Kandidatafhandling for Cand.jur.

10. semester

Databeskyttelsesretlig regulering af Internet of Things - oplysningspligt og samtykkekrav i en praktisk kontekst

(Data Protection Regulation of Internet of Things – Obligation to Inform and Consent Requirements in a practical view)

Det Samfundsvidenskabelige Fakultet

Forfatter: Malte Philbert Jessen

Fødselsdato: 07.04.95

Vejleder: Ayo Næsborg-Andersen, Juridisk Institut

Antal anslag: 139.522

Dato: 2. juni 2020

TRO OG LOVE-ERKLÆRING

Det erklæres herved på tro og love, at undertegnede egenhændigt og selvstændigt har udformet denne rapport. Alle citater i teksten er markeret som sådanne, og rapporten eller væsentlige dele af den har ikke tidligere været fremlagt i anden bedømmelsessammenhæng.

Malte Philbert Jessen

ABSTRACT

Based on relevant legal sources this master thesis analyses and assesses what issues the data protection obligations to inform and to obtain consent from the data subject create for the use of the Internet of Things (IoT), and how these practically can be solved. The work is based on the use of the dogmatic legal method which aims to derive the currently applicable law. Since the technology of IoT is relatively new, there is a conspicuous lack of classical sources of law, e.g. case law and *lex specialis*. Due to this, *soft law* plays an important role throughout the thesis, including Guidelines and Opinions made by the Article 29 Working Group and the Mauritius Declaration on the Internet of Things.

The basis of law for the above stated examination is firstly the General Data Protection Regulation's (GDPR) provisions on the obligation to inform and consent requirements and the principle of transparency, and secondly article 5(3) of the Directive on privacy and electronic communications (the ePrivacy directive) and the implementation hereof in Danish law. GDPR is applicable to IoT in connection to processing of personal data while the directive's article 5(3) and the implementation hereof in Danish law is applicable when information is stored in the terminal equipment of the subscriber or user regardless of whether the information contains personal data or not.

The thesis concludes that the use of IoT to collect *Big Data* must be in accordance with the GDPR provisions on the obligation to inform and consent requirements even when anonymization techniques have been used. That is due to an assessment that sufficient anonymization of Big Data is illusory.

The thesis states that while GDPR only protects natural persons, the ePrivacy directive protects both natural persons and legitimate interests of legal persons. It determines that several actors can be liable for violating the obligation to inform or the requirements of consent, e.g. device manufacturers, social media, application developers, data platform providers and in some cases even the end-user of the IoT device.

The thesis concludes that the classical privacy policies not always makes sense in the matter of IoT, e.g. if the product is without any screen to read the policy or collects data in such a high speed that the policy almost always will be outdated. The thesis concludes

that sound can be used as an alternate under these circumstances, e.g. use of Google Home Mini or other smart speakers.

The thesis concludes that in some cases it is obvious that the regulation is outdated due to the technological development. For example, the GDPR article 13 contains no duty to inform the data subject of the categories of personal data collected nor the source of the collected data if the personal data is collected from the data subject himself. This is probably due to a presumption that the data subject is aware of the data he is giving, and that they originate from himself. However, in the matter of IoT this is not always the case, given that lots of IoT users are not aware that data is collected from them by e.g. recordings from digital assistants and smart speakers.

The thesis concludes that the obligation to inform can be avoided in some cases of collection of Big Data from other sources than the data subject, e.g. if the collector is a pharmaceutical company that collects the data for scientific purposes, or a IoT device manufacturer that wants to use the data for statistical overview of consumer groups.

The thesis concludes that consent can be legally given in many ways, e.g. by *swipes* or by waving in front of a smart camera. It concludes that the obligation for the controller to be able to demonstrate that the data subject has consented can be fulfilled by making an electronic log of the *swipe* in the IoT device.

As the thesis will show, the Danish implementation of the consent requirements as set by article 5(3) of the ePrivacy Directive has been incompliant because the implementation act has set the consent requirement standards in accordance with the repealed Data Protection Directive instead of the more stringent requirements set by the GDPR. The thesis assesses, that even though the implementation has been incompliant, Danish IoT users do not have the right to legally rely directly on article 5(3). This leads to the conclusion, that Danish IoT users are only able to plead the more stringent consent requirements set by the GDPR when their personal data are processed and not if the information stored in their equipment only contains non-personal data.

As a final point, the thesis contains a judicial policy assessment of the value of the applicable law, including recommendations for change hereof.

Indholdsfortegnelse

1. PROBLEMFELT

1.1. Indledning

Begrebet *Internet of Things* (herefter forkortet "IoT") blev angiveligt første gang benyttet ved en virksomhedspræsentation i 1999, men det er først i de senere år, at det for alvor har gjort sit indtog.[1]

The Internet Society (ISOC) definerede i en rapport fra 2015 IoT på følgende måde:

"The term of Internet of Things generally refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention".[2]

Definitionen anerkendes af den internationale organisation for domænenavne, *Internet Corporation for Assigned Names and Numbers (ICANN)*, og vil også være udgangspunktet for nærværende afhandling.[3]

IoT er således et udtryk for, at internettet sniger sig ind i alt; ure, køleskabe, termostater, alarmsystemer etc., og der er tilmed udviklet *smarthomes*, som kan styre næsten alt i private hjem, herunder lys, varme og elektricitet.

Der er i disse år massiv vækst indenfor udvikling og brug af IoT. Eksperter forudsiger, at der i 2025 vil eksistere intet mindre end 100 mia. IoT-enheder på globalt plan.[4] Fænomenet er særligt udbredt i Danmark. I 2019 indtog vi således førstepladsen i en undersøgelse af EU-borgeres brug af smarthomes: 23 % af de danske forbrugere havde benyttet smarthomes indenfor de seneste 3 mdr., mens det gennemsnitlige tal for EU var 10 %.[5]

Denne udvikling er ikke uden retssikkerhedsmæssige betænkeligheder. IoT benyttes af producenter mv. til indsamling af såkaldt *Big Data*, dvs. enorme mængder af data, både strukturerede, semistrukturerede og ustrukturerede, som kan benyttes til analyser af brugeradfærd mv.[6] Dataene stammer fra IoT-brugere og kan potentielt dække over særdeles følsom information. Et eksempel herpå er de populære *smartwatches*; et ur der fungerer

[1] Ashton (2009)
[2] Rose m.fl., ISOC (2015)
[3] ICANN Security and Stability Advisory Committee (SSAC) (2019)
[4] Ibid.
[5] Danmarks Statistik (2020)
[6] Verma (2018)

via trådløs opkobling til internettet, dvs. en IoT-enhed. Smartwatches måler bl.a. brugerens puls, kalorieforbrænding, skridt pr. dag og søvnmønster.[7] Downloader brugeren andre sundhedsapps, f.eks. en apoteksapp med oversigt over brugerens medicinforbrug, og giver uret adgang til disse, kan IoT-producenten sammenkoble dataene og skabe en profil af brugerens helbredstilstand.

Adskillige IoT-løsninger, inkl. smartwatches og smarthomes, har tilknyttet en såkaldt *digital assistent*, der modtager input via stemmeoptagelse (f.eks. "Tænd lyset!") og derefter kommer med det ønskede output (tænder lyset). De digitale assistenter har været centrum for flere negative mediehistorier i de seneste år. F.eks. er det kommet frem, at digitale assistenter som Apples Siri eller Amazons Alexa utilsigtet bliver aktiveret op til 19 gange om dagen og i denne aktiveringstid lytter til brugerens samtaler og sender disse data videre til eksterne databaser.[8] Ansatte hos Google og Apple fortalte i 2019 til Politiken, at fysiske medarbejdere transskriberede samtaler, som de fik tilsendt fra digitale assistenter, herunder tilfælde hvor de aflyttede brugere tydeligvis ikke var klar over, at de blev optaget, f.eks. under samleje, skænderier eller almindelig sniksnak.[9]

Ovenstående problematikker gør det både aktuelt og relevant at undersøge de databeskyttelsesretlige aspekter af den stigende brug af IoT. Som de refererede mediehistorier vidner om, indsamles og behandles mange oplysninger via brug af IoT, og uden at de berørte brugere er klar over det. Det rejser i særlig grad spørgsmål i relation til de databeskyttelsesretlige krav om oplysningspligt og samtykke, hvilket vil være omdrejningspunktet for denne afhandling.

1.2. Problemformulering

Med udgangspunkt i relevante retskilder vil det analyseres og vurderes, hvilke problemstillinger de databeskyttelsesretlige krav om oplysningspligt og samtykke skaber for brugen af Internet of Things (IoT), og hvordan disse praktisk løses.

1.3. Metode

Som det kan udledes af problemformuleringen, er formålet med denne afhandling at undersøge, hvorledes IoT er underlagt de databeskyttelsesretlige krav om oplysningspligt

[7] Andersen, Lars Nøhr (2019)
[8] Matyszczyk (2020) & Vollandt (2020)
[9] Andersen, Pia Buhl m.fl. (2019)

og samtykke. Der er dermed tale om en undersøgelse af gældende ret, *de lege lata*. Undersøgelsen foretages ved at benytte den retsdogmatiske metode. Hermed forstås at gældende ret søges udledt ud fra en prognoseteori om, at hvis en regel er gældende, må det være en forudsigelse om, at en domstol fremover vil anvende reglen.[10] I denne afhandling vil metoden anvendes via systematisering, fortolkning og analyse af relevante retskilder. Den tidligere herskende opfattelse af, at der eksisterer et retskildehierarki, er principielt forladt i dag, og man anser således som udgangspunkt alle retskilder for ligestillede, idét de hver især kan være afgørende for løsningen af den konkrete problemstilling.[11] I denne afhandling tages der udgangspunkt i den nu fremherskende opfattelse af, at alle retskilder principielt er ligestillede.

Der tages udgangspunkt i databeskyttelsesforordningens krav til oplysningspligt og samtykke.[12] Oplysningspligten har rod i det generelle princip om transparens, der derfor også analyseres indgående i opgaven.[13] Derudover gennemgås ePrivacy-direktivets art. 5(3), da informationer indsamlet via IoT ofte også vil være underlagt denne bestemmelses krav om informeret samtykke. Dette uddybes i afsnit 3.

Da regulering af IoT er et meget nyt retsområde, er klassiske juridiske kilder som retspraksis og juridisk litteratur stort set ikkeeksisterende. Der vil derfor i høj grad lægges vægt på *soft law*, dvs. ikke-bindende retskilder, ved fortolkning af reglerne med det formål at besvare problemformuleringen.[14]

Danske retskilder på området for regulering af IoT er særdeles mangelfulde, grænsende til ikkeeksisterende. Samtidig tilsigter både databeskyttelsesforordningen og ePrivacy-direktivet at skabe et ensartet beskyttelsesniveau i samtlige medlemsstater.[15] Derfor vil denne afhandling primært inddrage intraeuropæiske retskilder som fortolkningsbidrag, herunder især udtalelser fra Artikel 29-gruppen. Disse udtalelser er ikke bindende og dermed at anse for soft law.[16] Til trods herfor har de vist sig at have en væsentlig

[10] Riis m.fl. (2013), s. 28
[11] Ibid., s. 32 og Blume (2016), s. 194
[12] Den generelle oplysningspligt fremgår af forordningens art. 13 og 14. Samtykket bruges som behandlingsgrundlag for almindelige personoplysninger, jf. art. 6(1)(a) og følsomme personoplysninger, jf. art. 9(2)(a). De generelle krav til samtykket fremgår af art. 4, nr. 11 og art. 7. Se afsnit 2.1.1 for uddybning.
[13] Princippet om transparens er kodificeret i forordningens art. 5(1)(a). Se afsnit 2.1.1 for uddybning.
[14] Ved *soft law* forstås *normative retskilder*, der hverken er retligt bindende eller judiciable, men som kan have en vis adfærdsregulerende eller vejledende funktion, jf. Harhoff (2017), s. 122 f.
[15] Se hertil forordningens præambelbetragtning 10, 1. pkt. og direktivets art. 1(1)
[16] Blume (2018): *Databeskyttelsesret*, s. 61 f.

retskildemæssig betydning for den europæiske databeskyttelsesret og har påvirket praksis siden gruppen blev nedsat i 1998.[17] Det skyldes især gruppens sammensætning med repræsentanter fra hvert EU-lands datatilsyn, som i fællesskab har udarbejdet udtalelserne og derfor lægger dem til grund i deres nationale praksis.[18] Ved forordningens ikrafttræden d. 25. maj 2018 blev Artikel 29-gruppen erstattet af Det Europæiske Databeskyttelsesråd (herefter EDPB), men udtalelserne fra direktivets tid er fortsat gældende.[19] Henvisninger til direktivet skal nu blot forstås som henvisninger til forordningen, jf. dennes art. 94, stk. 2, 1. pkt., og henvisninger til Artikel 29-gruppen skal forstås som henvisninger til EDPB, jf. 2. pkt. Retskildeværdien er dermed principielt uændret, men nye udtalelser om samme emner fra EDPB må dog antages at mindske de ældre udtalelsers retskildeværdi.

Denne afhandling vil lægge betydelig vægt på udtalelser fra Artikel 29-gruppen. Det skyldes for det første udtalelsernes høje retskildeværdi og betydning for udvikling af gældende ret, jf. ovenfor, og for det andet at der er mangel på *hard law*-kilder som direkte adresserer de problemstillinger, IoT fører med sig (mangel på *lex specialis*). Selvom indsamling af informationer via IoT både falder ind under databeskyttelsesforordningens og ePrivacy-direktivets anvendelsesområder, tager ingen af de to regelsæt således stilling til, hvordan de databeskyttelsesretlige krav rent praktisk skal forstås ved anvendelse af IoT-teknologien. Endelig er denne afhandling som førnævnt udarbejdet med et principielt udgangspunkt om, at alle retskilder er ligestillede, og *soft law* betragtes derfor som en lige så vigtig retskilde som *hard law*, hvis og såfremt det kan føre til løsning af afhandlingens problemformulering.

Udover intraeuropæiske retskilder vil der i enkelte tilfælde blive lagt vægt på internationale retskilder, hvis det i denne afhandling vurderes, at de vil have betydning for gældende ret på området i Danmark. Dette gælder særligt Mauritius-erklæringen, som Den Europæiske Tilsynsførende for Databeskyttelse (herefter EDPS) har tilsluttet sig.[20] EDPS' beføjelser og kompetencer reguleres i en særskilt forordning, EU-forordning 2018/1725 (herefter *EDPS-forordningen*). EDPS er tilsynsmyndighed for den behandling af personoplysninger, der foretages af EU's institutioner og organer, jf. EDPS-

[17] Ibid.
[18] Ibid.
[19] Ibid.
[20] *Mauritius Declaration on the Internet of Things* (2014)

forordningens art. 1(3), og Danmark er som sådan ikke underlagt tilsynet. EDPS spiller imidlertid en vigtig rolle i den databeskyttelsesretlige lovgivningsproces i EU og den efterfølgende fortolkning af reglerne. Det skyldes for det første, at der foreligger en pligt for EU-Kommissionen til at høre EDPS i forbindelse med vedtagelse af retsakter, der påvirker databeskyttelsesretten, jf. EDPS-forordningens art. 42(1), og for det andet at EDPS har mulighed for at intervenere i verserende sager som særlig rådgiver for EU-Domstolen i spørgsmål om fortolkning af databeskyttelsesretlige regler, jf. EDPS-forordningens art. 58(4).[21] Ved at tilslutte sig Mauritius-erklæringen har EDPS sat EU's politiske retning indenfor samspillet mellem IoT og databeskyttelsesretten, og erklæringen vil derfor med stor sandsynlighed danne baggrund for eventuelle fremtidige EU-retsakter på området og på EU-Domstolens fortolkning af databeskyttelsesretlige reglers samspil med IoT – og på den måde også have indvirkning på gældende ret i Danmark.

Der findes ikke vejledninger fra danske tilsynsmyndigheder, der direkte adresserer samspillet mellem IoT og databeskyttelsesretten. Der findes dog vejledninger, der adresserer generelle problemstillinger forbundet med bl.a. oplysningspligt og samtykke, og disse inddrages i afhandlingen i det omfang, det vurderes at kunne bidrage til løsning af problemformuleringen.

Det har ikke været muligt at fremskaffe juridisk litteratur, der på tilstrækkelig vis direkte belyser samspillet mellem IoT og de databeskyttelsesretlige krav om oplysningspligt og samtykke. Der vil dog undervejs henvises til juridisk litteratur, der generelt og uden specifikt at tage stilling til IoT belyser bl.a. oplysningspligten og samtykkekravet. Den aktuelle nedlukning af samfundet pga. COVID19 har begrænset muligheden for fremskaffelse af litteratur til DJØF's jurabibliotek og egne og bekendtes lærebøger fra andre juridiske fag. Indenfor disse rammer er litteraturen udvalgt på baggrund af relevant behandling af databeskyttelsesretlige problematikker, der undervejs i afhandlingen belyses. For så vidt angår forfatterne er der især lagt vægt på disses faglige baggrund, f.eks. henvises der ofte til Peter Blume og Henrik Udsen, da disse, i hvert fald i Danmark, er bredt anerkendt som juridisk kyndige indenfor hhv. databeskyttelses- og IT-retten. Nedlukningen har også

[21] EDPS havde også mulighed for at intervenere som særlig rådgiver for EU-Domstolen under det forudgående regelsæt på området, forordning EF/45/2001, og det er sket flere gange i praksis, se f.eks. Max Schrems-sagen (C-362/14) eller Digital Rights Ireland-sagerne (C-293/12 og C-594/12).

begrænset muligheden for fremskaffelse af udenlandsk litteratur, der derfor ikke inddrages i afhandlingen.

Undervejs i afhandlingen vil praktiske eksempler på IoT-løsninger blive inddraget til illustration, og der vil blive givet bud på, om og i givet fald hvordan oplysnings- og samtykkekravene vil kunne blive løst i praksis.

Afhandlingen indeholder som afslutning et retspolitisk afsnit, hvor der tilsigtes en vurdering af hensigtsmæssigheden af den nuværende regulering af IoT og forslag til ændringer på området.

1.4. Afgrænsning

1.4.1. Tidsmæssig afgrænsning

Retskilder og andet materiale, som er fremkommet, udgivet eller trådt i kraft efter d. 1. april 2020, inddrages ikke i denne afhandling.

1.4.2. Materiel afgrænsning

Afhandlingen vil af indholds-, struktur- og relevansmæssige årsager begrænses for at sikre en mere dybdegående analyse af problemformuleringens fokusområde.

Det betyder, at kun retskilder og bestemmelser, som direkte omhandler eller er grundlaget for de databeskyttelsesretlige krav om oplysningspligt og samtykke, inddrages.

Oplysningspligten har rod i det databeskyttelsesretlige princip om gennemsigtighed (transparens), som derfor også behandles indgående i afhandlingen.

De øvrige databeskyttelsesretlige principper inddrages kun i det omfang, det findes relevant for at besvare problemformuleringen.

Hvad angår oplysningspligten er fokus i afhandlingen alene på de oplysninger, der skal gives til brugeren af IoT forinden samtykke indhentes. Alle andre former for oplysningspligt falder udenfor afhandlingens afgrænsningsområde. Det betyder bl.a., at databeskyttelsesforordningens krav om hvilken information der skal gives i forbindelse med efterlevelse af indsigtsretten (art. 15) eller underretning af den registrerede i forbindelse med brud på persondatasikkerheden (art. 34) ikke behandles.

Særlige krav til samtykker og oplysningspligt i forbindelse med behandling af børns personoplysninger eller i forbindelse med direkte markedsføring, herunder

markedsføringsloven, falder udenfor afhandlingens afgrænsningsområde. Det samme gør sig gældende for behandling af oplysninger om strafbare forhold.

Fokus i afhandlingen vil være på kommercielle virksomheders indsamling af informationer via IoT. Særregler for offentlige myndigheders behandling af persondata og eventuelle brug af IoT falder derfor udenfor afhandlingens afgrænsningsområde.

Afhandlingen vil ikke have fokus på menneskeretlige aspekter af persondatabehandling, og derfor inddrages EMRK, EU-Charteret og andre menneskeretlige retskilder ikke.

1.5. Struktur

Afsnit 2 indeholder en redegørelse for retsgrundlaget, dvs. et overblik over de retskilder der er relevante for besvarelse af problemformuleringen, og som senere i afsnit 3 inddrages i analysen, samt deres historik. Først redegøres der for den egentlige lovregulering i afsnit 2.1 og dernæst for den ikke-bindende ret, *soft law*, i afsnit 2.2. Retskilder, der i afhandlingen kun inddrages perifært eller enkelte gange, gennemgås ikke i afsnit 2.

I afsnit 3 foretages den egentlige analyse, hvor de retskilder, der er blevet opremset i afsnit 2, kobles til indsamling af informationer via IoT – delt overordnet op i kravene om transparens (afsnit 3.1), oplysningspligt (afsnit 3.2) og samtykke (afsnit 3.3). Transparensprincippet behandles som nævnt i afsnit 1.3 og 1.4 som forudsætning for oplysningspligten, da disse to krav er nært beslægtede. Afsnit 3.1, 3.2 og 3.3 deles hver især op i fem delafsnit, der analyserer kravenes materielle og territoriale anvendelsesområder, beskyttelses- og ansvarssubjekter samt kravenes materielle indhold. For så vidt angår delafsnittene om anvendelsesområder og subjekter er der en del overlap mellem afsnit 3.1, 3.2 og 3.3. Derfor behandles disse delafsnit ekstra grundigt i afsnit 3.1 (transparens), mens der i afsnit 3.2 og 3.3 ved overlap henvises bagud. Dette skyldes hensynet til opgavens struktur og er ikke udtryk for en behandling af transparensprincippet på linje med oplysningspligten og samtykkekravet. Den tætte sammenhæng mellem oplysningspligten og transparensprincippet analyseres i afsnit 3.1.5. Undervejs i afsnit 3 inddrages praktiske eksempler, f.eks. hvordan konkrete løsninger fungerer/ikke fungerer på smartwatches mv.

I afsnit 4 vil afhandlingens resultater opsummeres i en afsluttende konklusion, og herefter vil der i afsnit 5 være en retspolitisk vurdering af den gældende rets værdi.

2. RETSGRUNDLAGET – HISTORIK OG OVERSIGT

Som nævnt i afsnit 1 er mængden af retskilder hvad angår databeskyttelsesretlig regulering af IoT særdeles beskeden, henset til at teknologien er relativt ny. Der eksisterer således hverken dansk eller EU-retlig lovgivning, der direkte adresserer problemstillingerne. Det betyder dog ikke, at IoT ikke er reguleret. Som det vil fremgå i det følgende, er teknologien omfattet af mere end ét databeskyttelsesretligt regelsæt. Dernæst kommer forskellige brugbare fortolkningsbidrag i form af *soft law*. I det følgende gennemgås først lovreguleringen af IoT i afsnit 2.1 og dernæst den ikke-bindende ret, soft law, i afsnit 2.2. Der redegøres kun for de i afhandlingen primært benyttede retskilder. Det betyder, at retskilder, der kun benyttes perifært eller enkelte gange, ikke gennemgås.

2.1. Lovregulering

I det følgende redegøres først for databeskyttelsesforordningen i afsnit 2.1.1, dernæst for ePrivacy-direktivet i afsnit 2.1.2 og endelig for cookiebekendtgørelsen i afsnit 2.1.3.

2.1.1. GDPR – databeskyttelsesforordningen

Databeskyttelsesforordningen - populært kendt som *GDPR* – trådte i kraft d. 25. maj 2018 og erstattede det daværende *persondatadirektiv* og dermed også den danske implementeringslov, *persondataloven*, der havde været gældende siden år 2000.[22]

GDPR finder kun anvendelse, hvis databehandlingen omfatter *personoplysninger*, jf. art. 2(1), hvilket er defineret ved, at en fysisk person er eller kan blive identificeret ud fra oplysningerne, jf. art. 4, nr. 1. Behandling af oplysninger om juridiske personer er ikke beskyttet af GDPR, jf. art. 1 modsætningsvist.

Man har efter GDPR mulighed for at behandle personoplysninger, hvis der foreligger et behandlingsgrundlag. Samtykke fra den registrerede kan benyttes som behandlingsgrundlag for behandling af almindelige personoplysninger, jf. art. 6(1)(a), og følsomme personoplysninger, jf. art. 9(2)(a).

Et samtykke skal for begge behandlingsgrundlags vedkommende leve op til kravene i art. 4, nr. 11 og art. 7. Derudover skal det for så vidt angår følsomme personoplysninger tillige være *udtrykkeligt*, jf. art. 9(2)(a).

[22] Direktiv 95/46/EF (*persondatadirektivet*) og LOV nr. 429 af 31/05/2000 (*persondataloven*)

Det afgivne samtykke skal være *informeret*, jf. art. 4, nr. 11, og af art. 13 og 14 fremgår den generelle oplysningspligt med en oplistning af konkrete informationer, der altid skal gives til den registrerede forud for behandling af vedkommendes personoplysninger.

Oplysningspligten har rod i det generelle princip om *transparens* - eller *gennemsigtighed* om man vil. Princippet var ikke nedskrevet i persondatadirektivet og ej heller i persondataloven. I praksis blev det anset for indbygget i princippet om *rimelighed og lovlighed*, jf. direktivets art. 6(1)(a), der i persondatalovens § 5, stk. 1 blev implementeret som *god databehandlingsskik*.[23] Princippet om transparens er nu kodificeret i forordningens art. 5(1)(a).

2.1.2. ePrivacy-direktivet

ePrivacy-direktivet blev vedtaget i 2002 og skulle fungere som supplement til persondatadirektivet med henblik på særligt at adressere behandlingen af persondata inden for den elektroniske kommunikationssektor.[24] Direktivet har gennemgået revision med et ændringsdirektiv i 2009.[25]

Det kan i denne afhandling være nødvendigt at skelne mellem de to direktiver. I disse tilfælde vil direktivet fra 2002 omtales som *EPD 2002* og ændringsdirektivet som *EPD 2009*. Ved brug af udtrykket *ePrivacy-direktivet* henvises der samlet til begge, dvs. direktivet fra 2002 med ændringer af 2009.

ePrivacy-direktivet består af en blandet pose bolsjer med mere eller mindre sammenhængende bestemmelser om bl.a. trafikdata, elektroniske abonnementsfortegnelser og uanmodet henvendelse via elektronisk kommunikation (spam). Langt de fleste bestemmelser er ikke relevante for besvarelse af denne afhandlings problemformulering og gennemgås derfor ikke. En enkelt bestemmelse er dog interessant at belyse. Det drejer sig om art. 5(3), der regulerer muligheden for at lagre eller opnå adgang til allerede lagrede informationer i en abonnents eller brugers terminaludstyr.[26]

---

[23] Dette anføres af Nielsen m.fl. (2020), s. 314, der henviser til, at Datatilsynets praksis inden forordningen allerede stillede krav om gennemsigtighed i fortolkningen af princippet om "rimelighed". Se hertil også Justitsministeriets bemærkninger i bet. nr. 1565/2017 s. 92 f., hvor de tillige vurderer, at kodifikationen af transparensprincippet ikke medfører en ændring af gældende ret.
[24] Direktiv 2002/58/EF. Formålet fremgår af art. 1, stk. 1 og 2.
[25] Direktiv 2009/136/EF
[26] For definition af "*terminaludstyr*" se afsnit 3.2.1.

Den oprindelige version af art. 5(3) i EPD 2002 var baseret på en *opt-out-model*, hvorefter lagring af og adgang til informationer i terminaludstyret som udgangspunkt var lovlig, hvis en oplysningspligt forinden var iagttaget, og som indebar, at lagring/adgang først skulle stoppes, når/hvis abonnenten/brugeren gjorde indsigelse.[27] Bestemmelsen blev skærpet med EPD 2009, som ved at indføre krav om forudgående samtykke resulterede i, at man overgik til en *opt in-model*, hvorefter lagring/adgang som udgangspunkt er ulovlig, medmindre abonnenten/brugeren forinden har givet et aktivt samtykke.[28] Dette er stadig gældende ret.

I modsætning til GDPR omfatter art. 5(3) også information, der ikke indeholder persondata, f.eks. hvor brugeren ikke kan identificeres eller data er anonymiserede.[29] Bestemmelsen har primært sigte på regulering af *cookies*, men er ikke begrænset hertil, idét den omfatter alle former for lagrede informationer.[30] Derudover beskytter bestemmelsen modsat GDPR ikke kun fysiske personer, men i et vist omfang også juridiske personer.[31]

2.1.3. Cookiebekendtgørelsen

EPD 2002 blev implementeret i adskillige danske love, herunder især *teledataloven*, men art. 5(3) blev dengang ikke direkte implementeret i dansk ret.[32] Interessen fra danske myndigheders side var til at overse, og det var således først, da bestemmelsen blev skærpet i 2009, at man fra lovgivers side tog initiativ til implementering.[33] Med ni års forsinkelse blev art. 5(3) i 2011 implementeret i Danmark med vedtagelsen af *cookiebekendtgørelsen*, der fastsætter specifikke krav til oplysningspligt og samtykke i forbindelse med lagring af og adgang til informationer i slutbrugerens terminaludstyr.[34]

Som det kan udledes af navnet, tager bekendtgørelsen ligesom direktivet primært sigte på regulering af cookies, men omfatter alle typer lagrede informationer på slutbrugerens terminaludstyr.[35]

---

[27] U.2010B.319
[28] Ibid.
[29] Det blev slået udtrykkeligt fast af EU-Domstolen i sag C-673/17 (Planet49), præmis 71
[30] Dette kan udledes af ordlyden og af præambelbetragtning 24 til EPD 2002, der som andre eksempler end cookies nævner *spionsoftware*, *web bugs* og *skjulte identifikatorer*.
[31] EPD 2002 art. 1(2). Se afsnit 3.2.3 for uddybning.
[32] U.2010B.319. Teledataloven har undergået adskillige revisioner og findes i dag som LBK nr. 128 af 07/02/2014 om elektroniske kommunikationsnet og -tjenester.
[33] U.2010B.319
[34] BEK nr. 1148 af 09/12/2011. Udstedt i medfør af teledatalovens §§ 9 og 81, stk. 2.
[35] Det kan bl.a. udledes af *cookievejledningen*, der omtaler "cookies og lignende teknologier"

2.2. Soft law

I det følgende redegøres først for udtalelser fra Artikel 29-gruppen i afsnit 2.2.1, dernæst for Mauritius-erklæringen i afsnit 2.2.2 og slutteligt for vejledninger fra danske tilsynsmyndigheder i afsnit 2.2.3.

2.2.1. Artikel 29-gruppens udtalelser

I forbindelse med vedtagelsen af persondatadirektivet blev der nedsat en arbejdsgruppe, som skulle fungere som uafhængig rådgiver for Kommissionen og bidrage til, at direktivet blev anvendt ensartet i medlemsstaterne.[36] Gruppens beføjelser fremgik af direktivets art. 29, og den fik derfor tilnavnet *Artikel 29-gruppen*. Gruppen bestod af repræsentanter fra hver medlemsstats datatilsyn samt fra EU, jf. direktivets art. 29(2), og havde bl.a. til opgave at komme med udtalelser, jf. art. 30, som dog ikke har bindende karakter.[37]

Til trods for gruppens formelt begrænsede magt har den haft stor indflydelse på fortolkningen af direktivets bestemmelser og begreber – langt større end man fra lovgivers side havde regnet med, da man i sin tid nedsatte gruppen.[38]

Artikel 29-gruppen blev ved databeskyttelsesforordningens ikrafttræden erstattet af EDPB, der har stort set samme opbygning, men til gengæld betydeligt mere magt, bl.a. fordi de er tildelt beslutningskompetence i visse grænseoverskridende sager.[39]

EDPB reguleres i forordningens art. 68-76, og alle henvisninger til Artikel 29-gruppen gælder nu som henvisninger til EDPB, jf. forordningens art. 94, stk. 2, 2. pkt. Udtalelser fremsat af Artikel 29-gruppen under direktivet er fortsat gældende under forordningen.[40] For en vurdering af udtalelsernes retskildeværdi se afsnit 1.3.

EDPB har endnu ikke udgivet færdige og officielle vejledninger eller udtalelser om samspillet mellem IoT og databeskyttelsesretten. Det gjorde Artikel 29-gruppen til gengæld i 2014 med udtalelsen *WP 223: Opinion 8/2014 on the on Recent Developments on the Internet of Things*. I udtalelsen slås det fast, at der ofte behandles persondata i forbindelse med indsamling af informationer via IoT, og at persondatadirektivet derfor under

[36] Persondatadirektivets præambelbetragtning 65
[37] Blume (2018): *Den nye persondataret*, s. 255 f.
[38] Ibid., s. 202
[39] Blume (2018): *Databeskyttelsesret*, s. 61 f.
[40] Ibid.

omstændighederne kan finde anvendelse.[41] Som bekendt blev persondatadirektivet afløst af databeskyttelsesforordningen i 2018, og eftersom det følger af forordningens art. 94(2), at henvisninger til direktivet nu gælder som henvisninger til forordningen, må ovenstående læses på den måde, at forordningen under omstændighederne kan finde anvendelse ved indsamling af informationer via IoT. Det slås også fast i udtalelsen, at ePrivacy-direktivets art. 5(3) vil finde anvendelse på indsamling af informationer via IoT, hvis dette indebærer, at der sker lagring af eller adgang til informationer i slutbrugerens terminaludstyr.[42] Udover en analyse af hvilke retsforskrifter der finder anvendelse ved indsamling af informationer via IoT, gennemgår udtalelsen en del specifikke problemstillinger, hvoraf flere er af interesse for denne afhandling og derfor inddrages i afsnit 3. Af interesse for denne afhandling er desuden to vejledninger fra Artikel 29-gruppen om fortolkning af reglerne under GDPR, som blev udgivet umiddelbart inden forordningens ikrafttræden. Det drejer sig om WP 260 om transparens og WP 259 om samtykke.[43] Vejledningerne omhandler ikke direkte IoT, men er generelt udformet og inddrages i afsnit 3 som fortolkningsbidrag i det omfang det findes relevant for besvarelse af problemformuleringen.

2.2.2. Mauritius-erklæringen

Kort efter at Artikel 29-gruppen havde afgivet udtalelse om IoT i 2014 samledes en række databeskyttelseskommissærer, bl.a. EDPS, til en international konference i Balaclava, Mauritius.[44] Konferencen førte til vedtagelsen af *Mauritius Declaration on the Internet of Things*. Der er tale om en ikke-bindende erklæring, som sætter en politisk retning.[45] I erklæringen oplistes en række observationer, hvoraf tre er af interesse for denne afhandling. For det første slås det fast, at data indsamlet via IoT, herunder Big Data, som udgangspunkt bør betragtes som personoplysninger. Det skyldes, at data forekommer i så store mængder og med så høj en kvalitet, at sandsynligheden for at den registrerede bliver identificeret er større end det modsatte. For det andet er det konferencedeltagernes opfattelse, at den værditilvækst, private virksomheder oplever ved salg af IoT-produkter, ikke kun ligger i selve produktet, men i høj grad også i selve brugen af IoT og i de konkrete data, som produkterne indsamler om brugerne. Observationen er interessant, fordi den

[41] WP 223, s. 10 f.
[42] Ibid., s. 14
[43] *Guidelines on transparency under Regulation 2016/679* (WP 260) & *Guidelines on consent under Regulation 2016/679* (WP 259)
[44] At EDPS var repræsenteret på konferencen fremgår af EDPS' årsberetning for 2014, s. 14 f.
[45] Covington & Burling LLP (2014)

belyser, at virksomheder har en særlig kommerciel interesse i at indhente persondata om brugerne. Indsamling af data er altså ikke en afledt bivirkning af brugen af IoT, men en del af selve formålet. Den tredje interessante observation i erklæringen omhandler oplysningspligten og samtykkekravet. Det er kommissærernes opfattelse, at transparens er af afgørende betydning, hvis tilliden til IoT-teknologien skal opretholdes. Det betyder, at der er visse informationer, som IoT-brugerne bør gives forinden brug. De aktører, der udbyder IoT-produkter, bør gøre brugerne opmærksomme på, hvilke data der indsamles, til hvilket formål de indsamles, og hvor lang tid de opbevares. Informationen bør gives på en korrekt, tilstrækkelig og forståelig måde, og det er kommissærernes opfattelse, at udbydernes privatlivspolitikker ikke altid lever op til dette krav. Kommissærerne slår desuden fast, at et samtykke til indsamling af informationer via IoT næppe kan betragtes som et informeret samtykke, hvis det er indhentet på baggrund af en sådan privatlivspolitik.

Datatilsynet var i modsætning til EDPS ikke repræsenteret på konferencen og har derfor ikke forholdt sig til erklæringen.[46] Selvom Datatilsynet ikke formelt har tilsluttet sig, må det anses for sandsynligt, at erklæringen får betydning for gældende ret i Danmark. Det skyldes, at EDPS har væsentlig indflydelse på både EU-lovgivningsprocessen og på EU-Domstolens fortolkning af databeskyttelsesretlige regler. For uddybende redegørelse herfor se afsnit 1.3.

2.2.3. Vejledninger fra danske tilsynsmyndigheder

I Danmark håndhæves databeskyttelsesforordningens krav til persondatabehandling af Datatilsynet.[47] Håndhævelsen af bestemmelserne i cookiebekendtgørelsen og dermed de implementerede krav fra ePrivacy-direktivets art. 5(3) varetages af Erhvervsstyrelsen.[48] Der eksisterer ingen vejledninger fra de to tilsynsmyndigheder, der direkte omhandler samspillet mellem IoT og samtykke- og oplysningskravene. Til gengæld foreligger der flere generelle vejledninger, som kan bidrage til en generel forståelse af kravene. I denne afhandlings afsnit 3 inddrages Datatilsynets vejledninger om de registreredes rettigheder og om samtykke samt Erhvervsstyrelsens vejledning til cookiebekendtgørelsen, "*Cookievejledningen*", hvor det findes relevant.

[46] Det oplyser Datatilsynet selv i en e-mail (se bilag 1). Derudover nævnes konferencen hverken i Datatilsynets årsberetning eller årsrapport for 2014.
[47] Udsen (2019), s. 452 in fine
[48] Ibid., s. 504 in fine

3. ANALYSE AF GÆLDENDE RET MED INDDRAGELSE AF PRAKTISKE EKSEMPLER

3.1. Transparensprincippet

Som nævnt i bl.a. afsnit 1.3, 1.5 og 2.1 har princippet om transparens betydning for oplysningspligten, hvorfor dette princip vil blive behandlet først. I det følgende vil der foretages en analyse af, hvilken betydning det databeskyttelsesretlige princip om transparens har for indsamling af informationer via IoT. Undervejs inddrages eksempler på praktiske problemstillinger, og der gives bud på løsninger herpå. Først analyseres princippets materielle anvendelsesområde i afsnit 3.1.1, dernæst det territoriale anvendelsesområde i afsnit 3.1.2. Princippets beskyttelsessubjekter analyseres i afsnit 3.1.3 og ansvarssubjekterne i afsnit 3.1.4. Til slut analyseres princippets materielle indhold i afsnit 3.1.5.

Da størstedelen af observationerne i afsnit 3.1.1, 3.1.2, 3.1.3 og 3.1.4 også gør sig gældende for oplysningspligten (afsnit 3.2) og samtykkekravet (afsnit 3.3), behandles disse delafsnit særligt grundigt.

Kravet om transparens er et grundlæggende princip indenfor databeskyttelsesretten. Som der blev redegjort for i afsnit 2.1.1, var det gældende ret allerede inden forordningen, selvom det hverken var skrevet ind i persondatadirektivet eller persondataloven. Der er altså tale om en form for retsgrundsætning, og det må derfor antages at gælde uafhængigt af forordningen. Selv uden nedskrevne regler må behandling af persondata være underlagt et krav om transparens. Det er derfor interessant at undersøge, om der reelt er forskel på retsgrundsætningen og den kodificerede version af princippet, og nedenstående analyser vil derfor tage stilling til begge dele.

3.1.1. Materielt anvendelsesområde

Princippet om transparens er som nævnt i afsnit 2.1.1 blevet kodificeret i databeskyttelsesforordningen. Forordningen finder anvendelse ved behandling af personoplysninger, jf. art. 2(1). Det er således uden for enhver tvivl, at transparensprincippet er gældende, hvis de indsamlede data indeholder personoplysninger.

En stor del af de data, der indsamles ved brug af IoT, er *Big Data*.[49] Det rejser spørgsmålet om, hvorvidt der foreligger krav om transparens, når disse enorme mængder data indsamles i anonymiseret form.

Anonymiserede data er ikke omfattet af forordningen. Det følger udtrykkeligt af præambelbetragtning 26:

"Databeskyttelsesprincipperne bør […] ikke gælde for anonyme oplysninger, dvs. oplysninger, der ikke vedrører en identificeret eller identificerbar fysisk person, eller for personoplysninger, som er gjort anonyme på en sådan måde, at den registrerede ikke eller ikke længere kan identificeres. Denne forordning vedrører derfor ikke behandling af sådanne anonyme oplysninger […]"

Det er af afgørende betydning, at den registrerede ikke kan identificeres længere. Hvis der ved brug af hjælpemidler kan ske identifikation, er der tale om pseudonymiserede oplysninger, og så finder forordningen alligevel anvendelse, jf. også betragtning 26:

" Personoplysninger der har været genstand for pseudonymisering, og som kan henføres til en fysisk person ved brug af supplerende oplysninger, bør anses for at være oplysninger om en identificerbar fysisk person."

Eftersom forordningen finder anvendelse på pseudonymiserede data, og princippet om transparens er kodificeret i forordningen, kan det slås fast, at der er krav om transparens ved indsamling af data i pseudonymiseret form.

Ovenfor blev det slået fast, at anonymiserede data ikke er omfattet af forordningen. Det betyder samtidig, at den kodificerede version af transparensprincippet ikke finder anvendelse på anonymiserede data. Spørgsmålet er dernæst, om anonymiserede data er underlagt transparensprincippet som retsgrundsætning? Der findes umiddelbart ikke noget belæg for den påstand, som derfor må afvises. Personoplysninger har til alle tider været defineret som behandling af oplysninger om identificerede eller identificerbare fysiske personer.[50] Anonymiserede oplysninger udgør derfor næppe personoplysninger i den ikke-nedskrevne ret. På baggrund af det forestående må det vurderes, at transparensprincippet som retsgrundsætning ligesom den kodificerede version ikke finder anvendelse på anonymiserede data.

[49] Verma (2018). *Big Data* defineres som begreb i afsnit 1.1.
[50] Se f.eks. forordningens art. 4, nr. 1, persondatadirektivets art. 2, litra a, persondatalovens § 3, nr. 1 og lov om private registre (LBK nr. 622 af 02/10/1987) § 1, stk. 2.

Eftersom anonymiserede data hverken er omfattet af forordningen eller retsgrundsætningen om transparens, kunne man foranlediges til at tro, at IoT-udbydere frit kan indsamle *Big Data* i anonymiseret form. Denne retsstilling blev på Mauritius-konferencen ikke anset for hensigtsmæssig, og det første punkt i den efterfølgende erklæring havde derfor følgende ordlyd:

"Internet of Things' sensor data is high in quantity, quality and sensitivity. This means the inferences that can be drawn are much bigger and more sensitive, and ***identifiability becomes more likely than not****. Considering that the identifiability and protection of big data already is a major challenge, it is clear that big data derived from internet of things devices makes this challenge many times larger. Therefore,* ***such data should be regarded and treated as personal data****."*[51] **(mine fremhævninger)**

EDPS har, som nævnt i afsnit 1.3 og 2.2.2, tilsluttet sig erklæringen, og i en udtalelse om Big Data fra 2015 erklærer EDPS sig enig i ovenstående punkt:

"Such 'big data' ***should be considered personal*** *even where* ***anonymization*** *techniques have been applied: it is becoming and will be ever easier to infer a person's identity by combining allegedly 'anonymous' data with publicly available information such as on social media.*"[52] (**mine fremhævninger**)

Synspunktet går igen i Artikel 29-gruppens udtalelse om IoT, om end i en mere moderat udgave (med brug af udtrykket "*may have*" i stedet for "*should be*"):

"[…] even data relating to individuals that is intended to be processed only after the implementation of pseudonymization, or even of ***anonymization*** *techniques* ***may have to be considered as personal data****. In fact, the large amount of data processed automatically in the context of IoT entails risks of re-identification.*"[53] (**mine fremhævninger**)

Der er altså i databeskyttelsesretlige organer bred enighed om, at *Big Data* skal betragtes som personoplysninger, uanset at de indsamlede data er anonymiserede. Argumentationen er, at mængden og kvaliteten af dataene gør det sandsynligt, at selv de bedste anonymiseringsværktøjer ikke i tilstrækkelig grad vil kunne forhindre re-identifikation af den registrerede.

Ud fra ovenstående betragtninger må retsstillingen derfor betegnes således, at anonymiserede oplysninger ikke er underlagt et krav om transparens, *men* at indsamling af Big Data *er* omfattet af kravet, fordi tilstrækkelig anonymisering af Big Data er illusorisk.

[51] Mauritius-erklæringen, pkt. 1
[52] EDPS (2015): *Opinion 7/2015 Meeting the challenges of big data*, s. 7
[53] WP 223, s. 11

Forordningen gælder ikke for persondatabehandling, som foretages af en fysisk person som led i rent personlige eller familiemæssige aktiviteter, jf. art. 2(2)(c). Artikel 29-gruppen anser denne undtagelse for at have et begrænset anvendelsesområde i relation til IoT.[54] Det skyldes, at indsamling og behandling af data via IoT mestendels foretages af kommercielle virksomheder og ikke af private husholdninger.[55] Dette synspunkt understøttes af den praktiske virkelighed som beskrevet i afsnit 1.1 og må derfor tilsluttes.

3.1.2. Territorialt anvendelsesområde

Vi lever i en globaliseret verden, og udbydere af tech-produkter, herunder IoT, har ofte ikke hovedkontor indenfor Unionens grænser, og registrerede rejser rundt i verden og køber udstyr udenfor land og rige. Det rejser flere relevante spørgsmål til, hvornår forordningen og kravet om transparens finder anvendelse.

Eksempelvis kunne man forestille sig følgende scenarium: Et smartwatch er produceret i Japan. En dansk turist køber det hos en lokal forhandler i Tokyo og tager det med hjem til Danmark. Uret indsamler informationer om danskerens løberuter, kalorieforbrænding, puls og gennemsnitshastighed og sender oplysningerne videre til producentens hovedkontor i Silicon Valley, Californien. Vil forordningen og transparensprincippet finde anvendelse i denne situation?

Det følger af databeskyttelsesforordningens art. 3(1), at den finder anvendelse på behandling af persondata, der foretages som led i aktiviteter, der udføres for en dataansvarlig eller en databehandler, som er etableret i EU, uanset om behandlingen finder sted i EU eller ej. Det er af EU-Domstolen slået fast, at *"enhver, selv minimal, reel og faktisk aktivitet, der udøves via en permanent struktur"* medfører, at der er tale om en etablering i Unionen.[56] Kravene, til hvornår den i eksemplet nævnte smartwatch-producent er etableret i EU og dermed omfattet af forordningen, er altså meget lave.

Hvis det relativt usandsynlige skulle ske, at etableringskravet ikke er opfyldt, følger det af art. 3(2), at forordningen alligevel finder anvendelse, hvis den registrerede befinder sig indenfor Unionen, og behandlingsaktiviteterne enten vedrører udbud af varer eller tjenesteydelser til den registrerede, uanset krav om betaling, eller overvågning af den

[54] WP 223, s. 13
[55] Ibid.
[56] Sag C-230/14 (Weltimmo), præmis 31

registreredes adfærd indenfor EU. Det betyder, at smartwatch-producenten i eksemplet vil være omfattet af forordningen, hvis indsamlingen af informationerne sker som led i aktiviteter, der er rettet mod et marked indenfor EU, eller hvis det sker med det formål at overvåge den dansker, der benytter uret. Ved vurderingen af hvorvidt ansvarssubjektet har rettet blikket mod et marked indenfor Unionen, ses der bl.a. på, om der anvendes et sprog eller kan betales med en valuta, der er almindeligt anvendt i Unionen.[57] Kan den danske smartwatch-bruger f.eks. indstille urets sprog til dansk, må det tale for, at producenten har blikket rettet mod det danske marked, og forordningen og transparensprincippet finder dermed anvendelse. Ved vurderingen af hvorvidt der er tale om en overvågning af den registreredes adfærd, ses der bl.a. på, om vedkommende spores og profileres med det formål at analysere eller forudsige den pågældendes præferencer, adfærd og holdninger.[58] Det betyder, at hvis smartwatch-producenten bruger de indsamlede informationer om den danske forbruger til at foretage direkte markedsføring, vil det tale for, at der foretages overvågning af den pågældende, og forordningen og transparensprincippet vil derfor også finde anvendelse i denne situation.

Hvis virksomheden ikke er etableret i EU, og hvis den registrerede samtidig befinder sig udenfor EU, vil forordningen kun finde anvendelse, hvis der foreligger jurisdiktion efter folkeretten, jf. art. 3(3). Det vil f.eks. være tilfældet, hvis persondatabehandlingen vedrører en medlemsstats diplomatiske eller konsulære repræsentation.[59] Bærer en diplomat på en dansk ambassade i udlandet et smartwatch, vil indsamlingen af informationer herigennem være reguleret af forordningen og dermed også af transparensprincippet.

Som illustreret ovenfor må det betragtes som en både besværlig og usandsynlig øvelse, hvis smartwatch-producenten som nævnt i eksemplet skal undvige forordningens regler.

Som nævnt i afsnit 3.1.1 er princippet om transparens en form for retsgrundsætning og gælder uanset kodifikationen i forordningen. Man kan derfor spørge sig selv, hvilket territorialt anvendelsesområde en sådan retsgrundsætning har. Eftersom der er tale om et princip udviklet indenfor EU-retten, er det nærliggende at antage, at det kun vil finde anvendelse, når EU-retten ellers finder anvendelse, og hvis EU-Domstolen på et tidspunkt

[57] Forordningens præambelbetragtning 23
[58] Forordningens præambelbetragtning 24
[59] Forordningens præambelbetragtning 25

skal tage stilling til dette meget teoretiske spørgsmål, må det formodes, at den vil falde tilbage på de regler, der er fastsat i forordningens art. 3, og som der er redegjort for herover. Det er dog som nævnt en meget teoretisk diskussion, og under alle omstændigheder er krav om transparens i forbindelse med behandling af persondata ikke et enestående EU-retligt fænomen, men findes også i retssystemer udenfor Unionen.[60]

3.1.3. Beskyttelsessubjekter

Det følger af forordningens art. 1, stk. 1 og 2, at formålet med regelsættet er at beskytte fysiske personers rettigheder og frihedsrettigheder i forbindelse med behandlingen af personoplysninger. Forordningens og dermed også det kodificerede transparensprincips beskyttelsessubjekt er altså fysiske personer.

Retsgrundsætningen om transparens er som førnævnt udviklet indenfor databeskyttelsesretten i EU, og denne databeskyttelsesret har historisk haft til formål at beskytte fysiske personer.[61] Det vurderes derfor, at beskyttelsessubjektet for retsgrundsætningen er det samme som for den kodificerede version af princippet, nemlig fysiske personer.

I en IoT-kontekst betyder ovenstående, at beskyttelsessubjektet er de fysiske personer, hvis persondata indsamles og behandles via IoT. Artikel 29-gruppen udtaler i WP 223, at dette beskyttelsessubjekt ikke altid er identisk med ejeren eller brugeren af IoT-produktet, og peger i den forbindelse særligt på *smartglasses*, altså briller koblet op til internettet.[62] Brillerne kan opfange de fysiske personer, som brillebæreren kigger på, og informationer om disse fysiske personers udseende og karakteristika kan derefter, uden bærerens vidende, indsamles og sendes ind til brilleproducenten med henblik på at forbedre brugeroplevelsen. I denne situation behandles persondata om de fysiske personer, som brillerne observerer, og de vil derfor blive betragtet som registrerede og dermed som beskyttelsessubjekter, selvom de hverken ejer eller bruger brillerne selv.

3.1.4. Ansvarssubjekter

I databeskyttelsesforordningen opererer man med begreberne *dataansvarlig* og *databehandler*. Den dataansvarlige defineres som den aktør, der alene eller sammen med andre bestemmer formålene med og hjælpemidlerne til persondatabehandlingen, jf.

[60] Dette kan bl.a. udledes af, at et krav om transparens er fastsat i Mauritius-erklæringen, der har folkeretlig karakter og dermed også er gældende udenfor EU's grænser.
[61] Se f.eks. persondatadirektivets art. 1(1) og præambelbetragtning 2, 27 og 62
[62] WP 223, s. 13

forordningens art. 4, nr. 7. Databehandleren defineres som den aktør, der behandler persondataene på den dataansvarliges vegne, jf. art. 4, nr. 8. Begge aktører kan være fysiske såvel som juridiske personer.[63] Den dataansvarlige er ansvarlig for både sin egen og sin databehandlers behandling af personoplysninger, mens databehandleren kun er ansvarlig for sin egen behandling.[64] Det betyder, at både den dataansvarlige og databehandleren kan betragtes som ansvarssubjekter i relation til overholdelse af forordningens regler, herunder transparensprincippet.

Der er mange aktører involveret i produktion, salg og indsamling af informationer via IoT. Det er derfor interessant at belyse, hvilke konkrete aktører der kan stilles til ansvar for brud på reglerne, altså hvem der kan betragtes som dataansvarlig eller databehandler. Til besvarelse af dette spørgsmål er der hjælp at hente hos Artikel 29-gruppen, der i WP 223 identificerer og analyserer fem aktører indenfor IoT-branchen, der alle vil kunne betragtes som ansvarssubjekter.[65]

Den første aktør er "*device manufacturers*", dvs. producenter af IoT-enheder. Artikel 29-gruppen betragter denne aktør som dataansvarlig og begrunder det med, at producenterne ofte ikke blot står bag den fysiske udformning af produktet, men også den indre programmering, herunder dataindsamlingen, hvoraf de selv bestemmer en stor del af indsamlingens formål.[66] Det kan illustreres med et praktisk eksempel: Sebastian har købt et *Apple TV* med tilhørende fjernbetjening, der bl.a. fungerer via stemmegenkendelse. Fjernbetjeningen registrerer, når Sebastian udtaler navnet på en tv-udsendelse og sender besked videre til tv'et, der dernæst afspiller udsendelsen. Apple har produceret fjernbetjeningen, inkl. dens indre programmering. Denne programmering sørger for, at oplysninger om Sebastians foretrukne tv-udsendelse indsamles og sendes videre til Apple med det formål at indkode Sebastians præferencer. Apple har selv fastlagt formålet med indsamlingen og er derfor at betragte som dataansvarlig – og dermed et ansvarssubjekt.

Den anden aktør er "*social platforms"*, altså sociale medier, som Artikel 29-gruppen i denne sammenhæng anser for dataansvarlige, fordi de ofte bruger de data, den

[63] Det følger af ordlyden i forordningens art. 4, nr. 7 og 8
[64] Blume (2018): *Databeskyttelsesret*, s. 66 ff.
[65] WP 223, s. 11 ff. Der er ikke tale om en udtømmende opremsning, men blot eksempler, der er særligt udvalgt til analyse, jf. brugen af udtrykket "*such as*" på s. 11.
[66] WP 223, s. 11

registrerede uploader til deres platforme, til at foretage direkte markedsføring, dvs. til deres egne formål.[67] Et eksempel herpå er løberen, som benytter sit smartwatch til at måle den tilbagelagte distance og herefter stolt uploader disse data til Facebook, hvorefter han den følgende dag modtager annoncer for løbesko i sit nyhedsfeed. Annoncerne illustrerer, at Facebook har behandlet data om løbeturen til deres eget formål: Direkte markedsføring. Facebook er derfor dataansvarlig for behandlingen og dermed et ansvarssubjekt.

Den tredje aktør er "*Third party application developers*", altså tredjeparter der udvikler apps til f.eks. smartwatches. Artikel 29-gruppen betragter denne aktør som databehandler og begrunder det med, at appudvikleren har adgang til persondata, og at adgang i sig selv udgør behandling.[68] Et eksempel herpå er den populære app Endomondo, som registrerer lokationsdata for f.eks. brugerens løbeture og kan downloades til diverse produkter. Brugeren giver Endomondo tilladelse til at registrere hans lokationsdata med det formål at registrere hans løberuter. Brugeren bestemmer selv til hvilke konkrete løbeture appen benyttes og dermed hvilke konkrete ruter, der skal registreres. Brugeren fastlægger således formålet med databehandlingen, nemlig registrering af de af brugeren valgte løberuter. Endomondo har dog stadig adgang til dataene og behandler dem efter instruks fra brugeren, f.eks. til kortlægning og systematisering. Endomondo skal derfor betragtes som databehandler og dermed et ansvarssubjekt.

Den fjerde aktør er "*Other third parties*". Det defineres som tredjeparter, der hverken er IoT-producenter eller appudviklere.[69] Artikel 29-gruppen anser denne aktør for at være dataansvarlig i det omfang, de indsamler og opbevarer data til egne formål.[70] Et eksempel herpå er et livsforsikringsselskab, der udleverer digitale skridttællere til kunder mod at få adgang til de af skridttælleren indsamlede data. Formålet er at hæve eller sænke forsikringspræmien alt afhængig af kundens helbred, der vurderes ud fra den fysiske aktivitet, som skridttælleren måler. Forsikringsselskabet har ikke selv udviklet skridttælleren, men indsamler alligevel dataene og behandler dem til egne formål. Forsikringsselskabet skal derfor anses for at være dataansvarlig og dermed et ansvarssubjekt.

[67] Ibid., s. 12
[68] Ibid.
[69] Ibid.
[70] Ibid.

Den femte aktør er "*IoT data platforms*". Artikel 29-gruppen definerer en dataplatform som en lokal database hos IoT-producenten, hvor data *hostes* (opbevares) og holdes adskilt fra andre data med det resultat, at IoT-brugeren bliver effektivt forhindret i at overføre eller kombinere data mellem forskellige IoT-enheder.[71] Artikel 29-gruppen anser udbydere af disse dataplatforme for at være dataansvarlige og begrunder det med, at indsamlingen og opbevaringen af dataene sker til egne formål.[72] Til illustration kan der bygges videre på eksemplet med Sebastians Apple TV, som nu har opfanget, at Sebastian ofte ser pressemøder med Donald Trump. Denne oplysning sendes til en af Apples dataplatforme og "låses inde". Sebastian bliver træt af Apple og køber et *Shield* (et Google TV). Sebastian har ikke mulighed for at overføre sin præference for Donald Trumps pressemøder fra sit Apple TV til sit Google TV, da data herfor er låst inde i dataplatformen. Apple har indhentet og opbevaret dataene til egne formål, nemlig at give Sebastian en bedre brugeroplevelse, og skal derfor anses for at være dataansvarlig og dermed et ansvarssubjekt.

Ovenstående fem aktører er de eneste, der gennemgås systematisk i WP 223, men herudover er der tegn på, at Artikel 29-gruppen anser en sjette aktør for et potentielt ansvarssubjekt. Et punkt i WP 223 peger nemlig i retning af, at IoT-brugere kan anses for at være ansvarssubjekter efter forordningen. Der står således at:

"Users of IoT devices should inform non-user data subjects whose data are collected of the presence of IoT devices and the type of collected data. They should also respect the data subject's preference not to have their data collected by the device."[73]

Der gives altså udtryk for, at IoT-brugere har en vis informationspligt overfor registrerede, der ikke er brugere. Det er et bemærkelsesværdigt krav at stille, især fordi det hverken uddybes eller begrundes.

Som nævnt i afsnit 3.1.3 er den registrerede og brugeren ikke altid identiske subjekter, da brugerens IoT-produkt i visse tilfælde kan behandle data om andre end brugeren. Det blev eksemplificeret med *smartglasses*, som indsamler informationer om individer i brillebærerens nærhed. Hertil er det interessant at belyse, hvorvidt bæreren i stedet kan betragtes som ansvarssubjekt, altså om bæreren kan kategoriseres som dataansvarlig eller

[71] Ibid., s. 13
[72] Ibid.
[73] Ibid., s. 24

databehandler. Data indsamlet om individer i bærerens nærhed behandles ofte til formål bestemt af brilleproducenten, f.eks. forbedring af brugeroplevelsen. Da bæreren ikke har bestemt formålet med behandlingen, kan han ikke anses for at være dataansvarlig. Spørgsmålet er dernæst, om bæreren behandler dataene på producentens vegne og dermed kan betragtes som databehandler. På den ene side kan man argumentere for, at bæreren er en form for mellemmand, der ved at benytte og evt. ændre på brillernes indstillinger sørger for, at data indsamles og videresendes til producenten og på denne måde foretager en form for databehandling. På den anden side har bæreren næppe overblik over de indsamlede data og ej heller adgang hertil, udover det øjeblik han observerer den registrerede gennem brillerne. Situationen er naturligvis en anden, hvis bæreren i stedet for blot at se på den registrerede tager et billede af ham ved at benytte fotofunktionen i brillerne. I så fald behandler bæreren persondata (billedet) til egne formål og skal derfor anses for dataansvarlig. Det er også muligt, at Artikel 29-gruppen med citatet ikke havde fysiske personer in mente, men derimod blikket rettet mod juridiske personers brug af IoT-produkter. Det er ren spekulation, men kunne give mening, da det kan give udfordringer i praksis. F.eks. kan man forestille sig en erhvervsvirksomhed installere intelligente kameraer på lageret, som automatisk observerer og giver besked om dovne medarbejdere. I et sådant tilfælde vil brugeren af produktet, erhvervsvirksomheden, indsamle persondata til eget formål og dermed være dataansvarlig.

Artikel 29-gruppen kommer i deres udtalelse ikke ind på, om de i situationer som ovenstående anser IoT-brugeren for dataansvarlig eller databehandler. De kommer som nævnt heller ikke med en begrundelse for, hvorfor de mener, at IoT-brugeren har en informationspligt overfor den registrerede. Det er derfor uvist, *hvorfor* og i hvilke situationer de anser IoT-brugeren for ansvarssubjektet. Det kan dog konstateres, at de anser det for en mulighed, og som denne afhandling netop har eksemplificeret ovenfor, kan der argumenteres for synspunktet i en praktisk kontekst. Det er derfor undertegnedes vurdering, at fysiske såvel som juridiske personer, der er brugere af et IoT-produkt, efter omstændighederne kan anses for ansvarssubjekter. Det betyder, at de kan ifalde ansvar ved manglende efterlevelse af forordningen, herunder transparensprincippet.

Retsgrundsætningen om transparens er udviklet gennem praksis, herunder fra Datatilsynet, som også var repræsenteret i Artikel 29-gruppen, da den kom med sin udtalelse om

IoT.[74] Det må derfor anses for usandsynligt, at Datatilsynet vil tillægge retsgrundsætningen et andet indhold end ovenstående. De subjekter, der kan ifalde ansvar efter retsgrundsætningen, vurderes derfor til at være identiske med de subjekter der er anført ovenfor.

3.1.5. Materielt indhold

Transparensprincippet er kodificeret i forordningens art. 5(1)(a), men bestemmelsen uddyber ikke princippets nærmere indhold, udover at gennemsigtigheden skal gælde *"i forhold til den registrerede".* Det er altså for den registreredes skyld, at der skal foreligge transparens. Eller som Blume (2018) indkapsler det: "*Det skal være muligt for den registrerede at overskue den behandling, der finder sted"*.[75]

I forordningens præambelbetragtning 39 uddybes princippets materielle indhold:

"Det bør være gennemsigtigt for de pågældende fysiske personer, at personoplysninger, der vedrører dem, indsamles, anvendes, tilgås eller på anden vis behandles, og i hvilket omfang personoplysninger behandles eller vil blive behandlet."

De registrerede skal altså have vished om, hvorvidt der indsamles eller på anden måde behandles persondata om dem, og i hvilket omfang det sker. Forbavsende ofte er dette krav ikke opfyldt. Som nævnt i afsnit 1.1 er registrerede ofte uvidende om, at deres persondata indsamles via IoT.

Betragtning 39 uddyber princippet yderligere:

"Princippet om gennemsigtighed tilsiger, at enhver information og kommunikation vedrørende behandling af disse personoplysninger er lettilgængelig og letforståelig, og at der benyttes et klart og enkelt sprog."

Transparens handler altså ikke kun om vished, men i lige så høj grad om formidling. De registrerede skal have vished på en måde, så de rent faktisk forstår, hvad der foregår.

Udtrykkene *"lettilgængelig og letforståelig"* og *"et klart og enkelt sprog"* går igen i forordningens art. 12(1), der fastsætter formkrav til, hvordan den dataansvarlige giver transparente oplysninger og meddelelser til de registrerede. Disse formkrav udspringer som illustreret direkte af transparensprincippet.

[74] At transparensprincippet er udviklet gennem praksis fra bl.a. Datatilsynet anføres af Nielsen m.fl. (2020), s. 314. Se afsnit 2.1.1 og note 23 for uddybning. At Datatilsynet var repræsenteret i Artikel 29-gruppen fremgår af persondatadirektivets art. 29(2).
[75] Blume (2018): *Den nye persondataret*, s. 86

I en digital tidsalder, hvor dataindsamling ofte foregår ved hjælp af komplicerede algoritmer, som de færreste mennesker forstår, kan disse krav give udfordringer i praksis. En kompliceret forklaring, om *hvordan* indsamlingen rent teknisk foregår med angivelse af formler mv., vil næppe leve op til kravet om transparens, da der ikke foreligger et "klart og enkelt sprog," og det vil næppe heller være "letforståeligt".[76] I stedet må man skrælle al det tekniske fra, skære ind til benet, være præcis og formidle i et sprog, som en ikke-fagkyndig person vil kunne forstå. Dette gøres i praksis ofte ved udarbejdelse af privatlivspolitikker og andre former for oplysningsdokumenter, der udleveres til den registrerede, enten i papirform eller elektronisk. I en IoT-kontekst vil dette ikke altid give mening. Man kan f.eks. forestille sig, at et kærestepar har købt en *Google Home Mini*. Det er en højttaler, der udover at afspille lyd har en indbygget *digital assistent*, der fungerer som et slags leksikon eller en googlesøgemaskine i lydformat. Du kan spørge den om alt, fra hvem der myrdede Kennedy til hvad klokken er i Amsterdam. Eftersom der er tale om en højttaler uden nogen form for skærm, kan en privatlivspolitik i digitalt format ikke komme på tale. Alternativt kan man vedlægge den i papirform i den æske, produktet bliver solgt i. Problemet her er blot, at denne privatlivspolitik hurtigt bliver forældet og næppe opfylder oplysningspligten korrekt og fyldestgørende. Sagen er nemlig den, at IoT-producenten ikke på forhånd ved, hvilke informationer, Google Home Mini vil indsamle om de registrerede. Det afhænger nemlig af, hvordan de registrerede bruger apparatet; hvad de spørger om, hvordan de indstiller det osv. Og vage og upræcise vendinger som *"vi vil måske indhente oplysninger om"* eller *"det er sandsynligt, at vi vil indsamle"* lever ikke op til transparensprincippet.[77] En oplagt måde at løse det problem på ville være at give informationen i lydformat via højttaleren. Den første besked kan gives, når brugeren første gang tænder for højttaleren, og efterfølgende vil der jævnligt kunne gives nye beskeder, når nye oplysninger indsamles. Man vil derudover kunne sørge for, at brugeren kan få genopfrisket oplysningerne ved at stille spørgsmål til højttaleren, f.eks. *"Hvilke personoplysninger behandler I om mig?"*. På den måde vil den registrerede løbende blive holdt informeret, også ved ændringer i behandlingen, og producenten vil slippe for dyrt og irriterende papirarbejde. Selvom denne ellers oplagte løsning vil være til gavn for alle

[76] Denne formodning understøttes af WP 260, s. 10, hvor der står: *"The information provided to a data subject should not contain overly legalistic, technical or specialist language or terminology."*
[77] Det fremgår af eksemplerne på s. 9 i WP 260, hvor det tillige udtrykkes, at *"Language qualifiers such as 'may', 'might', 'some', 'often' and 'possible' should […] be avoided."*

parter, er det usikkert, hvorvidt den lever op til forordningens formkrav. Af art. 12, stk. 1, 2. og 3. pkt. fremgår det således at:

*"Oplysningerne gives **skriftligt** eller med **andre midler**, herunder hvis det er hensigtsmæssigt, **elektronisk**. **Når den registrerede anmoder om det**, kan oplysningerne gives **mundtligt**, forudsat at den registreredes identitet godtgøres med andre midler."* **(mine fremhævninger)**

En oplæsning via en højttaler er selvsagt ikke en skriftlig formidling. Elektronisk formidling kan gives, når det er hensigtsmæssigt, mens mundtlig formidling kun er gyldig, hvis den registrerede anmoder om det. Er en formidling via en højttaler en elektronisk eller mundtlig formidling? Højttaleren er selvfølgelig et stykke elektronik, men omvendt er lyd jo også en form for mundtlig formidling – medmindre man antager, at "*mundtlig*" kun tæller lyd, der udspringer af en mund, der bæres af en fysisk person. I så fald vil lyd via højttaleren ikke være mundtlig, da stemmen ikke tilhører en bestemt person, men er autogenereret via kunstig intelligens. Uden at tage direkte stilling til dette modsætningsforhold berøres situationen sporadisk af Artikel 29-gruppen i en vejledning om, hvordan transparensprincippet skal forstås under forordningen (WP 260):

*"Non-written electronic **means** which may be used **in addition** to a layered privacy statement/notice might include videos and smartphone or **IoT voice alerts**."* (**mine fremhævninger**).[78]

"*Means*" er det begreb i den engelske udgave af forordningens art. 12(1), der svarer til "*midler*" i den danske udgave ("*Oplysningerne gives skriftligt eller med andre midler"*), og "*IoT voice alerts*" må antages at dække over en situation, hvor en højttaler autogenerisk via kunstig intelligens oplæser en privatlivspolitik.

Citatet fra vejledningen er ikke uddybet og er svær at blive klog på. I forordningens art. 12, stk. 1, 2. pkt. står der (**min fremhævning**), at "*Oplysningerne gives skriftligt **eller** med andre midler, herunder hvis det er hensigtsmæssigt, elektronisk.*" Brugen af ordet "*eller*" må medføre, at "*andre midler"* kan være et direkte alternativ til skriftlighed, medmindre midlerne er "*elektroniske*". I så fald er der et ekstra krav om, at det skal være "*hensigtsmæssigt*". Artikel 29-gruppen ser ud til at kategorisere lyd fra en IoT-højttaler ("*IoT voice alerts"*) som "*electronic means*", altså et elektronisk middel. Det burde umiddelbart betyde, at lyd fra en IoT-højttaler kan være et alternativ til en skriftlig privatlivspolitik, hvis det er *"hensigtsmæssigt"*, og dermed kommer man uden om problematikken

[78] WP 260, s. 12

med at definere mundtlighed. Det mærkværdige er dog, at Artikel 29-gruppen i citatet ovenfor skriver, at "*IoT voice alerts*" kun kan blive brugt "*in addition to a layered privacy statement/notice*", altså som et supplement til en form for skriftlig information og ikke som et alternativ.[79] I vejledningen har gruppen ligefrem markeret "*in addition"* med *kursiv* for at understrege budskabet.

Det er uvist, hvorfor og hvordan Artikel 29-gruppen er kommet frem til denne fortolkning. Som påvist herover vil en umiddelbar læsning af bestemmelsens ordlyd pege i retning af, at "*andre midler*" er et alternativ og ikke et supplement til skriftlighed, jf. brugen af ordet *"eller"*. Denne afhandlings forfatter kan derfor ikke tilslutte sig Artikel 29-gruppens postulat. På baggrund af ovenstående analyse vurderes det derfor, at lyd godt kan udgøre et alternativ til skriftlighed ved formidling af oplysninger til den registrerede.

Mauritius-erklæringen kommer også ind på spørgsmålet om transparens, og man kan her ane et ønske om at bevæge sig væk fra de klassiske privatlivspolitikker. Det følger således af pkt. 3, at "*transparency is the key*", og at dette indebærer, at "*proper, sufficient and understandable information*" bør gives til den registrerede ved brug af IoT, og at de nuværende privatlivspolitikker "*not always*" lever op til disse krav. Også på baggrund heraf bør kreative løsninger på opfyldelse af transparensprincippet imødegås.

Udover at stille krav til selve formidlingsformen indebærer transparensprincippet også, at der gives konkrete oplysninger til den registrerede i forbindelse med dataindsamlingen. I forordningens betragtning 39 fremgår det, at "*Dette princip vedrører navnlig"* at den registrerede gives konkrete informationer om bl.a. formålene med behandlingen og udøvelsen af rettigheder. Dette suppleres af betragtning 60, hvorefter *"Principperne om […] gennemsigtig behandling kræver"* at den registrerede bl.a. informeres om tilstedeværelsen af profilering og konsekvenserne heraf. De specifikke forhold, som den registrerede ifølge de to betragtninger skal informeres om, er gentaget i forordningens art. 13 og 14, dvs. i den generelle oplysningspligt, som analyseres i afsnit 3.2 nedenfor. Det interessante at bemærke her er, at man ud fra de to betragtninger kan se en direkte kobling mellem transparensprincippet og den generelle oplysningspligt. Forbindelsen er så tæt, at

[79] Med "*A layered privacy statement/notice"* menes en lagdelt skriftlig information på en hjemmeside, altså skriftlig elektronisk kommunikation, jf. WP 260, s. 11 f. Det fremgår ikke klart af vejledningen, hvorvidt skriftlig elektronisk kommunikation skal kategoriseres som "*skriftlig"* eller "*andre midler*".

manglende opfyldelse af oplysningspligten må antages ofte at føre til brud på transparensprincippet og vice versa.

Transparensprincippet som retsgrundsætning blev udviklet gennem praksis fra bl.a. Datatilsynet, inden det blev kodificeret i forordningen, og Datatilsynet var repræsenteret i Artikel 29-gruppen ved udarbejdelsen af den i dette afsnit citerede vejledning om transparens.[80] Det må derfor anses for usandsynligt, at Datatilsynet skulle tillægge retsgrundsætningen en anden fortolkning end den kodificerede version af princippet. Det vurderes derfor, at retsgrundsætningen og den kodificerede version har et identisk materielt indhold. Opdelingen mellem de to versioner af princippet har således ikke megen betydning i praksis. En enkelt væsentlig forskel er der dog: Den kodificerede version er afhængig af, at forordningen ikke ophæves eller sættes ud af kraft. Modsat vil retsgrundsætningen være levende, uanset om forordningen eksisterer. Eftersom de to versioner har et identisk indhold, er den i dette afsnit foretagne analyse at anse for gældende ret uafhængigt af forordningens eksistens.

3.2. Oplysningspligten

Databeskyttelsesforordningen, ePrivacy-direktivet og cookiebekendtgørelsen fastsætter alle krav om oplysningspligt i forbindelse med databehandling. I dette afsnit vil disse krav opsamles og analyseres i en IoT-kontekst. Først analyseres kravenes materielle anvendelsesområde i afsnit 3.2.1. Dernæst gennemgås deres territoriale anvendelsesområde i afsnit 3.2.2, deres beskyttelsessubjekter i afsnit 3.2.3, deres ansvarssubjekter i afsnit 3.2.4 og endelig deres materielle indhold i afsnit 3.2.5.

3.2.1. Materielt anvendelsesområde

Databeskyttelsesforordningen fastsætter i art. 13 og 14 krav om en generel oplysningspligt i forbindelse med dataindsamling. De to bestemmelser har ikke det samme anvendelsesområde. Indsamles dataene hos den registrerede, finder art. 13 anvendelse. Indsamles dataene derimod hos andre end den registrerede, er det art. 14, der finder anvendelse. Det er et krav for begge bestemmelsers vedkommende, at de indsamlede data indeholder personoplysninger, da forordningen ellers ikke finder anvendelse, jf. art. 2(1) modsætningsvist. For så vidt angår retsstillingen for indsamling af anonymiserede oplysninger

[80] Nielsen m.fl. (2020), s. 314 & persondatadirektivets art. 29(2). Se note 74 for uddybning.

og *Big Data* og for behandling som led i rent personlige eller familiemæssige aktiviteter henvises til afsnit 3.1.1.

ePrivacy-direktivet fastsætter i art. 5(3) krav om oplysningspligt ved lagring af eller adgang til informationer i en abonnents eller brugers terminaludstyr.[81] I modsætning til databeskyttelsesforordningen er det ikke et krav, at informationerne indeholder personoplysninger.[82]

Cookiebekendtgørelsen implementerer ePrivacy-direktivets art. 5(3) og udspecificerer det eksakte indhold af den information, der efter direktivet skal gives. Bekendtgørelsen benytter ikke begrebet "*personoplysninger*", men blot "*oplysninger*".[83] Sammenholdt med retsstillingen for direktivets art. 5(3) vurderes det derfor, at bekendtgørelsen finder anvendelse, uanset om de lagrede informationer indeholder personoplysninger eller ej.

Udtrykket "*terminaludstyr*" benyttes i både ePrivacy-direktivets art. 5(3) og i cookiebekendtgørelsen om det udstyr, som der for så vidt angår lagring af information stilles visse krav til. Direktivet definerer ikke udtrykket. Det gør bekendtgørelsen til gengæld i § 2, stk. 1, nr. 1:

"Terminaludstyr: Et produkt eller en relevant komponent heri, der muliggør kommunikation, og som er beregnet til at blive direkte eller indirekte tilsluttet nettermineringspunkter i offentlige elektroniske kommunikationsnet."

Bekendtgørelsen definerer hverken et "*nettermineringspunkt*" eller et "*offentligt elektronisk kommunikationsnet*". Bekendtgørelsen er udstedt med hjemmel i *teledatalovens* §§ 9 og 81, stk. 2. I teledataloven defineres et "*elektronisk kommunikationsnet"* som "*enhver form for radiofrekvens- eller kabelbaseret teleinfrastruktur, der anvendes til formidling af elektroniske kommunikationstjenester"*, jf. § 2, nr. 4. En sådan teleinfrastruktur kunne f.eks. tænkes at være de bredbånd, der muliggør transmission via internettet. At det er "*offentligt"* betyder, at det stilles til rådighed for en ikke på forhånd afgrænset kreds, jf. teledatalovens § 2, nr. 5. Ved en "*elektronisk kommunikationstjeneste*" forstås en tjeneste som "*helt eller delvis består i elektronisk overføring af kommunikation i form af lyd, billeder, tekst eller kombinationer heraf ved hjælp af radio- eller telekommunikationsteknik*

[81] For definition af begreberne "*abonnent*" og "*bruger*" se afsnit 3.2.3 om beskyttelsessubjekter
[82] Sag C-673/17 (Planet49), præmis 71
[83] Se f.eks. bekendtgørelsens §§ 1, 3 og 4

mellem netterminеringspunkter, herunder både tovejskommunikation og envejskommunikation", jf. teledatalovens § 2, nr. 7. Det kunne f.eks. være internettet, hvor man kan kommunikere, både ensidigt og med andre. Ved "*nettermineringspunkt*" forstås "*den fysiske eller logiske grænseflade i et elektronisk kommunikationsnet, der udgør en slutbrugers tilslutning til dette"*, jf. teledatalovens § 2, nr. 6. Det kunne f.eks. være den grænseflade i bredbåndet, der gør det muligt, at man som slutbruger kan koble op til internettet.

Skåret helt skarpt betyder de beskrevne definitioner, at "*terminaludstyr"* skal forstås som et produkt, der muliggør kommunikation, og som er beregnet til f.eks. at blive koblet op til internettet. *Cookievejledningen* nævner computere, smartphones og tablets som eksempler herpå. Definitionen er dog så bred, at den også bør omfatte de fleste, hvis ikke alle, former for IoT-produkter. Smartwatches, Google Home Mini og smartglasses er alle produkter, der gør kommunikation mulig, og er samtidig alle produkter, der er beregnet til at fungere via en internetforbindelse.

Ovenstående betyder, at ePrivacy-direktivets art. 5(3) og cookiebekendtgørelsen finder anvendelse, hvis der lagres eller gives adgang til allerede lagrede oplysninger i f.eks. smartwatches, Google Home Mini eller smartglasses.

3.2.2. Territorialt anvendelsesområde

For så vidt angår den i forordningens art. 13 og 14 fastsatte oplysningspligt henvises til afsnit 3.1.2, hvor forordningens territoriale anvendelsesområde blev analyseret.

Der er i ePrivacy-direktivet ikke fastsat bestemmelser om det territoriale anvendelsesområde for regelsættet. Det må derfor være op til medlemsstaterne at fastsætte dette ved implementering af direktivbestemmelserne. For så vidt angår direktivets art. 5(3) skulle dette i Danmark i så fald ske via cookiebekendtgørelsen eller teledataloven, som bekendtgørelsen er udstedt i medfør af. Det er dog ikke tilfældet. Hverken bekendtgørelsen eller teledataloven anfører et territorialt anvendelsesområde. Det må derfor lægges til grund, at bekendtgørelsen og dermed de implementerede krav fra direktivets art. 5(3) finder anvendelse, når der foreligger dansk jurisdiktion.

3.2.3. Beskyttelsessubjekter

Den generelle oplysningspligt som fastsat i forordningens art. 13 og 14 har det samme beskyttelsessubjekt som forordningen som helhed, dvs. fysiske personer. Se afsnit 3.1.3 for uddybning.

ePrivacy-direktivets art. 5(3) fastsætter krav til lagring af eller adgang til allerede lagrede oplysninger i "*en abonnents eller brugers*" terminaludstyr. Det må dermed være både abonnenter og brugere, der er beskyttet af bestemmelsen. En bruger defineres i EPD 2002 art. 2(a) som "*en fysisk person, som anvender en offentligt tilgængelig elektronisk kommunikationstjeneste i privat eller forretningsmæssigt øjemed, uden nødvendigvis at abonnere på den pågældende tjeneste.*"

Som forklaret i afsnit 3.2.1 defineres begrebet "*elektronisk kommunikationstjeneste*" ikke i direktivet, men derimod i teledataloven. Det blev slået fast, at begrebet bl.a. omfatter internettet. Det kan således konstateres, at ePrivacy-direktivets art. 5(3) beskytter fysiske personer, der anvender internettet, uanset om formålet er privat eller i forretningsøjemed. Eftersom formålet med IoT er, at produktet fungerer via internettet, som brugeren dermed anvender, må det vurderes, at IoT-brugere, som er fysiske personer, som udgangspunkt vil være beskyttet af art. 5(3), medmindre de aktivt har koblet enheden af internettet.

En "*abonnent*" defineres ikke i EPD 2002 art. 2, men det følger af art. 1(2), at direktivet beskytter "*legitime interesser hos abonnenter, der er juridiske personer*". Det fremgår ikke, hvad en "*legitim interesse*" i så fald skulle være, og der er ikke hjælp at hente i præambelbetragtningerne. Det må derfor antages at bero på en konkret vurdering.

Med baggrund i ovenstående kan det således konstateres, at ePrivacy-direktivets art. 5(3) beskytter IoT-brugere, hvad end de er fysiske eller juridiske personer. For sidstnævnte er det dog et krav, at de har en legitim interesse i beskyttelsen.

Cookiebekendtgørelsen beskytter "*slutbrugere"*, jf. § 1. Hermed menes brugere af elektroniske kommunikationsnet eller -tjenester, jf. § 2, stk. 1, nr. 2, dvs. internetbrugere og dermed også IoT-brugere. Det er et krav, at disse ikke på kommercielt grundlag stiller tjenesterne til rådighed for andre, jf. ibid. Her tænkes der nok primært på internetudbydere eller udbydere af hjemmesider. Kravet må derfor anses for at være af begrænset relevans for IoT. Bekendtgørelsens § 1 skelner ikke mellem juridiske og fysiske personer. Da

bekendtgørelsen har rod i direktivet, må det formodes, at en "*slutbruger"* kan være en fysisk person eller en juridisk person med en legitim interesse i beskyttelsen.

Ovenstående kan illustreres med et eksempel: Ib arbejder for en mindre erhvervsvirksomhed. En dag nævner han virksomhedens CVR-nummer overfor en kollega. Dette opsnappes af en smarthøjttaler, der står på hans skrivebord. Spørgsmålet er nu, om indsamlingen af CVR-nummeret medfører, at der skal gives oplysning til virksomheden herom, altså om virksomheden kan betragtes som et beskyttelsessubjekt. Databeskyttelsesforordningen beskytter ikke juridiske personer og finder derfor ikke anvendelse. ePrivacy-direktivet og cookiebekendtgørelsen *kan* finde anvendelse, *hvis* virksomheden har en legitim interesse i at beskytte CVR-nummeret.[84] Det er lidt svært at se, at der skulle være en særlig interesse heri, eftersom CVR-numre er offentligt tilgængelige. Vurderingen må derfor være, at ingen af regelsættene beskytter virksomheden, som derfor ikke har krav på at blive oplyst.

3.2.4. Ansvarssubjekter

Den oplysningspligt, der fremgår af forordningens art. 13 og 14, har de samme ansvarssubjekter som forordningen som helhed. Der henvises derfor til analysen heraf i afsnit 3.1.4.

ePrivacy-direktivets art. 5(3) pålægger medlemsstaterne at sikre en vis beskyttelse, men der angives ikke specifikke ansvarssubjekter i bestemmelsens ordlyd og ej heller i direktivets præambelbetragtninger. Det følger dog af betragtning 10 til EPD 2002, at persondatadirektivet finder anvendelse på databeskyttelsesretlige områder, der ikke er særligt reguleret i ePrivacy-direktivet, og af databeskyttelsesforordningens art. 94(2) følger det, at henvisninger til persondatadirektivet gælder som henvisninger til forordningen. Dette vil i så fald betyde, at ansvarssubjekterne efter ePrivacy-direktivets art. 5(3) er de samme som efter forordningen, dvs. dataansvarlige og databehandlere, jf. gennemgangen i afsnit 3.1.4. En sådan analog anvendelse af forordningen giver dog i dette tilfælde ikke megen mening. Dataansvarlige og databehandlere defineres nemlig begge som aktører, der behandler persondata, jf. forordningens art. 4, nr. 7 og 8, og som nævnt i bl.a. afsnit 2.1.2 finder ePrivacy-direktivets art. 5(3) anvendelse uanset om de lagrede informationer

[84] Dette forudsætter naturligvis, at direktivets art. 5(3) og cookiebekendtgørelsen i øvrigt finder anvendelse, dvs. at kravene til det materielle og territoriale anvendelsesområde er opfyldt.

indeholder persondata eller ej. En analog anvendelse af forordningen vil derfor føre til en ulogisk ansvarsfritagelse for de IoT-aktører, der lagrer ikke-personhenførbare oplysninger. Det vil medføre en retstilstand, hvor IoT-producenter er forbudt lagring af ikke-personhenførbare data i brugerens terminaludstyr, men samtidig ikke kan stilles til ansvar herfor. En sådan retstilstand er særdeles ulogisk og undergraver til dels formålet med regelsættet. Det vurderes derfor, at betragtning 10 ikke er et brugbart fortolkningsbidrag i dette tilfælde. I stedet må løsning af problemstillingen være op til medlemsstaterne ved implementering af direktivbestemmelsen, og dette er da også sket fra dansk side. I cookiebekendtgørelsen angives således "*fysiske eller juridiske personer*" som de ansvarssubjekter, der ikke må lagre eller tilgå informationer i slutbrugerens terminaludstyr, medmindre en række krav er opfyldt, jf. § 3, stk. 1. Det betyder, at både virksomheder og privatpersoner principielt kan stilles til ansvar for at have lagret eller tilgået lagrede informationer i slutbrugerens IoT-produkt.

3.2.5. Materielt indhold

Som nævnt i afsnit 3.2.1 finder databeskyttelsesforordningens art. 13 anvendelse, når informationerne indsamles hos den registrerede, mens art. 14 finder anvendelse, når informationerne indsamles hos andre end den registrerede. De oplysninger, der efter de to bestemmelser skal gives til den registrerede, skal gives af egen drift og ikke først efter henvendelse fra den registrerede.[85] Der er tale om to meget omfattende bestemmelser, og derfor foretages der kun en uddybende analyse af de krav og stykker, der anses for mest relevante for indsamling af informationer via IoT.

Art. 13 og 14 skelner begge mellem oplysninger, der altid skal gives til den registrerede, jf. art. 13(1) og 14(1), og oplysninger der skal gives "*for at sikre en rimelig og gennemsigtig behandling for så vidt angår den registrerede*", jf. art. 13(2) og 14(2). Det fremgår ikke klart, hvad denne opdeling præcist indebærer, og hvornår man i så fald skal benytte sig af den. Datatilsynet skriver i sin vejledning på området, at den dataansvarlige skal foretage en "*konkret vurdering"* af "*de specifikke omstændigheder og forhold*", og at en sådan vurdering "*ofte*" vil føre til, at der skal gives stk. 2-oplysninger.[86] Denne opfattelse begrundes ikke, den uddybes ikke, der gives ingen eksempler, og henset til de meget vage

[85] Se bl.a. Nielsen m.fl. (2020), s. 469 og 489
[86] Datatilsynets vejledning om de registreredes rettigheder, s. 17. Opfattelsen bakkes op af Justitsministeriet i bet. 1565/2017, s. 289 og 304.

formuleringer må det derfor i det store hele betragtes som et relativt intetsigende fortolkningsbidrag. Retsteoretikere har svært ved at belyse området, og i praksis gives stk. 1 og 2-oplysninger stort set altid samlet.[87] Ifølge Blume (2018) er det svært at forestille sig en situation, hvor man kan nøjes med at give informationer efter stk. 1 og se bort fra stk. 2.[88] I det følgende vil der derfor ikke skelnes mellem stk. 1 og stk. 2-oplysninger.

En lang række informationer skal gives til den registrerede, uanset om persondataene er indsamlet hos vedkommende selv eller hos andre. Det gælder identifikations- og kontaktoplysninger på den dataansvarlige og dennes evt. repræsentant, jf. art. 13(1)(a) og 14(1)(a), kontaktoplysninger på en evt. DPO, jf. art 13(1)(b) og 14(1)(b), formålet og retsgrundlaget for persondatabehandlingen, jf. art. 13(1)(c) og 14(1)(c), de legitime interesser der forfølges, hvis retsgrundlaget for behandlingen er interesseafvejningsreglen i art. 6(1)(f), jf. art. 13(1)(d) og 14(2)(b), modtagere eller kategorier af modtagere af persondataene, jf. art. 13(1)(e) og 14(1)(e), tredjelandsoverførsler hvis det er relevant, jf. art. 13(1)(f) og 14(1)(f), tidsrummet for dataenes opbevaring eller kriterier herfor, jf. art. 13(2)(a) og 14(2)(a), den registreredes rettigheder efter art. 15-21, jf. art. 13(2)(b) og 14(2)(c), retten til at trække et samtykke tilbage hvis retsgrundlaget er art. 6(1)(a) eller 9(2)(a), jf. art. 13(2)(c) og 14(2)(d), retten til at klage til en tilsynsmyndighed, jf. art. 13(2)(d) og 14(2)(e) samt forekomsten af automatiske afgørelser, herunder profilering, jf. art. 13(2)(f) og 14(2)(g). Hvis de indsamlede oplysninger viderebehandles til et nyt formål efter indsamlingen, skal den registrerede tillige informeres om dette, jf. art. 13(3) og 14(4). Det er herudover Artikel 29-gruppens opfattelse, at oplysning om retten til indsigelse, der er en af de rettigheder, der skal oplyses om, jf. forordningens art. 13(2)(b) og 14(2)(c), i en IoT-kontekst skal indeholde vejledning om, hvordan man kobler sit IoT-produkt *fra* internettet for at forhindre ansvarssubjektet i at få yderligere eller fortsat adgang til ens data.[89]

Udover ovenstående fælleskrav er der visse oplysninger, som kun skal gives efter art. 13 og ikke art. 14 og vice versa. De gennemgås straks herunder.

[87] Blume (2018): *Den nye persondataret*, s. 118 f.
[88] Ibid.
[89] WP 223, s. 17 in fine

Når et ansvarssubjekt indsamler oplysninger hos den registrerede, skal den registrerede oplyses om, hvorvidt der foreligger en meddelelsespligt, hvilket grundlag denne pligt har, og hvad konsekvenserne af manglende meddelelse vil være, jf. art. 13(2)(e). Praktisk betyder det f.eks., at Endomondo skal oplyse brugeren om, hvorvidt denne har pligt til at give appen adgang til sine lokationsdata, og hvad konsekvenserne ved manglende adgang vil være. Kravet vil være opfyldt, hvis Endomondo oplyser om, at brugeren ikke har pligt til at give appen adgang, men at appen i så fald ikke vil fungere optimalt.

Ved indsamling af oplysninger hos andre end den registrerede skal denne informeres om berørte kategorier af persondata, jf. art. 14(1)(d). Dette krav eksisterer ikke i art. 13, nok fordi man regner med, at den registrerede godt selv er klar over, hvilke oplysninger han videregiver til ansvarssubjektet. Dette vil dog ikke nødvendigvis være tilfældet i en IoT-kontekst. En Google Home Mini indsamler oplysninger ved at lytte til den registreredes spørgsmål, sniksnak mv. Hvis den registrerede f.eks. kort efter at have stillet et spørgsmål til højttaleren nævner overfor sit pigebesøg, at han har klamydia, kan denne oplysning opfanges af højttaleren og indsamles dermed af Google. Oplysningen om klamydia er givet af den registrerede og ikke indsamlet andre steder fra. Derfor finder art. 13 anvendelse, og da denne bestemmelse ikke indeholder en pligt til at oplyse om berørte kategorier af personoplysninger, har Google ikke pligt til at oplyse brugeren om, at denne ret følsomme information er blevet indsamlet. Dette til trods for, at brugeren højst sandsynligt slet ikke er klar over, at informationen er indsamlet hos ham. Retspolitisk kan man diskutere, om dette er hensigtsmæssigt, og det har da næppe heller været en tilsigtet følgevirkning af bestemmelsen.[90]

Efter art. 14(2)(f) skal den registrerede oplyses om, hvilken kilde persondataene hidrører fra, og om der evt. er tale om offentlige kilder. Dette er ikke et krav i art. 13, sandsynligvis pga. den førnævnte formodning om, at den registrerede ved, hvilke oplysninger han giver til ansvarssubjektet. Det betyder, at Google i det førnævnte klamydia-eksempel ikke har pligt til at oplyse den registrerede om, at de har indsamlet oplysningen hos ham.

Når persondataene indsamles hos den registrerede selv, skal ansvarssubjektet opfylde sin oplysningspligt senest på det tidspunkt, hvor indsamlingen foretages, jf. art. 13, stk. 1, 1. pkt. og 13, stk. 2, 1. pkt. De oplysninger, Google skal give i forbindelse med brug af

[90] Se afsnit 5 for en uddybende retspolitisk vurdering

Google Home Mini, skal altså gives senest i samme øjeblik, at dataene indsamles fra den registrerede, f.eks. når vedkommende stiller et spørgsmål. I afsnit 3.1.5 blev det analyseret, hvorvidt en autogenerisk lydoplæsning af en privatlivspolitik via Google Home Mini opfyldte formkravene i forordningens art. 12(1). Konklusionen blev, at lyd godt kunne udgøre et alternativ til skriftlighed, til trods for en uklar udmelding fra Artikel 29-gruppen. I klamydia-eksemplet vil Google således kunne opfylde tidsfristerne i art. 13 ved at udsende en autogenerisk besked om indsamling efter hver lydoptagelse. Dette er dog kun et krav, hvis optagelserne indsamler nye kategorier af persondata. Det skyldes, at oplysningspligten ikke finder anvendelse, hvis den registrerede allerede er bekendt med, at dataene indsamles, jf. art. 13(4). Google kan således opfylde reglerne, hvis højttaleren programmeres til kun at udsende autogeneriske beskeder ved indsamling af nye kategorier af persondata. Spørgsmålet er selvfølgelig, om det rent teknisk kan lade sig gøre at programmere højttaleren til at foretage denne differentiering af data. Hvis det ikke er tilfældet, er Google *"home safe"* ved at udsende en autogenerisk meddelelse efter hver eneste lydoptagelse. Udfordringen ved denne løsning er til gengæld, at en sådan konstant autogenerisk meddelelse sandsynligvis vil være et stort irritationsmoment for IoT-brugeren.

Ovenstående problemstilling vil ikke være aktuel, hvis oplysningerne indsamles hos andre end den registrerede, da der i disse tilfælde er fastsat mere fleksible tidsfrister på op til en måned efter at indsamlingen har fundet sted, jf. art. 14(3). Det vil f.eks. være tilfældet, hvis det ikke er den registrerede selv, men i stedet hans roomie der nævner klamydia-oplysningen i højttalerens nærvær. Også her er det afgørende, hvorvidt den brugte teknologi kan differentiere. Hvis Google Home Mini ikke kan differentiere mellem, om det er den registrerede selv eller hans roomie, der afgiver den indsamlede oplysning, vil en opdeling mellem art. 13 og 14 virke illusorisk i praksis. Er differentiering ikke mulig, må Google holde sig på den sikre side og overholde begge bestemmelsers krav. Et manglende overblik over hvilke kategorier af persondata der indsamles og hvorfra disse stammer vil alternativt føre til, at Google kan komme til at overtræde reglerne, tilsigtet eller ej.

Der gælder en række specifikke undtagelser til både art. 13 og 14. Ingen af bestemmelserne finder anvendelse, hvis den registrerede allerede er bekendt med de oplysninger, der efter bestemmelserne skal gives til ham, jf. art. 13(4) og 14(5)(a). Derudover finder art. 14 ikke anvendelse, hvis opfyldelse af oplysningspligten viser sig umulig, eller der

kræves en uforholdsmæssig stor indsats, jf. art. 14(5)(b).[91] Det følger af bestemmelsen, at der navnlig tages sigte på arkivformål i samfundets interesse, videnskabelige eller historiske forskningsformål eller statistiske formål. Indsamling af *Big Data* via IoT foretages som regel af kommercielle virksomheder og har i så fald ingen samfundsmæssig interesse. Man kan derimod forestille en situation, hvor et medicinalfirma indsamler oplysninger via IoT til brug for lægevidenskabelig forskning. Man kan desuden forestille sig, at visse indsamlede *Big Data* har til formål at levere statistiske opgørelser over f.eks. aldersgrupper, geografisk placering mv. af IoT-brugere. Efter omstændighederne vil ansvarssubjekter i disse tilfælde kunne undlade at informere IoT-brugerne om dataindsamlingen, jf. art. 14(5)(b). I så fald skal ansvarssubjektet træffe passende sikkerhedsforanstaltninger, herunder ved at gøre oplysningerne offentligt tilgængelige, jf. ibid. Artikel 14 finder heller ikke anvendelse, hvis indsamling eller videregivelse er udtrykkeligt fastsat i EU-retten eller medlemsstaternes nationale ret, eller hvis det følger af lovbestemt tavshedspligt, jf. art. 14(5)(c) og 14(5)(d). I forordningens art. 23 er der fastsat et nationalt råderum, hvorefter medlemsstaterne under visse betingelser kan indføre yderligere undtagelser til bl.a. oplysningspligten. Dette råderum er i Danmark blevet udnyttet med databeskyttelseslovens (herefter DBL) §§ 22-23.[92] Efter DBL § 22, stk. 1 kan oplysning undlades, hvis den registreredes interesse i at vide, at oplysningerne behandles, findes at burde vige for afgørende hensyn til private interesser. Forarbejderne nævner "*forretningshemmeligheder*" som et eksempel på en sådan privat interesse, der kan begrunde manglende iagttagelse af oplysningspligten.[93] Det betyder i praksis, at Google ikke har pligt til at oplyse IoT-brugeren om indsamling af informationer, hvis dette konkret medfører, at Google herved kommer til at røbe forretningshemmeligheder, f.eks. IoT-produktets kildekode el.lign. Dette kan naturligvis ikke bruges som begrundelse for en generel afvisning af at iagttage oplysningspligten, og det er svært at forestille sig konkrete scenarier, hvor Google og lignende aktører ved at opfylde oplysningspligten kommer til at røbe forretningshemmeligheder. Det må derfor antages, at bestemmelsen i en IoT-kontekst vil

[91] Ved *umulighed* tænkes særligt på de tilfælde, hvor der er så få tilgængelige oplysninger om den registrerede, at vedkommende ikke kan identificeres, jf. Datatilsynets vejledning om de registreredes rettigheder, s. 20. Begrebet "*uforholdsmæssig stor indsats*" indebærer en proportionalitetsvurdering; en konkret afvejning af underretningens betydning for den registrerede overfor den arbejdsindsats, der skal ydes af den dataansvarlige for at foretage denne underretning, jf. Nielsen, m.fl. (2020), s. 504.
[92] Lov nr. 502 af 23/05/2018
[93] Lovforslag 68, fremsat 25.10.2017, s. 191. Se hertil også Nielsen m.fl. (2020), s. 1147.

have et begrænset anvendelsesområde. DBL §§ 22, stk. 2-4 og 23 omhandler udelukkende offentlige myndigheder og gennemgås derfor ikke, jf. afgrænsningsafsnittet, afsnit 1.4.

Det følger af ePrivacy-direktivets art. 5(3), at ansvarssubjekter skal iagttage en oplysningspligt ved lagring af eller adgang til informationer i en abonnents eller brugers terminaludstyr. Af ordlyden følger det, at en sådan lagring eller adgang kun er tilladt, hvis abonnenten eller brugeren giver sit samtykke hertil "*efter i overensstemmelse med"* persondatadirektivet at have "*modtaget klare og fyldestgørende oplysninger, bl.a. om formålet med behandlingen.*" Eftersom henvisninger til persondatadirektivet nu gælder som henvisninger til databeskyttelsesforordningen, jf. dennes art. 94(2), betyder det, at ePrivacy-direktivet fastsætter krav om, at forordningens krav til oplysningspligten skal efterleves ved lagring af eller adgang til informationer i abonnentens eller brugerens terminaludstyr. Den oplysningspligt, der gælder efter ePrivacy-direktivets art. 5(3), er således identisk med den oplysningspligt, der gælder efter forordningens art. 13 og 14. At der i direktivets art. 5(3) specifikt er krav om oplysning om "*formålet med behandlingen*" er uden materiel betydning, da dette allerede er en eksplicit pligt efter forordningens art. 13(1)(c) og 14(1)(c). Mere interessant er det, at EU-Domstolen i en sag har slået fast, at direktivets art. 5(3) indeholder en forpligtelse til at oplyse brugeren eller abonnenten om, hvorvidt tredjemand har adgang til de lagrede informationer i terminaludstyret.[94] Dette begrundes med, at tredjepartsadgang omfattes udtrykket "*eventuelle modtagere eller kategorier af modtagere*" i forordningens art. 13(1)(e).[95] Det betyder i praksis, at Apple ikke blot skal oplyse smartwatch-brugeren om deres egen lagring af informationer i uret, men også om hvorvidt tredjepart har adgang hertil. Som det følger af ordlyden i direktivets art. 5(3), skal samtykket gives "*efter*", at oplysningerne gives. Det betyder, at tidspunktet for opfyldelse af oplysningspligten ligger forud for indhentelsen af samtykket. Bestemmelsen er overtrådt, hvis Apple først udsender en privatlivspolitik til smartwatch-brugeren efter at have indhentet dennes samtykke til lagringen.

Som nævnt i afsnit 2.1.2 og 3.2.1 finder ePrivacy-direktivets art. 5(3) anvendelse, uanset om de lagrede informationer indeholder persondata eller ej.[96] Dette medfører, at forordningens art. 13 og 14 ikke kun er gældende ved behandling af persondata, men også ved

[94] Sag C-673/17 (Planet49), præmis 81
[95] Ibid.
[96] Ibid., præmis 71

lagring af eller adgang til ikke-personhenførbare informationer i brugerens/abonnentens terminaludstyr. Det betyder f.eks., at der ved lokal lagring af informationer i et smartwatch er krav om iagttagelse af oplysningspligten i forordningens art. 13 og 14, selvom disse informationer ikke kan henføres til smartwatch-brugeren.

ePrivacy-direktivets art. 5(3) er i Danmark implementeret med cookiebekendtgørelsen, som uddyber indholdet af den oplysningspligt, der er gældende efter direktivet. I bekendtgørelsens § 3, stk. 2 oplistes en række eksplicitte krav til indholdet af de informationer, der som følge af oplysningspligten skal gives til slutbrugeren. For det første skal informationerne fremstå i et klart, præcist og letforståeligt sprog, jf. § 3, stk. 2, nr. 1. Bestemmelsen er efter forordningens ikrafttræden blevet overflødig, da et identisk krav følger af art. 12(1).[97] For det andet skal informationerne indeholde oplysning om formålet med den pågældende lagring eller adgang, jf. § 3, stk. 2, nr. 2. Også denne bestemmelse er blevet overflødig, da et identisk krav følger af forordningens art. 13(1)(c) og 14(1)(c). For det tredje fastsætter bekendtgørelsen et krav om, at slutbrugeren skal oplyses om identiteten på den fysiske eller juridiske person, der foranstalter lagringen af eller adgangen til informationerne i terminaludstyret, jf. § 3, stk. 2, nr. 3. Dette er ikke et krav efter forordningen, der kun fastsætter krav om oplysning om identiteten på den dataansvarlige, dennes evt. repræsentant og DPO, jf. art. 13(1)(a), 13(1)(b), 14(1)(a) og 14(1)(b). En dataansvarlig defineres bl.a. som den, der fastlægger formålet med behandlingen af personoplysningerne, jf. art. 4, nr. 7. Hvis der ikke behandles personoplysninger, eksisterer der således ikke en dataansvarlig. Det betyder, at Apple ved lagring af ikke-personhenførbare informationer i et smartwatch ikke efter forordningen har pligt til at oplyse smartwatch-brugeren om deres identitet. Det vil derimod være en pligt for dem efter cookiebekendtgørelsens § 3, stk. 2, nr. 3. For det fjerde er det efter bekendtgørelsen et krav, at slutbrugeren har en umiddelbart tilgængelig mulighed for at afslå eller trække sit samtykke tilbage, jf. § 3, stk. 2, nr. 4. Det kan godt vise sig at være en udfordring for så vidt angår lagrede informationer i et IoT-produkt. Ved smartwatches eller lignende produkter med skærm burde det kunne løses ved at have et ikon el.lign., der altid kan tilgås af brugeren, og som giver mulighed for at afslå eller trække samtykke tilbage. Brugeren skal naturligvis informeres om, at det er dette, der er formålet med ikonet. Det kan f.eks. stå i

[97] For analyse af art. 12(1) se afsnit 3.1.5

brugervejledningen til uret og ved klik på selve ikonet. For så vidt angår IoT-produkter uden skærm, f.eks. Google Home Mini, er udfordringen lidt sværere. I det konkrete tilfælde kan problemet tænkes løst ved at brugeren via højttaleren får en autogenerisk besked om, at samtykket f.eks. kan trækkes tilbage ved simpelthen at bede højttaleren om det.[98] For det femte er det et krav, at de oplysninger, der skal gives til slutbrugeren, er vedvarende tilgængelige for denne, jf. § 3, stk. 2, nr. 5. Også denne problemstilling kan løses ved at have et vedvarende tilgængeligt ikon på smartwatches og andre skærmprodukter og ved samtale med et Google Home Mini.

Der er i ePrivacy-direktivets art. 5(3) fastsat to undtagelser til kravet om oplysningspligt. Undtagelserne er blevet implementeret stort set ordret i cookiebekendtgørelsens § 4 og behandles derfor samlet her. Den første undtagelse omhandler lagring af informationer, som "*alene sker med det formål at overføre kommunikation via et elektronisk kommunikationsnetværk*", jf. bekendtgørelsens § 4, stk. 1, nr. 1. Hermed menes lagring af informationer, der er nødvendige for, at slutbrugeren kan koble op til internettet.[99] Det betyder praktisk, at Apple ikke vil være underlagt oplysningspligten efter direktivet eller bekendtgørelsen for så vidt angår de informationer, de har lagret i smartwatches for at gøre det muligt for brugeren at koble uret op til internettet. Den anden undtagelse omhandler informationer, som er "*påkrævet for at sætte tjenesteyderen af en informationssamfundstjeneste, som slutbrugeren udtrykkeligt har anmodet om, i stand til at levere denne tjeneste*", jf. bekendtgørelsens § 4, stk. 1, nr. 2, og herunder tilfælde hvor informationerne er en teknisk forudsætning for at "*kunne levere en tjeneste, der fungerer i overensstemmelse med tjenestens formål*", jf. § 4, stk. 2. Undtagelsen tager bl.a. sigte på de tilfælde, hvor det er nødvendigt at lagre cookies på en slutbrugers computer for at sikre, at brugeren ved besøg på en webshop ikke mister de varer, han har lagt i sin indkøbskurv, inden han klikker videre til betalingssiden.[100] I en IoT-kontekst kan undtagelsen tænkes anvendt i lignende situationer, f.eks. hvor det er nødvendigt at lagre information på et smartwatch i forbindelse med betaling for varer i en dagligvarebutik.[101]

[98] F.eks. ved at brugeren stiller sig foran højttaleren og siger: "*Jeg beder hermed om, at mit samtykke til lagring af informationer i mit Google Home Mini trækkes tilbage*."
[99] Udsen (2019), s. 505
[100] Ibid., s. 505 f.
[101] Det er muligt at betale for varer ved at benytte smartwatch, se f.eks. Power.dk (2020)

3.3. Samtykkekravet

Ligesom det er tilfældet med oplysningspligten, er der fastsat krav om samtykke i forbindelse med databehandling i både databeskyttelsesforordningen, ePrivacy-direktivet og cookiebekendtgørelsen. I dette afsnit opsamles og analyseres kravene i en IoT-kontekst. Først gennemgås kravenes materielle anvendelsesområde i afsnit 3.3.1, og dernæst deres territoriale anvendelsesområde i afsnit 3.3.2. Herefter følger en analyse af kravenes beskyttelsessubjekter i afsnit 3.3.3 og ansvarssubjekter i afsnit 3.3.4. Til sidst analyseres kravenes materielle indhold i afsnit 3.3.5.

3.3.1. Materielt anvendelsesområde

Efter databeskyttelsesforordningen kan samtykke udgøre et behandlingsgrundlag for almindelige persondata, jf. art. 6(1)(a) og følsomme persondata, jf. art. 9(2)(a). Generelle krav til samtykket findes i art. 4, nr. 11 og art. 7. Ingen af bestemmelserne finder anvendelse for så vidt angår data, der ikke indeholder personoplysninger, jf. art. 2(1) modsætningsvist. For analyse af retsstillingen for indsamling af anonymiserede oplysninger og *Big Data* og for behandling som led i rent personlige eller familiemæssige aktiviteter se afsnit 3.1.1.

ePrivacy-direktivets art. 5(3) fastsætter krav om samtykke ved lagring af eller adgang til informationer i en abonnents eller brugers terminaludstyr. Bestemmelsen er i Danmark implementeret med cookiebekendtgørelsen, der uddyber kravene til samtykket. Det materielle anvendelsesområde for både direktivets art. 5(3) og for cookiebekendtgørelsen blev analyseret i afsnit 3.2.1, som der derfor henvises til.

3.3.2. Territorialt anvendelsesområde

Databeskyttelsesforordningens bestemmelser om samtykke finder kun anvendelse, hvis forordningens territoriale anvendelsesområde er opfyldt. Der henvises derfor til analysen heraf i afsnit 3.1.2.

Det territoriale anvendelsesområde for ePrivacy-direktivets art. 5(3) er det samme, uanset om der tages sigte på oplysningspligten eller samtykkekravet. Det samme gør sig gældende for cookiebekendtgørelsen. Der henvises derfor for begge regelsæts vedkommende til afsnit 3.2.2, hvor deres respektive territoriale anvendelsesområder blev analyseret.

3.3.3. Beskyttelsessubjekter

Databeskyttelsesforordningens bestemmelser om samtykke har det samme beskyttelsessubjekt som forordningen som helhed, dvs. fysiske personer. Se afsnit 3.1.3 for uddybning.

ePrivacy-direktivets art. 5(3) har de samme beskyttelsessubjekter, uanset om der tages sigte på oplysningspligten eller samtykkekravet. Det samme gør sig gældende for cookiebekendtgørelsen. Begge regelsæt beskytter IoT-brugere, som enten er fysiske personer eller juridiske personer med legitim interesse i beskyttelsen. Se afsnit 3.2.3 for uddybning.

3.3.4. Ansvarssubjekter

Databeskyttelsesforordningens bestemmelser om samtykke har de samme ansvarssubjekter som forordningen som helhed. Der henvises derfor til analysen heraf i afsnit 3.1.4.

For så vidt angår ePrivacy-direktivets art. 5(3) er ansvarssubjekterne identiske for samtykkekravet og oplysningspligten. Det samme gør sig gældende for cookiebekendtgørelsen. Der henvises derfor for begge regelsæts vedkommende til analysen i afsnit 3.2.4.

3.3.5. Materielt indhold

Samtykke kan anvendes som behandlingsgrundlag for almindelige persondata, jf. forordningens art. 6(1)(a) og for følsomme persondata, jf. art. 9(2)(a). Samtykket skal for begge bestemmelsers vedkommende leve op til en række krav, der er fastsat i art. 4, nr. 11 og art. 7. Derudover skal samtykket for så vidt angår følsomme persondata tillige være *udtrykkeligt*, jf. art. 9(2)(a). I det følgende behandles først fælleskravene og dernæst udtrykkelighedsbetingelsen.

Et samtykke skal indhentes, inden persondatabehandlingen påbegyndes, og kan gives mundtligt, skriftligt eller digitalt.[102] Et stiltiende eller forudsat samtykke er ikke gyldigt.[103] Forordningens art. 4, nr. 11 definerer et samtykke fra den registrerede som "*enhver **frivillig**, **specifik**, **informeret** og **utvetydig** viljestilkendegivelse fra den registrerede, hvorved den registrerede ved **erklæring** eller **klar bekræftelse** indvilliger i, at personoplysninger, der vedrører den pågældende, gøres til genstand for behandling.*" (**mine fremhævninger**). At samtykket skal være "*frivilligt*" indebærer, at den registrerede skal have

[102] Forordningens præambelbetragtning 32 & Datatilsynets vejledning om samtykke, s. 5
[103] Ibid.

et reelt eller frit valg samt kunne afvise eller trække sit samtykke tilbage uden at det er til skade for den pågældende.[104] Det indebærer f.eks., at en smartwatch-bruger skal kunne afvise at give samtykke til, at vedkommendes lokationsdata indsamles, uden at uret derved stopper med at virke. Samtykket bliver dog ikke ugyldigt, hvis de af urets funktioner, der er afhængige af indsamlede lokationsdata, ikke fungerer optimalt.[105] Det afgørende er, om der er en sammenhæng mellem det afviste samtykke og den forringede funktionalitet.[106] En afvisning af samtykke til indsamling af lokationsdata vil således ikke medføre ugyldighed, hvis urets Endomondo-app ikke fungerer optimalt, eftersom formålet med appen bl.a. er at give brugeren et overblik over sine lokationer. Der vil derimod være tale om ugyldighed, hvis urets pulsmålerfunktion sættes ud af kraft. Det skyldes, at måling af puls og lokationsdata intet har med hinanden at gøre. Hvis der indsamles persondata til flere formål, skal samtykket *granuleres*, dvs. opdeles.[107] Det betyder, at den registrerede skal kunne vælge mellem, hvilke indsamlingsformål, han samtykker til.[108] Foreligger denne mulighed ikke, anses samtykket ikke for at være givet frivilligt, og det vil derfor være ugyldigt.[109] Indsamler Apple oplysninger til brug for dels brugeroptimering og dels markedsføring, skal smartwatch-brugeren således kunne vælge at samtykke til det ene formål uden at skulle samtykke til det andet. At samtykket skal være "*specifikt*" indebærer, at det ikke må være generelt udformet eller uden en præcis angivelse af formål.[110] Det skal være konkretiseret på sådan vis, at det klart og tydeligt fremgår, hvad der meddeles samtykke til, og den registrerede skal oplyses om, hvilke oplysninger der behandles til hvert enkelt formål.[111] Med andre ord må det ikke være uigennemskueligt for smartwatch-brugeren, hvad det præcis er, han giver samtykke til, og i tilfælde af granuleret samtykke skal han f.eks. vide, hvilke oplysninger der indsamles til brugeroptimering, og hvilke der indsamles til markedsføring. At samtykket skal være "*informeret*" indebærer, at der skal gives en række informationer til den registrerede, der gør denne i stand til at træffe

[104] Forordningens præambelbetragtning 42
[105] Det kan udledes af præambelbetragtning 43 og Datatilsynets vejledning om samtykke, s. 7
[106] Ibid.
[107] Det følger af præambelbetragtning 43 og Datatilsynets vejledning om samtykke, s. 8
[108] Ibid.
[109] Ibid.
[110] Datatilsynets vejledning om samtykke, s. 9 f., der desuden redegør for, at kravet om, at samtykket skal være "*specifikt*" hænger sammen med princippet om formålsbegrænsning, jf. forordningens art. 5(1)(b), hvorefter persondata bl.a. skal "*indsamles til udtrykkeligt angivne og legitime formål*."
[111] Ibid.

beslutning om samtykke på et oplyst grundlag.[112] Informationen skal som minimum indeholde oplysning om den dataansvarliges identitet, formålene med behandlingen, muligheden for at trække samtykket tilbage, og hvilke persondata der behandles.[113] Det kan udledes af Mauritius-erklæringen, at EDPS m.fl. ser skeptisk på privatlivspolitikkers evne til at opfylde dette krav, idét der i erklæringens pkt. 3 står, at "*Consent on the basis of such policies can hardly be considered to be informed consent*." En IoT-udbyder kan således næppe leve op til kravet om informeret samtykke ved blot at sende en generel privatlivspolitik ud til sine kunder. At samtykket skal være "*utvetydigt*" betyder, at der ikke må foreligge tvivl om, hvorvidt den registrerede har samtykket.[114] Dette kan ske ved "*erklæring*" eller "*klar bekræftelse*", jf. ordlyden i art. 4, nr. 11. Benyttes en samtykkeerklæring, bør denne erklæring i overensstemmelse med Rådets direktiv 93/13/EØF om urimelige kontraktvilkår i forbrugeraftaler både være udarbejdet i en letforståelig og letlilgængelig form og i et klart og enkelt sprog og ikke indeholde urimelige vilkår.[115] Ved en "*klar bekræftelse*" forstås at den registrerede skal have foretaget en aktiv handling for at give samtykket.[116] Det følger af forordningens præambelbetragtning 32, at et aktivt samtykke kan gives ved valg af tekniske indstillinger til informationssamfundstjenester eller ved at sætte et kryds i en boks på en hjemmeside.[117] Datatilsynet anser Facebook, Instagram og Snapchat for informationssamfundstjenester og anser derudover "*et swipe, et vink foran et smartkamera, at bevæge sin smartphone rundt med uret eller i en ottetalsbevægelse*" for efter omstændighederne at kunne udgøre et aktivt samtykke.[118] Det kan således konstateres, at formkravene til et aktivt samtykke er forholdsvis vige. Det giver et stort råderum for IoT-aktører til at agere kreativt. Det vigtige er altså ikke, *hvordan* samtykket rent teknisk indhentes, men at den registrerede *er klar over*, at det er sådan, der samtykkes. Der skal altså foreligge en form for fælles forståelse mellem ansvars- og beskyttelsessubjektet. I praksis kan man f.eks. forestille sig, at et samtykke indhentes allerede ved brugerens opsætning af sit smartwatch, hvorved der også vil kunne gives et

[112] Ibid., s. 10 in fine & forordningens præambelbetragtning 42
[113] Ibid.
[114] Datatilsynets vejledning om samtykke, s. 12
[115] Det følger af præambelbetragtning 42, hvor direktiv 93/13/EØF specifikt nævnes. Udtrykkene "*letforståelig og lettilgængelig"* og "*et klart og enkelt sprog*" benyttes også i forordningens art. 12(1), der fastsætter formkrav til bl.a. oplysningspligten i art. 13 og 14. For en analyse af begreberne se afsnit 3.1.5.
[116] Det kan udledes af Datatilsynets vejledning om samtykke, s. 12
[117] Forudafkrydsede felter udgør dog ikke et gyldigt samtykke, jf. præambelbetragtning 32 og sag C-673/17 (Planet49), præmis 62. Det samme gælder tavshed eller inaktivitet, jf. betragtning 32.
[118] Datatilsynets vejledning om samtykke, s. 12

granuleret samtykke, f.eks. ved at brugeren trykker ja og nej til en række spørgsmål a la "*giver du samtykke til indsamling af x-oplysninger til brug for markedsføring?"*, "*giver du samtykke til indsamling af y-oplysninger til brugeroptimering?*" etc.

Udover de ovenfor analyserede krav i art. 4, nr. 11 skal samtykket for at være gyldigt også leve op til krav fastsat i forordningens art. 7. Det er således et krav, at den dataansvarlige kan påvise, at den registrerede har afgivet samtykket, jf. art. 7(1).[119] Kan Apple ikke bevise, at smartwatch-brugeren har samtykket til indhentelse af informationer, kan de ikke benytte samtykke som behandlingsgrundlag. Brugen af udtrykket "*påvise"* indebærer, at bestemmelsen ikke indeholder et krav om skriftlig dokumentation.[120] Hvis Apple elektronisk kan logge en aktiv handling, der er udtryk for et samtykke, f.eks. et *swipe*, burde det således være tilstrækkeligt til at opfylde påvisningskravet i art. 7(1). Hvis den registrerede giver samtykke i en skriftlig erklæring, der også vedrører andre forhold end behandling af persondata, skal anmodningen om samtykket kunne skelnes fra de andre forhold i erklæringen, jf. art. 7, stk. 2, 1. pkt. Apple kan altså ikke slippe af sted med at "gemme" et samtykke inde i en 100 sider lang privatlivspolitik, som brugeren skal scrolle igennem og klikke godkend til inden brug af produktet. Erklæringens anmodning om samtykke skal forelægges i en letforståelig og lettilgængelig form og i et klart og enkelt sprog, jf. art. 7, stk. 2, 1. pkt., sidste led.[121] Samtykket er kun gyldigt, hvis alle dele af erklæringen overholder forordningen, jf. art. 7, stk. 2, 2. pkt. En erklæring givet til Apple kan altså risikere at være ugyldig, selvom selve samtykkeafsnittet i erklæringen er korrekt udformet, hvis der er andre dele af erklæringen, der er i strid med forordningen.

Den registrerede har til enhver tid ret til at trække sit samtykke tilbage, jf. art. 7, stk. 3, 1. pkt. Det betyder, at selvom smartwatch-brugeren har givet Apple tilladelse til at indsamle informationer om ham til markedsføringsformål, er dette ikke gældende for evigt. Smartwatch-brugeren har således til enhver tid ret til at bede Apple om at stoppe fortsat indsamling af informationer til f.eks. dette formål. Tilbagetrækningen af samtykket berører ikke lovligheden af den behandling, der er baseret på samtykket inden tilbagetrækningen, jf. art 7, stk. 3, 2. pkt. Det er således kun den fremtidige behandling af persondataene,

[119] Kravet hænger sammen med den generelle pligt, den dataansvarlige har til at påvise overholdelse af forordningens bestemmelser, jf. bl.a. princippet om ansvarlighed i art. 5(2) samt art. 24.
[120] Nielsen m.fl. (2020), s. 409 f.
[121] Dette følger også af præambelbetragtning 42. For en analyse af begreberne se afsnit 3.1.5, hvor identiske begreber i art. 12(1) analyseres. Eftersom begreberne er identiske, er analysen retvisende.

der berøres af tilbagetrækningen.[122] Det indebærer, at smartwatch-brugeren ikke kan bebrejde Apple for den indsamling af oplysninger, de allerede har foretaget, inden samtykket blev tilbagekaldt. En tilbagekaldelse medfører, at den dataansvarlige hurtigst muligt skal stoppe den behandling af persondata, der er baseret på det tilbagekaldte samtykke.[123] I enkelte tilfælde kan den dataansvarlige lovligt fortsætte behandlingen trods tilbagekaldelse af samtykke ved simpelthen at skifte behandlingsgrundlag.[124] Det er dog ikke udgangspunktet, og det er et krav, at behandlingen er rimelig i forhold til den registrerede.[125] Dette gør sig f.eks. gældende for fortsat behandling, der er nødvendig for at overholde bogføringsloven.[126] Det er i en IoT-kontekst svært at forestille sig et scenarium, der skulle kunne retfærdiggøre et sådant skift i behandlingsgrundlag efter tilbagekaldelse af samtykke, og risikoen for at det vil blive opfattet som et forsøg på omgåelse af reglerne er ret stor. Særligt ved indsamling af *Big Data* via IoT er det svært at argumentere for, at fortsat indsamling af disse enorme mængder data skulle være rimelig overfor den registrerede, som netop har trukket sit samtykke tilbage og herved har udtrykt et ønske om, at indsamlingen stoppes. På denne baggrund vurderes det derfor, at IoT-aktørers muligheder for at skifte behandlingsgrundlag i forbindelse med den registreredes tilbagekaldelse af samtykke i praksis er særdeles begrænsede. Hvis der skiftes behandlingsgrundlag undervejs, skal den registrerede oplyses herom samt om det nye formål mv.[127] Det skal være lige så let at trække sit samtykke tilbage som at give det, jf. art. 7, stk. 3, sidste pkt. Det er omvendt ikke et krav, at tilbagekaldelsen sker på samme måde, som samtykket oprindeligt var givet.[128] Det er Datatilsynets opfattelse, at hvis et samtykke er givet via "*et museklik, tasteslag eller swipe*" bør det også kunne tilbagekaldes på tilsvarende enkel måde, og at hvis samtykket er givet via "*en hjemmeside, en applikation eller via e-mail*" bør det kunne tilbagekaldes ved brug af samme løsning.[129] Dette må indebære, at et samtykke givet via klik på et ikon på et smartwatch kan tilbagekaldes ved at klikke på det samme ikon, eller at et samtykke givet ved at tale til Google Home Mini kan trækkes tilbage på tilsvarende vis. Ifølge Artikel 29-gruppen indebærer retten til at trække samtykket tilbage, at den

[122] Datatilsynets vejledning om samtykke, s. 14
[123] Ibid.
[124] Ibid., s. 15 & Nielsen m.fl. (2020), s. 411
[125] Ibid.
[126] Ibid.
[127] Datatilsynets vejledning om samtykke, s. 15 & Nielsen m.fl. (2020), s. 411 f.
[128] Datatilsynets vejledning om samtykke, s. 14
[129] Ibid.

registrerede skal tilbydes muligheden for at afkoble IoT-genstanden fra internettet og bruge den på "normal" vis.[130] Det betyder f.eks., at brugeren skal have mulighed for at koble sit smartwatch af internettet og bruge det som et almindeligt armbåndsur uden smarte funktioner. Den registrerede skal have mulighed for at trække sit samtykke tilbage, uden at det er til skade for den pågældende, herunder uden betaling af gebyrer.[131]

Når det vurderes, hvorvidt et samtykke er givet frit, skal der tages størst muligt hensyn til, om "*bl.a.*" opfyldelse af en kontrakt er gjort betinget af samtykket, selvom det ikke er nødvendigt for opfyldelse af kontrakten, jf. art. 7(4). Bestemmelsen antages af teoretikere at uddybe de hensyn, der skal tages ved vurderingen af, hvornår et samtykke er givet "*frivilligt*", jf. art. 4, nr. 11.[132] Det følger af forordningens præambelbetragtning 43, sidste pkt., at et samtykke "*formodes ikke at være givet frivilligt*", hvis opfyldelsen af en kontrakt gøres afhængig af samtykket, selvom samtykket ikke er nødvendigt for kontraktens opfyldelse. Læser man art. 7(4) i sammenhæng med betragtning 43 når man frem til, at det ved frivillighedsvurderingen af samtykket skal overvejes, hvorvidt en kontrakt er betinget af et samtykke, uden at det er nødvendigt herfor, og at der i så fald vil være en formodning for, at samtykket ikke er givet frivilligt. Brugen af udtrykket "*bl.a.*" i art. 7(4) åbner op for et bredt anvendelsesområde, og teoretikere forventer, at bestemmelsen i praksis vil kunne få betydning i situationer, hvor der foreligger en klar skævhed mellem den registrerede og den dataansvarlige.[133] I en IoT-kontekst vil bestemmelsen nok primært få betydning i de tilfælde, hvor brugeren som betingelse for download af apps mv. bedes give sit samtykke til, at der gives adgang til oplysninger, der ikke er relevante for den pågældende app. F.eks. hvis Endomondo som betingelse for download beder om samtykke til at få adgang til brugerens e-mail-indbakke. Et samtykke til indhentelse af oplysninger i brugerens indbakke er ikke nødvendigt for indgåelse af aftale om download af Endomondo. Et sådant samtykke vil derfor ikke leve op til frivillighedskravet i art. 4, nr. 11, jf. art. 7(4) og dermed være ugyldigt.

[130] WP 223, s. 20 in fine
[131] Datatilsynets vejledning om samtykke, s. 14. Opfattelsen understøttes desuden af forordningens præambelbetragtning 42, hvorefter et samtykke ikke anses for at være givet frivilligt og dermed er ugyldigt, hvis tilbagekaldelse af samtykke ikke kan ske, uden det er til skade for den registrerede.
[132] Nielsen m.fl. (2020), s. 413
[133] Ibid.

Den netop foretagne analyse af forordningens art. 4, nr. 11 og art. 7 angår både almindelige og følsomme persondata, da der er tale om krav, der skal opfyldes, uanset om samtykke benyttes som behandlingsgrundlag efter art. 6(1)(a) eller art. 9(2)(a). Som det kort blev nævnt i indledningen til dette afsnit, er der fastsat et yderligere krav for det samtykke, der indhentes ved behandling af følsomme persondata, jf. art. 9(2)(a). Det følger nemlig af bestemmelsens ordlyd, at samtykket skal være "*udtrykkeligt*". Udover art. 9(2)(a) benyttes begrebet "*udtrykkeligt*" i forordningens art. 22(2)(c) om det samtykke, der skal foreligge fra den registrerede, hvis den dataansvarlige ønsker at gøre den registrerede til genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering. Begrebet benyttes desuden i forordningens art. 49(1)(a) som betingelse for det samtykke, der under visse omstændigheder kan benyttes som overførselsgrundlag til et usikkert tredjeland. Begrebet "*udtrykkeligt*" benyttes til gengæld ikke i hverken art. 4, nr. 11, art. 7 eller art. 6(1)(a). Det er derfor interessant at belyse, hvad begrebet egentlig dækker over, og om det skærper kravet til samtykket i de førnævnte særlige situationer. Til besvarelse heraf er forordningens præambelbetragtninger ikke til megen hjælp. Efter Datatilsynets opfattelse medfører begrebet ikke et yderligere skærpet krav til samtykket, men skal derimod blot ses som en understregning af vigtigheden af, at der ikke må være tvivl om, at der er afgivet samtykke.[134] Datatilsynet giver ingen begrundelse for denne opfattelse, som derfor har karakter af et postulat. Opfattelsen er ikke selvindlysende. Pointen med en indholdsløs understregning er vel typisk at vække læserens opmærksomhed. Som nævnt gælder udtrykkelighedsbetingelsen for følsomme, men ikke for almindelige persondata. Den gennemsnitlige dataansvarlige må formodes at være mere opmærksom på at overholde reglerne ved behandling af følsomme persondata end ved almindelige. Menigmand må antages i almindelighed at være vidende om, at f.eks. en helbredsoplysning er mere følsom end en fødselsdato. En laissez faire-tilgang til reglerne, som en indholdsløs understregning vel har til hensigt at hindre, vil derfor nok være mere udbredt, når der behandles almindelige persondata. Rent logisk vil det derfor give mere mening at sætte en indholdsløs understregning ind i art. 6(1)(a), da det nok nærmere vil være ved anvendelse af dette behandlingsgrundlag, at den dataansvarliges pertentlighed risikerer at lide et knæk. *Udsen (2019)* er uenig med Datatilsynet og er i stedet af den opfattelse, at udtrykkelighedsbetingelsen skærper kravene til, hvor tydeligt den registrerede skal

[134] Datatilsynets vejledning om samtykke, s. 13

udtrykke sin vilje til at acceptere behandlingen af personoplysninger.[135] Ligesom Datatilsynet begrunder Udsen ikke sin opfattelse.[136] "*Udtrykkeligt*" er en oversættelse af "*explicit*" i den engelske version af forordningen, og dette udtryk behandles i et afsnit i Artikel 29-gruppens udtalelse om samtykke under forordningen.[137] Her redegøres der bl.a. for, at begrebet "*refers to the way consent is expressed by the data subject*", og der gives eksempler på udtrykkelige samtykker, bl.a. at de kan foreligge skriftligt, elektronisk eller mundtligt, herunder telefonisk.[138] Dette bliver man dog ikke meget klogere af. De angivne eksempler kunne lige så godt have eksemplificeret art. 6(1)(a), og det står fortsat uklart, hvordan et "*udtrykkeligt samtykke*" adskiller sig fra f.eks. en "*utvetydig viljestilkendegivelse*" i art. 4, nr. 11. Henset til de vage og manglende fortolkningsbidrag må retstilstanden på området anses for uafklaret. Indtil retstilstanden bliver afklaret, må IoT-aktørers indhentede samtykker i forbindelse med indsamling af følsomme persondata, ved automatiske afgørelser og profilering og ved overførsel til usikre tredjelande formodes at have nogenlunde samme gyldighed som samtykker indhentet i forbindelse med indsamling af almindelige persondata, hvis blot de lever op til kravene i forordningens art. 4, nr. 11 og art. 7 som analyseret i dette afsnit.

Det følger af ePrivacy-direktivets art. 5(3), at lagring af eller adgang til informationer i en abonnents eller brugers terminaludstyr kun er tilladt, hvis abonnenten eller brugeren "*har givet sit samtykke hertil*" efter "*i overensstemmelse med*" persondatadirektivet at have modtaget klare og fyldestgørende oplysninger. Det rejser spørgsmålet om, hvordan "*samtykke*" skal forstås i dette regelsæt. Det er der heldigvis taget specifikt stilling til fra EU-lovgivers side. Det følger nemlig af EPD 2002 art. 3, litra f, at "*samtykke*" efter ePrivacy-direktivet svarer til den registreredes samtykke efter persondatadirektivet. Da det i databeskyttelsesforordningens art. 94(2) er slået fast, at henvisninger til persondatadirektivet nu gælder som henvisninger til forordningen, betyder det, at samtykke efter ePrivacy-direktivets art. 5(3) skal leve op til de samme krav som samtykke efter forordningen. Der henvises derfor til den indgående analyse heraf ovenfor i nærværende afsnit. For så

[135] Udsen (2019), s. 384
[136] Ibid.
[137] WP 259, s. 18 ff.
[138] Ibid., s. 18

vidt angår de "*klare og fyldestgørende oplysninger*" der skal gives til brugeren eller abonnenten forinden samtykke indhentes, henvises der til analysen heraf i afsnit 3.2.5.

Som førnævnt er ePrivacy-direktivets art. 5(3) i Danmark implementeret i cookiebekendtgørelsen. Heraf følger det, at lagring af eller adgang til informationer i slutbrugerens terminaludstyr ikke er tilladt, medmindre slutbrugeren "*giver samtykke hertil*" efter at have modtaget en række oplysninger, jf. bekendtgørelsens § 3, stk. 1. Samtykke defineres som "*enhver frivillig, specifik og informeret viljestilkendegivelse, hvorved slutbrugeren indvilliger i, at der lagres oplysninger eller opnås adgang til allerede lagrede oplysninger i slutbrugerens terminaludstyr*", jf. bekendtgørelsens § 2, stk. 1, nr. 8. Formuleringen "*enhver frivillig, specifik og informeret viljestilkendegivelse*" er identisk med formuleringen i persondatadirektivets art. 2, litra h, der fastsatte krav til samtykke ved behandling af persondata, inden databeskyttelsesforordningen trådte i kraft. Cookiebekendtgørelsen trådte i kraft i 2011, og i stedet for at følge ePrivacy-direktivet og henvise til persondatadirektivets definition på samtykke, valgte man som påvist at kopiere formuleringen fra persondatadirektivet. Som tidligere anført medfører forordningens art. 94(2), at henvisninger til persondatadirektivet nu gælder som henvisninger til forordningen, hvorfor ePrivacy-direktivets henvisning til samtykkekravet i persondatadirektivet nu gælder som henvisning til samtykkekravet efter forordningen. Eftersom man i 2011 valgte ikke at indsætte en henvisning til persondatadirektivet i cookiebekendtgørelsen, bliver denne ikke grebet af forordningens art. 94(2). Det betyder, at bekendtgørelsens krav til samtykke ikke lever op til de krav til samtykke, der følger af ePrivacy-direktivet, nemlig dem der gælder efter forordningen. Situationen er i stedet således, at mens samtykkekravet efter ePrivacy-direktivet er sat efter forordningen, er samtykkekravet efter cookiebekendtgørelsen stadig sat efter persondatadirektivet. Dette ville muligvis være uden betydning, hvis forordningens krav til samtykke ikke adskilte sig væsentligt fra persondatadirektivets krav. Sådan forholder det sig imidlertid ikke. EU-Domstolen har således slået fast, at et samtykke efter forordningen er "*endnu strengere*" end efter persondatadirektivet.[139] Det skyldes især de nye krav om en "*utvetydig viljestilkendegivelse*" og "*klar bekræftelse*".[140] Ved samme lejlighed slog Domstolen fast, at et samtykke efter ePrivacy-direktivets art. 5(3) skal leve

[139] Sag C-673/17 (Planet49), præmis 61 og generaladvokatens forslag til afgørelse, punkt 70
[140] Ibid.

op til de skærpede krav i forordningen.[141] Henset til det foregående kan det således konkluderes, at cookiebekendtgørelsen ikke udgør en korrekt implementering af ePrivacy-direktivets art. 5(3). Det rejser spørgsmålet om, hvorvidt slutbrugere i Danmark kan støtte direkte ret på direktivets art. 5(3), altså om der foreligger umiddelbar anvendelighed. For så vidt angår direktiver og direktivbestemmelser skelner man i EU-retten mellem vertikal og horisontal umiddelbar anvendelighed.[142] Førstnævnte omhandler borgerens mulighed for at støtte ret på direktivet eller direktivbestemmelsen overfor staten, mens sidstnævnte omhandler forholdet mellem to private, f.eks. hvor en borger ønsker at støtte ret på en direktivbestemmelse overfor en anden borger eller virksomhed.[143] For så vidt angår nærværende afhandling er det kun den sidstnævnte situation, der har interesse, f.eks. hvor en IoT-bruger i Danmark overfor Apple påberåber sig ePrivacy-direktivets art. 5(3) ved lagring af informationer i brugerens smartwatch. I dette tilfælde er EU-Domstolens praksis til Apples fordel, idét Domstolen konsekvent har været afvisende overfor at tilkende direktiver og direktivbestemmelser horisontal umiddelbar anvendelighed.[144] Domstolen har som belæg for sin holdning især fremhævet, at det følger af Traktaten om den Europæiske Unions Funktionsmåde (TEUF) art. 288, at direktiver udelukkende er bindende for medlemsstaterne.[145] På baggrund af det forestående kan det således konstateres, at en IoT-bruger i Danmark ikke har mulighed for at støtte direkte ret på ePrivacy-direktivets art. 5(3) overfor private virksomheder som f.eks. Apple. Det har samtidig den konsekvens, at danske slutbrugere ikke har mulighed for at påberåbe sig forordningens skærpede samtykkekrav, medmindre deres persondata behandles. I så fald følger kravet direkte af forordningen, der som bekendt finder anvendelse ved behandling af persondata, jf. art. 2(1). En dansk smartwatch-bruger vil således ikke kunne påberåbe sig forordningens skærpede samtykkekrav, hvis de informationer, der lagres i uret, ikke er personhenførbare.

Der er i ePrivacy-direktivets art. 5(3) fastsat to undtagelser til kravet om samtykke, som er blevet implementeret stort set ordret i cookiebekendtgørelsens § 4. Undtagelserne er

[141] Ibid., præmis 42, 43 og 65
[142] Daniel m.fl. (2011), s. 269 ff.
[143] Ibid., s. 269
[144] Ibid., s. 271 in fine. Det forholder sig i øvrigt anderledes for så vidt angår direktiver og direktivbestemmelsers vertikale umiddelbare anvendelighed. Her kan der godt støttes ret, hvis visse betingelser er opfyldt, jf. ibid., s. 269 ff.
[145] Ibid., der henviser til sag 152/84 (Marshall), præmis 48, sag C-221/88 (Busseni), præmis 23 & sag C-106/89 (Marleasing), præmis 6

de samme som til de to regelsæts krav om oplysningspligt. Der henvises derfor til analysen heraf i afsnit 3.2.5.

4. KONKLUSION

Denne afhandling har hermed belyst, hvilke problemstillinger de databeskyttelsesretlige krav om oplysningspligt og samtykke skaber for brugen af IoT og angivet forslag til løsninger herpå i en praktisk kontekst.

Det konkluderes, at IoT er underlagt de databeskyttelsesretlige krav om oplysningspligt og samtykke, der følger af databeskyttelsesforordningen, ePrivacy-direktivets art. 5(3) og af cookiebekendtgørelsen, som implementerer den nævnte direktivbestemmelse i dansk ret. Forordningen finder anvendelse, hvis der behandles persondata via IoT, mens de to andre regelsæt finder anvendelse ved lagring af eller adgang til data i IoT-produktet, uanset om dataene er personhenførbare eller ej. Eftersom ingen af de tre regelsæt specifikt adresserer IoT har *soft law* som retskilde stor betydning, herunder især Artikel 29-gruppens udtalelse om IoT (WP 223) og Mauritius-erklæringen.

Det konkluderes, at indsamling af *Big Data* via IoT er underlagt forordningens krav om oplysningspligt og samtykke, idét tilstrækkelig anonymisering af Big Data anses for illusorisk.

Det konkluderes, at databeskyttelsesrettens territoriale anvendelsesområde gør det noget nær umuligt for IoT-udbydere, der indsamler data om danske brugere, at undslippe kravene om oplysningspligt og samtykke, uanset kompleksiteten i handels- og produktionsstrukturerne.

Det konkluderes, at databeskyttelsesforordningen beskytter IoT-brugere, som er fysiske personer, mens ePrivacy-direktivets art. 5(3) og cookiebekendtgørelsen beskytter IoT-brugere, som enten er fysiske personer eller juridiske personer med legitim interesse i beskyttelsen. Det bemærkes, at beskyttelsessubjektet ikke altid er identisk med brugeren eller ejeren af IoT-produktet, f.eks. når *smartglasses* indhenter data om et individ i brillebærerens nærhed. Her er det ikke bæreren, men individet der er beskyttelsessubjekt.

Det konkluderes, at adskillige IoT-aktører kan betragtes som databeskyttelsesretlige ansvarssubjekter, f.eks. producenter, sociale medier, appudviklere, udbydere af dataplatforme og i visse tilfælde IoT-brugeren, uanset om denne er en fysisk eller juridisk person.

Oplysningspligten har rod i transparensprincippet, som bl.a. fastsætter krav til oplysningernes forståelighed og formidlingsform. Det konkluderes, at den klassiske løsning med

at udsende privatlivspolitikker ikke altid giver mening i en IoT-kontekst, f.eks. fordi det solgte IoT-produkt ikke har en skærm, eller fordi indsamlingen af data går så hurtigt og er så uforudsigelig, at en på forhånd udarbejdet privatlivspolitik aldrig vil være retvisende. Det konkluderes, at oplysningspligten i praksis bør kunne opfyldes via anvendelse af lyd, f.eks. fra et Google Home Mini eller andre smarthøjttalere, hvor manglende skærm og uforudsigelighed gør skriftlig opfyldelse af oplysningspligten illusorisk.

Det konkluderes, at den generelle oplysningspligt som fastsat i forordningens art. 13 og 14 ikke kun skal iagttages ved behandling af persondata via IoT, men også ved lagring af eller adgang til ikke-personhenførbare data i brugerens IoT-produkt. Som led i opfyldelse af oplysningspligten skal beskyttelsessubjektet desuden vejledes om, hvordan IoT-produktet frakobles internettet, så fortsat adgang til og indsamling af data forhindres.

Det konkluderes, at det i visse tilfælde er tydeligt, at forordningen ikke har taget højde for den teknologiske udvikling. F.eks. skal der efter forordningens art. 13 hverken gives oplysning om berørte kategorier af persondata eller om den kilde persondataene hidrører fra, hvis dataene indsamles hos den registrerede. Dette til trods for, at den registrerede ved benyttelse af IoT ikke altid er klar over, at data indsamles hos vedkommende, f.eks. hvis en smarthøjttaler tilfældigt overhører og indsamler data fra en fortrolig samtale, hvor den registrerede italesætter egen sygdom.

Det konkluderes, at indsamling af Big Data via IoT hos andre end den registrerede under visse omstændigheder kan undtages oplysningspligten, jf. forordningens art. 14(5)(b). Det gælder f.eks., hvis indsamlingen foretages af en medicinalvirksomhed til lægevidenskabelig forskning eller af IoT-producenten til udarbejdelse af statistiske opgørelser over kundegrupper. Herudover kan oplysningspligt i enkelte, konkrete tilfælde undlades, hvis ansvarssubjektet risikerer at røbe forretningshemmeligheder som f.eks. IoT-produktets kildekode, jf. DBL § 22, stk. 1.

Det konkluderes, at forordningens krav til samtykke skal iagttages i forbindelse med behandling af persondata via IoT. Det betyder bl.a., at samtykket skal være frivilligt, specifikt, informeret og utvetydigt og gives ved erklæring eller klar bekræftelse samt for så vidt angår følsomme persondata tillige være udtrykkeligt. Herudover skal samtykket bl.a. kunne påvises og kunne trækkes tilbage, og det må ikke være skjult i en lang privatlivspolitik, som IoT-brugeren skal scrolle igennem og godkende inden download af apps.

Det konkluderes, at IoT-forhandlere næppe vil leve op til kravet om informeret samtykke ved blot at vedlægge en privatlivspolitik ved salg af produktet til deres kunder, jf. Mauritius-erklæringens pkt. 3.

Det konkluderes, at formkravene til samtykkeafgivelsen er vige. Det kan indhentes mundtligt, skriftligt eller digitalt, f.eks. via *swipes* eller ved at vinke foran et smartkamera. Det afgørende er ikke, *hvordan* samtykket indhentes, men at der foreligger en fælles forståelse mellem ansvars- og beskyttelsessubjektet om formen.

Det konkluderes, at påvisningskravet ikke indebærer et krav om skriftlig dokumentation, men f.eks. kan opfyldes ved elektronisk logning af swipes.

Det konkluderes, at ansvarssubjekters mulighed for at skifte behandlingsgrundlag ved beskyttelsessubjektets tilbagekaldelse af samtykke i en IoT-kontekst sjældent vil komme på tale, da det oftest vil være urimeligt overfor den registrerede, især ved indsamling af Big Data. Det konkluderes desuden, at formkravene til tilbagekaldelsen ligesom ved indhentelsen er vige, og at det f.eks. kan ske ved at snakke med sin smarthøjtaler.

Det konkluderes, at samtykkekravet i ePrivacy-direktivets art. 5(3) siden databeskyttelsesforordningens ikrafttræden i 2018 ikke har været korrekt implementeret i dansk ret. Det skyldes, at cookiebekendtgørelsens samtykkekrav er fastsat efter persondatadirektivet, mens ePrivacy-direktivets krav nu følger forordningen. Det vurderes, at danske slutbrugere ikke kan støtte direkte ret på direktivets art. 5(3), da EU-Domstolen konsekvent har afvist at give direktivbestemmelser horisontal umiddelbar anvendelighed. Det betyder, at danske IoT-brugere kun kan påberåbe sig forordningens skærpede samtykkekrav, hvis deres persondata behandles, og ikke hvis der lagres eller gives adgang til ikke-personhenførbare data på deres IoT-udstyr.

Det konkluderes, at både oplysningspligt og indhentelse af samtykke kan undlades ved lagring af eller adgang til data i IoT-produktet, hvis dataene er nødvendige for at koble produktet op til internettet, eller hvis de er nødvendige til udførelse af en bestemt handling, som brugeren udtrykkeligt har anmodet om, f.eks. betaling for varer, jf. ePrivacy-direktivets art. 5(3) som implementeret i cookiebekendtgørelsens § 4.

5. RETSPOLITISK VURDERING

I det følgende foretages en retspolitisk vurdering af den gældende rets værdi, og der gives enkelte anbefalinger til ændringer på området.

Som påpeget i afsnit 1.3 er der påfaldende mangel på *lex specialis* indenfor databeskyttelsesretlig regulering af IoT. I enkelte tilfælde giver det anledning til udfordringer i praksis. F.eks. blev det i afsnit 3.1.5 påvist, at der foreligger uklare regler for, hvorvidt lyd kan bruges som alternativ til skriftlig opfyldelse af oplysningspligten, jf. forordningens art. 12(1). Denne uklarhed er ikke hensigtsmæssig i en virkelighed, hvor spørgsmålet i stigende grad aktualiseres i takt med udbredelsen af smarthøjttalere i private hjem. Regelforvirring kan resultere i, at producenter bruger unødige ressourcer på at overholde fiktive krav eller bryder regler pga. fejlfortolkning eller uvidenhed. Selvom forordningen kun har to år på bagen, skinner det i visse tilfælde igennem, at den teknologiske udvikling allerede har overhalet regelsættet indenom. F.eks. skal der som påvist i afsnit 3.2.5 ikke gives oplysning om berørte kategorier af persondata eller om den kilde dataene hidrører fra, hvis dataene indsamles hos den registrerede. Årsagen hertil er formentlig en formodning om, at oplysning er unødvendig, fordi den registrerede ved, hvilke data han afgiver til ansvarssubjektet. I en anden teknologisk tidsalder ville dette også være tilfældet, f.eks. hvor sælgeren beder kunden om navn og adresse, og kunden derfor godt ved, at disse to kategorier indsamles og hidrører fra ham selv. Dataindsamling via IoT fungerer imidlertid ikke på denne måde, og som nævnt i afsnit 1.1 er det næsten mere reglen end undtagelsen, at de registrerede ikke ved, hvilke data de afgiver via deres IoT-produkter. En præcisering af forordningens bestemmelser vil derfor være ønskelig i ovennævnte tilfælde. Man kan desuden rejse spørgsmålet om, hvorvidt der bør indføres databeskyttelsesretlig *lex specialis* for IoT. Fordelen herved vil oplagt være en mere klar retstilstand. Ulempen omvendt, at denne retstilstand med den løbende teknologiske udvikling in mente risikerer at blive forældet med samme hast som forordningen. Man skal således være påpasselig med alt for teknologispecifikke regler. En løbende ændring af forordningen vil muligvis være en bedre løsning, men risikerer at blive bremset eller forsinket af politiske uenigheder. Ved den næste revision af forordningen bør man derfor så vidt muligt brede bestemmelsernes anvendelsesområde ud, så så meget ny teknologi som muligt kan omfavnes, uden at en konstant ændring af reglerne er nødvendig. F.eks. bør formkrav som dem i art. 12(1) så vidt muligt undgås, da disse oplagt medfører praktiske vanskeligheder ved opfindelse af

ny teknologi. Herudover henstilles der til en mere proaktiv tilgang til reguleringen fra dansk side, så man undgår situationer som den i afsnit 3.3.5 beskrevne med cookiebekendtgørelsen, der to år efter forordningens ikrafttræden stadig anvender formuleringer fra persondatadirektivets tid. En fortsat uklar retstilstand gavner hverken ansvars- eller beskyttelsessubjekter, som således begge vil få gavn af de ovenfor foreslåede ændringer.

LITTERATUR- OG KILDELISTE

1. Litteratur

1.1. Bøger

- Blume, Peter (2016): *Retssystemet og juridisk metode*, 3. udg., Jurist- og Økonomforbundets Forlag.
- Blume, Peter (2018): *Databeskyttelsesret*, 5. udg., Jurist- og Økonomforbundets Forlag.
- Blume, Peter (2018): *Den nye persondataret*, 2. udg., Jurist- og Økonomforbundets Forlag.
- Daniel, Bugge Thorbjørn, Thomas Elholm, Peter Starup og Michael Steinicke (2011): *Grundlæggende EU-ret – EU efter Lissabontraktaten*, 2. udg., Jurist- og Økonomforbundets Forlag.
- Harhoff, Frederik (red.) (2017): *Folkeret*, 1. udg., Hans Reitzels Forlag.
- Nielsen, Kristian Korfits og Anders Lotterup (2020): *Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer*, 1. udg., Jurist- og Økonomforbundets Forlag.
- Riis, Thomas og Jan Trzaskowski (red.) (2013): *Skriftlig jura – den juridiske fremstilling*, 1. udg., Ex Tuto Publishing.
- Udsen, Henrik (2019): *IT-ret*, 4. udg., Ex Tuto Publishing.

1.2. Artikler

1.2.1. Juridiske artikler

- Nielsen, Jesper Løffler (2010): *Cookies og internetmarkedsføring – regulering og (manglende) håndhævelse.* U.2010B.319.

1.2.2. Ikke-juridiske artikler

- Andersen, Lars Nøhr (2019): *Løbeure, smartwatches og aktivitetsmålere: Hvad måler de?*, Forbrugerrådet Tænk, 7. oktober 2019, https://taenk.dk/test-og-forbrugerliv/elektronik/aktivitetsmaaler-smartwatch-og-loebeure-hvad-maaler-de (set d. 27. marts 2020)
- Andersen, Pia Buhl & Johann Thor Haahr Hansen (2019): *Afsløring: Techgiganter har hørt og nedskrevet indhold fra danskeres telefoner og smarthøjtalere*,

Politiken, 19. august 2019, https://politiken.dk/viden/Tech/art7334954/Techgiganter-har-hørt-og-nedskrevet-indhold-fra-danskeres-telefoner-og-smarthøjtalere (set d. 27. marts 2020)

- Ashton, Kevin (2009): *That 'Internet of Things' Thing*, RFID Journal, 22. juni 2009, https://www.rfidjournal.com/articles/view?4986 (set d. 29. marts 2020)
- Covington & Burling LLP, Inside Privacy (2014): *Data Protection Officials Adopt Internet of Things Declaration and Big Data Resolution*, 16. oktober 2014, https://www.insideprivacy.com/international/data-protection-officials-adopt-internet-of-things-declaration-and-big-data-resolution/ (set d. 27. marts 2020)
- Danmarks Statistik (2020): *Europarekord i brug af 'smart home'-produkter*, Nyt fra Danmarks Statistik, 3. marts 2020, nr. 83, https://www.dst.dk/da/Statistik/nyt/NytHtml?cid=36216 (set d. 27. marts 2020)
- Matyszczyk, Chris (2020): *Don't worry, Alexa and friends only record you up to 19 times a day*, ZDNet, 22. februar 2020, https://www.zdnet.com/article/dont-worry-alexa-and-friends-only-record-you-up-to-19-times-a-day/ (set d. 27. marts 2020)
- Power.dk (2020): *Mobilbetalinger – betal med dit smartwatch*, https://www.power.dk/magasinet/mobilbetalinger-betal-med-dit-smartwatch/ (set d. 29. marts 2020)
- Verma, Amit (2018): *Internet of Things and Big Data – Better Together*, Whizlabs Education Inc., 1. august 2018, https://www.whizlabs.com/blog/iot-and-big-data/ (set d. 27. marts 2020)
- Vollandt, Jonas Blume (2020): *Ny undersøgelse: Dine smart-enheder optager op til 19 gange i døgnet*, Version 2, 25. februar 2020, https://www.version2.dk/artikel/ny-undersoegelse-dine-smart-enheder-optager-19-gange-doegnet-1090098 (set d. 27. marts 2020)

1.3. Rapporter og beretninger

1.3.1. Fra juridiske organer

- Datatilsynets årsberetning 2014 (ISSN 1601-5657), Rosendahl A/S
- Datatilsynets årsrapport 2014

- Europæisk Tilsynsførende for Databeskyttelse: *Årsberetning 2014, Resumé* (ISSN 1831-0451)

1.3.2. Fra andre organisationer

- ICANN Security and Stability Advisory Committee (SSAC): *SAC105 The DNS and the Internet of Things: Opportunities, Risks, and Challenges*, 28. maj 2019.
- Rose, Karen, Scott Eldridge & Lyman Chapin: *The Internet of Things: An Overview – Understanding the Issues and Challenges of a More Connected World*, The Internet Society (ISOC), oktober 2015.

2. Retsforskrifter og forarbejder

2.1. EU-retten

2.1.1. Traktater

- Traktaten om den Europæiske Unions Funktionsmåde. *TEUF*.

2.1.2. Forordninger

- Europa-Parlamentets og Rådets forordning 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse). *Databeskyttelsesforordningen. GDPR.*
- Europa-Parlamentet og Rådets forordning 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF. *EDPS-forordningen.*
- Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger. *Den tidligere EDPS-forordning* (ophævet).

2.1.3. Direktiver

- Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation). *EPD 2002.*
- 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. *EPD 2009.*

- Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger. *Persondatadirektivet* (ophævet).
- Rådets direktiv 93/13/EØF af 5. april 1993 om urimelige kontraktvilkår i forbrugeraftaler.

2.2. Dansk ret

2.2.1. Love og lovbekendtgørelser

- Lov nr. 502 af 23/05/2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven). *Databeskyttelsesloven. DBL.*
- LBK nr. 128 af 07/02/2014 om elektroniske kommunikationsnet og -tjenester. *Teledataloven*.
- Lov nr. 429 af 31/05/2000 som senest ændret ved lov nr. 426 af 03/05/2017 om behandling af personoplysninger. *Persondataloven* (ophævet).
- LBK nr. 622 af 02/10/1987 om private registre m.v. (ophævet).

2.2.2. Bekendtgørelser

- BEK nr. 1148 af 09/12/2011 om krav til information og samtykke ved lagring af eller adgang til oplysninger i slutbrugerens terminaludstyr. *Cookiebekendtgørelsen*.

2.2.3. Betænkninger

- Betænkning nr. 1565, 2017, *Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning*, del I – bind 1.

2.2.4. Lovforslag

- Lovforslag 68, fremsat 25.10.2017

3. Soft law

3.1. EU

3.1.1. Artikel 29-gruppen

- Artikel 29-gruppens udtalelse af 16. september 2014 (WP 223): *Opinion 8/2014 on the on Recent Developments on the Internet of Things*.
- Artikel 29-gruppens vejledning af 28. november 2017, revideret 10. april 2018 (WP 259): *Guidelines on consent under Regulation 2016/679*.
- Artikel 29-gruppens vejledning af 29. november 2017, revideret 11. april 2018 (WP 260): *Guidelines on transparency under Regulation 2016/679.*

3.1.2. Den Europæiske Tilsynsførende for Databeskyttelse (EDPS)

- Den Europæiske Tilsynsførende for Databeskyttelses udtalelse af 19. november 2015: *Opinion 7/2015 Meeting the challenges of big data – A call for transparency, user control, data protection by design and accountability*.

3.2. Danmark

3.2.1. Datatilsynet

- Datatilsynets vejledning om de registreredes rettigheder (juli 2018)
- Datatilsynets vejledning om samtykke (september 2019)

3.2.2. Erhvervsstyrelsen

- Erhvervsstyrelsens vejledning nr. 10189 af 10. december 2019 til bekendtgørelse om krav til information og samtykke ved lagring af eller adgang til oplysninger i slutbrugerens terminaludstyr, "Cookiebekendtgørelsen". *Cookievejledningen*.

3.3. Internationalt

- *Mauritius Declaration on the Internet of Things*, 14. oktober 2014. *Mauritius-erklæringen.*

4. Retspraksis

4.1. EU-Domstolen

- *Forenede sager C-293/12 og C-594/12*, Digital Rights Ireland Ltd mod Minister for Communications, Marine and Natural Resources m.fl. og Kärntner Landesregierung m.fl., 8. april 2014.
- *Sag 152/84*, M. H. Marshall mod Southampton and South-West Hampshire Area Health Authority (Teaching).
- *Sag C-106/89*, Marleasing SA mod Comercial Internacional de Alimentación SA.
- *Sag C-221/88*, Det Europæiske Kul- og Stålfællesskab mod Konkursboet efter Acciaierie e ferriere Busseni SpA.
- *Sag C-230/14*, Weltimmo s. r. o. mod Nemzeti Adatvédelmi és Információszabadság Hatóság, 1. oktober 2015
- *Sag C-362/14*, Maximillian Schrems mod Data Protection Commisioner, 6. oktober 2015.
- *Sag C-673/17*, Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV mod Planet49 GmbH, 1. oktober 2019.

BILAG

1. E-mail fra Datatilsynet, hvor de oplyser, at de ikke var repræsenteret på Mauritius-konferencen i 2014 og derfor ikke har forholdt sig til Mauritius-erklæringen.

Bilag 1

Kære Malte Philbert Jessen

Ved e-mail af 23. februar 2020 har du rettet henvendelse til Datatilsynet vedrørende Mauritius-erklæringen.

Datatilsynet kan oplyse, at tilsynet ikke var repræsenteret på konferencen, og at tilsynet derfor ikke har forholdt sig til erklæringen.

Datatilsynet foretager sig ikke yderligere i anledning af din henvendelse.

Med venlig hilsen

DATATILSYNET

Carl Jacobsens Vej 35
2500 Valby
T 33 19 32 00
dt@datatilsynet.dk
www.datatilsynet.dk

Att. rette vedkommende

Jeg er i gang med at skrive speciale og har i den anledning nogle spørgsmål.

1) **Var Datatilsynet repræsenteret på konferencen på Mauritius i 2014, der førte til vedtagelsen af *Mauritius Declaration on the Internet of Things*,**
2) **og har Danmark i så fald tilsluttet sig erklæringen?**

Jeg har læst jeres årsberetning og årsrapport fra 2014, hvor I ikke nævner noget om konferencen.

På forhånd tak for svar.

Med venlig hilsen
Malte Philbert Jessen