Retningslinjer 2/2023 om det tekniske anvendelsesområde for artikel 5, stk. 3, i e-databeskyttelsesdirektivet

Version 2.0

Vedtaget den 7. oktober 2024

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

Oversigt over versioner

Version 1.0	14. november 2023	Vedtagelse af retningslinjerne til offentlig høring
Version 2.0	7. oktober 2024	Vedtagelse af retningslinjerne efter offentlig høring

Resumé

I disse retningslinjer behandler Databeskyttelsesrådet anvendeligheden af artikel 5, stk. 3, i e-databeskyttelsesdirektivet for så vidt angår forskellige tekniske løsninger. Disse retningslinjer supplerer Artikel 29-Gruppens udtalelse 9/2014 om anvendelsen af e-databeskyttelsesdirektivet på device fingerprinting og har til formål at give en klar forståelse af de tekniske operationer, der er omfattet af artikel 5, stk. 3, i e-databeskyttelsesdirektivet.

Fremkomsten af nye sporingsmetoder, der både erstatter eksisterende sporingsværktøjer (f.eks. cookies, fordi nogle browserleverandører ikke længere understøtter tredjepartscookies), og skaber nye forretningsmodeller, er blevet et væsentligt anliggende inden for databeskyttelse. Mens anvendeligheden af artikel 5, stk. 3, i e-databeskyttelsesdirektivet er almindelig anerkendt og implementeret for nogle sporingsteknologier såsom cookies, er der behov for at løse uklarheder i forbindelse med anvendelsen af den nævnte bestemmelse på de nyeste sporingsværktøjer.

Retningslinjerne identificerer tre nøgleelementer med hensyn til anvendeligheden af artikel 5, stk. 3, i e-databeskyttelsesdirektivet (afsnit 2.1), nemlig "oplysninger", "en abonnents eller brugers terminaludstyr" og "opnåelse af adgang" og "lagring af oplysninger" og "lagrede oplysninger". Retningslinjerne indeholder endvidere en detaljeret analyse af hvert enkelt element (afsnit 2.2-2.6).

I afsnit 3 anvendes denne analyse på en ikke-udtømmende liste over use cases, der repræsenterer almindelige teknikker, nemlig:

- URL- og pixelsporing
- Lokal behandling
- Sporing udelukkende baseret på IP
- Intermitterende og formidlet IoT-rapportering
- Entydig identifikator

Indholdsfortegnelse

Det Europæiske Databeskyttelsesråd har –

under henvisning til artikel 70, stk. 1, litra e), i Europa-Parlamentets og Rådets forordning 2016/679/EU 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 (i det følgende benævnt "GDPR"),

under henvisning til EØS-aftalen, særlig bilag XI og protokol 37, som ændret ved Det Blandede EØS-Udvalgs afgørelse nr. 154/2018 af 6. juli 2018[1],

under henvisning til artikel 15, stk. 3, i 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, ændret ved direktiv 2009/136/EF (i det følgende benævnt "e-databeskyttelsesdirektivet"),

under henvisning til artikel 12 og artikel 22 i forretningsordenen –

VEDTAGET FØLGENDE RETNINGSLINJER:

1 INDLEDNING

1. I henhold til artikel 5, stk. 3, i e-databeskyttelsesdirektivet er "*lagring af oplysninger*" eller opnåelse af adgang til "*oplysninger, der er lagret i en abonnents eller brugers terminaludstyr*" kun tilladt på grundlag af samtykke, eller hvis det er påkrævet til specifikke formål fastsat i nævnte artikel. Som anført i betragtning 24 i e-databeskyttelsesdirektivet[2] er formålet med denne bestemmelse at beskytte brugernes terminaludstyr, da de er en del af brugernes privatsfære. Det følger af artiklens ordlyd, at artikel 5, stk. 3, i e-databeskyttelsesdirektivet ikke udelukkende finder anvendelse på cookies, men også på "tilsvarende" teknologier. Der findes imidlertid i øjeblikket ingen omfattende liste over de tekniske operationer, der er omfattet af artikel 5, stk. 3, i e-databeskyttelsesdirektivet.

2. Artikel 29-Gruppen ("WP29") har allerede i sin udtalelse 9/2014 om anvendelsen af e-databeskyttelsesdirektivet på device fingerprinting ("WP29-udtalelse 9/2014") præciseret, at optagelse af fingeraftryk er omfattet af det tekniske anvendelsesområde for artikel 5, stk. 3, i e-databeskyttelsesdirektivet[3], men at der på grund af den teknologiske udvikling er behov for yderligere vejledning med hensyn til de sporingsteknikker, der i øjeblikket anvendes. Det tekniske landskab har udviklet sig i løbet af det seneste årti med den stigende brug af identifikatorer indlejret i operativsystemer samt fremkomsten af nye værktøjer, der gør det muligt at lagre oplysninger i terminaludstyr.

[1] Henvisninger til "medlemsstater" i dette dokument skal forstås som henvisninger til "EØS-medlemsstater".
[2] "Terminaludstyr for brugere af elektroniske kommunikationsnet og alle oplysninger, der er lagret på sådant udstyr, er en del af brugernes privatsfære, der kræver beskyttelse i henhold til den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder. Såkaldt spionsoftware, såkaldte web bugs, skjulte identifikatorer og andre tilsvarende anordninger kan komme ind i brugerens terminal uden dennes viden for at skaffe adgang til oplysninger, for at lagre skjulte oplysninger eller for at spore brugerens aktiviteter og kan alvorligt krænke disse brugeres privatliv. Brugen af sådanne anordninger til andet end lovlige formål bør kun være tilladt med de pågældende brugeres viden."
[3] WP29-udtalelse 9/2014, s. 11.

3. Uklarhederne omkring anvendelsesområdet for artikel 5, stk. 3, i e-databeskyttelsesdirektivet har skabt incitamenter til at gennemføre alternative løsninger til sporing af internetbrugere og medført en tendens til at omgå de retlige forpligtelser i artikel 5, stk. 3, i e-databeskyttelsesdirektivet. Alle sådanne situationer giver anledning til bekymring og kræver en supplerende analyse for at supplere den tidligere vejledning fra Databeskyttelsesrådet.

4. Formålet med disse retningslinjer er at foretage en teknisk analyse af anvendelsesområdet for artikel 5, stk. 3, i e-databeskyttelsesdirektivet, nemlig at afklare, hvad der teknisk set menes med formuleringen "*med henblik på lagring af oplysninger eller med henblik på at opnå adgang til oplysninger, der er lagret i en abonnents eller brugers terminaludstyr*". Disse retningslinjer omhandler ikke de omstændigheder, hvorunder en behandlingsaktivitet kan være omfattet af undtagelserne fra kravet om samtykke i e-databeskyttelsesdirektivet[4], da disse omstændigheder bør analyseres fra sag til sag under hensyntagen til den eller de relevante medlemsstaters gennemførelse(er) i national ret, og vejledning udstedt af de nationale kompetente myndigheder.

5. En ikke-udtømmende liste over specifikke use cases vil blive analyseret i den sidste del af disse retningslinjer.

2 ANALYSE

2.1 Nøgleelementer med hensyn til anvendeligheden af artikel 5, stk. 3, i e-databeskyttelsesdirektivet

6. Artikel 5, stk. 3, i e-databeskyttelsesdirektivets finder anvendelse, hvis:

   a. **KRITERIUM A:** de gennemførte operationer vedrører "*oplysninger*". Bemærk, at det anvendte udtryk ikke er "personoplysninger", men "oplysninger".

   b. **KRITERIUM B:** de operationer, der udføres, omfatter en abonnents eller brugers "*terminaludstyr*" (B.1), hvilket indebærer et behov for at vurdere begrebet "*"offentligt kommunikationsnet*" (B.2).

   c. **KRITERIUM C:** de udførte operationer vitterligt udgør "*lagring*" (C.1) eller "*opnåelse af adgang*" (C.2). Disse to begreber kan undersøges uafhængigt, jf. WP29-udtalelse 9/2014, hvor det fastslås, at brugen af formuleringen "med henblik på lagring af oplysninger eller med henblik på at opnå adgang til oplysninger" indikerer, at lagringen og opnåelsen af adgang ikke behøver at ske inden for samme kommunikation og ikke behøver at blive udført af den samme part[5].

   For nemheds skyld vil den enhed, der opnår adgang til oplysninger lagret i brugerens terminaludstyr, herefter blive benævnt som "den enhed, der opnår adgang".

2.2 Begrebet "oplysninger" – Kriterium A

7. Som udtrykt i KRITERIUM A beskriver dette afsnit, hvad der hører ind under begrebet "oplysninger". Valget af begrebet "oplysninger", der dækker bredere end "personoplysninger", hænger sammen med e-databeskyttelsesdirektivets anvendelsesområde.

[4] Som anført i artikel 5, stk. 3, i e-databeskyttelsesdirektivet: "*Dette er ikke til hinder for teknisk lagring eller adgang til oplysninger, hvis det alene sker med det formål at overføre eller lette overføring af kommunikation via et elektronisk kommunikationsnet eller er absolut påkrævet for at levere en informationssamfundstjeneste, abonnenten eller brugeren udtrykkeligt ønsker.*"

[5] WP29-udtalelse 9/2014, s. 8.

8. Formålet med artikel 5, stk. 3, i e-databeskyttelsesdirektivet er at beskytte brugernes privatsfære som anført i betragtning 24: "*Terminaludstyr for brugere af elektroniske kommunikationsnet og alle oplysninger, der er lagret på sådant udstyr, er en del af brugernes privatsfære, der kræver beskyttelse i henhold til den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder*". Den er også beskyttet af artikel 7 i EU's charter om grundlæggende rettigheder.

9. Faktisk er scenarier, der trænger ind i denne privatsfære, selv uden at involvere personoplysninger, udtrykkeligt omfattet af artikel 5, stk. 3, og betragtning 24 i e-databeskyttelsesdirektivet, f.eks. lagring af virus på brugerens terminaludstyr. Dette viser, at definitionen af begrebet "oplysninger" ikke bør være begrænset til den egenskab, at de er knyttet til en identificeret eller identificerbar fysisk person.

10. Dette er blevet bekræftet af EU-Domstolen: "*Denne beskyttelse finder anvendelse på alle oplysninger, der er lagret på dette terminaludstyr, uafhængigt af, om der er tale om personoplysninger eller ej, og den tilsigter bl.a., således som det fremgår af samme betragtning, at beskytte brugerne mod risikoen for, at skjulte identifikatorer eller andre tilsvarende anordninger kommer ind i disse brugeres terminal uden deres viden*"[6].

11. Spørgsmålene om, hvorvidt oprindelsen af disse oplysninger og årsagerne til, at de lagres i terminaludstyret, bør tages i betragtning ved vurderingen af anvendeligheden af artikel 5, stk. 3, i e-databeskyttelsesdirektivet, er tidligere blevet afklaret. For eksempel i WP29-udtalelse 9/2014, hvor det fastslås, at dette ikke skal forstås således, at tredjeparten er undtaget fra forpligtelsen til at indhente samtykke for at tilgå disse oplysninger, blot fordi vedkommende ikke lagrede dem. Kravet om samtykke gælder også, når en read-only-værdi tilgås (f.eks. ved anmodning om MAC-adressen for en netgrænseflade via OS API'en)[7].

12. Konklusionen er, at begrebet oplysninger omfatter både ikke-personoplysninger og personoplysninger, uanset hvordan disse oplysninger blev lagret og af hvem, dvs. om det var af en ekstern enhed (herunder også andre enheder end den, der har adgang), af brugeren eller af en producent, eller et hvilket som helst andet scenarie.

2.3 Begrebet "en abonnents eller brugers terminaludstyr" – Kriterium B.1

13. Dette afsnit bygger på definitionen i direktiv 2008/63/EF – som refereret i artikel 2 i direktiv (EU) 2018/1972 – hvor "terminaludstyr" defineres som: "*alt udstyr, der direkte eller indirekte er tilsluttet et offentligt telekommunikationsnets grænseflade med henblik på at transmittere, behandle eller modtage informationer; i begge tilfælde, ved såvel direkte som indirekte tilslutning, kan denne etableres gennem ledning, lysleder eller elektromagnetisk; tilslutningen er indirekte, hvis der er indskudt et apparat mellem terminaludstyr og det offentlige grænsefladenet*"[8].

14. Betragtning 24 i e-databeskyttelsesdirektivet giver en klar forståelse af terminaludstyrets rolle for den beskyttelse, der ydes med artikel 5, stk. 3, i e-databeskyttelsesdirektivet. E-databeskyttelsesdirektivet beskytter brugernes privatliv, ikke kun i forhold til fortroligheden af deres oplysninger, men også ved at sikre integriteten af brugerens terminaludstyr. Denne forståelse vil være retningsgivende for fortolkningen af begrebet terminaludstyr i disse retningslinjer.

15. Artikel 3 i e-databeskyttelsesdirektivet fastslår, at for at e-databeskyttelsesdirektivet kan finde anvendelse, skal behandlingen af personoplysninger udføres i forbindelse med, at offentligt

[6] Domstolens dom af 1. oktober 2019, Planet 49, sag C-673/17, ECLI:EU:C:2019:801, præmis 70.
[7] WP29-udtalelse 9/2014, s. 8.
[8] Artikel 1, stk. 1, i Kommissionens direktiv 2008/63/EF af 20. juni 2008 om konkurrence på markederne for teleterminaludstyr (kodificeret udgave).

tilgængelige elektroniske kommunikationstjenester stilles til rådighed via offentlige kommunikationsnet. Dette indebærer, at en enhed bør kunne bruges i forbindelse med en sådan tjeneste, og at den for at kunne betegnes som terminaludstyr bør være tilsluttet eller kunne tilsluttes[9] grænsefladen til et offentligt kommunikationsnet. Databeskyttelsesrådet bemærker, at de ændringer, der blev foretaget i 2009[10] i ordlyden af artikel 5, stk. 3, i e-databeskyttelsesdirektivet, udvidede beskyttelsen af terminaludstyr ved at slette henvisningen til "anvendelse af elektroniske kommunikationsnet" som et middel til at lagre oplysninger eller opnå adgang til oplysninger lagret i terminaludstyret. Så længe en enhed har en netgrænseflade, der gør den egnet til tilslutning (selv om der ingen tilslutningsmulighed er), gælder artikel 5, stk. 3, i e-databeskyttelsesdirektivet således for enhver enhed, der ville lagre og opnå adgang til oplysninger, der allerede er lagret i terminaludstyret, uanset måden hvorpå terminaludstyret tilgås, og uanset om den er tilsluttet eller frakoblet et net.

16. Udstyr, der er en del af selve det offentligt tilgængelige elektroniske kommunikationsnet, vil ikke være at betragte som terminaludstyr i henhold til artikel 5, stk. 3, i e-databeskyttelsesdirektivet[11].

17. Terminaludstyr kan bestå af flere enkelte stykker hardware, som tilsammen udgør terminaludstyret. Det kan være i form af en fysisk lukket enhed, der indeholder al skærm-, behandlings-, lagrings- og periferihardware (f.eks. smartphones, laptops, netværkstilsluttede lagringsenheder, forbundne biler eller forbundne tv'er, intelligente briller).

18. I e-databeskyttelsesdirektivet anerkendes det, at beskyttelsen af fortroligheden af oplysninger lagret på en brugers terminaludstyr og integriteten af brugerens terminaludstyr ikke er begrænset til beskyttelsen af fysiske personers privatsfære, men også vedrører retten til respekt for deres korrespondance eller juridiske personers legitime interesser[12]. Som sådan er terminaludstyr, der understøtter denne korrespondance og juridiske personers legitime interesser, beskyttet i henhold til artikel 5, stk. 3, i e-databeskyttelsesdirektivet.

19. Brugeren eller abonnenten kan eje eller leje eller på anden måde komme i besiddelse af terminaludstyret. Flere brugere eller abonnenter kan dele det samme terminaludstyr.

20. Denne beskyttelse garanteres af e-databeskyttelsesdirektivet for det terminaludstyr, der er tilknyttet brugeren eller abonnenten, og den er ikke afhængig af, om brugeren har foranlediget adgangen (f.eks. om vedkommende har indledt den elektroniske kommunikation), eller endda om brugeren har kendskab til den nævnte adgang).

[9] Dvs. have den tekniske kapacitet til at blive tilsluttet nettet, selv om denne forbindelse ikke er etableret på nuværende tidspunkt.

[10] Artikel 2, stk. 5, og betragtning 65 i Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009 om ændring af direktiv 2002/22/EF om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester, direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor og forordning (EF) nr. 2006/2004 om samarbejde mellem nationale myndigheder med ansvar for håndhævelse af lovgivning om forbrugerbeskyttelse (EØS-relevant tekst) (EUT L 337 af 18.12.2009).

[11] For at identificere nettets grænser i forskellige sammenhænge henvises til BEREC's retningslinjer for fælles tilgang til identifikation af nettermineringspunktet i forskellige nettopologier (BoR (20) 46).

[12] Som anført i artikel 2, stk. 13, i Europa-Parlamentets og Rådets direktiv (EU) 2018/1972 af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation kan brugeren være en fysisk eller juridisk person.

2.4 Begrebet "offentligt kommunikationsnet" – Kriterium B.2

21. Da den situation, der reguleres af e-databeskyttelsesdirektivet, er den, hvor "*offentligt tilgængelige elektroniske kommunikationstjenester stilles til rådighed via offentlige kommunikationsnet i Fællesskabet*"[13], og definitionen af terminaludstyr specifikt indeholder begrebet "*offentligt kommunikationsnet*", er det afgørende at præcisere dette begreb for at identificere sammenhængen, hvori artikel 5, stk. 3, i e-databeskyttelsesdirektivet finder anvendelse.

22. Begrebet elektronisk kommunikationsnet er ikke defineret i selve e-databeskyttelsesdirektivet. Der blev oprindeligt henvist til dette begreb i direktiv 2002/21/EF (rammedirektivet) om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester[14], der efterfølgende blev erstattet af artikel 2, stk. 1, i direktiv 2018/1972 (den europæiske kodeks for elektronisk kommunikation). Ordlyden er nu følgende:

> *"elektronisk kommunikationsnet": transmissionssystemer, uanset om de bygger på en permanent infrastruktur eller centraliseret administrationskapacitet, og, hvor det er relevant, koblings- og dirigeringsudstyr og andre ressourcer, herunder netelementer, der ikke er aktive, som gør det muligt at overføre signaler ved hjælp af trådforbindelse, radiobølger, lyslederteknik eller andre elektromagnetiske midler, herunder satellitnet, jordbaserede fastnet (kredsløbs- og pakkekoblede, herunder i internettet) og mobilnet, elkabelsystemer, i det omfang de anvendes til transmission af signaler, net, som anvendes til radio- og tv-spredning, samt kabel-tv-net, uanset hvilken type information der overføres.*[15]

23. Denne definition er neutral med hensyn til transmissionsteknologier. Et elektronisk kommunikationsnet er ifølge denne definition ethvert netsystem, der tillader transmission af elektroniske signaler mellem dets knudepunkter, uanset udstyret og protokollerne, der anvendes.

24. Begrebet elektronisk kommunikationsnet i henhold til direktiv 2018/1972 afhænger ikke af infrastrukturens offentlige eller private karakter eller af måden, nettet etableres eller forvaltes på ("*uanset om de bygger på en permanent infrastruktur eller centraliseret administrationskapacitet*"[16]). Definitionen af elektronisk kommunikationsnet i henhold til artikel 2 i direktiv 2018/1972 er således tilstrækkelig bred til at omfatte enhver form for infrastruktur. Den omfatter net administreret eller ej af en operatør, net administreret i fællesskab af en gruppe operatører, eller endda ad hoc-net, hvor terminaludstyr dynamisk kan tilslutte sig eller forlade en maske af andet terminaludstyr ved hjælp af transmissionsprotokoller med kort rækkevidde.

25. Denne definition af net rummer ikke nogen begrænsning med hensyn til mængden af terminaludstyr til stede i nettet på noget tidspunkt. Nogle netværksmodeller er afhængige af, at knudepunkter videresender oplysninger på ad hoc-basis til forbundne knudepunkter[17] og kan på et givet tidspunkt bestå af blot to ligeværdige knudepunkter, der kommunikerer. Sådanne tilfælde ville være omfattet af

[13] Artikel 3 i e-databeskyttelsesdirektivet.
[14] Europa-Parlamentets og Rådets direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet)
[15] Artikel 2, stk. 1, i Europa-Parlamentets og Rådets direktiv (EU) 2018/1972 af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation (omarbejdning) (EØS-relevant tekst).
[16] Artikel 2, stk. 1, i Europa-Parlamentets og Rådets direktiv (EU) 2018/1972 af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation (omarbejdning) (EØS-relevant tekst).
[17] F.eks. i sammenhæng med en forsinkelsestolerant netværksmodel, hvor "store-and-forward-teknikker" gennemføres, såsom Briar-open source-projektet.

e-databeskyttelsesdirektivets generelle anvendelsesområde, så længe netværksprotokollen giver mulighed for yderligere inddragelse af ligeværdige knudepunkter.

26. Det er nødvendigt, at kommunikationsnetværket er offentligt tilgængeligt, for at udstyret kan betragtes som et terminaludstyr og dermed for anvendeligheden af e-databeskyttelsesdirektivets artikel 5, stk. 3. Det bør bemærkes, at den omstændighed, at nettet stilles til rådighed for en begrænset del af offentligheden (f.eks. abonnenter, betalende eller ej, afhængigt af adgangskrav), ikke gør et sådant net privat[18].

2.5 Begrebet "opnåelse af adgang" – Kriterium C.1

27. For at definere begrebet "opnåelse af adgang" korrekt er det vigtigt at se på e-databeskyttelsesdirektivets anvendelsesområdet, som fastsat i dets artikel 1: "*at sikre et ensartet niveau i beskyttelsen af de grundlæggende rettigheder og frihedsrettigheder og navnlig privatlivets fred i forbindelse med behandling af personoplysninger inden for den elektroniske kommunikationssektor, og [...] at sikre fri omsætning af sådanne oplysninger og af elektronisk kommunikationsudstyr og elektroniske kommunikationstjenester i Fællesskabet*".

28. Kort fortalt er e-databeskyttelsesdirektivet et retligt instrument til beskyttelse af privatlivets fred, der har til formål at beskytte kommunikationshemmeligheden og integriteten af udstyr. I betragtning 24 i e-databeskyttelsesdirektivet præciseres det, at når der er tale om fysiske personer, er brugeres terminaludstyr en del af deres privatsfære, og at opnåelse af adgang til oplysninger, der er lagret på det, uden deres viden kan krænke deres privatliv i alvorlig grad.

29. Juridiske personer er også beskyttet af e-databeskyttelsesdirektivet[19]. Som følge heraf skal begrebet "opnåelse af adgang" i henhold til artikel 5, stk. 3, i e-databeskyttelsesdirektivet fortolkes på en sådan måde, at disse rettigheder beskyttes mod krænkelse fra tredjeparter.

30. Lagring af oplysninger eller opnåelse af adgang kan være uafhængige operationer og udføres af uafhængige enheder. Betingelserne lagring af oplysninger og opnåelse af adgang til allerede lagrede oplysninger behøver ikke begge at være opfyldt, for at artikel 5, stk. 3, i e-databeskyttelsesdirektivet finder anvendelse.

31. Som bemærket i WP29-udtalelse 9/2014 angiver formuleringen "med henblik på lagring af oplysninger eller med henblik på at opnå adgang til oplysninger, der er lagret i en abonnents eller brugers terminaludstyr", at lagring og opnåelse af adgang ikke behøver at ske inden for samme kommunikation og ikke behøver at blive udført af den samme part. Oplysninger, der lagres af én part (herunder oplysninger, der lagres af brugeren eller producenten af enheden), og som en anden part senere får adgang til, er derfor omfattet af anvendelsesområdet for artikel 5, stk. 3[20]. Derfor er der ingen begrænsninger på oprindelsen af oplysninger på terminaludstyret, for at begrebet "opnåelse af adgang" kan finde anvendelse.

32. Når en enhed tager skridt til at opnå adgang til oplysninger lagret i terminaludstyret, finder artikel 5, stk. 3, i e-databeskyttelsesdirektivet anvendelse. Dette indebærer normalt, at den enhed, der opnår adgang, proaktivt giver terminaludstyret specifikke instrukser for at tilbagemodtage de ønskede oplysninger. Dette er f.eks. tilfældet for cookies, hvor den enhed, der opnår adgang, giver

[18] For yderligere analyse af identifikationen af offentlige kommunikationsnet henvises til BEREC's retningslinjer om gennemførelse af forordningen om det åbne internet (BoR (20) 112).
[19] Betragtning 26 i e-databeskyttelsesdirektivet, jf. punkt 17 ovenfor.
[20] WP29-udtalelse 9/2014, s. 8.

terminaludstyret instruks om proaktivt at sende oplysninger om hvert efterfølgende Hypertext Transfer Protocol-opkald ("HTTP-opkald").

33. Dette er ligeledes tilfældet, når den enhed, der opnår adgang, distribuerer software på brugerens terminaludstyr, der lagres, og derefter proaktivt ringer til en applikationsprogrammeringsgrænseflade ("API") via nettet. Yderligere eksempler omfatter JavaScript-kode, hvor den enhed, der opnår adgang, giver brugerens browser instruks om at sende asynkrone anmodninger med de ønskede oplysninger. En sådan opnåelse af adgang falder klart ind under anvendelsesområdet for artikel 5, stk. 3, i e-databeskyttelsesdirektivet, da den enhed, der opnår adgang, udtrykkeligt giver terminaludstyret instruks om at sende oplysningerne.

34. I nogle tilfælde er enheden, der giver terminaludstyret instruks om at sende de ønskede data tilbage, muligvis ikke den samme som enheden, der modtager oplysninger. Dette kan skyldes tilvejebringelsen og/eller anvendelsen af en fælles mekanisme mellem de to enheder. Instruering af enheden om at sende allerede lagrede oplysninger (f.eks. ved brug af en protokol eller et SDK[21], der indebærer proaktiv afsendelse af oplysninger fra terminaludstyret) gør det muligt at trænge ind i terminaludstyret, og derfor udløser en sådan adgang anvendelsen af artikel 5, stk. 3, i e-databeskyttelsesdirektivet. Som nævnt i WP29-udtalelse 9/2014 kan dette være tilfældet, når et websted giver terminaludstyret instruks om at sende oplysninger til tredjeparts reklametjenester ved at inkludere en sporingspixel[22]. Denne use case uddybes yderligere i afsnit 3.1.

2.6 Begreberne "lagring af oplysninger" og "lagrede oplysninger" – Kriterium C.2

35. Lagring af oplysninger som omhandlet i artikel 5, stk. 3, i e-databeskyttelsesdirektivet henviser til placeringen af oplysninger på et fysisk, elektronisk lagringsmedium, der er en del af en brugers eller abonnents terminaludstyr[23].

36. Typisk lagres oplysninger ikke i en brugers eller abonnents terminaludstyr gennem en anden parts direkte adgang til enhedens hukommelse, men snarere ved at give software på terminaludstyret instruks om at generere specifikke oplysninger. Lagring, der finder sted ved hjælp af sådanne instrukser, anses for at være initieret direkte af den anden part. Dette omfatter anvendelse af etablerede protokoller som f.eks. lagring af browsercookies samt skræddersyet software, uanset hvem der oprettede eller installerede protokollerne eller softwaren på terminaludstyret.

37. Der angives i e-databeskyttelsesdirektivet ikke nogen øvre eller nedre grænse for, hvor længe oplysninger skal forblive på et lagringsmedie for at tælle som lagret, eller for hvor mange oplysninger, der skal lagres.

38. Begrebet "lagring" beror heller ikke på, hvilken type medie oplysningerne lagres på. Typiske eksempler omfatter harddiskdrev ("HDD"), solid-state-drev ("SSD"), elektrisk sletbar, programmerbar, skrivebeskyttet hukommelse ("EEPROM") og random-access-hukommelse ("RAM"), men mindre typiske scenarier, der involverer et medium som en cache til magnetbånd eller centralbehandlingsenheder ("CPU'er"), er ikke udelukket fra anvendelsesområdet. Lagringsmediet kan være forbundet internt (f.eks. gennem en SATA-forbindelse), eksternt (f.eks. gennem en USB-forbindelse)

[21] Et SDK ("softwareudviklingssæt") er en pakke softwareudviklingsværktøjer, der stilles til rådighed for at lette udviklingen af applikationssoftware.
[22] WP29-udtalelse 9/2014, s. 9.
[23] Som defineret i afsnit 2.3 i disse retningslinjer.

39. "Lagrede oplysninger" henviser til oplysninger, der allerede findes på terminaludstyret, uanset oprindelsen eller arten af disse oplysninger. Dette omfatter ethvert resultat af lagring af oplysninger, jf. artikel 5, stk. 3, i e-databeskyttelsesdirektivet, som beskrevet ovenfor (enten af den samme part, som senere ville opnå adgang, eller af en anden tredjepart). Det omfatter desuden resultater af lagringsprocesser uden for anvendelsesområdet for artikel 5, stk. 3, i e-databeskyttelsesdirektivet, såsom: lagring på terminaludstyret foretaget af brugeren eller abonnenten selv eller af en hardwareproducent (såsom MAC-adresser på netkort), sensorer integreret i terminaludstyret, eller processer og programmer udført på terminaludstyret, der måske eller måske ikke producerer oplysninger, der er afhængige af eller afledt af lagrede oplysninger.

3 USE CASES

40. Som påpeget i indledningen til disse retningslinjer[24] er der ikke tale om en analyse af anvendelsen af undtagelserne fra forpligtelsen til at indhente samtykke i henhold til artikel 5, stk. 3, i e-databeskyttelsesdirektivet. Databeskyttelsesrådet minder om, at det i alle tilfælde, hvor der lagres oplysninger eller opnås adgang til allerede lagrede oplysninger, skal vurderes, om der er behov for samtykke, eller om en undtagelse i henhold til artikel 5, stk. 3, i e-databeskyttelsesdirektivet kan finde anvendelse. Læseren bør derfor overveje undtagelserne i deres use case i forbindelse med denne tekniske analyse.

41. Uden at foregribe den specifikke sammenhæng, hvori disse tekniske kategorier kan anvendes, som er nødvendige for at afgøre, om artikel 5, stk. 3, i e-databeskyttelsesdirektivet finder anvendelse, er det muligt på en ikke-udtømmende måde at identificere brede kategorier af identifikatorer og oplysninger, der er almindeligt anvendt og kan være omfattet af artikel 5, stk. 3, i e-databeskyttelsesdirektivet.

42. Netværkskommunikation er normalt baseret på en lagdelt model, der gør det nødvendigt at anvende identifikatorer for at muliggøre en korrekt etablering og gennemførelse af kommunikationen. Instruksen om kommunikationen af disse identifikatorer til eksterne aktører gives via software ved overholdelse af aftalte kommunikationsprotokoller. Som beskrevet ovenfor udelukker det forhold, at den modtagende enhed måske ikke er den enhed, der giver instruks om at sende oplysninger, ikke anvendelsen af artikel 5, stk. 3, i e-databeskyttelsesdirektivet. Dette kan vedrøre routing-identifikatorer såsom terminaludstyrets MAC- eller IP-adresse, men også sessionsidentifikatorer (SSRC, Websocket-identifikator) eller autentificeringstokens.

43. På samme måde kan applikationsprotokollen indeholde flere mekanismer til at levere kontekstdata (såsom HTTP-header inklusive "accept"-felt eller brugeragent), caching-mekanisme (såsom ETag[25]) eller andre funktioner (bl.a. cookies, eller HSTS[26]). Igen kan anvendelse af disse mekanismer til indsamling af oplysninger (f.eks. i forbindelse med optagelse af fingeraftryk[27] eller sporing af ressourceidentifikatorer) føre til anvendelse af artikel 5, stk. 3, i e-databeskyttelsesdirektivet.

44. På den anden side er der visse sammenhænge, hvor lokale applikationer installeret i terminaludstyret anvender visse oplysninger strengt internt i terminalen, som tilfældet kan være med API'er for

[24] Jf. punkt 4 ovenfor.
[25] HTTP ETag er en identifikator, der gør det muligt at foretage betingede anmodninger baseret på gyldigheden af de cachelagrede klientdata.
[26] HTTP Strict Transport Security (HSTS) giver servere mulighed for at specificere, hvilke ressourcer der altid bør anmodes om ved hjælp af HTTPS-forbindelser.
[27] Som nævnt i indledningen, se WP29-udtalelse 9/2014 om anvendelsen af e-databeskyttelsesdirektivet på device fingerprinting.

smartphone-systemer (adgang til kamera, mikrofon, GPS-sensor, acceleratorchip, radiochip, lokal filadgang, kontaktliste, adgang til identifikatorer osv.). Dette kan også være tilfældet for webbrowsere, der behandler oplysninger gemt eller genereret i enheden (f.eks. cookies, lokal lagring, WebSQL, eller endda oplysninger leveret af brugerne selv). En applikations brug af sådanne oplysninger ville ikke udgøre "opnåelse af adgang" til allerede "lagrede oplysninger" i henhold til artikel 5, stk. 3, i e-databeskyttelsesdirektivet, så længe oplysningerne ikke forlader enheden, men når der opnås adgang til disse oplysninger eller en afledning af disse oplysninger, ville artikel 5, stk. 3, i e-databeskyttelsesdirektivet finde anvendelse.

45. Endelig distribuerer aktører i nogle tilfælde skadelige softwareelementer, f.eks. kryptominingsoftware eller, mere generelt, malware, der udnytter terminaludstyrets processorkapacitet til gavn for den distribuerende aktør. Distributionen af den pågældende skadelige software i brugerens terminaludstyr ville udgøre en "oplagring" som omhandlet i artikel 5, stk. 3, i e-databeskyttelsesdirektivet. Hvis softwaren desuden etablerer en netværksforbindelse for at sende oplysninger på et senere tidspunkt, ville det udgøre "opnåelse af adgang" som omhandlet i artikel 5, stk. 3, i e-databeskyttelsesdirektivet.

46. For en undergruppe af disse kategorier, som er af særlig interesse, enten på grund af deres udbredte anvendelse, eller fordi der er behov for en særlig undersøgelse af omstændighederne ved deres anvendelse, gives der en særlig analyse nedenfor.

3.1 URL- og pixelsporing

47. En sporingspixel er et hyperlink til en ressource, som regel en billedfil, indlejret i et stykke indhold som et websted eller en e-mail. Denne pixel tjener normalt ikke noget formål relateret til selve det ønskede indhold; dens eneste formål er automatisk at etablere en kommunikation fra klienten til værten for pixelen, som ellers ikke ville have fundet sted. Dette er imidlertid ikke systematisk, og sporingspixeler kan også skabes ved at tilføje yderligere oplysninger til billeder, der indsætter hyperlinks, som er relevante for det indhold, der vises til brugeren. Ved etablering af kommunikationen overføres forskellige oplysninger til værten for pixelen afhængigt af den specifikke use case.

48. I tilfælde af en e-mail kan afsenderen inkludere en sporingspixel for at registrere, hvornår modtageren læser e-mailen. Sporingspixels på websteder kan linke til en enhed, der modtager mange sådanne anmodninger og dermed er i stand til at spore brugernes adfærd. Sådanne sporingspixler kan også indeholde yderligere identifikatorer, metadata eller indhold som en del af linket. Disse datapunkter kan tilføjes af ejeren af webstedet, muligvis relateret til brugerens aktivitet på det pågældende websted, så der kan genereres analytiske rapporter om anvendelse. De kan også genereres dynamisk gennem applikationslogik på klientsiden leveret af enheden.

49. Sporingslinks kan fungere på samme måde, men identifikatoren er knyttet til webadressen. Når brugeren besøger URL'en, indlæser det pågældende websted den anmodede ressource, men indsamler også en identifikator, der ikke er relevant med hensyn til ressourceidentifikation. De anvendes meget ofte af e-handelswebsteder til at identificere oprindelsen af deres indgående trafik. For eksempel kan sådanne websteder levere sporede links til partnere, som de kan bruge på deres domæne, så e-handelswebstedet ved, hvilken af deres partnere der er ansvarlig for et salg og betaler en provision, såkaldt affiliate marketing.

50. Både sporingslinks og sporingspixels kan distribueres gennem en lang række forskellige kanaler, f.eks. via e-mails, websteder eller, i tilfælde af sporingslinks, gennem enhver form for tekstmeddelelsessystemer. Denne distribution til brugerens terminaludstyr udgør lagring, i det mindste gennem caching-mekanismen i softwaren på klientsiden. Som sådan finder artikel 5, stk. 3, i e-databeskyttelsesdirektivet anvendelse, selv om denne oplagring ikke er permanent.

51. Tilføjelsen af sporingsoplysninger til URL'er eller billeder (pixels) sendt til brugeren udgør en instruks til terminaludstyret om at sende de ønskede oplysninger tilbage (den specificerede identifikator). I tilfælde af dynamisk konstruerede sporingspixels er det distributionen af den applikative logik (normalt en JavaScript-kode), der udgør instruksen. Som følge heraf kan indsamlingen af identifikatorer leveret gennem sådanne sporingsmekanismer betragtes som "opnåelse af adgang" som omhandlet i artikel 5, stk. 3, i e-databeskyttelsesdirektivet, og det gælder derfor også for dette trin.

3.2 Lokal behandling

52. Nogle teknologier er afhængige af, at der gives instruks om lokal behandling ved hjælp af software distribueret på brugernes terminaludstyr, hvor de oplysninger, der produceres af den lokale behandling, derefter stilles til rådighed for udvalgte aktører gennem API'er på kundesiden. Dette kan f.eks. være tilfældet for en API leveret af webbrowseren, hvor lokalt genererede resultater kan tilgås på afstand.

53. Hvis de behandlede oplysninger på et hvilket som helst tidspunkt og f.eks. i koden på klientsiden stilles til rådighed for en tredjepart, f.eks. sendes tilbage via nettet til en server, vil en sådan operation (instrueret af den enhed, der producerer koden på kundesiden, der distribueres på brugerterminaludstyret) udgøre "opnåelse af adgang" til allerede "lagrede oplysninger". Den omstændighed, at disse oplysninger produceres lokalt, udelukker ikke anvendelsen af artikel 5, stk. 3, i e-databeskyttelsesdirektivet.

3.3 Sporing udelukkende baseret på IP

54. Nogle udbydere udvikler løsninger, der kun er afhængige af indsamlingen af én komponent, nemlig IP-adressen, for at kunne spore brugerens navigation[28], i nogle tilfælde på tværs af flere domæner. I denne sammenhæng kan artikel 5, stk. 3, i e-databeskyttelsesdirektivet finde anvendelse, selv om instruksen om at stille IP'en til rådighed er blevet givet af en anden enhed end den modtagende enhed.

55. Opnåelse af adgang til IP-adresser ville imidlertid kun udløse anvendelsen af artikel 5, stk. 3, i e-databeskyttelsesdirektivet i tilfælde, hvor disse oplysninger stammer fra en abonnents eller brugers terminaludstyr. Selvom det ikke systematisk er tilfældet (f.eks. når CGNAT[29] er aktiveret), vil den statiske udgående IPv4, der kommer fra en brugers router, falde ind under denne case, såvel som IPV6-adresser, da de delvist er defineret af værten. Medmindre enheden kan sikre, at IP-adressen ikke stammer fra en brugers eller abonnents terminaludstyr, skal den træffe alle de foranstaltninger, der er omhandlet i artikel 5, stk. 3, i e-databeskyttelsesdirektivet.

56. Selv om disse retningslinjer ikke analyserer anvendelsen af undtagelserne fra forpligtelsen til at indhente samtykke i henhold til artikel 5, stk. 3, i e-databeskyttelsesdirektivet, er det vigtigt igen at minde om, at anvendeligheden af denne artikel ikke systematisk betyder, at der skal indhentes samtykke. Databeskyttelsesrådet minder derfor om, at det i hvert enkelt tilfælde skal vurderes, om der er behov for samtykke, eller om en undtagelse i henhold til artikel 5, stk. 3, i e-databeskyttelsesdirektivet kan finde anvendelse[30].

[28] Dette er i tillæg til og uafhængigt af brugen og funktionen af en IP-adresse til etablering og formidling eller transmission af underliggende teknisk kommunikation, eller det faktum, at der måske eller måske ikke er tale om personlige data (med hensyn til e-databeskyttelsesanalyse er der tale om "oplysninger").
[29] Carrier-grade NAT eller CGNAT anvendes af internetudbydere til at maksimere brugen af begrænset IP-adresseplads. Den grupperer et antal abonnenter under den samme offentlige IP-adresse.
[30] WP29-udtalelse 9/2014 giver nogle eksempler på, hvornår samtykke ikke er nødvendigt.

3.4 Intermitterende og formidlet IoT-rapportering

57. IoT-enheder producerer løbende oplysninger over tid, f.eks. gennem sensorer indlejret i enheden, som kan forbehandles lokalt eller ej. I mange tilfælde stilles oplysninger til rådighed for en fjernserver, men de nærmere vilkår for denne indsamling kan variere.

58. Nogle IoT-enheder har direkte forbindelse til et offentligt kommunikationsnetværk med et mobilt SIM-kort. Andre kan have en indirekte forbindelse til et offentligt kommunikationsnet, f.eks. gennem brug af wi-fi eller videresendelse af information til en anden enhed gennem en punkt-til-punkt-forbindelse (f.eks. gennem bluetooth). Den anden enhed kan f.eks. være en smartphone eller en dedikeret gateway, som måske eller måske ikke forbehandler oplysningerne, før de sendes til serveren.

59. IoT-enheder kan have fået instruks fra producenten om altid at streame de indsamlede oplysninger, men alligevel cache oplysningerne lokalt først, f.eks. indtil en forbindelse er tilgængelig.

60. Under alle omstændigheder vil IoT-enheden, når den er forbundet (direkte eller indirekte) til et offentligt kommunikationsnet, selv blive betragtet som terminaludstyr. Det faktum, at oplysningerne streames eller caches til intermitterende rapportering, ændrer ikke oplysningernes karakter. I begge situationer finder artikel 5, stk. 3, i e-databeskyttelsesdirektivet anvendelse, da der gennem instruktionen med kode på IoT-enheden om at sende de dynamisk lagrede data til fjernserveren finder "opnåelse af adgang" sted.

3.5 Entydig identifikator

61. Et almindeligt værktøj blandt virksomheder er "entydige identifikatorer" eller "vedvarende identifikatorer". Sådanne identifikatorer kan udledes af vedvarende personoplysninger (for- og efternavn, e-mail, telefonnummer osv.), der er hashet på brugerens enhed, indsamlet og delt mellem flere dataansvarlige med henblik på entydigt at identificere en person over forskellige datasæt (brugsdata indsamlet ved brug af websted eller applikation, data vedrørende kunderelationsstyring (CRM) i forbindelse med online- eller offlinekøb eller -abonnementer osv.). På websteder indhentes de vedvarende personoplysninger generelt i forbindelse med autentificering eller abonnement på nyhedsbreve.

62. Som beskrevet ovenfor ville det forhold, at brugeren indlæser oplysninger, ikke udelukke anvendelsen af artikel 5, stk. 3, i e-databeskyttelsesdirektivet for så vidt angår lagring, da disse oplysninger opbevares midlertidigt på terminaludstyret, inden de indsamles.

63. I forbindelse med indsamling af "entydige identifikatorer" på websteder eller mobilapplikationer giver den indsamlende enhed browseren instruks (gennem distribution af kode på klientsiden) om at sende disse oplysninger. Som sådan er der tale om "opnåelse af adgang", og artikel 5, stk. 3, i e-databeskyttelsesdirektivet finder anvendelse.