup>24</sup>. Med hensyn til **virksomheder, der udleverer apparater eller udstyr til personer, indeholder den foreslåede forordning ikke en (egnet) undtagelse** til forbuddet mod indgreb. Et eksempel er, når en arbejdsgiver ønsker at opdatere en telefon udleveret af virksomheden. Et andet eksempel er, når en arbejdsgiver tilbyder medarbejderne leasingbiler eller til administrative formål lader en tredjepart indsamle lokaliseringsdata via et apparat i en bil. I begge tilfælde har arbejdsgiveren en interesse i at gribe ind i disse apparater.

Dette indgreb kan ikke anses for nødvendigt for at levere en informationssamfundstjeneste (artikel 8, stk. 1, litra c)) eller for måling af internetbesøgende (artikel 8, stk. 1, litra d)). Dette kan løses ved at indføre en ny undtagelse, som omhandler en situation, hvor i) arbejdsgiveren leverer bestemt udstyr inden for rammerne af et ansættelsesforhold, ii) medarbejderen er bruger af dette udstyr, og iii) indgrebet er strengt nødvendigt for medarbejderens brug af udstyret (som indebærer anvendelsen af proportionalitets- og nærhedsprincippet i forbindelse med indsamlingen af data). Kun hvis disse betingelser er opfyldt, bør arbejdsgiveren kunne gribe ind i slutbrugerens apparat.

- c. **Forbedrede muligheder for at annullere automatisk viderestilling af opkald.** I artikel 14 gives slutbrugerne en vigtig mulighed for at annullere automatisk viderestilling af opkald fra en tredjepart. Denne beskyttelse kan forbedres yderligere ved allerede fra starten at kræve slutbrugerens samtykke til indledningen af viderestillingen.

#### *PRÆCISERINGER VEDRØRENDE LOKALISERINGSDATA OG ANDRE METADATA*

- 42. Artikel 29-Gruppen foreslår en præcisering af følgende for så vidt angår lokaliseringsdata og andre metadata:

- a. Betydningen af **"lokaliseringsdata, der genereres i forbindelse med andet end levering af elektroniske kommunikationstjenester" i betragtning 17 bør præciseres**. Det er ikke klart, om dette vedrører data indsamlet gennem f.eks. apps, der bruger dataene fra GPS-funktionen i intelligente enheder, og/eller som genererer lokaliseringsdata baseret på WiFi-routere i nærheden, og/eller som bruger lokaliseringsdata indsamlet med navigationsudstyr i bilen, og/eller andre metoder til at generere lokaliseringsdata. Denne mangel på klarhed skaber usikkerhed om retstilstanden med hensyn til forpligtelsens anvendelsesområde. Lokaliseringsdata på en fysisk persons terminaludstyr er under alle omstændigheder personoplysninger, og behandlingen af disse data er derfor omfattet af forpligtelserne i den generelle forordning om databeskyttelse.

---

<sup>24</sup> Se udtalelse 15/2011 om definitionen af samtykke (WP 187), udtalelse 8/2001 om behandling af personoplysninger i ansættelsesforhold (WP48) og den nye udtalelse om databehandling på arbejdspladsen (vedtaget samtidig med denne udtalelse).

- b. Det bør præciseres, at **legitim behandling af lokaliseringsdata og andre metadata ikke kræver en unik identifikator**. I betragtning 17 nævnes heatmaps som et eksempel på kommerciel anvendelse af elektroniske kommunikationsmetadata hos leverandører af elektroniske kommunikationstjenester. For at oprette et grundlæggende heatmap er der imidlertid ikke behov for unikke identifikatorer. Det er tilstrækkeligt med en ren statistisk optælling. Et andet eksempel, der nævnes i betragtningen, brugen af – og presset på – infrastruktur, kan også optælles ved brug af bestemte målepunkter, f.eks. ved at opstille aggregerede statistikker om brugen af sendemaster for at få en indikation af presset på et bestemt sted på et bestemt tidspunkt, uden at det er nødvendigt at kende de tilsluttede personers identitet.

I betragtningen nævnes som et eksempel desuden visning af trafikbevægelserne i visse retninger i løbet af en bestemt periode, hvor det er nødvendigt med en identifikator, der kan forbinde personers positioner i bestemte intervaller. Med dette eksempel legitimeres den yderligere behandling af disse data til støtte for "big data"-analyse tilsyneladende i betragtningen. Den eneste betingelse i henhold til den foreslåede forordning for denne type behandling er forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse, *hvis det er sandsynligt, at en type behandling vil medføre en højere risiko for fysiske personers rettigheder og frihedsrettigheder*. Denne betingelse er utilstrækkelig. Det er også i strid med forpligtelsen i artikel 6, hvorefter denne type behandling kun må udføres med brugernes samtykke, og kun hvis dataene ikke kan gøres anonyme, dvs. uden unikke identifikatorer. Brugere kan ofte ikke afvise, at leverandører af elektroniske kommunikationstjenester indsamler deres geolokaliseringsdata, når en sådan indsamling er teknisk nødvendig for at overføre kommunikationen til brugeren, eller når sådan behandling er nødvendig for at levere den bestilte tjeneste (f.eks. navigation). I tidligere udtalelser har Artikel 29-Gruppen konkluderet, at sådanne lokaliseringsdata fra intelligente enheder er følsomme personoplysninger, og at fordelene ved at analysere disse data ikke har forrang for brugernes rettigheder til beskyttelse af deres kommunikationsmetadata, og at de heller ikke har forrang for deres generelle ret til databeskyttelse i henhold til den generelle forordning om databeskyttelse. Det skal derfor i det mindste i betragtningen anføres, at leverandører skal overholde de forpligtelser, der følger af artikel 25 i den generelle forordning om databeskyttelse, når de foretager yderligere behandling af lokaliseringsdata eller andre metadata. Dette betyder, at i det mindst følgende foranstaltninger skal træffes:

- i) brugen af midlertidige pseudonymer
- ii) sletning af en eventuel omvendt opslagstabel mellem disse pseudonymer og de oprindelige identifikatorer
- iii) aggregering til et niveau, hvor individuelle brugere ikke længere kan identificeres ved deres bestemte rejseruter
- iv) sletning af yderpunkter, hvor identifikation stadig er mulig (alle disse foranstaltninger skal anvendes samlet).

Endelig skal e-databeskyttelsesforordningen forpligte parter, der er involveret i behandlingen af lokaliseringsdata og andre metadata, til at offentliggøre deres metoder til anonymisering og yderligere aggregering, uden at det berører den fortrolighed, der er garanteret ved lov. Dette vil sætte både tilsynsmyndighederne og offentligheden generelt i stand til nemt at kontrollere, om den valgte metode er tilstrækkelig.

#### *PRÆCISERINGER VEDRØRENDE UANMODET KOMMUNIKATION*

43. Artikel 29-Gruppen foreslår en præcisering af følgende for så vidt angår uanmodet kommunikation:

- a. **Ordlyden af forbuddet mod direkte markedsføring uden samtykke.** I forordningsforslagets artikel 16, stk. 1, anføres det nu, at elektroniske kommunikationstjenester "kan" bruges til at sende direkte markedsføringsmeddelelser til slutbrugere (med samtykke), men der er ikke anført et udtrykkeligt forbud mod at sende (dirigere eller vise) direkte markedsføring uden samtykke. Dette er i strid med tilgangen i de øvrige bestemmelser, hvor der først formuleres et forbud, som derefter følges op af visse specifikke undtagelser. Den nuværende ordlyd foreslår en lempeligere tilgang (som formodentlig ikke er tilsigtet). Artikel 29-Gruppen foreslår en mindre ændring af ordlyden af den nuværende bestemmelse i e-datadirektivets artikel 13, stk. 1: "Fysiske eller juridiske personers anvendelse af elektroniske kommunikationstjenester, herunder opkald, automatiske opkalds- og kommunikationssystemer, herunder halvautomatiske systemer, der forbinder opkaldsmottagere med en person, fax, e-mail eller andre former for elektroniske kommunikationstjenester med henblik på direkte markedsføring til slutbrugere kan kun tillades over for slutbrugere, som forudgående har givet deres samtykke hertil."
- b. **Anvendelsesområdet for bestemmelser om markedsføringsmeddelelser og opkald til eksisterende kontakter.** Hvis en person indhenter elektroniske kontaktoplysninger til e-mail fra en eksisterende kunde, må den pågældende i henhold til artikel 16, stk. 2, anvende disse oplysninger til direkte markedsføring af sine egne produkter eller tjenester, hvis kunderne klart og utvetydigt får mulighed for let og gebyrfrit at afvise en sådan anvendelse i hver meddelelse. Dette gælder i øjeblikket kun kommercielle kontaktoplysninger, der er indhentet "i forbindelse med salget af et produkt eller en tjeneste" og til yderligere kommerciel markedsføring af egne lignende produkter eller tjenester. Eftersom bestemmelserne om direkte markedsføring også gælder for ikkekommercielle markedsføringsaktiviteter (f.eks. velgørende organisationers eller politiske partiers aktiviteter), bør denne bestemmelse ændres, så den gælder tilsvarende for ikkekommercielle organisationers kontakter til tidligere støtter, når de promoverer deres egne lignende mål eller idealer, og den samme ret til afvisning bør gælde for direkte markedsføringsopkald. Der bør desuden fastsættes en tidsfrist for gyldigheden af "eksisterende kundekontakter" i elektroniske kommunikationsmeddelelser i kommercielt, velgørende eller politisk øjemed,

og denne tidsfrist bør også gælde for direkte markedsføringsopkald. Hvis medlemsstater har fastsat, at slutbrugere kan frabede sig markedsføringsopkald, tilsidesætter en "eksisterende kunderelation" registreringen i et register over personer, der ikke ønsker markedsføringsopkald. Under disse omstændigheder har slutbrugere ingen effektiv mulighed for at blokere generende opkald fra virksomheder eller organisationer, som de engang har haft kontakt med, men ikke længere ønsker at være i berøring med. Der bør derfor som udgangspunkt i forordningen fastlægges en gyldighedsperiode for denne undtagelse vedrørende "eksisterende kunder", f.eks. et eller to år, i forhold til de berørte slutbrugeres legitime forventninger.

- c. **Anvendelsen af reglerne om direkte markedsføring på juridiske personer.** I henhold til forordningsforslagets artikel 16, stk. 5, skal medlemsstaterne sikre, at de legitime interesser for slutbrugere, som er juridiske personer, for så vidt angår uanmodet kommunikation, nyder tilstrækkelig beskyttelse. Det nuværende e-datadirektivs artikel 13, stk. 5, omhandler de legitime interesser for abonnenter, der ikke er fysiske personer. Betydningen af denne ændring af ordlyden er uklar. Det bør præciseres i betragtningerne, at denne ændring ikke afspejler en hensigt om at sænke beskyttelsesniveauet. I denne forbindelse vedrører forbuddet mod direkte markedsføring uden samtykke "slutbrugere, som er fysiske personer og har givet samtykke hertil" (fremhævelse tilføjet). Det bør præciseres, at dette omfatter fysiske personer, *der arbejder for* juridiske personer. Samtykke bør på den anden side ikke kræves for at henvende sig til juridiske personer gennem generiske kontaktoplysninger, som de har offentliggjort til dette formål (f.eks. "info@virksomhedsnavn.eu").
- d. **Anvendelsen af bestemmelser om direkte markedsføring på personer, der handler som (politiske) repræsentanter:** Artikel 16 kan med den nuværende formulering være til hinder for visse meddelelser, der sendes til valgte repræsentanter, og som vedrører kommercielle anliggender eller interesser. Det bør præciseres, at forordningen ikke er til hinder for sådanne meddelelser.

#### *PRÆCISERINGER VEDRØRENDE ANVENDELSEN AF RETSAKTER TIL BESKYTTELSE AF GRUNDLÆGGENDE RETTIGHEDER*

- 44. **Anvendelsen af chartret og den europæiske menneskerettighedskonvention på national lovgivning om dataopbevaring** bør præciseres. I betragtning 26 anføres det, at foranstaltninger, som medlemsstaterne træffer for at sikre offentlige interesser, f.eks. lovlig opfangning af kommunikation, skal være i overensstemmelse med chartret (og den europæiske menneskerettighedskonvention). Dette er ønskeligt, da det følger af Domstolens ræsonnement i Tele2/Watson-dommen, at nationale undtagelser til EU-retten om databeskyttelse er underlagt chartret (og derfor kan overtrædelser gennem national lov indbringes for EU-Domstolen). I forordningsforslagets artikel 11 bemærkes det imidlertid kun, at begrænsninger af anvendelsesområdet for forordningsforslagets artikel 5-8 skal respektere kernen i de

grundlæggende rettigheder og frihedsrettigheder og skal være en nødvendig og forholdsmæssig foranstaltning. Der bør her medtages en udtrykkelig henvisning til chartret og den europæiske menneskerettighedskonvention.

45. **Kommunikationsmeddelelsers fortrolighed er også beskyttet i henhold til artikel 8 i den europæiske menneskerettighedskonvention.** I begrundelsens afsnit 1.1 og i betragtning 1 forklares det, at den foreslåede forordning gennemfører chartrets artikel 7. Dette gentages i betragtning 19. Den grundlæggende ret til fortrolig kommunikation er imidlertid ikke kun beskyttet ved denne bestemmelse, men også i henhold til artikel 8 i den europæiske menneskerettighedskonvention. Medtagelsen af en udtrykkelig henvisning i en artikel i den foreslåede forordning vil yderligere bekræfte, at Den Europæiske Menneskerettighedsdomstols relevante praksis også skal tages i betragtning ved vurderingen af den endelige forordning. Denne henvisning findes således allerede i betragtning 20 (vedrørende terminaludstyr) og betragtning 26 (vedrørende lovlig opfangning) og understøttes yderligere af bemærkningerne i begrundelsens afsnit 2.1 (vedrørende forholdet mellem chartret og den europæiske menneskerettighedskonvention for så vidt angår juridiske personer), men ikke i nogen af de relevante artikler så som artikel 11, stk. 1.

#### ANDRE PRÆCISERINGER

46. Det bør præciseres, at **forpligtelserne i henhold til den generelle forordning om databeskyttelse, f.eks. med hensyn til brud på persondatasikkerheden og konsekvensanalyser vedrørende databeskyttelse, stadig er gældende**, når parter behandler personoplysninger i forbindelse med elektroniske kommunikationsdata. I forordningsforslagets betragtning 5 anføres det, at den foreslåede forordning udgør særlovgivning i forhold til den generelle forordning om databeskyttelse, og at behandling af elektroniske kommunikationsdata kun bør være tilladt i overensstemmelse med den foreslåede forordning, og det er derfor relevant at spørge, om visse forpligtelser i henhold til den generelle forordning om databeskyttelse også finder anvendelse inden for rammerne af den foreslåede forordning. Dette gælder navnlig i de tilfælde, hvor den foreslåede forordning kan fortolkes til at omfatte en bestemt forpligtelse, som også er omhandlet i den generelle forordning om databeskyttelse. Vejledende eksempler omfatter:
- (i) I henhold til den foreslåede forordning skal "konstaterede" sikkerhedstrusler (artikel 17) meddeles (se også bemærkning 35), mens den generelle forordning om databeskyttelse omhandler et system til anmeldelse af brud på persondatasikkerheden (artikel 33 og 34).
  - (ii) I den foreslåede forordning nævnes det, at gennemførelsen af en konsekvensanalyse vedrørende databeskyttelse og høring af tilsynsmyndigheden i overensstemmelse med den generelle forordning om databeskyttelse er påkrævet under visse omstændigheder (betragtning 17 og 19 samt artikel 6, stk. 3, litra b)). I den generelle forordning om databeskyttelse fastlægges det allerede, hvornår en konsekvensanalyse vedrørende databeskyttelse skal gennemføres, og hvornår høring er påkrævet (artikel 35 og 36).

- (iii) Det anføres ikke udtrykkeligt, at en person, der overholder de nødvendige betingelser for en undtagelse til forbuddet mod behandling i forordningsforslagets artikel 5, stadig skal overholde alle relevante forpligtelser i henhold til den generelle forordning om databeskyttelse, når der er tale om behandling af personoplysninger og anden behandling, som er forbudt i henhold til den generelle forordning om databeskyttelse. Det bør præciseres, at forenelighedstesten i artikel 6, stk. 4, i den generelle forordning om databeskyttelse derfor ikke finder anvendelse.
- (iv) Forordningsforslaget indeholder ikke certificeringsmekanismer svarende til artikel 42 og 43 i den generelle forordning om databeskyttelse. Da anvendelsesområdet for artikel 42 i den generelle forordning om databeskyttelse strengt taget er begrænset til fastlæggelse af certificeringsmekanismer for databeskyttelse samt databeskyttelsesmærkninger og -mærker med henblik på at påvise overensstemmelse med den generelle forordning om databeskyttelse, bør det overvejes, om en tilsvarende bestemmelse ikke bør indføres med henblik på at tillade certificering af behandlingsaktiviteter, standarder, produkter eller tjenester for deres overholdelse af e-databeskyttelsesforordningen.

Med henblik på at sikre, at denne mangel på klarhed ikke bruges som argument for at sænke beskyttelsesniveauet i den foreslåede forordning, bør det præciseres, at dataansvarlige i alle disse tilfælde også skal overholde den generelle forordning om databeskyttelse.

- 47. Det bør desuden præciseres, at **kravet vedrørende tilbagetrækning af samtykke også finder anvendelse i forbindelse med indgreb i terminaludstyr.** Forordningsforslagets artikel 8, stk. 1, litra b), omhandler muligheden for at gribe ind i slutbrugernes terminaludstyr med samtykke. I henhold til artikel 9, stk. 3, skal slutbrugere have mulighed for til enhver tid at trække deres samtykke tilbage, men dette gælder kun for samtykke til analyse af metadata og indhold. Det bør præciseres, at denne forpligtelse også gælder for indgreb i terminaludstyr.
- 48. I denne forbindelse bør det præciseres, at **påmindelsen om muligheden for tilbagetrækning af samtykke også gælder for samtykke givet gennem browserindstillinger.** I henhold til artikel 9, stk. 3, skal slutbrugere hver sjette måned mindes om muligheden for til enhver tid at trække deres samtykke tilbage. Mens Artikel 29-Gruppen mener, at generelle indstillinger i browsere og anden software, herunder operativsystemer, apps og softwaregrænseflader til internet og things-tilsluttede apparater (dvs. ikke på grundlag af specifikke indstillinger), ikke kan være en gyldig foranstaltning til at give samtykke, da generelle indstillinger ikke er egnede til at give specifikt samtykke til specifikke scenarier (se bemærkning 24), bør standardindstillinger være brugervenlige (se bemærkning 19). Hvis dette forbliver i den foreslåede forordning, skal indstillingerne være tilstrækkeligt detaljerede til at kontrollere alle databehandlingsaktiviteter, som brugeren giver sit samtykke til, og dække alle funktioner i udstyret, der kan føre til databehandling. Slutbrugeren bør desuden med regelmæssige intervaller (hver sjette måned) mindes om muligheden for at ændre disse indstillinger.

49. Det er glædeligt, at software på markedet i henhold til den foreslåede forordning skal oplyse slutbrugeren om mulighederne i privatlivsindstillingerne (artikel 10). **Det er imidlertid ikke klart, hvordan dette reelt kan finde anvendelse på ældre produkter** og produkter, som ikke længere understøttes. Det bør endvidere præciseres, hvordan denne forpligtelse vil finde anvendelse på open source-software, som udvikles på en åben og decentral måde.
50. Det bør præciseres, at **muligheden for at blokere (tredjeparts)cookies i forordningsforslagets artikel 10 har forrang for undtagelsen vedrørende måling af internetbesøgende** omhandlet i artikel 8, stk. 1, litra d). Det betyder med andre ord følgende: Selv om et websted må anvende analyser til at foretage måling af internetbesøgende i henhold til artikel 8, stk. 1, litra d), bør brugere stadig have ret til at blokere disse sporingsteknologier i deres browser.
51. **Definitionen af (halv)automatiserede opkalds- og kommunikationssystemer bør præciseres.** I definition af dette udtryk i forordningsforslagets artikel 4, stk. 3, litra h), henvises der til udtrykket selv i anden halvdel af punktummet ("herunder opkald foretaget ved hjælp af automatiserede opkalds- og kommunikationssystemer, som sætter den opkaldte person i forbindelse med et menneske"). Det foreslås, at dette sidste punktum slettes fra definitionen, og at definitionen i artikel 4, stk. 3, litra g), ændres til at omfatte opkald foretaget ved hjælp af halvautomatiserede kommunikationssystemer, f.eks. automatiske opkaldssystemer, som sætter den opkaldte person i forbindelse med et menneske.
52. Udtrykket **"oplysninger, som er en del af abonnementet på en tjeneste" bør forklares.** I betragtning 14 nævnes det, at elektroniske kommunikationsmetadata kan omfatte "oplysninger, som er en del af abonnementet på en tjeneste, hvis disse oplysninger behandles med henblik på at videresende, distribuere eller muliggøre udveksling af elektronisk kommunikationsindhold". Det er uklart, hvad der menes med dette.
53. **Anvendelsen af sammenhængs- og samarbejdsmekanismerne** bør præciseres. I betragtning 38 bemærkes det, at den foreslåede forordning tager udgangspunkt i sammenhængsmekanismen i den generelle forordning om databeskyttelse. I artikel 18, stk. 1, bestemmes det, at kapitel VI og VII i den generelle forordning om databeskyttelse finder tilsvarende anvendelse. I artikel 19 bemærkes det videre, at Det Europæiske Databeskyttelsesråd skal udføre de opgaver, der er fastsat i artikel 70 i den generelle forordning om databeskyttelse. Selv om anvendelsen af disse bestemmelser er relativt klar, kan det ikke udelukkes, at der vil opstå spørgsmål om fortolkningen af de centrale begreber, der er knyttet til sammenhængs- og samarbejdsmekanismerne omhandlet i den generelle forordning om databeskyttelse. Mekanismen for den ledende tilsynsmyndighed finder f.eks. anvendelse i de tilfælde, hvor der er tale om "grænseoverskridende behandling" (artikel 56, stk. 1, den generelle forordning om databeskyttelse): Det er usikkert, hvordan den finder anvendelse, når der er tale om indgreb i terminaludstyr eller analyse af indhold eller metadata, i henhold til den foreslåede forordning. Anvendelsen af disse centrale begreber bør derfor præciseres i en betragtning, og det bør understreges, at eventuelle tilbageværende spørgsmål vedrørende anvendelsen af disse kapitler i den generelle

forordning om databeskyttelse inden for rammerne af den foreslåede forordning vil blive afgjort ved at fortolke bestemmelserne i disse kapitler i overensstemmelse med deres hensigt. Det bør endvidere præciseres, at artikel 70 finder tilsvarende anvendelse på Det Europæiske Databeskyttelsesråd i forbindelse med den foreslåede forordning (dette mangler nu i betragtningen).

\* \* \*