

Databeskyttelsesrådets udtalelser (artikel 64)



Udtalelse nr. 5/2019 om samspillet mellem e-databeskyttelsesdirektivet og GDPR, navnlig med hensyn til databeskyttelsesmyndighedernes kompetence, opgaver og beføjelser

Vedtaget den 12. marts 2019

Translations proofread by EDPB Members.
This language version has not yet been proofread.

INDHOLDSFORTEGNELSE

1	Kort fremstilling af de faktiske omstændigheder	4
2	De retlige rammer	5
2.1	Relevante bestemmelser i GDPR	5
2.2	Relevante bestemmelser i rammedirektivet	6
2.3	Relevante bestemmelser i e-databeskyttelsesdirektivet.....	6
3	Udtalelsens anvendelsesområde	8
3.1	Spørgsmål, som falder uden for anvendelsesområdet for GDPR.....	9
3.2	Spørgsmål, som falder uden for anvendelsesområdet for e-databeskyttelsesdirektivet	9
3.2.1	E-databeskyttelsesdirektivets generelle materielle anvendelsesområde	9
3.2.2	Det udvidede materielle anvendelsesområde for e-databeskyttelsesdirektivets artikel 5, stk. 3, og 13	11
3.3	Spørgsmål inden for det materielle anvendelsesområde for både e-databeskyttelsesdirektivet og GDPR.....	11
4	Samspil mellem e-databeskyttelsesdirektivet og GDPR	14
4.1	"At specificere"	14
4.2	"At supplere"	15
4.3	Betydningen af artikel 95 i GDPR	15
4.4	Sameksistens	16
5	Om databeskyttelsesmyndighedernes kompetence, opgaver og beføjelser	17
5.1	Håndhævelse af GDPR	19
5.2	Håndhævelse af e-databeskyttelsesdirektivet.....	20
5.3	Håndhævelse, hvor GDPR og e-databeskyttelsesdirektivet krydser hinanden	21
5.3.1	Spørgsmål 1: Er visse databehandlingsaktiviteter "forbudt område" for databeskyttelsesmyndighederne?	21
5.3.2	Spørgsmål to: Er de nationale e-databeskyttelsesbestemmelser "forbudt område"? ..	23
6	Om anvendelsen af samarbejds- og sammenhængsmekanismerne	25
7	Konklusion	26

Det Europæiske Databeskyttelsesråd har —

under henvisning til artikel 63 og artikel 64, stk. 2, i 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 ("GDPR"),

under henvisning til EØS-aftalen, særlig bilag XI og protokol 37 som ændret ved afgørelse nr. 154/2018 truffet af Det Blandede EØS-Udvalg den 6. juli 2018,

under henvisning til artikel 10 og artikel 22 i sin forretningsorden af 25. maj 2018 som ændret den 23. november 2018,

og ud fra følgende betragtninger:

(1) Det Europæiske Databeskyttelsesråds ("Databeskyttelsesrådets") vigtigste rolle er at sikre en ensartet anvendelse af forordning (EU) 2016/679 ("GDPR") i hele Det Europæiske Økonomiske Samarbejdsområde. I artikel 64, stk. 2, i GDPR hedder det, at en tilsynsmyndighed, formanden for Databeskyttelsesrådet eller Kommissionen kan kræve, at ethvert almenyldigt spørgsmål eller ethvert spørgsmål, der har virkninger i mere end én medlemsstat, drøftes af Databeskyttelsesrådet med henblik på en udtalelse. Formålet med denne udtalelse er at undersøge et almenyldigt spørgsmål, der har virkninger i mere end én medlemsstat.

(2) Den 3. december 2018 anmodede den belgiske databeskyttelsesmyndighed Databeskyttelsesrådet om at undersøge og afgive en udtalelse om samspillet mellem GDPR og e-databeskyttelsesdirektivet, navnlig med hensyn til databeskyttelsesmyndighedernes kompetence, opgaver og beføjelser.

(3) Databeskyttelsesrådets udtalelse vedtages i henhold til artikel 64, stk. 3, i GDPR, sammenholdt med artikel 10, stk. 2, i Databeskyttelsesrådets forretningsorden senest otte uger fra den første arbejdsdag efter, at formanden og den kompetente tilsynsmyndighed har besluttet, at sagen er fuldstændig. Efter formandens beslutning kan denne frist forlænges med yderligere seks uger under hensyntagen til sagens kompleksitet —

VEDTAGET FØLGENDE UDTALELSE:

1 KORT FREMSTILLING AF DE FAKTISKE OMSTÆNDIGHEDER

1. Den 3. december 2018 anmodede den belgiske databeskyttelsesmyndighed Databeskyttelsesrådet om at undersøge og afgive en udtalelse om samspillet mellem e-databeskyttelsesdirektivet¹ og GDPR og stillede følgende spørgsmål:
 - a. Hvad angår databeskyttelsesmyndighedernes **kompetence, opgaver og beføjelser**², hvorvidt
 - i. databeskyttelsesmyndighederne er i stand til eller ikke i stand til at udøve deres kompetence, opgaver og beføjelser i forbindelse med behandling, som i hvert fald med hensyn til visse behandlingsaktiviteter er omfattet af det materielle anvendelsesområde for både GDPR og e-databeskyttelsesdirektivet, og i så fald, hvorvidt
 - ii. databeskyttelsesmyndighederne kan eller bør tage hensyn til bestemmelserne i e-databeskyttelsesdirektivet og/eller de nationale love til gennemførelse deraf, når de udøver deres kompetence, opgaver og beføjelser i henhold til GDPR (f.eks. ved vurderingen af lovligheden af behandlingen), og i så fald, i hvilket omfang.
 - b. Hvorvidt **samarbejds- og sammenhængsmekanismerne** kan eller bør anvendes i forbindelse med behandling, som i hvert fald med hensyn til visse behandlingsaktiviteter er omfattet af det materielle anvendelsesområde for både GDPR og e-databeskyttelsesdirektivet.
 - c. I hvilket omfang behandlingen **kan være omfattet af bestemmelserne i både** e-databeskyttelsesdirektivet og GDPR, og hvorvidt dette påvirker svarene på spørgsmål 1 og 2.
2. Databeskyttelsesrådet mener, at disse spørgsmål vedrører et almengyldigt spørgsmål om GDPR, idet der er et klart behov for en konsekvent fortolkning blandt databeskyttelsesmyndighederne om rækkevidden af deres kompetencer, opgaver og beføjelser. Der er især behov for præcisering for at sikre bl.a. en konsekvent ydelse af gensidig bistand i overensstemmelse med artikel 61 i GDPR og fælles aktiviteter i overensstemmelse med artikel 62 i GDPR.
3. Denne udtalelse omhandler ikke en sådan opdeling af kompetencer, opgaver og beføjelser for databeskyttelsesmyndighederne i forbindelse med forslaget til e-databeskyttelsesforordningen.

¹ 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 (Direktiv om databeskyttelse inden for elektronisk kommunikation), som ændret ved direktiv 2006/24/EF og 2009/136/EF.

² Jf. artikel 55-58 i GDPR. Begrebet "databeskyttelsesmyndigheder" (i modsætning til "tilsynsmyndigheder") bruges i denne udtalelse for at sondre klart imellem de "tilsynsmyndigheder", der er omhandlet i GDPR, og andre typer tilsynsmyndigheder, som f.eks. de nationale tilsynsmyndigheder, der er nævnt i direktiv 2002/58/EF.

2 DE RETLIGE RAMMER

2.1 Relevante bestemmelser i GDPR

4. I henhold til artikel 2, stk. 1, i GDPR, finder den "*anvendelse på behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling, og på anden ikkeautomatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register*".

I artikel 2, stk. 2, fastlægges det, at GDPR ikke gælder for behandling af personoplysninger:

"a) under udøvelse af aktiviteter, der falder uden for EU-retten

b) som foretages af medlemsstaterne, når de udfører aktiviteter, der falder inden for rammerne af afsnit V, kapitel 2, i TEU

c) som foretages af en fysisk person som led i rent personlige eller familiemæssige aktiviteter

d) som foretages af kompetente myndigheder med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod og forebygge trusler mod den offentlige sikkerhed."

5. Artikel 5 har titlen "Principper for behandling af personoplysninger" og omhandler de principper, der gælder for enhver behandling af personoplysninger, herunder kravet om, at personoplysninger skal behandles lovligt og rimeligt³. Artikel 6 beskriver, under hvilke omstændigheder behandlingen af personoplysninger er lovlige, hvoraf den ene vedrører den registreredes samtykke. Artikel 7 omhandler betingelserne for indhentning af gyldigt samtykke i henhold til GDPR⁴.
6. Artikel 51, stk. 1, fastlægger databeskyttelsesmyndighedernes retlige mandat, som er at føre tilsyn med anvendelsen af GDPR, for at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder i forbindelse med behandling og for at lette fri udveksling af personoplysninger i Unionen. Artikel 55, 57 og 58 angiver de enkelte databeskyttelsesmyndigheders kompetencer, opgaver og beføjelser. Kapitel VII i GDPR har titlen "Samarbejde og sammenhæng" og beskriver de forskellige måder, som databeskyttelsesmyndighederne skal samarbejde på for at bidrage til en ensartet anvendelse af GDPR.
7. I artikel 94, "Ophævelse af direktiv 95/46", hedder det:
- "1. Direktiv 95/46/EF ophæves med virkning fra den 25. maj 2018.*
 - 2. Henvisninger til det ophævede direktiv gælder som henvisninger til denne forordning. Henvisninger til Gruppen vedrørende Beskyttelse af Personer i forbindelse med Behandling af Personoplysninger, der er nedsat ved artikel 29 i direktiv 95/46/EF, gælder som henvisninger til Det Europæiske Databeskyttelsesråd oprettet ved denne forordning."*

³ Jf. også betragtning 39 i GDPR ("*Enhver behandling af personoplysninger bør være lovlige og rimelige. [...]*").

⁴ Jf. Artikel 29-Gruppens Retningslinjer vedrørende samtykke i henhold til forordning 2016/679, WP 259 rev. 01, godkendt af Databeskyttelsesrådet den 25. maj 2018.

8. I artikel 95, "Forhold til direktiv 2002/58/EF", fastlægges følgende:

"Denne forordning indfører ikke yderligere forpligtelser for fysiske eller juridiske personer for så vidt angår behandling i forbindelse med levering af offentligt tilgængelige elektroniske kommunikationstjenester i offentlige kommunikationsnet i Unionen for så vidt angår spørgsmål, hvor de er underlagt specifikke forpligtelser med samme formål som det, der er fastsat i direktiv 2002/58/EF."

9. I betragtning 173 i GDPR hedder det:

"(173) Denne forordning bør gælde for alle forhold vedrørende beskyttelse af grundlæggende rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger, som ikke er underlagt specifikke forpligtelser med samme formål som fastsat i Europa-Parlamentets og Rådets direktiv 2002/58/EF, herunder den dataansvarliges forpligtelser og fysiske personers rettigheder. For at afklare forholdet mellem denne forordning og direktiv 2002/58/EF bør nævnte direktiv ændres i overensstemmelse hermed. Når denne forordning er vedtaget, bør direktiv 2002/58/EF revideres, navnlig for at sikre forenelighed med denne forordning."

2.2 Relevante bestemmelser i rammedirektivet

10. I rammedirektivets⁵ artikel 2, litra g), defineres en "national tilsynsmyndighed" som

"den eller de instanser, der af en medlemsstat har fået til opgave at varetage de tilsynsopgaver, der pålægges i dette direktiv og i særdirektiverne"

11. Rammedirektivets artikel 2, litra l), indeholder følgende definition:

"særdirektiver': direktiv 2002/20/EF (tilladelsesdirektivet), direktiv 2002/19/EF (adgangsdirektivet), direktiv 2002/22/EF (forsyningspligt-direktivet) og Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktivet om databeskyttelse inden for elektronisk kommunikation)"

12. Rammedirektivets artikel 3, stk. 1, har følgende ordlyd:

"Medlemsstaterne sikrer, at alle opgaver, de nationale tilsynsmyndigheder får pålagt i dette direktiv og i særdirektiverne, varetages af et kompetent organ."

2.3 Relevante bestemmelser i e-databeskyttelsesdirektivet

13. I e-databeskyttelsesdirektivets artikel 1, stk. 2, hedder det:

"Med henblik på at nå de i stk. 1 omhandlede mål specificerer og supplerer dette direktivs bestemmelser [forordning (EU) 2016/679]. Nærværende bestemmelser beskytter desuden legitime interesser hos abonnenter, der er juridiske personer."⁶

⁵ Europa-Parlamentets og Rådets direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet).

⁶ I henhold til artikel 94, stk. 2, i GDPR er alle henvisninger til direktiv 95/46 i e-databeskyttelsesdirektivet blevet erstattet med "[forordning (EU) 2016/679]", og henvisninger til "Gruppen vedrørende Beskyttelse af Personer i forbindelse med Behandling af Personoplysninger, der er nedsat ved artikel 29 i direktiv 95/46/EF", er blevet erstattet med "[Det Europæiske Databeskyttelsesråd]".

14. E-databeskyttelsesdirektivets artikel 2, litra f), indeholder følgende definition:
- "samtykke": givet af bruger eller abonnent svarer til den registreredes samtykke i [forordning (EU) 2016/679]"*
15. I e-databeskyttelsesdirektivets artikel 15, stk. 2, hedder det:
- "Bestemmelserne i [forordning (EU) 2016/679], [kapitel VIII om retsmidler, ansvar og sanktioner], finder anvendelse på nationale bestemmelser, der vedtages til nærværende direktivs gennemførelse, og på individuelle rettigheder afledt af nærværende direktiv."*
16. I e-databeskyttelsesdirektivets artikel 15, stk. 3, hedder det:
- "[Det Europæiske Databeskyttelsesråd] varetager også de opgaver, der er fastsat i [artikel 70 i forordning (EU) 2016/679] med hensyn til de af dette direktiv omfattede forhold, dvs. beskyttelse af grundlæggende rettigheder og frihedsrettigheder samt legitime interesser i den elektroniske kommunikationssektor."*
17. Artikel 15a har titlen "Gennemførelse og håndhævelse" og fastlægger følgende:
- "1. Medlemsstaterne fastsætter bestemmelser om sanktioner, herunder strafferetlige foranstaltninger, hvis det er relevant, for overtrædelse af de nationale bestemmelser, der er vedtaget i medfør af dette direktiv, og træffer alle nødvendige foranstaltninger til at sikre gennemførelsen heraf. [...]"*
- 2. Uden at det berører en eventuel klageadgang, sikrer medlemsstaterne, at den kompetente nationale myndighed og, hvor det er relevant, andre nationale organer har beføjelse til at beordre overtrædelser som omhandlet i stk. 1 bragt til ophør."*
- 3. Medlemsstaterne sikrer, at den kompetente nationale myndighed, og, hvor det er relevant, andre nationale organer, har de nødvendige beføjelser og ressourcer til efterforskning, herunder beføjelser til at skaffe sig relevante oplysninger, som de måtte have brug for under overvågningen og håndhævelsen af nationale bestemmelser, der er vedtaget i medfør af dette direktiv."*
- 4. De relevante nationale tilsynsmyndigheder kan træffe foranstaltninger til at sikre et effektivt samarbejde hen over grænserne om at håndhæve de nationale love, der vedtages i medfør af dette direktiv, og til at tilvejebringe harmoniserede vilkår for udbuddet af tjenester, der medfører datastrømme hen over grænserne."*
- De nationale tilsynsmyndigheder skal i god tid, inden de træffer sådanne foranstaltninger, tilsende Kommissionen et sammendrag af foranstaltningerne, begrundelsen herfor og den foreslåede fremgangsmåde. Kommissionen kan efter at have undersøgt sådanne oplysninger og hørt Det Europæiske Agentur for Net- og Informationssikkerhed og [Det Europæiske Databeskyttelsesråd], fremsætte kommentarer eller henstillinger herom, navnlig med henblik på at sikre, at foranstaltningerne ikke påvirker det indre markedes funktion negativt. De nationale tilsynsmyndigheder skal tage størst muligt hensyn til Kommissionens kommentarer eller henstillinger, når de træffer afgørelse om foranstaltningerne."*
18. I betragtning 10 i e-databeskyttelsesdirektivet hedder det:
- "I den elektroniske kommunikationssektor finder [forordning (EU) 2016/679] navnlig anvendelse på alle forhold vedrørende beskyttelse af grundlæggende rettigheder og frihedsrettigheder, som ikke særligt er omfattet af bestemmelserne i dette direktiv, herunder*

den registeransvarliges forpligtelser og fysiske personers rettigheder. [Forordning (EU) 2016/679] anvendes på ikke-offentlige kommunikationstjenester."

3 UDTALELSENS ANVENDELSESOMRÅDE

19. Formålet med GDPR er at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder, navnlig deres ret til beskyttelse af personoplysninger, samt den frie udveksling af personoplysninger i Unionen⁷. For at nå dette mål fastsættes der i GDPR fælles regler for databehandling med henblik på at sikre ensartet og effektiv beskyttelse af personoplysninger i hele Unionen og hindre, at forskelle hæmmer den frie udveksling af personoplysninger på det indre marked. Reglerne tjener til at sikre en balance mellem (de potentielle) fordele og (de potentielle) ulemper ved databehandlingen.
20. E-databeskyttelsesdirektivet tager sigte på en harmonisering af nationale bestemmelser, der er nødvendig for at sikre et ensartet niveau i beskyttelsen af de grundlæggende rettigheder og frihedsrettigheder og navnlig retten til privatliv og fortrolighed i forbindelse med behandling af personoplysninger inden for den elektroniske kommunikationssektor, og for at sikre fri omsætning af sådanne oplysninger og af elektronisk kommunikationsudstyr og elektroniske kommunikationstjenester i Fællesskabet⁸. E-databeskyttelsesdirektivet har derfor til formål at sikre fuld overholdelse af rettighederne i charterets artikel 7 og 8. I denne henseende har e-databeskyttelsesdirektivet til formål at specificere og supplere bestemmelserne i GDPR med hensyn til behandling af personoplysninger i den elektroniske kommunikationssektor⁹.
21. De spørgsmål, som Databeskyttelsesrådet har modtaget, omhandler kun behandling, som er omfattet af det materielle anvendelsesområde for både GDPR og e-databeskyttelsesdirektivet. For at præcisere anvendelsesområdet for denne udtalelse nærmere beskriver følgende afsnit:
 - de tilfælde, hvor der ikke er noget samspil mellem GDPR og e-databeskyttelsesdirektivet, fordi spørgsmålet falder uden for anvendelsesområdet for GDPR
 - de tilfælde, hvor der ikke er noget samspil mellem GDPR og e-databeskyttelsesdirektivet, fordi spørgsmålet falder uden for anvendelsesområdet for e-databeskyttelsesdirektivet
 - de tilfælde, hvor der er et samspil mellem GDPR og e-databeskyttelsesdirektivet, fordi spørgsmålet falder inden for det materielle anvendelsesområde for både GDPR og e-databeskyttelsesdirektivet.

⁷ Artikel 1 i GDPR.

⁸ E-databeskyttelsesdirektivets artikel 1, stk. 1.

⁹ E-databeskyttelsesdirektivets artikel 1, stk. 1 og 2, som skal læses i lyset af artikel 94, stk. 2, i GDPR.

3.1 Spørgsmål, som falder uden for anvendelsesområdet for GDPR

22. Det materielle anvendelsesområde for GDPR omfatter i princippet enhver form for behandling af personoplysninger, uanset den anvendte teknologi¹⁰. GDPR finder ikke anvendelse, når:
- der ikke behandles nogen personoplysninger (f.eks. udgør et telefonnummer til en juridisk persons automatiske kundeservice eller IP-adressen på en digital kopimaskine i et firmanetværk ikke personoplysninger)
 - aktiviteterne falder uden for det materielle anvendelsesområde for GDPR, idet der tages hensyn til artikel 2, stk. 2 og 3, i GDPR eller
 - aktiviteterne falder uden for det territoriale anvendelsesområde for GDPR¹¹.

3.2 Spørgsmål, som falder uden for anvendelsesområdet for e-databeskyttelsesdirektivet

23. En særegenhed i e-databeskyttelsesdirektivet er, at to af bestemmelserne deri har et bredere anvendelsesområde end de andre bestemmelser, hvor anvendelsesområdet er begrænset til tilrådighedsstillelse af offentligt tilgængelige elektroniske kommunikationstjenester via offentlige kommunikationsnet. Derfor er der, som beskrevet i følgende afsnit, to spørgsmål, der skal besvares for at afgøre, hvorvidt en aktivitet falder inden eller uden for det materielle anvendelsesområde for e-databeskyttelsesdirektivet.

3.2.1 E-databeskyttelsesdirektivets generelle materielle anvendelsesområde

24. Ifølge artikel 3 i e-databeskyttelsesdirektivet finder det anvendelse "*på behandling af persondata i forbindelse med, at offentligt tilgængelige elektroniske kommunikationstjenester stilles til rådighed via offentlige kommunikationsnet i Fællesskabet, herunder offentlige kommunikationsnet med dataindsamlings- og identifikationsudstyr*".
25. E-databeskyttelsesdirektivet omhandler først og fremmest offentligt tilgængelige elektroniske kommunikationstjenester og elektroniske kommunikationsnet¹². Ifølge den europæiske kodeks for elektronisk kommunikation¹³ er tjenester, som er funktionelt ækvivalente til elektroniske kommunikationstjenester, omfattet.

¹⁰ Jf. også betragtning 46 i e-databeskyttelsesdirektivet.

¹¹ Artikel 3 i GDPR. Jf. Databeskyttelsesrådets retningslinjer 3/2018 om det geografiske anvendelsesområde for GDPR (artikel 3), 16.11.2018.

¹² Arbejdsdokument fra Kommissionens tjenestegrene, "Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC", COM SWD(2017)005, s. 20. Rapport til Kommissionen, "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation", SMART 2013/0071, s. 24 ff.

¹³ Europa-Parlamentets og Rådets direktiv (EU) 2018/1972 af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation.

26. Hvad angår det materielle anvendelsesområde, finder e-databeskyttelsesdirektivet anvendelse, når hver af følgende betingelser er opfyldt:
- der er en elektronisk kommunikationstjeneste (ECS)¹⁴
 - tjenesten tilbydes via et elektronisk kommunikationsnet¹⁵
 - tjenesten og nettet er offentligt tilgængelige¹⁶
 - tjenesten og nettet tilbydes i EU.
27. Aktiviteter, som ikke opfylder alle de ovennævnte kriterier, er generelt ikke omfattet af e-databeskyttelsesdirektivets anvendelsesområde.

Eksempler:

Et firmanetværk, som kun er tilgængeligt for de ansatte til arbejdsrelaterede formål, udgør ikke en "offentligt tilgængelig" elektronisk kommunikationstjeneste. Derfor hører transmission af lokaliseringsdata via et sådant netværk ikke under det materielle anvendelsesområde for e-databeskyttelsesdirektivet¹⁷.

En ursynkroniseringstjeneste sender et signal via et elektronisk kommunikationsnet til alle ure, der bruger synkroniseringsprotokollen (ubestemt antal modtagere). Denne tjeneste er en radio- og fjernsynstransmissionstjeneste og ikke en kommunikationstjeneste i den aktuelle kontekst og ville også falde uden for det materielle anvendelsesområde for e-databeskyttelsesdirektivet.

¹⁴ I e-databeskyttelsesdirektivets artikel 2, litra d), præciseres det, at "kommunikation" betyder, "oplysninger, som udveksles eller overføres mellem et begrænset antal parter via en offentligt tilgængelig elektronisk kommunikationstjeneste", og radio- og fjernsynstransmissionstjenester, som i teorien kan nå et ubegrænset publikum, udelukkes. Begrebet "offentligt kommunikationsnet" er i øjeblikket defineret i rammedirektivets artikel 2, litra d), men fra den 21. december 2020 vil definitionen i artikel 2, stk. 4, i kodeksen for elektronisk kommunikation være gældende.

¹⁵ "Elektronisk kommunikationsnet" er i øjeblikket defineret i rammedirektivets artikel 2, litra a), men fra den 21. december 2020 vil definitionen i artikel 2, stk. 1, i kodeksen for elektronisk kommunikation være gældende.

¹⁶ En tjeneste til offentligheden er en tjeneste, der står til rådighed for alle medlemmer af offentligheden på samme grundlag, og ikke kun offentligt ejede tjenester. Til sammenligning: EDPS, udtalelse 5/2016, "Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC)", s. 12, og Kommissionens meddelelse til Europa-Parlamentet og Rådet om status over og gennemførelse af direktiv 90/388/EØF om liberalisering af markedet for teletjenester, KOM(95) 113 endelig af 4.4.1995, s. 14.

¹⁷ Arbejdsdokument fra Kommissionens tjenestegrene, "Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC", COM SWD(2017)005, s. 21, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0005&from=EN>; Rapport til Kommissionen, "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation", SMART 2013/0071, s. 14. <https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data>.

3.2.2 Det udvidede materielle anvendelsesområde for e-databeskyttelsesdirektivets artikel 5, stk. 3, og 13

28. Det overordnede mål i e-databeskyttelsesdirektivet er at sikre beskyttelsen af de grundlæggende rettigheder og frihedsrettigheder for befolkningen, når de bruger elektroniske kommunikationsnet¹⁸. I lyset af dette mål finder e-databeskyttelsesdirektivets artikel 5, stk. 3, og artikel 13 anvendelse på udbydere af elektroniske kommunikationstjenester samt webstedsoperatører (f.eks. for cookies) eller andre virksomheder (f.eks. for direkte markedsføring)¹⁹.

Eksempler:

Søgemaskinetjenester, der lagrer eller får adgang til cookies på en brugers enhed, hører under det udvidede materielle anvendelsesområde for e-databeskyttelsesdirektivets artikel 5, stk. 3²⁰.

Uønsket elektronisk post sendt fra en webstedsoperatør med henblik på direkte markedsføring falder også inden for det udvidede materielle anvendelsesområde for e-databeskyttelsesdirektivets artikel 13²¹.

3.3 Spørgsmål inden for det materielle anvendelsesområde for både e-databeskyttelsesdirektivet og GDPR

29. Der er mange eksempler på behandlingsaktiviteter, der ligger inden for det materielle anvendelsesområde for både e-databeskyttelsesdirektivet og GDPR. Et klart eksempel herpå er brugen af cookies. I sin udtalelse om adfærdsbaseret annoncering på internettet anførte Artikel 29-Gruppen følgende:

*"Hvis de oplysninger, der indsamles, efter at oplysninger er gemt eller hentet via en cookie eller lignende anordning, kan betragtes som personoplysninger, finder direktiv 95/46/EF anvendelse i tillæg til artikel 5, stk. 3."*²²

30. Den Europæiske Unions Domstols (EU-Domstolens) retspraksis bekræfter, at det er muligt, at behandling falder inden for det materielle anvendelsesområde for både e-databeskyttelsesdirektivet og GDPR samtidig. I *Wirtschaftsakademie*²³ anvendte EU-Domstolen 95/46/EF, uanset at den

¹⁸ E-databeskyttelsesdirektivets artikel 1, stk. 1, har følgende ordlyd: "Dette direktiv tager sigte på en harmonisering af nationale bestemmelser, der er nødvendig for at sikre et ensartet niveau i beskyttelsen af de grundlæggende rettigheder og frihedsrettigheder og navnlig retten til privatliv og fortrolighed i forbindelse med behandling af personoplysninger inden for den elektroniske kommunikationssektor, og for at sikre fri omsætning af sådanne oplysninger og af elektronisk kommunikationsudstyr og elektroniske kommunikationstjenester i Fællesskabet."

¹⁹ Artikel 29-Gruppen, udtalelse nr. 2/2010 om adfærdsbaseret annoncering på internettet, 22.6.2010, WP 171, afsnit 3.2.1, s. 9. Udtalelse nr. 1/2008 om databeskyttelsesproblemer i forbindelse med søgemaskiner (WP 148), afsnit 4.1.3, s. 12. Rapport til Kommissionen, "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation", SMART 2013/0071, s. 9.

²⁰ Udtalelse nr. 1/2008 om databeskyttelsesproblemer i forbindelse med søgemaskiner (WP 148), afsnit 4.1.3, s. 12.

²¹ Udtalelse nr. 1/2008 om databeskyttelsesproblemer i forbindelse med søgemaskiner (WP 148), afsnit 4.1.3, s. 12.

²² Artikel 29-Gruppen, udtalelse nr. 2/2010 om adfærdsbaseret annoncering på internettet af 22.6.2010, WP 171, s. 9. Jf. også udtalelse nr. 1/2008 om databeskyttelsesproblemer i forbindelse med søgemaskiner (WP 148), afsnit 4.1.3, s. 12.

²³ EU-Domstolen, C-210/16, 5. juni 2018, ECLI:EU:C:2018:388. Se navnlig præmis 33-34.

underliggende behandling også omfattede behandlingsaktiviteter, der henhørte under det materielle anvendelsesområde for e-databeskyttelsesdirektivet. I den verserende Fashion Id-sag udtalte generaladvokaten, at begge regelsæt muligvis kan anvendes i en sag, der omhandler sociale plug-ins og cookies²⁴.

31. GDPR erstattede direktiv 95/46/EF den 25. maj 2018, men den analyse, som EU-Domstolen og Artikel 29-Gruppen foretog, og som konkluderede, at begge retsakter kan finde anvendelse samtidig, er relevant. I betragtning 30 i GDPR beskrives definitionen af "onlineidentifikatorer" på en måde, som understøtter den fortolkning, at behandling af personoplysninger kan være underlagt det materielle anvendelsesområde for både GDPR og e-databeskyttelsesdirektivet.

"Fysiske personer kan tilknyttes onlineidentifikatorer, som tilvejebringes af deres enheder, applikationer, værktøjer og protokoller, såsom IP-adresser og cookieidentifikatorer, eller andre identifikatorer, såsom radiofrekvensidentifikationsmærker. Dette kan efterlade spor, der, navnlig når de kombineres med unikke identifikatorer og andre oplysninger, som serverne modtager, kan bruges til at oprette profiler om fysiske personer og identificere dem."

32. Det er især værd at bemærke, at "IP-adresser" og "cookieidentifikatorer" nævnes i betragtning 30, hvor det anføres, at IP-adresser og cookieidentifikatorer kan kombineres med andre "unikke identifikatorer" og andre oplysninger, som serverne modtager, til at oprette profiler om fysiske personer.
33. Med andre ord henviser GDPR selv i beskrivelsen af sit eget materielle anvendelsesområde (begrebet personoplysninger) udtrykkeligt til behandlingsaktiviteter, som også, i hvert fald til dels, er omfattet af det materielle anvendelsesområde for e-databeskyttelsesdirektivet.
34. Et andet eksempel på en aktivitet, der kan være omfattet af det materielle anvendelsesområde for både e-databeskyttelsesdirektivet og GDPR, er kundeforholdet mellem udbydere af elektroniske kommunikationstjenester og en fysisk person, der bruger disse tjenester, som omfatter behandling af personoplysninger om kunderne på den ene side og også er underlagt de særlige regler om f.eks. abonnentfortegnelser, udspecificeret fakturering og nummervisning. Trafikdata og lokaliseringsdata, der genereres af elektroniske kommunikationstjenester, kan også omfatte behandling af personoplysninger, for så vidt som de vedrører fysiske personer.
35. Endelig bekræfter artikel 95 betragtning 173 i GDPR lex generalis/lex specialis-forholdet mellem GDPR og e-databeskyttelsesdirektivet, hvor det i artikel 95 bestemmes, at GDPR ikke indfører yderligere forpligtelser for fysiske eller juridiske personer for så vidt angår behandling i forbindelse med levering af offentligt tilgængelige elektroniske kommunikationstjenester i offentlige kommunikationsnet i Unionen for så vidt angår spørgsmål, hvor de er underlagt specifikke forpligtelser med samme formål som det, der er fastsat i e-databeskyttelsesdirektivet.

36. Denne udtalelse har til formål at skabe klarhed omkring databeskyttelsesmyndighedernes kompetence, opgaver og beføjelser med hensyn til de tilfælde, der hører under det materielle anvendelsesområde for både e-databeskyttelsesdirektivet og GDPR, som kort beskrevet i de

²⁴ Forslag til afgørelse fra generaladvokat M. Bobek i Fashion ID, C-40/17, 19. december 2018, ECLI:EU:C:2018:1039. Se navnlig præmis 111-115.

foregående afsnit. Følgende afsnit beskriver nogle eksempler på samspil mellem bestemmelserne i e-databeskyttelsesdirektivet og GDPR, og forbindelsen mellem de to regelsæt.

4 SAMSPIL MELLEM E-DATABESKYTTELSESDIREKTIVET OG GDPR

37. Selv om der er overlapning mellem det materielle anvendelsesområde for e-databeskyttelsesdirektivet og GDPR, betyder det ikke nødvendigvis, at der er uoverensstemmelser mellem reglerne. Ud over at dette fremgår tydeligt, hvis man læser de forskellige bestemmelser side om side, angives det udtrykkeligt i artikel 1, stk. 2, i e-databeskyttelsesdirektivet, at "*dette direktivs bestemmelser [specificerer og supplerer] direktiv 95/46/EF*"²⁵. For at kunne forstå samspillet mellem e-databeskyttelsesdirektivet og GDPR er det nødvendigt først at præcisere betydningen af e-databeskyttelsesdirektivets artikel 1, stk. 2. Derefter forklares betydningen og virkningerne af artikel 95 i GDPR.

4.1 "At specificere"

38. En række bestemmelser i e-databeskyttelsesdirektivet "*specificerer*" bestemmelserne i GDPR med hensyn til behandling af personoplysninger i den elektroniske kommunikationssektor. Det følger af princippet om, at *lex specialis* går forud for *lex generalis*, at særlige bestemmelser har forrang for generelle bestemmelser i de situationer, som de specifikt tager sigte på at regulere²⁶. I situationer, hvor e-databeskyttelsesdirektivet "*specificerer*" reglerne i GDPR (dvs. gør dem mere specifikke), har e-databeskyttelsesdirektivets (specifikke) bestemmelser som "*lex specialis*" forrang for GDPR's (mere generelle) bestemmelser²⁷. Enhver behandling af personoplysninger, som ikke specifikt er omfattet af e-databeskyttelsesdirektivet (eller for hvilken e-databeskyttelsesdirektivet ikke indeholder en "særlig regel"), er dog stadig underlagt bestemmelserne i GDPR.
39. Ét eksempel, hvor e-databeskyttelsesdirektivet "*specificerer*" bestemmelserne i GDPR, findes i e-databeskyttelsesdirektivets artikel 6, som omhandler behandling af såkaldte "trafikdata". Normalt kan behandlingen af personoplysninger finde sted af hver enkelt af de lovlige grunde, der er nævnt i artikel 6 i GDPR. Dog kan hele spektret af mulige lovlige grunde i artikel 6 i GDPR ikke anvendes af udbyderen af en elektronisk kommunikationstjeneste til behandling af trafikdata, fordi artikel 6 i e-databeskyttelsesdirektivet udtrykkeligt begrænser de betingelser, hvorunder trafikdata, herunder personoplysninger, kan behandles. I dette tilfælde har de mere specifikke bestemmelser i e-databeskyttelsesdirektivet forrang for de mere generelle bestemmelser i GDPR. Artikel 6 i e-databeskyttelsesdirektivet begrænser imidlertid ikke anvendelsen af andre bestemmelser i GDPR, som f.eks. den registreredes rettigheder. Samtidig berører den ikke kravet om, at behandlingen af personoplysninger skal være lovlig og rimelig (artikel 5, stk. 1, litra a), i GDPR).
40. En lignende situation opstår med hensyn artikel 5, stk. 3, i e-databeskyttelsesdirektivet, for så vidt som de oplysninger, der er lagret i slutbrugerens enhed, udgør personoplysninger. Ifølge artikel 5, stk. 3, i e-databeskyttelsesdirektivet kræves der som hovedregel samtykke til lagring af oplysninger eller til at

²⁵ I henhold til artikel 94, stk. 2, i GDPR gælder henvisninger til det ophævede direktiv 95/46 som henvisninger til GDPR.

²⁶ Domstolens dom af 22. april 2016 i forenede sager T-60/06, RENV II, og T-62/06, RENV II, ECLI:EU:T:2016:233, præmis 81.

²⁷ Artikel 29-Gruppen, udtalelse nr. 2/2010 om adfærdsbaseret annoncering på internettet af 22.6.2010, WP 171, s. 10.

skaffe adgang til oplysninger, der allerede er lagret, i en abonnents eller brugers terminaludstyr²⁸. I det omfang, at de oplysninger, der lagres i slutbrugerens enhed, udgør personoplysninger, har artikel 5, stk. 3, i e-databeskyttelsesdirektivet forrang for artikel 6 i GDPR med hensyn til lagring eller adgang til disse oplysninger. Resultatet er det samme i samspillet mellem artikel 6 i GDPR og artikel 9 og 13 i e-databeskyttelsesdirektivet. Hvor disse artikler kræver samtykke til de specifikke foranstaltninger, de beskriver, kan den registeransvarlige ikke anvende alle de mulige lovlige grunde i artikel 6 i GDPR.

41. En naturlig følge af *lex specialis*-princippet er, at der kun kan ske undtagelse fra hovedreglen, for så vidt som den lov, der regulerer et nærmere bestemt emne, indeholder en særlig regel. De faktiske omstændigheder i sagen skal analyseres grundigt for at finde ud af, hvor langt undtagelsen rækker, især i tilfælde hvor data gennemgår mange forskellige former for behandling – enten parallelt eller sekventielt.

Eksempel:

En datamægler beskæftiger sig med profilering på grundlag af oplysninger om enkeltpersoners browsingadfærd, som er indsamlet ved hjælp af cookies, men som også kan indeholde personoplysninger, der er opnået via andre kilder (f.eks. "kommercielle partnere"). I et sådant tilfælde skal en delmængde af den pågældende behandling, nemlig anbringelse eller læsning af cookies, være i overensstemmelse med den nationale bestemmelse, der gennemfører artikel 5, stk. 3, i e-databeskyttelsesdirektivet. Den efterfølgende behandling af personoplysninger, herunder personoplysninger, der er indsamlet ved hjælp af cookies, skal også have hjemmel i artikel 6 i GDPR for at være lovlig²⁹.

4.2 "At supplere"

42. E-databeskyttelsesdirektivet indeholder også bestemmelser, som "supplerer" bestemmelserne i GDPR med hensyn til behandling af personoplysninger i den elektroniske kommunikationssektor. Flere af bestemmelserne i e-databeskyttelsesdirektivet har eksempelvis til formål at beskytte "abonnenter" og "brugere" af en offentligt tilgængelig elektronisk kommunikationstjeneste. Abonnenter på offentligt tilgængelige elektroniske kommunikationstjenester kan være fysiske eller juridiske personer. Som supplement til GDPR beskytter bestemmelserne i e-databeskyttelsesdirektivet ikke bare fysiske personers grundlæggende rettigheder, navnlig deres ret til privatlivets fred, men også juridiske personers legitime interesser³⁰.

4.3 Betydningen af artikel 95 i GDPR

43. I artikel 95 i GDPR bestemmes det, at GDPR ikke indfører "*yderligere forpligtelser for fysiske eller juridiske personer for så vidt angår behandling i forbindelse med levering af offentligt tilgængelige elektroniske kommunikationstjenester i offentlige kommunikationsnet i Unionen for så vidt angår*

²⁸ I henhold til artikel 5, stk. 3, kan oplysninger, der er lagret i en abonnents eller brugers terminaludstyr, også lagres, eller der kan opnås adgang til dem, for så vidt det udgør teknisk lagring eller adgang til oplysninger, hvis det alene sker med det formål at overføre eller lette overføring af kommunikation via et elektronisk kommunikationsnet eller er absolut påkrævet for at levere en informationsfundstjeneste, som abonnenten eller brugeren udtrykkelig ønsker.

²⁹ Databeskyttelsesmyndighederne kan ikke håndhæve artikel 5, stk. 3, i e-databeskyttelsesdirektivet (medmindre den nationale lovgivning giver dem denne kompetence), men de bør tage hensyn til, at behandlingen som helhed indebærer specifikke aktiviteter, for hvilke EU-lovgiveren har søgt at skabe yderligere beskyttelse for at undgå at underminere denne beskyttelse.

³⁰ E-databeskyttelsesdirektivets betragtning 12.

spørgsmål, hvor de er underlagt specifikke forpligtelser med samme formål som det, der er fastsat i direktiv 2002/58/EF" (understregning tilføjet).

44. Formålet med artikel 95 i GDPR er dermed at undgå at pålægge unødige administrative byrder på registeransvarlige, som ellers ville være underlagt tilsvarende, men ikke helt identiske administrative byrder. Et eksempel, der illustrerer anvendelsen af denne artikel, vedrører forpligtelsen til at informere om brud på persondatasikkerheden, som findes både i e-databeskyttelsesdirektivet³¹ og GDPR³². De indfører begge en forpligtelse til at garantere sikkerhed samt en forpligtelse til at informere henholdsvis den kompetente nationale myndighed og databeskyttelsesmyndigheden om brud på persondatasikkerheden. Disse forpligtelser gælder parallelt under de to forskellige retsakter i overensstemmelse med deres respektive anvendelsesområder. Det er klart, at en underretningsforpligtelse i henhold til begge retsakter, én i henhold til GDPR og én i henhold til den nationale e-databeskyttelseslovgivning, ville udgøre en ekstra byrde uden umiddelbare synlige fordele for databeskyttelsen. Ifølge artikel 95 i GDPR bliver udbydere af elektroniske kommunikationstjenester, der har anmeldt et brud på persondatasikkerheden i overensstemmelse med den gældende nationale e-databeskyttelseslovgivning, ikke forpligtet til særskilt at underrette databeskyttelsesmyndighederne om samme brud i henhold til artikel 33 i GDPR.

4.4 Sameksistens

45. Hvor der gælder specifikke bestemmelser for en bestemt behandlingsaktivitet eller en række aktiviteter, bør de særlige bestemmelser være gældende (*lex specialis*), men i alle andre tilfælde (dvs. hvor ingen særlige bestemmelser regulerer en bestemt behandlingsaktivitet eller en række aktiviteter) vil hovedreglen finde anvendelse (*lex generalis*).
46. I betragtning 173 bekræftes det, at med hensyn til behandling af personoplysninger, som e-databeskyttelsesdirektivets specifikke forpligtelser ikke finder anvendelse på, bør GDPR gælde:

"for alle forhold vedrørende beskyttelse af grundlæggende rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger, som ikke er underlagt specifikke forpligtelser med samme formål som fastsat i Europa-Parlamentets og Rådets direktiv 2002/58/EF, herunder den dataansvarliges forpligtelser og fysiske personers rettigheder"³³.

47. I betragtning 173 til GDPR gentages det, som allerede er nævnt i betragtning 10 til e-databeskyttelsesdirektivet: *"I den elektroniske kommunikationssektor finder [forordning (EU) 2016/679] navnlig anvendelse på alle forhold vedrørende beskyttelse af grundlæggende rettigheder og frihedsrettigheder, som ikke særligt er omfattet af bestemmelserne i dette direktiv, herunder den registeransvarliges forpligtelser og fysiske personers rettigheder."*
48. For eksempel skal en udbyder af et offentligt kommunikationsnet eller en offentligt tilgængelig elektronisk kommunikationstjeneste overholde de nationale regler til gennemførelse af artikel 6, stk. 2, i e-databeskyttelsesdirektivet vedrørende datatrafik, når denne behandler data, som er nødvendige

³¹ E-databeskyttelsesdirektivets artikel 4.

³² Artikel 32-34 i GDPR.

³³ Det hedder videre i betragtning 173, at "For at afklare forholdet mellem denne forordning og direktiv 2002/58/EF bør nævnte direktiv ændres i overensstemmelse hermed. Når denne forordning er vedtaget, bør direktiv 2002/58/EF revideres, navnlig for at sikre forenelighed med denne forordning." Denne revision er stadig i gang.

med henblik på debitering af abonnenten og afregning for samtrafik. Eftersom der ikke findes specifikke e-databeskyttelsesbestemmelser om f.eks. retten til adgang, finder bestemmelserne i GDPR anvendelse. Samtidig bekræfter betragtning 32 i e-databeskyttelsesdirektivet, at hvis udbyderen af en elektronisk kommunikationstjeneste eller en tillægstjeneste har underleveranceaftale om behandlingen af personoplysninger med henblik på levering af disse tjenester til en anden enhed, må denne underleverance og den efterfølgende databehandling være i fuld overensstemmelse med kravene til registeransvarlige og registerførere i forbindelse med personoplysninger, således som fastlagt i GDPR.

49. Det foregående afsnit beskrev samspillet mellem bestemmelserne i e-databeskyttelsesdirektivet og GDPR med hensyn til behandling, der hører under det materielle anvendelsesområde for begge instrumenter.
- De følgende afsnit omhandler de spørgsmål, der er blevet stillet til Databeskyttelsesrådet vedrørende databeskyttelsesmyndighedernes kompetence, opgaver og beføjelser med hensyn til sager, der i det mindste delvist falder inden for rammerne af e-databeskyttelsesdirektivet.

5 OM DATABESKYTTELSESMYNDIGHEDERNES KOMPETENCE, OPGAVER OG BEFØJELSER

50. De belgiske tilsynsmyndigheder forelagde to spørgsmål vedrørende databeskyttelsesmyndighedernes kompetence, opgaver og beføjelser – som fastsat i artikel 55-58 i GDPR – for Databeskyttelsesrådet. Disse spørgsmål kan formuleres som følger:
- Begrænser den omstændighed, at behandlingen af personoplysninger er omfattet af det materielle anvendelsesområde for både GDPR og e-databeskyttelsesdirektivet, databeskyttelsesmyndighedernes kompetencer, opgaver og beføjelser i henhold til GDPR? Er der med andre ord en delmængde af behandlingsaktiviteter, de ikke bør tage stilling til, og i bekræftende fald i hvilket omfang?
 - I forbindelse med udøvelsen af deres kompetencer, opgaver og beføjelser i henhold til GDPR bør databeskyttelsesmyndighederne da tage hensyn til bestemmelserne i e-databeskyttelsesdirektivet (f.eks. i forbindelse med vurderingen af behandlingens lovlighed), og i bekræftende fald i hvilket omfang? Med andre ord bør overtrædelser af nationale e-databeskyttelsesbestemmelser tages i betragtning i eller udelades fra vurderingen af overholdelsen af GDPR, og i bekræftende fald under hvilke omstændigheder?
51. Indledningsvis skal det bemærkes, at medlemsstaterne er forpligtet til at sikre EU-rettens fulde virkning, navnlig ved at fastsætte passende håndhævelsesmekanismer. Denne forpligtelse er baseret på princippet om loyalt samarbejde som fastsat i artikel 4, stk. 3, i TEU³⁴. Følgende afsnit beskriver i

³⁴ I artikel 4, stk. 3, i TEU, hedder det: "*I medfør af princippet om loyalt samarbejde respekterer Unionen og medlemsstaterne hinanden og bistår hinanden ved gennemførelsen af de opgaver, der følger af traktaterne. Medlemsstaterne træffer alle almindelige eller særlige foranstaltninger for at sikre opfyldelsen af de forpligtelser, der følger af traktaterne eller af retsakter vedtaget af EU-institutionerne. Medlemsstaterne bistår Unionen i gennemførelsen af dens opgaver og afholder sig fra at træffe foranstaltninger, der kan bringe virkeliggørelsen af Unionens mål i fare.*"

korte træk håndhævelsesbestemmelserne i henholdsvis GDPR og e-databeskyttelsesdirektivet og samspillet mellem dem.

5.1 Håndhævelse af GDPR

52. I henhold til GDPR skal bestemmelserne deri håndhæves af uafhængige databeskyttelsesmyndigheder. I denne forbindelse skal det også bemærkes, at artikel 8 i charteret om Den Europæiske Unions grundlæggende rettigheder (charteret) bestemmer, at behandlingen af personoplysninger er underlagt kontrol fra en uafhængig myndighed:

"Artikel 8 Beskyttelse af personoplysninger

1. *Enhver har ret til beskyttelse af personoplysninger, der vedrører den pågældende.*

2. *Disse oplysninger skal behandles rimeligt, til udtrykkeligt angivne formål og på grundlag af de berørte personers samtykke eller på et andet berettiget ved lov fastsat grundlag. Enhver har ret til adgang til indsamlede oplysninger, der vedrører den pågældende, og til berigtigelse heraf.*

3. Overholdelsen af disse regler er underlagt en uafhængig myndigheds kontrol."

53. I artikel 51, stk. 1, i GDPR får databeskyttelsesmyndighederne et retligt mandat, som er at føre tilsyn med anvendelsen af GDPR, for at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder i forbindelse med behandling og for at lette fri udveksling af personoplysninger i Unionen.

54. GDPR indeholder én undtagelse og en mulighed for at fravige dette mandat:

- Tilsynsmyndigheder er ikke kompetente til at føre tilsyn med domstoles behandling af personoplysninger, når disse handler i deres egenskab af domstol (artikel 55, stk. 3, i GDPR).
- Til behandling i journalistisk øjemed eller med henblik på akademisk, kunstnerisk eller litterær virksomhed kan medlemsstaterne fastsætte undtagelser eller fravigelser fra bl.a. kapitel VI (uafhængige tilsynsmyndigheder) og kapitel VII (samarbejde og sammenhæng) i GDPR (artikel 85 i GDPR).

Derudover kan databeskyttelsesmyndighedernes beføjelser udvides i overensstemmelse med artikel 58, stk. 6, i GDPR, således at de navnlig får beføjelse til at pålægge offentlige myndigheder og organer bøder, hvis medlemsstaten fastsætter regler derom (artikel 83, stk. 7, i GDPR).

Eftersom disse bestemmelser er undtagelser til hovedreglen, bør de fortolkes snævert.

55. I de tilfælde, hvor GDPR begrænser eller tillader undtagelser til databeskyttelsesmyndighedernes kompetencer, opgaver og beføjelser, sker det eksplicit. GDPR udelukker heller ikke, at databeskyttelsesmyndighederne på nogen måde kan udøve deres kompetencer, opgaver og beføjelser i forbindelse med behandling, i det omfang det er omfattet af det materielle anvendelsesområde for GDPR. Spørgsmålet bliver derfor, om EU-lovgiveren har forudset eller tilladt en undtagelse til databeskyttelsesmyndighedernes generelle kompetence i de tilfælde, hvor bestemmelserne i e-databeskyttelsesdirektivet finder anvendelse på den pågældende behandling.

5.2 Håndhævelse af e-databeskyttelsesdirektivet

56. Håndhævelsen af bestemmelserne i e-databeskyttelsesdirektivet er tæt knyttet til rammedirektivet³⁵, hvori det i artikel 3, stk. 1, hedder følgende: "*Medlemsstaterne sikrer, at alle opgaver, de nationale tilsynsmyndigheder får pålagt i dette direktiv og i særdirektiverne, varetages af et kompetent organ*"³⁶.
57. I rammedirektivets artikel 2, litra g), defineres en "national tilsynsmyndighed" som
- "den eller de instanser, der af en medlemsstat har fået til opgave at varetage de tilsynsopgaver, der pålægges i dette direktiv og i særdirektiverne".*
58. Medlemsstaterne har valgt at tildele opgaven med at håndhæve de nationale e-databeskyttelsesbestemmelser til en eller flere instanser på forskellige måder³⁷. Disse forskelle er mulige, fordi e-databeskyttelsesdirektivet kun opstiller nogle generelle mål, der skal opfyldes af medlemsstaterne på dette område.
59. Det fremgår ikke af e-databeskyttelsesdirektivet, at kun ét nationalt organ har kompetence til at håndhæve bestemmelserne. Faktisk fastsættes det udtrykkeligt i artikel 15a i e-databeskyttelsesdirektivet, at mere end ét nationalt organ kan have kompetence til at håndhæve bestemmelserne deri. Artikel 15a indeholder også bestemmelser om gennemførelse og håndhævelse af direktivet i medlemsstaterne, herunder at medlemsstaterne fastsætter bestemmelser om sanktioner, giver beføjelse til at beordre overtrædelser bragt til ophør, giver beføjelser til efterforskning og tildeler ressourcer:

"1. Medlemsstaterne fastsætter bestemmelser om sanktioner, herunder strafferetlige foranstaltninger, hvis det er relevant, for overtrædelse af de nationale bestemmelser, der er vedtaget i medfør af dette direktiv, og træffer alle nødvendige foranstaltninger til at sikre gennemførelsen heraf. De sanktioner, der pålægges, skal være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning, og skal kunne anvendes i en periode svarende til overtrædelsens varighed, også selv om overtrædelsen i mellemtiden er bragt til ophør. Medlemsstaterne giver inden den 25. maj 2011 Kommissionen meddelelse om disse bestemmelser, og meddeler den omgående enhver senere ændring heraf.

2. Uden at det berører en eventuel klageadgang, sikrer medlemsstaterne, at den kompetente nationale myndighed og, hvor det er relevant, andre nationale organer har beføjelse til at beordre overtrædelser som omhandlet i stk. 1 bragt til ophør.

3. Medlemsstaterne sikrer, at den kompetente nationale myndighed, og, hvor det er relevant, andre nationale organer, har de nødvendige beføjelser og ressourcer til efterforskning, herunder beføjelser til at skaffe sig relevante oplysninger, som de måtte have brug for under

³⁵ Europa-Parlamentets og Rådets direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet), som ændret.

³⁶ I rammedirektivets artikel 2, litra l), præciseres følgende: "*'særdirektiver': direktiv 2002/20/EF (tilladelsesdirektivet), direktiv 2002/19/EF (adgangsdirektivet), direktiv 2002/22/EF (forsyningspligt-direktivet) og Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktivet om databeskyttelse inden for elektronisk kommunikation)*".

³⁷ Rapport til Kommissionen, "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation", SMART 2013/0071, s. 33 ff.

overvågningen og håndhævelsen af nationale bestemmelser, der er vedtaget i medfør af dette direktiv.

4. De relevante nationale tilsynsmyndigheder kan træffe foranstaltninger til at sikre et effektivt samarbejde hen over grænserne om at håndhæve de nationale love, der vedtages i medfør af dette direktiv, og til at tilvejebringe harmoniserede vilkår for udbuddet af tjenester, der medfører datastrømme hen over grænserne."

60. Ud over artikel 15, stk. 2, indeholder e-databeskyttelsesdirektivet en bestemmelse, hvor der henvises til direktiv 95/46/EF om retsmidler, ansvar og sanktioner, som nu skal læses som en henvisning til GDPR:

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

61. I e-databeskyttelsesdirektivets artikel 15, stk. 3, hedder det også:

"Den gruppe vedrørende beskyttelse af personer i forbindelse med behandling af personoplysninger, som blev nedsat ved artikel 29 i direktiv 95/46/EF, varetager også de opgaver, der er fastsat i artikel 30 i direktiv 95/46/EF med hensyn til de af dette direktiv omfattede forhold, dvs. beskyttelse af grundlæggende rettigheder og frihedsrettigheder samt legitime interesser i den elektroniske kommunikationssektor."³⁸

5.3 Håndhævelse, hvor GDPR og e-databeskyttelsesdirektivet krydser hinanden

62. E-databeskyttelsesdirektivet specificerer og supplerer GDPR og henviser endvidere til bestemmelserne i GDPR om retsmidler, ansvar og sanktioner (artikel 15, stk. 2, i e-databeskyttelsesdirektivet) læst i sammenhæng med artikel 94 i GDPR).

5.3.1 Spørgsmål 1: Er visse databehandlingsaktiviteter "forbudt område" for databeskyttelsesmyndighederne?

- *Begrænser den omstændighed, at behandlingen af personoplysninger er omfattet af det materielle anvendelsesområde for både GDPR og e-databeskyttelsesdirektivet, databeskyttelsesmyndighedernes kompetencer, opgaver og beføjelser i henhold til GDPR? Er der med andre ord en delmængde af behandlingsaktiviteter, de ikke bør tage stilling til, og i bekræftende fald hvilke behandlingsaktiviteter?*
63. Medlemsstaterne skal i henhold til GDPR have udpeget en eller flere tilsynsmyndigheder. Medlemsstaterne kan have udpeget den samme myndighed, der har kompetence til (en del af)

³⁸ I e-databeskyttelsesdirektivets artikel 15, stk. 3, hedder det: "Den gruppe vedrørende beskyttelse af personer i forbindelse med behandling af personoplysninger, som blev nedsat ved artikel 29 i direktiv 95/46/EF, varetager også de opgaver, der er fastsat i artikel 30 i direktiv 95/46/EF med hensyn til de af dette direktiv omfattede forhold, dvs. beskyttelse af grundlæggende rettigheder og frihedsrettigheder samt legitime interesser i den elektroniske kommunikationssektor."

Det bestemmes i artikel 94, stk. 2, i GDPR, at "henvisninger til det ophævede direktiv gælder som henvisninger til denne forordning. Henvisninger til Gruppen vedrørende Beskyttelse af Personer i forbindelse med Behandling af Personoplysninger, der er nedsat ved artikel 29 i direktiv 95/46/EF, gælder som henvisninger til Det Europæiske Databeskyttelsesråd oprettet ved denne forordning."

Dermed skal artikel 30 i direktiv 95/46 fortolkes som en henvisning til de relevante afsnit i artikel 70 i GDPR (Databeskyttelsesrådets opgaver).

håndhævelsen af den nationale gennemførelse af e-databeskyttelsesdirektivet, men kan også have valgt en eller flere andre myndigheder, f.eks. en national telekommunikationstilsynsmyndighed, en forbrugerbeskyttelsesorganisation eller et ministerium.

64. E-databeskyttelsesdirektivet giver medlemsstaterne fleksibilitet med hensyn til, hvilken myndighed eller hvilket organ de vil overlade håndhævelsen af bestemmelserne deri til.
65. Mens e-databeskyttelsesdirektivet henviser til bestemmelserne i GDPR om retsmidler, ansvar og sanktioner (artikel 15, stk. 2, i e-databeskyttelsesdirektivet), beskriver artikel 15a, stk. 1, i e-databeskyttelsesdirektivet bestemmelserne om "Gennemførelse og håndhævelse" i e-databeskyttelsesdirektivet nærmere. Eksempelvis fastsættes følgende i artikel 15a, stk. 1: "*Medlemsstaterne fastsætter bestemmelser om sanktioner, herunder strafferetlige foranstaltninger, hvis det er relevant, for overtrædelse af de nationale bestemmelser, der er vedtaget i medfør af dette direktiv, og træffer alle nødvendige foranstaltninger til at sikre gennemførelsen heraf.*" E-databeskyttelsesdirektivet giver som sådan udtrykkeligt medlemsstaterne skønsmæssig beføjelse til at fastsætte bestemmelser om sanktioner, og artikel 15, stk. 2, berører ikke medlemsstaternes håndhævelsesbeføjelser (dvs. til at afgøre, hvem der håndhæver bestemmelserne i e-databeskyttelsesdirektivet)³⁹.
66. I tilfælde, hvor den nationale lovgivning giver databeskyttelsesmyndigheden kompetence til håndhævelse af e-databeskyttelsesdirektivet, bør lovgivningen også fastlægge, hvilke opgaver og beføjelser databeskyttelsesmyndigheden har i forhold til håndhævelsen af e-databeskyttelsesdirektivet. Databeskyttelsesmyndigheden har ikke automatisk de opgaver og beføjelser, der er fastsat i GDPR, til at træffe foranstaltninger til at håndhæve de nationale e-databeskyttelsesregler, da disse GDPR-opgaver og -beføjelser er bundet til håndhævelsen af GDPR. Den nationale lovgivning kan tildele opgaver og beføjelser inspireret af GDPR, men kan også give andre opgaver og beføjelser til databeskyttelsesmyndigheden med henblik på håndhævelse af de nationale e-databeskyttelsesregler i overensstemmelse med artikel 15a i e-databeskyttelsesdirektivet.
67. Der er kun en skønsmæssig margen i forhold til de krav og begrænsninger, der er fastsat i lovgivning på et højere niveau. I charterets artikel 8, stk. 3, kræves det, at overholdelsen af reglerne om beskyttelse af personoplysninger er underlagt kontrol fra en uafhængig myndighed⁴⁰.
68. Når behandlingen af personoplysninger er omfattet af det materielle anvendelsesområde for både GDPR og e-databeskyttelsesdirektivet, har databeskyttelsesmyndighederne kun kompetence til at granske de delmængder af behandlingen, som er underlagt nationale regler til gennemførelse af e-databeskyttelsesdirektivet, hvis den nationale lovgivning giver dem denne kompetence. Men databeskyttelsesmyndighedernes kompetence i henhold til GDPR er under alle omstændigheder ikke berørt med hensyn til behandlingsaktiviteter, som ikke er omfattet af særlige regler i e-databeskyttelsesdirektivet. Denne afgrænsning kan ikke ændres af den nationale lovgivning til gennemførelse af e-databeskyttelsesdirektivet (f.eks. ved at udvide det materielle anvendelsesområde

³⁹ Bemærk, at artikel 15a, stk. 1, i e-databeskyttelsesdirektivet blev indført ved direktiv 2009/136/EF (dvs. en ændring til e-databeskyttelsesdirektivet).

⁴⁰ EU-Domstolens retspraksis vedrørende artikel 28 i direktiv 95/46 har præciseret kravene med hensyn til uafhængighed: jf. f.eks. dom af 9. marts 2010, C-518/07 (Kommissionen mod Tyskland), præmis 17 ff., dom af 16. oktober 2012, C-614/10 (Kommissionen mod Østrig), præmis 36 ff., dom af 6. oktober 2015, C-362/14 (Safe Harbour), præmis 41 ff., dom af 21. december 2016, C-203/15 og C-698/15, (Tele2/Watson), præmis 123.

ud over, hvad der kræves i e-databeskyttelsesdirektivet, og give enekompetence dertil til den nationale tilsynsmyndighed).

69. Databeskyttelsesmyndighederne har kompetence til at håndhæve GDPR. Den omstændighed, at en delmængde af behandlingen er omfattet af e-databeskyttelsesdirektivets anvendelsesområde, begrænser ikke databeskyttelsesmyndighedernes kompetence i henhold til GDPR.
70. Hvis der gives enekompetence til en anden instans end databeskyttelsesmyndigheden, bestemmer den nationale retspleje, hvad der skal ske, hvis registrerede alligevel indgiver klager til databeskyttelsesmyndigheden om f.eks. behandling af personoplysninger i form af trafik- eller lokaliseringsdata, uanmodet elektronisk kommunikation eller indsamling af personoplysninger ved hjælp af cookies uden også at klage over en (potentiell) krænkelse af GDPR.

5.3.2 Spørgsmål to: Er de nationale e-databeskyttelsesbestemmelser "forbudt område"?

- *I forbindelse med udøvelsen af deres kompetencer, opgaver og beføjelser i henhold til GDPR bør databeskyttelsesmyndighederne da tage hensyn til bestemmelserne i e-databeskyttelsesdirektivet (f.eks. i forbindelse med vurderingen af behandlingens lovlighed), og i bekræftende fald i hvilket omfang? Med andre ord bør overtrædelser af nationale e-databeskyttelsesbestemmelser tages i betragtning i eller udelades fra vurderingen af overholdelsen af GDPR, og i bekræftende fald under hvilke omstændigheder?*
71. Et eksempel illustrerer forskellen i forhold til spørgsmål 1. Tænk på en datamægler, der beskæftiger sig med profilering på grundlag af oplysninger fra to forskellige kilder. Den første kilde er data vedrørende enkeltpersoners browsingadfærd, som er indsamlet ved hjælp af cookie- og/eller enhedsidentifikatorer. Den anden kilde er data indsamlet via kommercielle partnere, der deler data om deltagere i lodtrækninger eller bonusprogrammer.
 72. Profilering af personer på grundlag af personoplysninger falder generelt inden for anvendelsesområdet for GDPR og henhører derfor under databeskyttelsesmyndighedernes kompetence. Hvis en databeskyttelsesmyndighed modtager en klage vedrørende datamæglerens profileringsaktiviteter, hvordan skal databeskyttelsesmyndighederne da anvende bestemte regler, i dette tilfælde de nationale e-databeskyttelsesregler, når de vurderer overholdelsen af GDPR?
 73. Det er værd at bemærke, at e-databeskyttelsesdirektivet er et konkret eksempel på en lov, der yder særlig beskyttelse til bestemte kategorier af oplysninger, som kan være personoplysninger. Andre retsakter giver også særlig beskyttelse til bestemte typer af oplysninger, som kan være personoplysninger, af forskellige årsager (f.eks. behandlingssituationen, oplysningernes art eller risikoen for de registrerede)⁴¹.

⁴¹ Et eksempel fra den finansielle sektor kan illustrere dette: Der ydes særlig beskyttelse, hvad angår oplysninger, der bruges til at vurdere en persons kreditværdighed, eller offentliggørelse af administrative sanktioner. Jf. artikel 21, stk. 1, i Europa-Parlamentets og Rådets direktiv 2014/17/EU af 4. februar 2014 om forbrugerkreditaftaler i forbindelse med fast ejendom til beboelse og om ændring af direktiv 2008/48/EF og 2013/36/EU og forordning (EU) nr. 1093/2010, artikel 68-69 i Europa-Parlamentets og Rådets direktiv 2013/36/EU af 26. juni 2013 om adgang til at udøve virksomhed som kreditinstitut og om tilsyn med kreditinstitutter og investeringsselskaber, om ændring af direktiv 2002/87/EF og om ophævelse af direktiv

74. Medlemsstaterne er forpligtet til at udpege en eller flere myndigheder til at føre tilsyn med overholdelsen af den nationale lovgivning til gennemførelse af e-databeskyttelsesdirektivet, og sådan eller sådanne myndigheder er således ansvarlige for håndhævelsen af denne lov. Den nationale lovgivning til gennemførelse af e-databeskyttelsesdirektivet gælder for den eller de konkrete behandlingsaktiviteter, der er underlagt e-databeskyttelsesdirektivet (f.eks. en behandlingsaktivitet, som består i lagring af eller adgang til oplysninger gemt på slutbrugernes enhed).
75. Medmindre den nationale lovgivning giver dem en sådan kompetence, kan databeskyttelsesmyndighederne ikke håndhæve bestemmelserne i (den nationale lov til gennemførelse af) e-databeskyttelsesdirektivet som sådan, når de udøver deres beføjelser i henhold til GDPR. Men som tidligere nævnt, kan behandling af personoplysninger, der involverer aktiviteter, der er omfattet af det materielle anvendelsesområde for e-databeskyttelsesdirektivet, omfatte yderligere aspekter, for hvilke e-databeskyttelsesdirektivet ikke indeholder en "særregel". F.eks. indeholder artikel 5, stk. 3, i e-databeskyttelsesdirektivet en særregel om lagring af oplysninger eller adgang til oplysninger, der allerede er lagret, i en slutbrugers terminaludstyr. Det indeholder ikke en særlig regel for eventuelle tidligere eller senere behandlingsaktiviteter (f.eks. lagring og analyse af data vedrørende webbrowsingaktivitet med henblik på adfærdsbaseret annoncering online eller til sikkerhedsformål). Derfor bevarer databeskyttelsesmyndighederne den fulde kompetence til at vurdere lovligheden af alle andre behandlingsaktiviteter, der følger efter lagring af eller adgang til oplysningerne i slutbrugers terminaludstyr⁴².
76. En overtrædelse af GDPR kan også udgøre en overtrædelse af de nationale e-databeskyttelsesregler. Databeskyttelsesmyndigheden kan tage denne faktuelle overtrædelse af e-databeskyttelsesreglerne i betragtning ved anvendelsen af GDPR (f.eks. når de vurderer overholdelsen af princippet om lovlighed og rimelighed i artikel 5, stk. 1, litra a), i GDPR). Dog skal enhver håndhævelsesbeslutning være baseret på GDPR, medmindre medlemsstatens lovgivning giver databeskyttelsesmyndigheden yderligere kompetencer.

2006/48/EF

og

2006/49/EF.

Et andet eksempel kan findes i reglerne om kliniske forsøg: jf. artikel 28-35 i Europa-Parlamentets og Rådets forordning (EU) nr. 536/2014 af 16. april 2014 om kliniske forsøg med humanmedicinske lægemidler og om ophævelse af direktiv 2001/20/EF.

⁴² I denne forbindelse skal der henvises til udtalelsen fra Artikel 29-Gruppen om den registeransvarliges legitime interesse (6/2014) og Artikel 29-Gruppens udtalelse om formålsbegrænsning (3/2013), hvori det præciseres, at visse former for adfærdsbaseret annoncering kræver samtykke fra den registrerede, og ikke kun på grundlag af artikel 5, stk. 3. I udtalelsen om formålsbegrænsning hedder det:

"Det andet potentielle scenarie er, når en organisation specifikt ønsker at analysere eller forudsige enkelte kunders personlige præferencer, adfærd og holdninger for derefter at bruge dem til 'foranstaltninger eller beslutninger', der træffes over for disse kunder. I disse tilfælde vil frivilligt, utvetydigt, informeret og udtrykkeligt ""tilvalgssamtykke"" næsten altid være nødvendigt, hvis yderligere brug skal betragtes som værende foreneligt. Sådant samtykke bør navnlig kræves til f.eks. sporing og profilering med henblik på direkte markedsføring, adfærdsbaseret annoncering, datamæglervirksomhed, lokationsbaseret annoncering eller sporingsbaserede digitale markedsundersøgelser."

I udtalelsen om legitim interesse hedder det:

"I stedet for blot at tilbyde muligheden for at fravælge denne type profilering og målrettet reklame ville et informeret samtykke være påkrævet i henhold til artikel 7, litra a), men også artikel 5, stk. 3, i e-databeskyttelsesdirektivet. Derfor bør artikel 7, litra f), ikke anvendes som retsgrundlag for behandlingen."

77. Hvis den nationale lovgivning udpeger databeskyttelsesmyndigheden som kompetent myndighed i henhold til e-databeskyttelsesdirektivet, har denne databeskyttelsesmyndighed kompetence til direkte at håndhæve de nationale e-databeskyttelsesregler ud over GDPR (ellers har den ikke).
78. Som en generel bemærkning, hvor flere myndigheder har kompetence til de forskellige retsakter, bør de sikre, at håndhævelsen af begge instrumenter er konsekvent, bl.a. for at undgå at overtræde non bis in idem-princippet i tilfælde af, at der er en tæt forbindelse mellem overtrædelser af bestemmelserne i GDPR og e-databeskyttelsesdirektivet, som fandt sted i forbindelse med en behandlingsaktivitet.

6 OM ANVENDELSEN AF SAMARBEJDS- OG SAMMENHÆNGSMEKANISMERNE

79. Det tredje spørgsmål fra den belgiske databeskyttelsesmyndighed til Databeskyttelsesrådet kan formuleres som følger:
- *I hvilket omfang finder samarbejds- og sammenhængsmekanismerne anvendelse på behandling, som i hvert fald med hensyn til visse behandlingsaktiviteter er omfattet af det materielle anvendelsesområde for både GDPR og e-databeskyttelsesdirektivet?*
80. Ifølge kapitel VII i GDPR omfatter de samarbejds- og sammenhængsmekanismer, der er til rådighed for databeskyttelsesmyndighederne i henhold til GDPR, overvågning af anvendelsen af GDPR-bestemmelserne. GDPR-mekanismerne gælder ikke for håndhævelsen af bestemmelserne i e-databeskyttelsesdirektivet som sådan.
81. Under alle omstændigheder hedder det også i e-databeskyttelsesdirektivets artikel 15, stk. 3:
- "[Det Europæiske Databeskyttelsesråd] varetager også de opgaver, der er fastsat i [artikel 70 i forordning (EU) nr. 2016/679] med hensyn til de af dette direktiv omfattede forhold, dvs. beskyttelse af grundlæggende rettigheder og frihedsrettigheder samt legitime interesser i den elektroniske kommunikationssektor."*
82. For så vidt angår samarbejdet mellem de myndigheder, der har kompetence til at håndhæve e-databeskyttelsesdirektivet, fastsættes følgende i e-databeskyttelsesdirektivets artikel 15a, stk. 4: *"De relevante nationale tilsynsmyndigheder kan træffe foranstaltninger til at sikre et effektivt samarbejde hen over grænserne om at håndhæve de nationale love, der vedtages i medfør af dette direktiv, og til at tilvejebringe harmoniserede vilkår for udbuddet af tjenester, der medfører datastrømme hen over grænserne."*
83. Et sådant grænseoverskridende samarbejde mellem myndighederne med ansvar for håndhævelse af e-databeskyttelsesdirektivet, herunder databeskyttelsesmyndigheder, nationale tilsynsmyndigheder og andre myndigheder, kan finde sted i det omfang, de relevante nationale tilsynsmyndigheder træffer foranstaltninger til at sikre et sådant samarbejde.
84. Det skal dog bemærkes, at samarbejds- og sammenhængsmekanismen fortsat finder fuld anvendelse, for så vidt som behandlingen er underlagt de generelle bestemmelser i GDPR (og ikke en "særlig regel" i e-databeskyttelsesdirektivet). For eksempel gælder det, at selv om behandlingen af

personoplysninger (f.eks. profilering) delvist er afhængig af adgang til oplysninger, der er lagret i slutbrugerens enhed, er de databeskyttelsesregler, der ikke er fastsat i e-databeskyttelsesdirektivet (f.eks. de registreredes rettigheder, principperne for behandling) for enhver behandling af personoplysninger, der finder sted efter at have opnået adgang til oplysninger lagret i slutbrugerens enhed, underlagt bestemmelserne i GDPR, herunder samarbejds- og sammenhængsmekanismerne.

85. I praksis vil databeskyttelsesmyndighederne omhyggeligt vælge, hvilken "kommunikationslinje", der skal bruges, og især hvis de ikke kun håndhæver GDPR, men også har kompetence til at håndhæve (en del af) de nationale bestemmelser til gennemførelse af e-databeskyttelsesdirektivet. Standardkommunikationslinjen – som beskrevet i kapitel VII (Samarbejde og sammenhæng) i GDPR – skal bruges til enhver del af en procedure, der skal benytte de håndhævelsesbeføjelser, der gælder i henhold til GDPR, som reaktion på en overtrædelse af GDPR.

Databeskyttelsesmyndighederne kan også vælge at bruge en anden kommunikationslinje i forbindelse med de specifikke håndhævelsesbeføjelser, de har i henhold til de nationale bestemmelser til gennemførelse af e-databeskyttelsesdirektivet, og kun for så vidt som proceduren har til formål at reagere på overtrædelser af de nationale e-databeskyttelsesregler, der gælder for de former for adfærd, der er reguleret af e-databeskyttelsesdirektivet. Så snart det drejer sig om forhold, der er omfattet af anvendelsesområdet for GDPR, er databeskyttelsesmyndighederne forpligtet til at anvende samarbejds- og sammenhængsmekanismen i GDPR.

7 KONKLUSION

- *Begrænser den omstændighed, at behandlingen af personoplysninger er omfattet af det materielle anvendelsesområde for både GDPR og e-databeskyttelsesdirektivet, databeskyttelsesmyndighedernes kompetencer, opgaver og beføjelser i henhold til GDPR? Er der med andre ord en delmængde af databehandlingsaktiviteter, de ikke bør tage stilling til, og i bekræftende fald i hvilket omfang?*
86. Når behandlingen af personoplysninger er omfattet af det materielle anvendelsesområde for både GDPR og e-databeskyttelsesdirektivet, har databeskyttelsesmyndighederne kun kompetence til at undersøge de databehandlingsaktiviteter, der er underlagt de nationale e-databeskyttelsesregler, hvis den nationale lovgivning giver dem denne kompetence, og en sådan undersøgelse skal foretages inden for de tilsynsbeføjelser, der er tildelt myndigheden i medfør af den nationale lovgivning til gennemførelse af e-databeskyttelsesdirektivet.
87. Databeskyttelsesmyndighederne har kompetence til at håndhæve GDPR. Den omstændighed, at en delmængde af behandlingen er omfattet af e-databeskyttelsesdirektivets anvendelsesområde, begrænser ikke databeskyttelsesmyndighedernes kompetence i henhold til GDPR.
- *I forbindelse med udøvelsen af deres kompetencer, opgaver og beføjelser i henhold til GDPR bør databeskyttelsesmyndighederne da tage hensyn til bestemmelserne i e-databeskyttelsesdirektivet, og i bekræftende fald i hvilket omfang? Med andre ord bør overtrædelser af nationale e-databeskyttelsesbestemmelser udelades fra vurderingen af overholdelsen af GDPR, og i bekræftende fald under hvilke omstændigheder?*
88. Den eller de myndigheder, som medlemsstaterne har udpeget som kompetente i medfør af e-databeskyttelsesdirektivet, er udelukkende ansvarlige for at håndhæve de nationale bestemmelser,

der gennemfører e-databeskyttelsesdirektivet, og som gælder for den pågældende behandlingsaktivitet, herunder i tilfælde, hvor behandlingen af personoplysninger er omfattet af det materielle anvendelsesområde for både GDPR og e-databeskyttelsesdirektivet. Ikke desto mindre har databeskyttelsesmyndighederne den fulde kompetence med hensyn til eventuelle behandlingsaktiviteter, der foretages for personoplysninger, som ikke er omfattet af en eller flere specifikke regler i e-databeskyttelsesdirektivet.

89. En overtrædelse af GDPR kan også udgøre en overtrædelse af de nationale e-databeskyttelsesregler. Databeskyttelsesmyndigheden kan tage denne faktuelle overtrædelse af e-databeskyttelsesreglerne i betragtning ved anvendelsen af GDPR (f.eks. når de vurderer overholdelsen af princippet om lovlighed og rimelighed i artikel 5, stk. 1, litra a), i GDPR). Dog skal enhver håndhævelsesbeslutning være baseret på GDPR, medmindre medlemsstatens lovgivning giver databeskyttelsesmyndigheden yderligere kompetencer.
90. Hvis den nationale lovgivning udpeger databeskyttelsesmyndigheden som kompetent myndighed i henhold til e-databeskyttelsesdirektivet, har denne databeskyttelsesmyndighed kompetence til direkte at håndhæve de nationale e-databeskyttelsesregler ud over GDPR (ellers har den ikke).
- *I hvilket omfang finder samarbejds- og sammenhængsmekanismerne anvendelse på behandling, som i hvert fald med hensyn til visse behandlingsaktiviteter er omfattet af det materielle anvendelsesområde for både GDPR og e-databeskyttelsesdirektivet?*
91. De samarbejds- og sammenhængsmekanismer, der er til rådighed for databeskyttelsesmyndighederne i henhold til kapitel VII i GDPR, omfatter overvågning af anvendelsen af GDPR-bestemmelserne. GDPR-mekanismerne gælder ikke for håndhævelsen af de nationale bestemmelser til gennemførelse af e-databeskyttelsesdirektivet. Samarbejds- og sammenhængsmekanismen gælder imidlertid fortsat fuldt ud for behandling, der er underlagt de generelle bestemmelser i GDPR (og ikke en "særlig regel" i e-databeskyttelsesdirektivet).

92. Databeskyttelsesrådet anerkender, at ovenstående fortolkning ikke berører resultatet af de igangværende forhandlinger om e-databeskyttelsesforordningen. Den foreslåede forordning omhandler mange vigtige elementer, herunder med hensyn til databeskyttelsesmyndighedernes kompetencer, men også med hensyn til en række andre meget vigtige spørgsmål. Databeskyttelsesrådet gentager sin holdning om, at vedtagelsen af en e-databeskyttelsesforordning er vigtig⁴³.

For Det Europæiske Databeskyttelsesråd

Formanden

⁴³ Databeskyttelsesrådet har opfordret Kommissionen, Europa-Parlamentet og Rådet til at samarbejde for at sikre en hurtig vedtagelse af den nye e-databeskyttelsesforordning (erklæring offentliggjort den 25. maj 2018).

(Andrea Jelinek)