Yttrande från styrelsen (art. 64)

Yttrande 5/2019 om samspelet mellan direktivet om integritet och elektronisk kommunikation och den allmänna dataskyddsförordningen, särskilt när det gäller dataskyddsmyndigheternas behörighet, uppgifter och befogenheter

Antaget den 12 mars 2019

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

INNEHÅLLSFÖRTECKNING

Europeiska dataskyddsstyrelsen

med beaktande av artiklarna 63 och 64.2 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning),

med beaktande av EES-avtalet, särskilt bilaga XI och protokoll 37 till detta, ändrat genom gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018,

med beaktande av artiklarna 10 och 22 i dess arbetsordning av den 25 maj 2018, ändrad den 23 november 2018, och

av följande skäl:

1) Europeiska dataskyddsstyrelsens (nedan kallad *styrelsen*) huvudsakliga uppgift är att säkerställa en konsekvent tillämpning av förordning 2016/679 (nedan kallad *dataskyddsförordningen*) inom hela Europeiska ekonomiska samarbetsområdet. Enligt artikel 64.2 i dataskyddsförordningen får varje tillsynsmyndighet, styrelsens ordförande eller kommissionen i syfte att erhålla ett yttrande begära att styrelsen granskar en fråga med allmän räckvidd eller som har följder i mer än en medlemsstat. Syftet med detta yttrande är att undersöka en fråga med allmän räckvidd eller som har effekter i mer än en medlemsstat.

2) Den 3 december 2018 begärde den belgiska dataskyddsmyndigheten att Europeiska dataskyddsstyrelsen skulle undersöka och utfärda ett yttrande om samspelet mellan direktivet om integritet och elektronisk kommunikation (nedan *direktivet om e-integritet)* och dataskyddsförordningen, särskilt när det gäller dataskyddsmyndigheternas behörighet, uppgifter och befogenheter.

3) Styrelsens yttrande ska antas i enlighet med artikel 64.3 i dataskyddsförordningen, jämförd med artikel 10.2 i dataskyddsstyrelsens arbetsordning, inom åtta veckor från den första arbetsdag då ordföranden och den behöriga tillsynsmyndigheten har beslutat att akten är fullständig. Ordföranden får besluta att förlänga denna period med ytterligare sex veckor med hänsyn till ämnets komplexitet.

HÄRIGENOM AVGES FÖLJANDE YTTRANDE:

1 SAMMANFATTNING AV OMSTÄNDIGHETERNA

1. Den 3 december 2018 begärde den belgiska dataskyddsmyndigheten att Europeiska dataskyddsstyrelsen skulle undersöka och avge ett yttrande om samspelet mellan direktivet om e-integritet[1] och dataskyddsförordningen och lämnade in följande frågor:

   a. Vad gäller dataskyddsmyndigheternas[2] **behörighet, uppgifter och befogenheter**, var frågan om
      i. dataskyddsmyndigheter kan utöva sina behörigheter, utföra sina uppgifter och utöva sina befogenheter eller inte när det gäller behandling som omfattas av – åtminstone i förhållande till vissa behandlingsprocesser – det materiella tillämpningsområdet för både dataskyddsförordningen och direktivet om e-integritet, och i så fall om
      ii. dataskyddsmyndigheter kan eller bör beakta bestämmelserna i direktivet om e-integritet och/eller dess nationella tillämpningar när de utövar sin behörighet, utför sina uppgifter och utövar sina befogenheter i enlighet med dataskyddsförordningen (t.ex. när de utvärderar lagligheten i viss behandling), och i så fall, i vilken omfattning.
   b. Om **mekanismerna för samarbete och enhetlighet** kan eller bör tillämpas med avseende på behandling som omfattas av – åtminstone i förhållande till vissa behandlingsprocesser – det materiella tillämpningsområdet för både dataskyddsförordningen och direktivet om e-integritet.
   c. I vilken omfattning behandling **kan regleras genom bestämmelserna i både** direktivet om e-integritet och dataskyddsförordningen, och huruvida detta påverkar svaren på frågorna 1 och 2.

2. Styrelsen anser att dessa frågor har allmän räckvidd vad gäller tillämpningen av dataskyddsförordningen, eftersom det finns ett tydligt behov av att dataskyddsmyndigheterna gör en konsekvent tolkning av gränserna för deras behörighet, uppgifter och befogenheter. Ett förtydligande är särskilt angeläget bland annat för att säkerställa en konsekvent praxis för ömsesidigt bistånd i enlighet med artikel 61 i dataskyddsförordningen och gemensamma insatser i enlighet med artikel 62 i dataskyddsförordningen.

3. Detta yttrande hänför sig inte till någon uppdelning av dataskyddsmyndigheters behörighet, uppgifter och befogenheter enligt förslaget till förordning om integritet och elektronisk kommunikation.

[1] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) i dess ändrade lydelse enligt direktiv 2006/24/EG och direktiv 2009/136/EG.

[2] I enlighet med artiklarna 55–58 i dataskyddsförordningen. Termen *dataskyddsmyndigheter* (i motsats till *tillsynsmyndigheter*) kommer att användas i hela detta yttrande för att tydligt särskilja de *tillsynsmyndigheter* som avses i dataskyddsförordningen från andra typer av tillsynsmyndigheter, såsom de nationella regleringsmyndigheter som omnämns i direktiv 2002/58/EG.

2 RÄTTSLIG BAKGRUND

2.1 Relevanta bestämmelser i dataskyddsförordningen

4. Enligt artikel 2.1 är dataskyddförordningen tillämplig på ”sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register”.
I artikel 2.2 i dataskyddsförordningen föreskrivs att dataskyddsförordningen inte ska vara tillämplig vid behandling av personuppgifter vilka

> ”a) utgör ett led i en verksamhet som inte omfattas av unionsrätten,
>
> b) medlemsstaterna utför när de bedriver verksamhet som omfattas av avdelning V kapitel 2 i EU-fördraget,
>
> c) en fysisk person utför som ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll,
>
> d) behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten”.

5. Artikel 5, ”Principer för behandling av personuppgifter”, innehåller de principer som är tillämpliga på all behandling av personuppgifter, inklusive kravet om att alla personuppgifter ska behandlas på ett lagligt och korrekt vis.[3] Artikel 6 beskriver under vilka omständigheter som behandling av personuppgifter är laglig och en av punkterna berör den registrerades samtycke. I artikel 7 anges villkoren för giltigt samtycke i den mening som avses i dataskyddsförordningen.[4]

6. I artikel 51.1 fastställs dataskyddsmyndigheters rättsliga mandat, vilket är att övervaka tillämpningen av dataskyddsförordningen, i syfte att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandling samt att underlätta det fria flödet av sådana uppgifter inom unionen. Artiklarna 55, 57 och 58 beskriver närmare dataskyddsmyndigheternas behörighet, uppgifter och befogenheter. I kapitel VII i dataskyddsförordningen, ”Samarbete och enhetlighet”, anges de olika sätt på vilka dataskyddsmyndigheter ska samarbeta för att bidra till en konsekvent tillämpning av dataskyddsförordningen.

7. I artikel 94, ”Upphävande av direktiv 95/46/EG”, anges följande:

> ”1. Direktiv 95/46/EG ska upphöra att gälla med verkan från och med den 25 maj 2018.
>
> 2. Hänvisningar till det upphävda direktivet ska anses som hänvisningar till denna förordning. Hänvisningar till arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter, som inrättades genom artikel 29 i direktiv 95/46/EG, ska anses som hänvisningar till Europeiska dataskyddsstyrelsen, som inrättas genom denna förordning.”

[3] Se även skäl 39 i dataskyddsförordningen (”Varje behandling av personuppgifter måste vara laglig och rättvis. […]”).
[4] Se Artikel 29-gruppens riktlinjer om samtycke enligt förordning (EU) 2016/679, WP 259 rev.01, godkända av Europeiska dataskyddsstyrelsen den 25 maj 2018.

8. I artikel 95, ”Förhållande till direktiv 2002/58/EG”, fastställs följande:

> ”Denna förordning ska inte innebära några ytterligare förpliktelser för fysiska eller juridiska personer som behandlar personuppgifter inom ramen för tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster i allmänna kommunikationsnät i unionen, när det gäller områden inom vilka de redan omfattas av särskilda skyldigheter för samma ändamål i enlighet med direktiv 2002/58/EG.”

9. I skäl 173 i dataskyddsförordningen anges följande:

> ”(173) Denna förordning bör vara tillämplig på alla frågor som gäller skyddet av grundläggande rättigheter och friheter i förhållande till behandlingen av personuppgifter, vilka inte omfattas av särskilda skyldigheter med samma mål som anges i Europaparlamentets och rådets direktiv 2002/58/EG, däribland den personuppgiftsansvariges skyldigheter och fysiska personers rättigheter. För att klargöra förhållandet mellan denna förordning och direktiv 2002/58/EG bör det direktivet ändras. När denna förordning har antagits, bör direktiv 2002/58/EG ses över, framför allt för att säkerställa konsekvens med denna förordning”.

2.2 Relevanta bestämmelser i ramdirektivet

10. I artikel 2g i ramdirektivet[5] definieras *nationella regleringsmyndigheter* som

> ”ett eller flera organ som av en medlemsstat har fått i uppdrag att utföra någon av de regleringsuppgifter som fastställs i detta direktiv och i särdirektiven”.

11. I artikel 2l i ramdirektivet definieras *särdirektiv* som

> ”särdirektiv: direktiv 2002/20/EG (auktorisationsdirektivet), direktiv 2002/19/EG (tillträdesdirektivet), direktiv 2002/22/EG (direktivet om samhällsomfattande tjänster) och Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktivet om integritet och elektronisk kommunikation)”.

12. I artikel 3.1 i ramdirektivet anges följande:

> ”Medlemsstaterna skall säkerställa att alla uppgifter som åvilar de nationella regleringsmyndigheterna enligt detta direktiv och enligt särdirektiven fullgörs av ett behörigt organ.”

2.3 Relevanta bestämmelser i direktivet om e-integritet

13. I artikel 1.2 i direktivet om e-integritet fastställs följande:

> ”Bestämmelserna i detta direktiv skall precisera och komplettera [förordning (EU) 2016/679] i de syften som anges i paragraf 1. Bestämmelserna är vidare avsedda att skydda berättigade intressen för de abonnenter som är juridiska personer.”[6]

[5] Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektiv).

[6] Enligt artikel 94.2 i dataskyddsförordningen har alla hänvisningar till direktiv 95/46 i direktivet om e-integritet ersatts med [förordning (EU) 2016/679] och hänvisningar till arbetsgruppen för skydd av enskilda med avseende på behandling av personuppgifter som inrättades genom artikel 29 i direktiv 95/46/EG ersatts med [Europeiska dataskyddsstyrelsen].

14. I artikel 2f i direktivet om e-integritet fastställs följande:

> ”[S]amtycke: en användares eller abonnents samtycke motsvarar den registrerades samtycke i [förordning (EU) 2016/679].”

15. I artikel 15.2 i direktivet om e-integritet fastställs följande:

> ”Bestämmelserna om [rättslig prövning, ansvar och sanktioner i kapitel VIII] i [förordning (EU) 2016/679] skall gälla för de nationella bestämmelser som antas i enlighet med det här direktivet och för de individuella rättigheter som kan härledas från det här direktivet.”

16. I artikel 15.3 i direktivet om e-integritet fastställs följande:

> ”[Europeiska dataskyddsstyrelsen] skall också utföra de uppgifter som avses i [artikel 70 i förordning (EU) 2016/679] när det gäller frågor som omfattas av det här direktivet, nämligen skyddet av de grundläggande fri- och rättigheterna samt berättigade intressen inom sektorn för elektronisk kommunikation.”

17. I artikel 15a, ”Genomförande och efterlevnad”, fastställs följande:

> ”1. Medlemsstaterna ska besluta om systemet för påföljder, inklusive eventuella straffrättsliga sanktioner, som ska gälla överträdelser av de nationella bestämmelserna vid tillämpningen av detta direktiv samt vidta alla nödvändiga åtgärder för att säkerställa genomförandet av dessa. […]
>
> 2. Utan att det påverkar tillämpningen av eventuella tillgängliga rättsåtgärder ska medlemsstaterna se till att den behöriga nationella myndigheten och, där det är relevant, andra nationella organ har befogenhet att besluta att överträdelserna i punkt 1 ska upphöra.
>
> 3. Medlemsstaterna ska se till att behöriga nationella myndigheter och, där det är relevant, andra nationella organ har de nödvändiga undersökande befogenheterna och resurserna, inbegripet tillgång till all information de kan behöva, för att kunna övervaka de nationella bestämmelser som antagits i enlighet med detta direktiv och se till att de efterlevs.
>
> 4. De behöriga nationella regleringsmyndigheterna får anta åtgärder i syfte att säkerställa effektivt samarbete över gränserna för kontroll av efterlevnaden av de nationella lagar som antagits i enlighet med detta direktiv och för att skapa harmoniserade villkor för tillhandahållandet av tjänster som rör dataflöden över gränserna.
>
> I god tid innan sådana eventuella åtgärder antas ska de nationella regleringsmyndigheterna förse kommissionen med en sammanfattning av skälen, de planerade åtgärderna och det föreslagna tillvägagångssättet. Efter att ha undersökt denna information och efter att ha hört Enisa och [Europeiska dataskyddsstyrelsen], får kommissionen lämna synpunkter eller utfärda rekommendationer i frågan, framför allt i syfte att säkerställa att åtgärderna inte inverkar negativt på den inre marknadens funktion. De nationella regleringsmyndigheterna ska ta största möjliga hänsyn till kommissionens synpunkter eller rekommendationer när de fattar beslut om åtgärderna.”

18. I skäl 10 i direktivet om e-integritet anges följande:

> ”[Förordning (EU) 2016/679] är tillämplig på området för elektronisk kommunikation, i synnerhet beträffande alla de frågor avseende skydd av grundläggande fri- och rättigheter som inte särskilt omfattas av bestämmelserna i det här direktivet, inbegripet den registeransvariges

skyldigheter och enskilda personers rättigheter. [Förordning (EU) 2016/679] tillämpligt på de kommunikationstjänster som inte är offentliga.”

3 OMFATTNINGEN AV DETTA YTTRANDE

19. Syftet med dataskyddsförordningen är att skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter, samt att säkerställa det fria flödet av personuppgifter inom unionen.[7] För att uppnå detta syfte fastställer dataskyddsförordningen gemensamma regler om behandling av personuppgifter som ska säkra ett effektivt skydd av personuppgifter i unionen och förhindra avvikelser som hindrar den fria rörligheten av personuppgifter inom den inre marknaden. Reglerna syftar till att tillförsäkra en balans mellan de (potentiella) fördelarna med databehandling och de (potentiella) nackdelarna.

20. Direktivet om e-integritet syftar till att harmonisera nationella bestämmelser för att säkerställa ett likvärdigt skydd av de grundläggande fri- och rättigheterna, särskilt rätten till integritet och konfidentialitet, när det gäller behandling av personuppgifter inom sektorn för elektronisk kommunikation, samt för att säkerställa fri rörlighet för sådana uppgifter samt för utrustning och tjänster avseende elektronisk kommunikation inom gemenskapen.[8] Direktivet om e-integritet syftar därför till att säkra att de rättigheter som anges i artiklarna 7 och 8 i stadgan respekteras. Därför är direktivet om e-integritet ämnat att *precisera och komplettera* bestämmelserna i dataskyddsförordningen avseende behandling av personuppgifter inom elektronisk kommunikation.[9]

21. Frågorna som har hänskjutits till styrelsen är begränsade till behandling som omfattas av både dataskyddsförordningen och direktivet om e-integritet. För att tydligare definiera tillämpningsområdet för detta yttrande kommer nedanstående avsnitt att förtydliga följande:

- De fall i vilka det inte finns något samspel mellan dataskyddsförordningen och direktivet om e-integritet eftersom frågan inte omfattas av dataskyddsförordningen.
- De fall i vilka det inte finns något samspel mellan dataskyddsförordningen och direktivet om e-integritet eftersom frågan inte omfattas av direktivet om e-integritet.
- De fall i vilka det finns något samspel mellan dataskyddsförordningen och direktivet om e-integritet eftersom frågan faller inom det materiella tillämpningsområdet för både dataskyddsförordningen och direktivet om e-integritet.

[7] Artikel 1 i dataskyddsförordningen.
[8] Artikel 1.1 i direktivet om e-integritet.
[9] Artikel 1.1–1.2 i direktivet om e-integritet ska läsas mot bakgrund av artikel 94.2 i dataskyddsförordningen.

3.1 Frågor som inte omfattas av dataskyddsförordningen

22. I princip omfattar dataskyddsförordningens materiella tillämpningsområde all sorts behandling av personuppgifter, oavsett vilken teknik som används.[10] Dataskyddsförordningen ska inte vara tillämplig i följande fall:

- Om inga personuppgifter behandlas (ett telefonnummer till en juridisk persons automatiserade kundtjänst eller IP-adressen till en digital kopieringsapparat i ett företagsnätverk räknas inte som personuppgifter).
- Om verksamheten inte omfattas av dataskyddsförordningens materiella tillämpningsområde, med beaktande av artikel 2.2 och 2.3 i dataskyddsförordningen.
- Om verksamheten inte omfattas av dataskyddsförordningens territoriella tillämpningsområde.[11]

3.2 Frågor som inte omfattas av direktivet om e-integritet

23. Direktivet om e-integritet har två bestämmelser som har ett bredare tillämpningsområde än övriga bestämmelser, eftersom tillämpningsområdet för de övriga bestämmelserna är begränsat till elektroniska kommunikationstjänster i allmänna kommunikationsnät. Som framgår av följande avsnitt finns det följaktligen två frågor som behöver besvaras för att man ska kunna avgöra om en viss verksamhet faller inom det materiella tillämpningsområdet för direktivet om e-integritet.

3.2.1 Det allmänna materiella tillämpningsområdet för direktivet om e-integritet

24. Enligt artikel 3 i direktivet om e-integritet är direktivet tillämpligt på ”behandling av personuppgifter i samband med att allmänt tillgängliga elektroniska kommunikationstjänster tillhandahålls i allmänna kommunikationsnät inom gemenskapen, inbegripet allmänna kommunikationsnät som stöder datainsamling och identifieringsutrustning”.

25. Direktivet om e-integritet riktar sig alltså i första hand till allmänt tillgängliga elektroniska kommunikationstjänster och elektroniska kommunikationsnät.[12]
Enligt kodexen för elektronisk kommunikation[13] ska tjänster som är funktionellt likvärdiga med elektroniska kommunikationstjänster omfattas.

[10] Se även skäl 46 i direktivet om e-integritet.
[11] Artikel 3 i dataskyddförordningen. Europeiska dataskyddsstyrelsens riktlinjer 3/2018 om det territoriella tillämpningsområdet för den allmänna dataskyddsförordningen (artikel 3) av den 16 november 2018.
[12] Arbetsdokument från kommissionens avdelningar, *Ex-post REFIT evaluation of the ePrivacy Directive* 2002/58/EC, COM SWD(2017)005 rapport, s. 20 (ej översatt till svenska). Rapport till kommissionen: *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation*, SMART 2013/0071, s. 24 (ej översatt till svenska).
[13] Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation.

26. Det allmänna materiella tillämpningsområdet för direktivet om e-integritet är beroende av att samtliga följande villkor uppfylls:

- Det finns en elektronisk kommunikationstjänst[14].
- Tjänsten erbjuds via ett elektroniskt kommunikationsnät[15].
- Tjänsten och nätverket är allmänt tillgängliga[16].
- Tjänsten och nätverket erbjuds inom EU.

27. Verksamhet som inte uppfyller alla ovannämnda kriterier omfattas i allmänhet inte av direktivet om e-integritet.

Exempel:

Ett företagsnät som är tillgängligt enbart för anställda i yrkesutövningen räknas inte som en *allmänt tillgänglig* elektronisk kommunikationstjänst. Därför omfattas överföringen av platsuppgifter via ett sådant nätverk inte av det materiella tillämpningsområdet för direktivet om e-integritet. [17]

En tjänst för synkronisering av klockor skickar en signal via ett elektroniskt kommunikationsnät till alla klockor som följer dess synkroniseringsprotokoll (obestämt antal mottagare). Denna tjänst är i detta sammanhang en sändningstjänst och inte en kommunikationstjänst och omfattas alltså inte av tillämpningsområdet för direktivet om e-integritet.

[14] Artikel 2d i direktivet om e-integritet specificerar att *kommunikation* avser ”all information som utbyts eller överförs mellan ett begränsat antal parter genom en allmänt tillgänglig elektronisk kommunikationstjänst” och inte omfattar sändningstjänster för rundradio eller TV vilka – teoretiskt – kan nå en obegränsad publik. Termen *elektronisk kommunikationstjänst* definieras för närvarande i artikel 2d i ramdirektivet, men med verkan från den 21 december 2020 ska den definieras av artikel 2.4 i kodexen för elektronisk kommunikation.

[15] Termen *elektroniskt kommunikationsnät* definieras för närvarande i artikel 2a i ramdirektivet, men med verkan från den 21 december 2020 ska den definieras av artikel 2.1 i kodexen för elektronisk kommunikation.

[16] En tjänst för allmänheten är en tjänst som är tillgänglig för alla medborgare på samma grunder och inte enbart offentligt ägda tjänster. Jämför: Europeiska datatillsynsmannens yttrande 5/2016, Europeiska datatillsynsmannens preliminära yttrande om översynen av direktivet om integritet och elektronisk kommunikation (2002/58/EG), s. 12, och kommissionens meddelande till Europaparlamentet och rådet om status och genomförande av direktiv 90/388/EEG om konkurrens på marknaderna för teletjänster KOM (95) 113 slutlig, 4 april 1995, s. 14.

[17] Arbetsdokument från kommissionens avdelningar, *Ex-post REFIT evaluation of the ePrivacy Directive* 2002/58/EC, COM SWD(2017)005 rapport, s. 21 (ej översatt till svenska). , https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0005&from=EN Rapport till kommissionen: *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation*”, SMART 2013/0071, s. 14 (ej översatt till svenska). https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data

3.2.2 Det utvidgade materiella tillämpningsområdet för artiklarna 5.3 och 13 i direktivet om e-integritet

28. Det övergripande syftet med direktivet om e-integritet är att säkerställa skyddet av allmänhetens grundläggande rättigheter och friheter i samband med användningen av elektroniska kommunikationsnät.[18] Detta syfte gör artiklarna 5.3 och 13 tillämpliga på leverantörer av elektroniska kommunikationstjänster och webbplatsoperatörer (t.ex. i fråga om kakor) eller andra typer av affärsverksamheter (t.ex. i fråga om direktmarknadsföring).[19]

> Exempel:
>
> Sökmotorer som lagrar eller får tillgång till kakor på en användares enhet omfattas av det utökade materiella tillämpningsområdet för artikel 5.3 i direktivet om e-integritet.[20]
>
> Icke begärd e-post som skickas av en webbplatsoperatör i syfte att genomföra direktmarknadsföring omfattas också av det utökade materiella tillämpningsområdet för artikel 13 i direktivet om e-integritet.[21]

3.3 Frågor som faller inom det materiella tillämpningsområdet för både direktivet om e-integritet och dataskyddsförordningen

29. Det finns många exempel på behandling som faller inom det materiella tillämpningsområdet för både direktivet om e-integritet och dataskyddsförordningen. Ett tydligt exempel är användningen av kakor. I sitt yttrande om beteendebaserad reklam på internet anger artikel 29-gruppen att

> ”om, som ett resultat av lagring och hämtning av information genom en cookie eller liknande funktion, information som samlats in kan räknas som personuppgifter gäller, förutom artikel 5.3, även direktiv 95/46/EG.”.[22]

30. I Europeiska unionens domstols rättspraxis bekräftas att behandling kan omfattas av det materiella tillämpningsområdet för både direktivet om e-integritet och dataskyddsförordningen. I målet Wirtschaftsakademie[23] tillämpade EU-domstolen direktiv 95/46/EG trots att den bakomliggande behandlingen också inbegrep behandlingsprocesser som omfattades av det materiella

[18] I artikel 1.1 i direktivet om e-integritet anges följande: ”Genom detta direktiv möjliggörs en harmonisering av nationella bestämmelser för att säkerställa ett likvärdigt skydd av de grundläggande fri- och rättigheterna, särskilt rätten till integritet och konfidentialitet, när det gäller behandling av personuppgifter inom sektorn för elektronisk kommunikation, samt för att säkerställa fri rörlighet för sådana uppgifter samt för utrustning och tjänster avseende elektronisk kommunikation inom gemenskapen.”

[19] Artikel 29-arbetsgruppens yttrande 2/2010 om beteendebaserad reklam på Internet, 22 juni 2010, WP 171, avsnitt 3.2.1 s. 9. Artikel 29-arbetsgruppens yttrande 1/2008 om dataskyddsfrågor med anknytning till sökmotorer, WP 148, avsnitt 4.1.3 s.12. Rapport till kommissionen: *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation*”, SMART 2013/0071, s. 9 (ej översatt till svenska).

[20] Artikel 29-arbetsgruppens yttrande 1/2008 om dataskyddsfrågor med anknytning till sökmotorer, WP 148, avsnitt 4.1.3 s.12.

[21] Artikel 29-arbetsgruppens yttrande 1/2008 om dataskyddsfrågor med anknytning till sökmotorer, WP 148, avsnitt 4.1.3 s.12.

[22] Artikel 29-arbetsgruppens yttrande 2/2010 om beteendebaserad reklam på Internet, 22 juni 2010, WP 171, s. 9. Se också Artikel 29-gruppens yttrande 1/2008 om uppgiftsskyddsfrågor relaterade till sökmotorer, WP148, avsnitt 4.1.3 s.12–139

[23] Domstolens dom av den 5 juni 2018, C-210/16, ECLI:EU:C:2018:388. Se särskilt punkterna 33–34.

tillämpningsområdet för direktivet om e-integritet. I det pågående målet Fashion ID ansåg generaladvokaten att båda dessa uppsättningar regler kan vara tillämpliga i ett ärende som omfattar sociala insticksprogram och kakor.[24]

31. Även om dataskyddsförordningen ersatte direktiv 95/46/EG den 25 maj 2018, är den analys relevant som gjordes av Europeiska unionens domstol och artikel 29-gruppen enligt vilken båda rättsakterna kan tillämpas samtidigt. I skäl 30 i dataskyddsförordningen beskrivs definitionen av *nätidentifierare* på ett sätt som stöder tolkningen att behandlingen av personuppgifter kan omfattas av både dataskyddsförordningen och direktivet om e-integritet:

> ”Fysiska personer kan knytas till nätidentifierare som lämnas av deras utrustning, applikationer, verktyg och protokoll, t.ex. ip-adresser, kakor eller andra identifierare, som radiofrekvensetiketter. Detta kan efterlämna spår som, särskilt i kombination med unika identifierare och andra uppgifter som tas emot av servrarna, kan användas för att skapa profiler för fysiska personer och identifiera dem.”

32. Det är i synnerhet värt att notera att *ip-adresser* och *kakor* nämns i skäl 30, vilket anger att ip-adresser och kakor kan kombineras med andra *unika identifierare* och annan information mottagen av servrarna för att skapa profiler för fysiska personer.

33. Med andra ord innehåller dataskyddsförordningen, i tydliggörandet av sitt eget materiella tillämpningsområde (begreppet personuppgifter), en uttrycklig hänvisning till behandlingsverksamhet som också, åtminstone delvis, faller inom det materiella tillämpningsområdet för direktivet om e-integritet.

34. Ett annat exempel på en verksamhet som omfattas av både direktivet om e-integritet och dataskyddsförordningen är kundrelationen mellan leverantörer av elektroniska kommunikationstjänster och fysiska personer som är användare av dessa tjänster. Denna relation omfattar å ena sidan behandling av kunders personuppgifter men styrs å den andra också av särskilda regler för exempelvis abonnentregister, specificerade räkningar och nummerpresentation. Trafik- och platsuppgifter som genereras av elektroniska kommunikationstjänster kan också omfatta behandling av personuppgifter i den mån som de berör fysiska personer.

35. Slutligen bekräftas i artikel 95 i dataskyddsförordningen och skäl 173 i dataskyddsförordningen förhållandet *lex generalis/lex specialis* mellan dataskyddsförordningen och direktivet om e-integritet, eftersom det i artikel 95 föreskrivs att dataskyddsförordningen inte ska innebära några ytterligare förpliktelser för fysiska eller juridiska personer som behandlar personuppgifter inom ramen för tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster i allmänna kommunikationsnät i unionen, när det gäller områden inom vilka de redan omfattas av särskilda skyldigheter för samma ändamål i enlighet med direktivet om e-integritet.

***

36. Syftet med detta yttrande är att skapa klarhet vad gäller dataskyddsmyndigheternas behörighet, uppgifter och befogenheter med avseende på ärenden som omfattas av både direktivet om e-integritet och dataskyddsförordningen, vilket kort beskrivits i tidigare avsnitt. I följande avsnitt beskrivs

[24] Förslag till avgörande av generaladvokat Bobek i målet Fashion ID, C-40/17, föredraget den 19 december 2018, ECLI:EU:C:2018:1039. Se särskilt punkterna 111–115.

några fall där bestämmelserna i direktivet om e-integritet och dataskyddsförordningen samspelar och hur de olika reglerna anknyter till varandra.

4 SAMSPELET MELLAN DIREKTIVET OM E-INTEGRITET OCH DATASKYDDSFÖRORDNINGEN

37. Även om direktivet om e-integritet och dataskyddsförordningen har överlappande materiella tillämpningsområden leder detta inte nödvändigtvis till en regelkonflikt. Förutom att detta tydligt framgår vid en jämförelse av de olika bestämmelserna, förskrivs det också i artikel 1.2 i direktivet om e-integritet att ”[b]estämmelserna i detta direktiv skall precisera och komplettera direktiv 95/46/EG (…)”[25]. För att korrekt förstå samspelet mellan direktivet om e-integritet och dataskyddsförordningen är det nödvändigt att först klargöra innebörden av artikel 1.2 i direktivet om e-integritet. Efter detta ska innebörden och omfattningen av artikel 95 i dataskyddsförordningen klargöras.

4.1 Precisera

38. Ett antal bestämmelser i direktivet om e-integritet *preciserar* bestämmelserna i dataskyddsförordningen vad gäller behandling av personuppgifter inom den elektroniska kommunikationssektorn. Enligt principen *lex specialis derogat legi generali* har specialbestämmelser företräde framför allmänna regler i de situationer som specialbestämmelserna särskilt syftar till att reglera.[26] I situationer där direktivet om e-integritet *preciserar* (dvs. närmare beskriver) reglerna i dataskyddsförordningen ska (special)bestämmelserna i direktivet om e-integritet enligt *lex specialis* har företräde framför (de mer allmänna) bestämmelserna i dataskyddsförordningen.[27] All behandling av personuppgifter som inte specifikt regleras av direktivet om e-integritet (eller för vilken direktivet om e-integritet inte innehåller någon specialregel) ska dock också fortsättningsvis omfattas av dataskyddsförordningens bestämmelser.

39. Ett exempel på hur bestämmelserna i dataskyddsförordningen *preciseras* i direktivet om e-integritet återfinns i artikel 6 i direktivet om e-integritet, som avser behandling av så kallade *trafikuppgifter.* Vanligtvis kan behandlingen av personuppgifter motiveras på grundval av de grunder för laglig behandling som anges i artikel 6 i dataskyddsförordningen. Alla tänkbara skäl till behandling som anges i artikel 6 i dataskyddsförordningen kan dock inte tillämpas av leverantörer av elektroniska kommunikationstjänster för behandling av trafikuppgifter, eftersom artikel 6 i direktivet om e-integritet innehåller en uttrycklig begränsning av de villkor enligt vilka trafikuppgifter, inklusive personuppgifter, kan behandlas. I dessa fall måste de mer specifika bestämmelserna i direktivet om e-integritet ha företräde framför de mer allmänt hållna bestämmelserna i dataskyddsförordningen. Artikel 6 i direktivet om e-integritet innebär emellertid inte någon begränsning av tillämpningen av andra bestämmelser i dataskyddsförordningen, som t.ex. den registrerades rättigheter. Och den

[25] I artikel 94.2 i dataskyddsförordningen föreskrivs att hänvisningar till det upphävda direktiv 95/46 ska anses som hänvisningar till dataskyddsförordningen.
[26] Domstolens dom av den 22 april 2016 i förenade målen T-60/06 RENV II och T-62/06 RENV II, ECLI:EU:T:2016:233, punkt 81.
[27] Artikel 29-arbetsgruppens yttrande 2/2010 om beteendebaserad reklam på Internet, 22 juni 2010, WP 171, s. 10.

innebär inte heller att kravet på att personuppgifter ska behandlas på ett lagligt och korrekt sätt upphävs (artikel 5.1 a i dataskyddsförordningen).

40. En liknande situation uppstår med avseende på artikel 5.3 i direktivet om e-integritet så länge som informationen som lagras i slutanvändarens enhet utgör personuppgifter. I artikel 5.3 i direktivet om e-integritet anges att tidigare samtycke krävs för att få lagra information eller för att få tillgång till information som redan finns lagrad, i en abonnents eller användares terminalutrustning.[28] I den mån som informationen lagrad i slutanvändarens enhet utgör personuppgifter kommer artikel 5.3 i direktivet om e-integritet att ha företräde framför artikel 6 i dataskyddsförordningen i fråga om lagring av eller tillgång till denna information. Detta resultat liknar samspelet mellan artikel 6 i dataskyddsförordningen och artiklarna 9 och 13 i direktivet om e-integritet. I fall där dessa artiklar kräver samtycke för de specifika handlingar som beskrivs i artiklarna kan den personuppgiftsansvarige inte hänvisa till alla möjliga grunder för laglig behandling som anges i artikel 6 i dataskyddsförordningen.

41. En följd av principen om *lex specialis* är att man endast kan avvika från den allmänna regeln så länge som den lag som reglerar ett specifikt ämne innehåller en specialregel. Uppgifterna i ärendet måste noggrant analyseras för att avgöra hur långt det är möjligt att avvika, särskilt i fall där uppgifterna genomgår många olika typer av behandling – antingen parallellt eller i ordningsföljd.

> Exempel:
> En datamäklare ägnar sig åt profilering med utgångspunkt i information om individers surfvanor som har samlats in genom användning av kakor, men som också kan omfatta personuppgifter från andra källor (t.ex. *affärspartner*). I sådant fall måste en del av den berörda behandlingen, dvs. lagringen eller avläsningen av kakor, följa den nationella bestämmelse som införlivar artikel 5.3 i direktivet om e-integritet. Efterföljande behandling av personuppgifter, inklusive personuppgifter som samlats in med hjälp av kakor, måste även ha en grund för laglig behandling i enlighet med artikel 6 i dataskyddsförordningen för att vara tillåten.[29]

4.2 Komplettera

42. Direktivet om e-integritet innehåller även bestämmelser som *kompletterar* bestämmelserna i dataskyddsförordningen om behandling av personuppgifter inom sektorn för elektronisk kommunikation. Det finns t.ex. flera bestämmelser i direktivet om e-integritet som är avsedda att skydda *abonnenter* och *användare* av allmänt tillgängliga elektroniska kommunikationstjänster. Abonnenter av en allmänt tillgänglig elektronisk kommunikationstjänst kan vara antingen fysiska eller juridiska personer. Genom att komplettera dataskyddsförordningen skyddar direktivet om e-integritet inte bara fysiska personers grundläggande rättigheter, och särskilt deras rätt till integritetsskydd, utan även juridiska personers berättigade intressen.[30]

[28] Enligt artikel 5.3 är det också möjligt att lagra eller få tillgång till information som är lagrad i en abonnents eller användares terminalutrustning om det handlar om teknisk lagring eller åtkomst som endast sker för att utföra överföringen av en kommunikation via ett elektroniskt kommunikationsnät eller som är absolut nödvändig för att leverantören ska kunna tillhandahålla en av informationssamhällets tjänster som användaren eller abonnenten uttryckligen har begärt.
[29] Även om dataskyddsmyndigheter inte kan genomföra artikel 5.3 i direktivet om e-integritet (såvida inte nationell lagstiftning ger dem denna behörighet), bör de beakta att behandlingen som helhet omfattar specifik verksamhet som unionslagstiftningen har försökt skydda ytterligare för att undvika att detta skydd undergrävs.
[30] Skäl 12 i direktivet om e-integritet.

4.3 Innebörden i artikel 95 i dataskyddsförordningen

43. I artikel 95 i dataskyddsförordningen anges att dataskyddsförordningen ”inte ska [...] innebära några ytterligare förpliktelser för fysiska eller juridiska personer som behandlar personuppgifter inom ramen för tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster i allmänna kommunikationsnät i unionen, när det gäller områden inom vilka de redan omfattas av särskilda skyldigheter för samma ändamål i enlighet med direktiv 2002/58/EG” (understrykning tillagd).

44. Syftet med artikel 95 i dataskyddsförordningen är alltså att undvika onödiga administrativa bördor för personuppgiftsansvariga som annars skulle bli föremål för liknande men inte helt identiska administrativa bördor. Ett exempel som illustrerar tillämpningen av denna artikel rör skyldigheten att anmäla personuppgiftsincidenter, vilken fastställs i både direktivet om e-integritet[31] och dataskyddsförordningen[32]. I båda dessa rättsakter föreskrivs en skyldighet att garantera uppgifternas säkerhet och en skyldighet att anmäla personuppgiftsincidenter till den behöriga nationella myndigheten respektive till dataskyddsmyndigheten. Dessa skyldigheter är parallellt tillämpliga enligt dessa två olika rättsakter, i enlighet med deras respektive tillämpningsområden. En skyldighet att anmäla enligt båda rättsakter, dels i enlighet med dataskyddsförordningen och dels i enlighet med den nationella lagstiftningen om e-integritet, skulle tveklöst innebära en extra börda utan några direkta fördelar för uppgiftsskyddet. I enlighet med artikel 95 i dataskyddsförordningen är leverantörer av elektroniska kommunikationstjänster som har anmält en personuppgiftsincident i enlighet med tillämplig nationell lagstiftning om e-integritet inte skyldiga att separat underrätta dataskyddsmyndigheterna om samma incident i enlighet med artikel 33 i dataskyddsförordningen.

4.4 Samexistens

45. När det finns särskilda bestämmelser som reglerar en specifik behandlingsprocess eller en serie av behandlingsprocesser, ska de särskilda bestämmelserna vara tillämpliga (*lex specialis*), i andra fall (dvs. där det inte finns särskilda bestämmelser som reglerar en specifik behandlingsprocess eller en serie av behandlingsprocesser) kommer de allmänna reglerna att vara tillämpliga (*lex generalis*).

46. I skäl 173 i dataskyddsförordningen bekräftas att dataskyddsförordningen ska fortsätta att vara tillämplig på den behandling av personuppgifter som de särskilda skyldigheterna i direktivet om e-integritet inte kan tillämpas på:

> ”[A]lla frågor som gäller skyddet av grundläggande rättigheter och friheter i förhållande till behandlingen av personuppgifter, vilka inte omfattas av särskilda skyldigheter med samma mål som anges i Europaparlamentets och rådets direktiv 2002/58/EG, däribland den personuppgiftsansvariges skyldigheter och fysiska personers rättigheter.”[33]

47. I skäl 173 upprepas vad som redan anges i skäl 10 i direktivet om e-integritet. I skäl 10 föreskrivs följande: ”[Förordning (EU) 2016/679] är tillämplig på området för elektronisk kommunikation, i synnerhet beträffande alla de frågor avseende skydd av grundläggande fri- och rättigheter som inte

[31] Artikel 4 i direktivet om e-integritet.
[32] Artiklarna 32–34 i dataskyddsförordningen.
[33] I skäl 173 anges sedan ”[f]ör att klargöra förhållandet mellan denna förordning och direktiv 2002/58/EG bör det direktivet ändras. När denna förordning har antagits, bör direktiv 2002/58/EG ses över, framför allt för att säkerställa konsekvens med denna förordning”. Denna granskningsprocess pågår fortfarande.

särskilt omfattas av bestämmelserna i det här direktivet, inbegripet den registeransvariges skyldigheter och enskilda personers rättigheter.”

48. Till exempel måste en leverantör av ett allmänt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst följa nationella bestämmelser som införlivar artikel 6.2 i direktivet om e-integritet avseende trafikuppgifter när denna behandlar uppgifter som är nödvändiga för abonnentfakturering och betalning av samtrafikuppgifter. Eftersom det saknas särskilda bestämmelser i direktivet om e-integritet avseende t.ex. åtkomsträtt är dataskyddsförordningen tillämplig. I skäl 32 bekräftas att om leverantören av en elektronisk kommunikationstjänst eller av en mervärdestjänst lägger ut behandlingen av de personuppgifter som är nödvändiga för dessa tjänster på en underleverantör, bör denna underleverans och därpå följande behandling av uppgifterna fullt ut överensstämma med de krav för personuppgiftsansvariga och personuppgiftsbiträden när det gäller personuppgifter som fastställs i dataskyddsförordningen.

***

49. I de föregående avsnitten beskrivs hur bestämmelserna i direktivet om e-integritet och dataskyddsförordningen interagerar avseende behandling som omfattas av båda akternas materiella tillämpningsområden.
I de närmast följande avsnitten ligger fokus på att lösa de frågor som hänskjutits till styrelsen när det gäller dataskyddsmyndigheternas behörighet, uppgifter och befogenheter i fall som åtminstone delvis omfattas av direktivet om e-integritet.

5 DATASKYDDSMYNDIGHETERNAS BEHÖRIGHET, UPPGIFTER OCH BEFOGENHETER

50. Den belgiska myndigheten hänsköt två frågor om dataskyddsmyndigheternas behörighet, uppgifter och befogenheter – fastställda i artiklarna 55–58 i dataskyddsförordningen – till styrelsen, vilka kan omformuleras på följande vis:

- Begränsar enbart det faktum att behandlingen av personuppgifter faller inom det materiella tillämpningsområdet för både dataskyddsförordningen och direktivet om e-integritet dataskyddsmyndigheternas behörighet, uppgifter och befogenheter i enlighet med dataskyddsförordningen? Finns det, med andra ord, en undergrupp av behandlingsprocesser som bör undantas från datamyndigheternas bedömning, och i så fall i vilken utsträckning?
- Bör dataskyddsmyndigheter beakta bestämmelserna i direktivet om e-integritet när de utövar sin behörighet, utför sina uppgifter och utövar sina befogenheter i enlighet med dataskyddsförordningen (t.ex. när de utvärderar behandlingens laglighet), och i så fall, i vilken omfattning? Bör, med andra ord, överträdelser av nationella regler om e-integritet beaktas eller lämnas utan beaktande vid bedömningen av efterlevnad av dataskyddsförordningen. Om ja, under vilka omständigheter?

51. Till att börja med bör det noteras att medlemsstaterna är skyldiga att säkerställa unionsrättens fulla verkan, särskilt genom att tillhandahålla lämpliga genomförandemekanismer. Denna skyldighet

grundar sig på principen om lojalt samarbete som fastställs i artikel 4.3 i EUF-fördraget.[34] I de närmast följande avsnitten beskrivs kort genomförandebestämmelserna i dataskyddsförordningen och direktivet om e-integritet samt samspelet mellan dessa.

5.1 Genomförande av dataskyddsförordningen

52. I dataskyddsförordningen föreskrivs att dess bestämmelser ska genomföras av oberoende dataskyddsmyndigheter. Här ska även noteras att artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad *stadgan*) föreskriver att behandling av personuppgifter ska kontrolleras av en oberoende myndighet:

> ”**Artikel 8, Skydd av personuppgifter**
>
> 1. Var och en har rätt till skydd av de personuppgifter som rör honom eller henne.
>
> 2. Dessa uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem.
>
> 3. **En oberoende myndighet ska kontrollera** att **dessa** regler efterlevs.”

53. Artikel 51.1 i dataskyddsförordningen fastställer dataskyddsmyndigheternas rättsliga mandat, vilket är att övervaka tillämpningen av dataskyddsförordningen, i syfte att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandling samt att underlätta det fria flödet av uppgifter inom unionen.

54. Dataskyddsförordningen innehåller ett undantag och en möjlighet att avvika från detta mandat:

- Tillsynsmyndigheterna ska inte vara behöriga att utöva tillsyn över domstolar som behandlar personuppgifter i sin dömande verksamhet *(*artikel 55.3, dataskyddsförordningen).
- Medlemsstaterna kan för behandling som sker för journalistiska ändamål, eller för akademiskt, konstnärligt eller litterärt skapande, fastställa undantag eller avvikelser från bland annat kapitel VI (oberoende tillsynsmyndigheter) samt kapitel VII (samarbete och enhetlighet) i dataskyddsförordningen (artikel 85, dataskyddsförordningen).

Dessutom kan dataskyddsmyndigheters befogenheter utökas i enlighet med artikel 58.6 i dataskyddsförordningen. Myndigheterna kan i synnerhet tilldelas befogenhet att bötfälla offentliga myndigheter och organ om en medlemsstat föreskriver detta i den nationella lagstiftningen (artikel 83.7, dataskyddsförordningen).

Eftersom det rör sig om undantag från den allmänna regeln ska dessa bestämmelser tolkas snävt.

[34] I artikel 4.3 i EUF-fördraget föreskivs följande: ”Enligt principen om lojalt samarbete ska unionen och medlemsstaterna respektera och bistå varandra när de fullgör de uppgifter som följer av fördragen.
Medlemsstaterna ska vidta alla lämpliga åtgärder, både allmänna och särskilda, för att säkerställa att de skyldigheter fullgörs som följer av fördragen eller av unionens institutioners akter.
Medlemsstaterna ska hjälpa unionen att fullgöra sina uppgifter, och de ska avstå från varje åtgärd som kan äventyra fullgörandet av unionens mål.”

55. I de fall där dataskyddsförordningen innehåller begränsningar eller medger avvikelser avseende dataskyddsmyndigheternas behörighet, uppgifter och befogenheter görs detta uttryckligen. Dataskyddsförordningen hindrar dessutom inte på något sätt dataskyddsmyndigheter ifrån att utöva sin behörighet, utföra sina uppgifter och utöva sina befogenheter vad gäller behandling så länge som den omfattas av dataskyddsförordningens materiella tillämpningsområde. Frågan är därför om unionslagstiftaren avsett eller tillåtit avvikelser gällande dataskyddsmyndigheternas allmänna behörighet vad gäller ärenden där bestämmelserna i direktivet om e-integritet är tillämpliga på den aktuella behandlingen.

5.2 Genomförande av direktivet om e-integritet

56. Genomförandet av bestämmelserna i direktivet om e-integritet är nära sammankopplat med ramdirektivet[35], enligt vars artikel 3.1 det fastslås att ”[m]edlemsstaterna skall säkerställa att alla uppgifter som åvilar de nationella regleringsmyndigheterna enligt detta direktiv och enligt särdirektiven fullgörs av ett behörigt organ[36]”.

57. I Artikel 2g i ramdirektivet definieras *nationell regleringsmyndighet* som

> ”ett eller flera organ som av en medlemsstat har fått i uppdrag att utföra någon av de regleringsuppgifter som fastställs i detta direktiv och i särdirektiven”.

58. Medlemsstaterna har valt olika sätt att tilldela en eller flera enheter uppgiften att genomföra nationella bestämmelser om e-integritet.[37] Denna stora variation är möjlig eftersom direktivet om e-integritet endast fastställer vissa allmänna mål som ska uppnås av medlemsstaterna i denna fråga.

59. Direktivet om e-integritet innehåller ingen bestämmelse om att endast ett nationellt organ ska ha behörighet att genomföra dess bestämmelser. I artikel 15a i direktivet om e-integritet anges i själva verket uttryckligen att mer än ett nationellt organ kan vara behörigt att genomföra dess bestämmelser. I artikel 15a föreskrivs också att medlemsstater ska tillämpa och genomföra direktivet, inklusive skyldigheten att medlemsstater ska fastställa regler om påföljder, tilldela befogenheter, ålägga upphörande av överträdelser, tilldela utredningsbefogenheter och resurser osv. enligt följande:

> ”1. Medlemsstaterna ska besluta om systemet för påföljder, inklusive eventuella straffrättsliga sanktioner, som ska gälla överträdelser av de nationella bestämmelserna vid tillämpningen av detta direktiv samt vidta alla nödvändiga åtgärder för att säkerställa genomförandet av dessa. Påföljderna som då fastställs bör vara effektiva, proportionerliga och avskräckande och kan tillämpas för att täcka den tid då lagöverträdelsen varar, även om dessa senare rättats till. Medlemsstaterna skall anmäla bestämmelserna till kommissionen senast den 25 maj 2011 och

[35] Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektiv), i dess ändrade lydelse.
[36] I artikel 2l i ramdirektivet klargörs att ”särdirektiv: direktiv 2002/20/EG (auktorisationsdirektivet), direktiv 2002/19/EG (tillträdesdirektivet), direktiv 2002/22/EG (direktivet om samhällsomfattande tjänster) och Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktivet om integritet och elektronisk kommunikation)”.
[37] Rapport till kommissionen: *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation*, SMART 2013/0071, s. 33 (ej översatt till svenska).

skall utan dröjsmål underrätta kommissionen om alla eventuella senare ändringar av dessa bestämmelser.

2. Utan att det påverkar tillämpningen av eventuella tillgängliga rättsåtgärder ska medlemsstaterna se till att den behöriga nationella myndigheten **och, där det är relevant, andra nationella organ** har befogenhet att besluta att överträdelserna i punkt 1 ska upphöra.

3. Medlemsstaterna ska se till att behöriga nationella myndigheter **och, där det är relevant, andra nationella organ** har de nödvändiga undersökande befogenheterna och resurserna, inbegripet tillgång till all information de kan behöva, för att kunna övervaka de nationella bestämmelser som antagits i enlighet med detta direktiv och se till att de efterlevs.

4. De behöriga nationella regleringsmyndigheterna får anta åtgärder i syfte att säkerställa effektivt samarbete över gränserna för kontroll av efterlevnaden av de nationella lagar som antagits i enlighet med detta direktiv och för att skapa harmoniserade villkor för tillhandahållandet av tjänster som rör dataflöden över gränserna."

60. Dessutom innehåller artikel 15.2 i direktivet om e-integritet en bestämmelse som hänvisar till bestämmelserna i direktiv 95/46/EG om rättslig prövning, ansvar och sanktioner som nu ska läsas som en hänvisning till dataskyddsförordningen:

> "Bestämmelserna om rättslig prövning, ansvar och sanktioner i kapitel III i direktiv 95/46/EG skall gälla för de nationella bestämmelser som antas i enlighet med det här direktivet och för de individuella rättigheter som kan härledas från det här direktivet."

61. I artikel 15.3 i direktivet om e-integritet föreskrivs också följande:

> "Den arbetsgrupp för skydd av enskilda med avseende på behandling av personuppgifter som inrättades genom artikel 29 i direktiv 95/46/EG skall också utföra de uppgifter som avses i artikel 30 i det direktivet när det gäller frågor som omfattas av det här direktivet, nämligen skyddet av de grundläggande fri- och rättigheterna samt berättigade intressen inom sektorn för elektronisk kommunikation."[38]

5.3 Genomförande där dataskyddsförordningen och direktivet om e-integritet överlappar varandra

62. Genom direktivet om e-integritet preciseras och kompletteras dataskyddsförordningen. Dessutom hänvisar det till förordningens bestämmelser om rättslig prövning, ansvar och sanktioner (artikel 15.2 i direktivet om e-integritet tolkad mot bakgrund av dataskyddsförordningens artikel 94).

[38] I artikel 15.3 i direktivet om e-integritet föreskrivs följande: "Den arbetsgrupp för skydd av enskilda med avseende på behandling av personuppgifter som inrättades genom artikel 29 i direktiv 95/46/EG skall också utföra de uppgifter som avses i artikel 30 i det direktivet när det gäller frågor som omfattas av det här direktivet, nämligen skyddet av de grundläggande fri- och rättigheterna samt berättigade intressen inom sektorn för elektronisk kommunikation."
I artikel 94.2 i dataskyddsförordningen föreskrivs att "hänvisningar till det upphävda direktivet ska anses som hänvisningar till denna förordning. Hänvisningar till arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter, som inrättades genom artikel 29 i direktiv 95/46/EG, ska anses som hänvisningar till Europeiska dataskyddsstyrelsen, som inrättas genom denna förordning".
Därför tolkas hänvisningen till artikel 30 i direktiv 95/46 som en hänvisning till de relevanta styckena i artikel 70 i dataskyddsförordningen (Styrelsens uppgifter).

5.3.1 Fråga ett: Saknar dataskyddsmyndigheter behörighet att bedöma vissa behandlingsprocesser?

- *Begränsar enbart det faktum att behandlingen av personuppgifter faller inom det materiella tillämpningsområdet för både dataskyddsförordningen och direktivet om e-integritet dataskyddsmyndigheternas behörighet, uppgifter och befogenheter i enlighet med dataskyddsförordningen? Med andra ord, finns det en undergrupp av behandlingsprocesser som bör undantas från datamyndigheternas bedömning, och i så fall, vilka behandlingsprocesser är det som ska undantas?*

63. I enlighet med dataskyddsförordningen måste medlemsstaterna ha utsett en eller flera tillsynsmyndigheter. Medlemsstaterna kan ha utsett samma myndighet som behörig för (en del av) genomförandet av den nationella tillämpningen av direktivet om e-integritet, men kan också ha valt en eller flera andra myndigheter, t.ex. en nationell tillsynsmyndighet inom telekommunikationsområdet, en konsumentskyddsorganisation, eller ett departement.

64. Direktivet om e-integritet ger medlemsstaterna utrymme att bestämma vilken myndighet eller vilket organ som ska ansvara för genomförandet av direktivets bestämmelser.

65. Medan direktivet om e-integritet hänvisar till bestämmelserna i dataskyddsförordningen vad gäller rättslig prövning, ansvar och sanktioner (artikel 15.2 i direktivet om e-integritet), anger artikel 15a.1 i direktivet om e-integritet sina bestämmelser om genomförande och efterlevnad. I exempelvis artikel 15a.1 föreskrivs att ”medlemsstaterna ska besluta om systemet för påföljder, inklusive eventuella straffrättsliga sanktioner, som ska gälla överträdelser av de nationella bestämmelserna vid tillämpningen av detta direktiv samt vidta alla nödvändiga åtgärder för att säkerställa genomförandet av dessa”. Direktivet om e-integritet ger uttryckligen medlemsstaterna ett utrymme att efter eget gottfinnande besluta om påföljder, och artikel 15.2 inkräktar inte på det utrymme för egenbestämmande som erbjuds medlemsstaterna när det gäller genomförandet (dvs. att avgöra vem som ska genomföra bestämmelserna i direktivet om e-integritet).[39]

66. Om nationell lagstiftning ger dataskyddsmyndigheten behörighet att genomföra direktivet om e-integritet så bör lagen också fastställa dataskyddsmyndighetens uppgifter och befogenheter i samband med genomförandet av detta direktiv. Dataskyddsmyndigheten kan inte automatiskt förlita sig på uppgifter och befogenheter i dataskyddsförordningen om de vill vidta årgärder för att genomföra nationella bestämmelser om e-integritet. Dataskyddsförordningens uppgifter och befogenheter i är knutna till genomförandet av dataskyddsförordningen. Nationell lagstiftning kan medge uppgifter och befogenheter inspirerade av dataskyddsförordningen, men kan också medge andra uppgifter och befogenheter till dataskyddsmyndigheten för att denna ska kunna genomföra nationella bestämmelser om e-integritet i enlighet med artikel 15a i direktivet om e-integritet.

[39] Observera att artikel 15a.1 i direktivet om e-integritet infördes av direktiv 2009/136/EG (dvs. en ändring av direktivet om e-integritet).

67. Utrymmet för egenbestämmande existerar enbart enligt de krav och gränser som har fastställs i överordnade rättsregler. Artikel 8.3 i stadgan kräver att efterlevnad av regler om skydd av personuppgifter ska kontrolleras av en oberoende myndighet.[40]

68. När behandling av personuppgifter faller inom det materiella tillämpningsområdet för både dataskyddsförordningen och direktivet om e-integritet är dataskyddsmyndigheter endast behöriga att beakta de undergrupper av behandling som styrs av nationella regler som införlivar direktivet om e-integritet om den nationella lagstiftningen ger dem denna behörighet. Dataskyddsmyndigheternas behörighet enligt dataskyddsförordningen förblir dock oförändrad med avseende på behandlingsprocesser som inte omfattas av specialregler i direktivet om e-integritet. Denna demarkationslinje får inte modifieras av nationell lagstiftning som införlivar direktivet om e-integritet (t.ex. genom att utöka det materiella tillämpningsområdet utöver vad direktivet om e-integritet kräver och ge den nationella regleringsmyndigheten exklusiv behörighet).

69. Dataskyddsmyndigheter är behöriga att genomföra dataskyddsförordningen. Det faktum att en del av behandlingen omfattas av direktivet om e-integritet begränsar inte dataskyddsmyndigheters behörighet enligt dataskyddsförordningen.

70. Om en annan myndighet än dataskyddsmyndigheten har fått exklusiv behörighet avgör den nationella processrätten vad som ska hända om registrerade ändå lämnar in klagomål till dataskyddsmyndigheten om exempelvis behandling av personuppgifter i form av trafik- eller lokaliseringsuppgifter, icke begärd elektronisk kommunikation eller insamling av personuppgifter genom användning av kakor utan att även klaga på en (potentiell) överträdelse av reglerna i dataskyddsförordningen.

5.3.2 Fråga två: Saknar dataskyddsmyndigheter behörighet att beakta nationella bestämmelser från direktivet om e-integritet?

- *Bör dataskyddsmyndigheter beakta bestämmelserna i direktivet om e-integritet när de utövar sin behörighet, utför sina uppgifter och utövar sina befogenheter i enlighet med dataskyddsförordningen* (t.ex. när de utvärderar behandlingens lagligheten)*, och i så fall, i vilken omfattning? Bör, med andra ord, överträdelser av nationella regler om e-integritet beaktas eller lämnas utan beaktande vid bedömningen av efterlevnaden av dataskyddsförordningen? Om ja, under vilka omständigheter?*

71. Ett exempel illustrerar skillnaden i jämförelse med fråga ett. Tänk på en datamäklare som ägnar sig åt profilering med utgångspunkt i information som denna fått från två olika källor. Från den första källan kommer uppgifter om enskildas surfvanor som samlats in genom användning av kakor och/eller annan produktidentifiering. Den andra källan hämtas från affärspartner som delar uppgifter om deltagare i pristävlingar eller bonusprogram.

[40] Rättspraxis från europeiska unionens domstol gällande artikel 28 i direktiv 95/46 har klargjort kraven vad gäller oberoende: se t.ex. domstolens dom av den 9 mars 2010, C-518/07, (Europeiska kommissionen mot Förbundsrepubliken Tyskland), punkt 17 ff; Domstolens dom av den 16 oktober 2012 i mål C-614/10 (Europeiska kommissionen mot Republiken Österrike), punkt 36 ff; Domstolens dom av den 6 oktober 2015 i mål C-362/14 (Safe Harbor), punkt 41 ff; Domstolens dom av den 21 december 2016 i mål C-203/15 och C-698/15 (Tele2/Watson), punkt 123.

72. Profilering av enskilda personer med utgångspunkt i personuppgifter omfattas normalt sett av dataskyddsförordningen och därmed också av dataskyddsmyndigheters behörighet. Om det till en dataskyddsmyndighet inkommer ett klagomål om datamäklarens profileringsverksamhet, vilken hänsyn bör dataskyddsmyndigheten då ta med avseende på särskilda regler, i detta fall nationella regler om e-integritet, vid bedömningen av efterlevnaden av dataskyddsförordningen?

73. Det bör noteras att direktivet om e-integritet är ett specifikt exempel på en lag som erbjuder ett särskilt skydd för vissa kategorier av uppgifter som kan vara personuppgifter. Andra rättsakter ger också ett särskilt skydd för specifika typer av uppgifter som av olika skäl kan vara personuppgifter (t.ex. behandlingens kontext, uppgifternas art eller riskerna för de registrerade).[41]

74. Medlemsstaterna är skyldiga att utse en eller flera myndigheter med ansvar för att övervaka efterlevnaden av den nationella lagstiftning som införlivar direktivet om e-integritet. Dessa myndigheter ansvarar därefter för att genomföra denna lag. Den nationella lag som införlivar direktivet om e-integritet är tillämplig på de specifika behandlingsprocesser som regleras av direktivet om e-integritet (t.ex. en behandlingsprocess som består av lagring av eller tillgång till information som lagras på slutanvändarens enhet).

75. Om dataskyddsmyndigheterna inte fått sådan behörighet genom nationell lagstiftning kan de inte se till att bestämmelserna i (den nationella lagstiftning som tillämpar) direktivet om e-integritet genomförs när de utövar sin behörighet i enlighet med dataskyddsförordningen. Som nämns ovan kan dock behandling av personuppgifter som inbegriper processer som faller inom det materiella tillämpningsområdet för direktivet om e-integritet inbegripa ytterligare aspekter för vilka direktivet om e-integritet inte innehåller någon specialregel. T.ex. innehåller artikel 5.3 i direktivet om e-integritet en specialregel om att lagra, eller få tillgång till information som redan finns lagrad, i en slutanvändares terminalutrustning. Direktivet innehåller inte någon specialregel om någon föregående eller senare behandling (t.ex. lagring och analys av uppgifter om surfning i syften som rör beteendestyrd annonsering på nätet eller säkerhet). Dataskyddsmyndigheter är därför fortfarande fullt behöriga att bedöma lagenligheten för alla andra behandlingsprocesser som sker i samband med lagringen av eller tillgången till information på slutanvändarens terminalutrustning.[42]

---

[41] Ett exempel på detta finns i finanssektorn: Uppgifter som används för att bedöma en persons kreditvärdighet och uppgifter om offentliggörandet av administrativa sanktioner omfattas av särskilt skydd. Se: Artikel 21.1 i Europaparlamentets och rådets direktiv 2014/17/EU av den 4 februari 2014 om konsumentkreditavtal som avser bostadsfastighet och om ändring av direktiven 2008/48/EG och 2013/36/EU och förordning (EU) nr 1093/2010; Artiklarna 68–69 i Europaparlamentets och rådets direktiv 2013/36/EU av den 26 juni 2013 om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut och värdepappersföretag, om ändring av direktiv 2002/87/EG och om upphävande av direktiv 2006/48/EG och 2006/49/EG.
Ett annat exempel finns i reglerna om kliniska prövningar: Se artiklarna 28–35 i Europaparlamentets och rådets förordning (EU) nr 536/2014 av den 16 april 2014 om kliniska prövningar av humanläkemedel och om upphävande av direktiv 2001/20/EG.

[42] I detta avseende bör det hänvisas till artikel 29-arbetsgruppens yttrande om berättigade intressen (06/2014) och artikel 29-gruppens yttrande om ändamålsbegränsning (yttrande 03/2013), där det klargörs att vissa former av beteendestyrd annonsering kräver samtycke från den registrerade, inte bara i enlighet med artikel 5.3. I yttrandet om ändamålsbegränsning anges följande:
Det andra möjliga scenariot är när en organisation specifikt vill analysera eller förutsäga personliga preferenser, beteende och attityder hos enskilda kunder, vilka senare kommer att styra ”åtgärder eller beslut” som tas avseende dessa kunder. I dessa fall skulle det nästan alltid krävas ett fritt, specifikt, informerat och tydligt aktivt

76. En överträdelse av dataskyddsförordningen kan också utgöra en överträdelse av nationella bestämmelser om e-integritet. Dataskyddsmyndigheten kan beakta dessa iakttagelser när det gäller en överträdelse av bestämmelserna i direktivet om e-integritet vid tillämpningen av dataskyddsförordningen (t.ex. vid bedömningen av efterlevnad med principen om laglighet och korrekthet enligt artikel 5.1 i dataskyddsförordningen). Alla genomförandebeslut måste dock motiveras med utgångspunkt i dataskyddsförordningen om inte dataskyddsmyndigheten har getts ytterligare behörighet i enlighet med medlemsstaternas lagstiftning.

77. Om dataskyddsmyndigheten utses till behörig myndighet enligt nationell lagstiftning med stöd i direktivet om e-integritet, har myndigheten behörighet att direkt genomföra nationella bestämmelser om e-integritet utöver att också genomföra dataskyddsförordningen (utan behörighet är detta inte möjligt).

78. Generellt gäller att i de fall där flera myndigheter är behöriga för de olika rättsliga instrumenten bör de se till att genomförandet av instrumenten är konsekvent. Detta bland annat för att undvika att bryta mot principen *non bis in idem* i fall där överträdelser mot bestämmelserna i dataskyddsförordningen och i direktivet om e-integritet, som har ägt rum inom ramen av en behandlingsaktivitet, är nära sammankopplade med varandra.

6 OM TILLÄMPLIGHETEN AV MEKANISMERNA FÖR SAMARBETE OCH ENHETLIGHET

79. Den tredje frågan från den belgiska dataskyddsmyndigheten till styrelsen kan sammanfattas på följande sätt:

- *I vilken omfattning är mekanismerna för samarbete och enhetlighet tillämpliga vad gäller behandling som – åtminstone i förhållande till vissa behandlingsprocesser – faller inom det materiella tillämpningsområdet för både dataskyddsförordningen och direktivet om e-integritet?*

80. I enlighet med kapitel VII i dataskyddsförordningen ska de mekanismer för samarbete och enhetlighet som är tillgängliga för dataskyddsmyndigheter i enlighet med dataskyddsförordningen röra översynen av hur bestämmelserna i dataskyddsförordningen tillämpas. Dataskyddsförordningens mekanismer är inte tillämpliga på bestämmelserna i direktivet om e-integritet som sådant.

81. Artikel 15.3 i direktivet om e-integritet föreskrivs följande:

> ”[Europeiska dataskyddsstyrelsen] skall också utföra de uppgifter som avses i [artikel 70 i förordning (EU) 2016/679] när det gäller frågor som omfattas av det här direktivet, nämligen

samtycke för att senare användning ska anses vara förenlig med fördraget. Det är viktigt att notera att sådant samtycke bör krävas för t.ex. spårning och profilering i syfte att genomföra direkt marknadsföring, beteendestyrd annonsering, datamäklares försäljning av uppgifter, platsbaserad annonsering eller spårningsbaserade digitala marknadsundersökningar.
I yttrandet om legitima intressen anges följande:
”I stället för att bara erbjuda en möjlighet att välja att avstå från denna typ av profilering och riktad reklam är det enligt artikel 7 a, men även enligt artikel 5.3 i direktivet om integritet och elektronisk kommunikation, nödvändigt att inhämta ett informerat samtycke. Följaktligen bör artikel 7 f inte kunna åberopas som rättslig grund för behandlingen.”

skyddet av de grundläggande fri- och rättigheterna samt berättigade intressen inom sektorn för elektronisk kommunikation.”

82. Vad gäller samarbete mellan myndigheter med behörighet att genomföra direktivet om e-integritet föreskrivs i artikel 15a.4 i direktivet om e-integritet att ”de behöriga nationella regleringsmyndigheterna får anta åtgärder i syfte att säkerställa effektivt samarbete över gränserna för kontroll av efterlevnaden av de nationella lagar som antagits i enlighet med detta direktiv och för att skapa harmoniserade villkor för tillhandahållandet av tjänster som rör dataflöden över gränserna”.

83. Sådant gränsöverskridande samarbete mellan de myndigheter som är behöriga att genomföra direktivet om e-integritet, inklusive dataskyddsmyndigheter, nationella regleringsmyndigheter och andra myndigheter kan ske i den omfattning som relevanta nationella regleringsmyndigheter antar åtgärder som tillåter ett sådant samarbete.

84. Det bör dock noteras att mekanismen för samarbete och enhetlighet förblir till fullo tillämplig i den mån som behandlingen omfattas av de allmänna bestämmelserna i dataskyddsförordningen (och inte av en specialregel i direktivet om e-integritet). Även om exempelvis behandlingen av personuppgifter (t.ex. profilering) delvis bygger på tillgång till information lagrad på slutanvändarens enhet, hämtas ur dataskyddsförordningen de regler om personuppgiftsskydd som inte finns i direktivet om e-integritet (t.ex. den registrerades rättigheter och behandlingsprinciper) vad gäller den behandling av personuppgifter som sker efter tillgången till informationen lagrad på slutanvändarens enhet. Alltså ska sådan behandling omfattas av dataskyddsförordningens bestämmelser, inklusive mekanismerna för samarbete och enhetlighet.

85. I praktiken kommer dataskyddsmyndigheter att noggrant få välja vilka kommunikationsvägar de ska använda, särskilt om de inte bara tillämpar dataskyddsförordningen utan även är behöriga att genomföra (en del av) den nationella lagstiftning som införlivar direktivet om e-integritet. Den normala kommunikationsvägen – som beskrivs i kapitel VII (Samarbete och enhetlighet) i dataskyddsförordningen – ska användas för alla eventuella delar av ett förfarande som är avsett att använda den genomförandebefogenhet som tilldelas i enlighet med dataskyddsförordningen som ett svar på en överträdelse av dataskyddsförordningen.
Den skönsmässigt valda kommunikationsvägen kan användas av dataskyddsmyndigheter inom ramen för de särskilda genomförandebefogenheter fastställda genom nationell lagstiftning som införlivar direktivet om e-integritet och får endast användas så länge som förfarandet syftar till att bemöta överträdelser mot nationella bestämmelser om e-integritet vilka styr det specifika beteenden som regleras av direktivet om e-integritet. Så snart ärendet berör frågor som omfattas av dataskyddsförordningen, är dataskyddsmyndigheter skyldiga att tillämpa den mekanism för samarbete och enhetlighet som föreskrivs i dataskyddsförordningen.

7 SLUTSATS

- *Begränsar enbart det faktum att behandlingen av personuppgifter faller inom det materiella tillämpningsområdet för både dataskyddsförordningen och direktivet om e-integritet dataskyddsmyndigheternas behörighet, uppgifter och befogenheter i enlighet med dataskyddsförordningen? Finns det, med andra ord, en undergrupp av behandlingsprocesser som inte bör övervägas, och i så fall när?*

86. När behandlingen av personuppgifter omfattas av både dataskyddsförordningen och direktivet om e-integritet är dataskyddsmyndigheter behöriga att granska behandlingsprocesser som styrs av nationella regler om e-integritet enbart om de har denna behörighet enligt nationell lagstiftning. Sådan granskning måste dessutom ske inom de tillsynsbefogenheter som myndigheten har enligt den nationella lag som införlivar direktivet om e-integritet.

87. Dataskyddsmyndigheter är behöriga att genomföra dataskyddsförordningen. Det faktum att en del av behandlingen omfattas av direktivet om e-integritet begränsar inte dataskyddsmyndigheters behörighet enligt dataskyddsförordningen.

- *Bör dataskyddsmyndigheter beakta bestämmelserna i direktivet om e-integritet när de utövar sin behörighet, utför sina uppgifter och utövar sina befogenheter i enlighet med dataskyddsförordningen och i så fall, i vilken omfattning? Bör, med andra ord, överträdelser av direktivet om e-integritet lämnas utan beaktande vid bedömningen av efterlevnaden av dataskyddsförordningen, och om ja, under vilka omständigheter?*

88. Den eller de myndigheter som får behörighet av medlemsstaten i den mening som avses i direktivet om e-integritet ansvarar helt och hållet för att genomföra de nationella bestämmelser som införlivar direktivet om e-integritet tillämpliga på den specifika behandlingsprocessen också i de fall där behandlingen av personuppgifter faller inom det materiella tillämpningsområdet för både dataskyddsförordningen och direktivet om e-integritet. Dataskyddsmyndigheterna fortsätter dock att ha full behörighet med avseende på alla behandlingsprocesser som utförs på personuppgifter vilka inte omfattas av en eller flera specialbestämmelser i direktivet om e-integritet.

89. En överträdelse av dataskyddsförordningen kan också utgöra en överträdelse av nationella bestämmelser om e-integritet. Dataskyddsmyndigheten kan beakta dessa iakttagelser när det gäller en överträdelse av bestämmelserna i direktivet om e-integritet vid tillämpningen av dataskyddsförordningen (t.ex. vid bedömningen av efterlevnad med principen om laglighet och korrekthet enligt artikel 5.1 i dataskyddsförordningen). Alla genomförandebeslut måste dock motiveras med utgångspunkt i dataskyddsförordningen om inte dataskyddsmyndigheten har getts ytterligare behörighet i enlighet med medlemsstaternas lagstiftning.

90. Om dataskyddsmyndigheten utses till behörig myndighet enligt nationell lagstiftning med stöd i direktivet om e-integritet, har myndigheten behörighet att direkt genomföra nationella bestämmelser om e-integritet utöver att också genomföra dataskyddsförordningen (utan behörighet är detta inte möjligt).

- *I vilken omfattning är mekanismerna för samarbete och enhetlighet tillämpliga vad gäller behandling som – åtminstone i förhållande till vissa behandlingsprocesser – faller inom det materiella tillämpningsområdet för både dataskyddsförordningen och direktivet om e-integritet?*

91. De mekanismer för samarbete och enhetlighet som är tillgängliga för dataskyddsmyndigheter i enlighet med kapitel VII i dataskyddsförordningen rör övervakningen av hur bestämmelserna i dataskyddsförordningen tillämpas. Dataskyddsförordningens mekanismer är inte tillämpliga på de nationella bestämmelser som införlivar direktivet om e-integritet. Mekanismen för samarbete och enhetlighet förblir till fullo tillämplig i den mån som behandlingen omfattas av de allmänna bestämmelserna i dataskyddsförordningen (och inte av en specialregel i direktivet om e-integritet).

***

92. Styrelsen bekräftar att tolkningen ovan inte påverkar resultatet av de pågående förhandlingarna om förordningen om integritet och elektronisk kommunikation. Den föreslagna förordningen tar upp många viktiga element, inbegripet vad gäller dataskyddsmyndigheternas behörighet, men också ett stort antal andra mycket viktiga frågor. Styrelsen vill upprepa sin ståndpunkt om vikten av att förordningen om integritet och elektronisk kommunikation antas.[43]

För Europeiska dataskyddsstyrelsen

Ordförande

(Andrea Jelinek)

[43] Den europeiska dataskyddsstyrelsen har uppmanat kommissionen, Europaparlamentet och rådet att arbeta tillsammans för att få till stånd ett snabbt antagande av den nya förordningen om integritet och elektronisk kommunikation (Uttalande av Europeiska dataskyddsstyrelsen publicerat den 25 maj 2018).