Overholder Facebooks mobilapp den nye EU persondataforordning 2016/679, ved indsamling af samtykke til behandling af persondata?

Kandidatspeciale

Rasmus Hynneke Waidtløw | Aalborg Universitet | Erhvervsjura

2017

Titelblad

Titel

Overholder Facebooks mobilapp den nye EU persondataforordning 2016/679, ved indsamling af samtykke til behandling af persondata?

English title

Is Facebooks' app in compliance with the new EU regulation 2016/679, when collecting consent for processing personal data?

Studie

Kandidatspeciale, Erhvervsjura (HA-JUR)

Fag

Persondataret

Vejleder

Søren Sandfeld Jakobsen

Antal sider (inkl. bilag)

69

Anslag (ekskl. bilag)

138.897

Dato for aflevering

10/5-2017

Rasmus Hynneke Waidtløw 20114225 _____

1 INDHOLD

2 INTRODUKTION

Den 25 maj 2018 træder den nye persondataforordning fra EU i kraft. Dette gør den i stedet for direktiv 95/46 EF, som siden 1995 har styret det persondataretlige område i EU. Grunden til udskiftningen er, at der siden 1995 er sket en voldsom udvikling inden for elektronisk udstyr, herunder også benyttelse af data på disse elektroniske enheder. Det har simpelthen ikke været muligt rent juridisk at følge med den teknologiske udvikling på baggrund af direktiv 95/46 EF. Dette kan tydeligt ses med internettets frigivelse i 1994 og dets derefter hurtige udvikling, som ingen havde været i stand til at forudse. Internettet har gjort det muligt at handle let på tværs af lande, hurtigt finde information om alt man kan undre sig over, uanset hvor du befinder dig.[1] Dette medfører imidlertid også et marked for de data, som opfanges på internettet. Dette kan være i form af indkøbsvaner, interesseområder eller andet, som virksomheder, direkte eller indirekte, vil kunne tjene penge på, bl.a. gennem reklame, brugerforbedringer og salg af data. Et eksempel på, hvor stort dataindsamling er blevet i vores samfund, er Big Data. Big Data er vigtigt i forhold til målinger af forskellige forhold og til udvikling af forskellige teknologier, men det giver juridisk set også nogle komplikationer, som f.eks. hvordan disse data bruges. Som udgangspunkt bruges de data der indsamles til at forbedre den service der bliver udbudt.[2] Det kan være kreditkort virksomheder som VISA, der f.eks. benytter sig af Big Data til at finde ud af, om kunden er på ferie, når der bliver foretaget en transaktion i udlandet. I dette tilfælde hjælper Big Data til både at optimere kundens brugeroplevelse og minimere bedrageri. Ifølge en analyse fra analyseselskabet SAS, kunne VISA spare op til 2 milliarder USD om året på forhindring af svigagtige transaktioner, ved benyttelse af Big Data analytics.[3]

Data er altså en god ting for virksomheder, som kan forøge og forbedre deres service ved indsamling og benyttelse af disse data. Men omvendt skal der også være et sikkerhedsnet for brugeren, så alle ikke kommer til at vide alt, hvad brugeren har foretaget sig, mens han har været på internettet, eller på anden måde lækket data. Det er vigtigt at holde sig for øje, at databeskyttelse har sit udgangspunkt i artikel 7 i Det Europæiske Charter (2000) og artikel 8 i EMRK, som begge handler om beskyttelse af privatlivets fred, herunder også beskyttelse af persondata i chartres art. 8. Et eksempel på hvor galt det kan gå, er unges deling af nøgenbilleder på nettet. Her kan det ses, at når først data er blevet lagt ud på nettet, er det meget svært at få det helt væk derfra igen.

[1] http://www.nethistory.info/History%20of%20the%20Internet/web.html
[2] http://www.sas.com/en_us/insights/big-data/what-is-big-data.html
[3] http://www.sas.com/en_us/insights/big-data/what-is-big-data.html#m=visa-summary

Forordningen er som sagt baseret på Det Europæiske Charter (2000) artikel 7 og 8 samt EMRK artikel 8, om beskyttelse at privatliv og persondata. Denne beskyttelse medfører imidlertid et problem, set fra virksomheders øjne. Det mindsker nemlig den teknologiske udvikling, set på den måde, at der skal tages højde for de krav, som forordninger stiller, hvilket bliver både dyrere og mindre innovationsskabende. Resultatet heraf er, at forordningen forsøger at lave en mellemvej mellem borgernes og virksomhedernes interesser. Et eksempel herpå er forordningens artikel 5, stk. 1 litra c), som siger, at persondata skal "*være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles*".[4] Der er her tale om en beskyttelse af, at der ikke bliver registret data om den registrerede i uhensigtsmæssige store mængder, men udelukkende hvad der er relevant til det pågældende formål. Omvendt siger den også, at det står virksomheden frit at få disse relevante data, medmindre den registrerede har tilbagekaldt samtykke til behandling af nogle behandlingsområder efter artikel 7, stk. 3 eller begrænsning af behandlingen efter artikel 18. På baggrund af denne mellemvej som forordningen forsøger at gå, bliver dens artikler generelle, hvilket bl.a. kan ses i artikel 32 om behandlingssikkerhed, som primært siger, at virksomhederne skal sikre et passende teknisk og organisatorisk sikkerhedsniveau.

Grunden til at forordningen ikke er specificerende kan skyldes to ting. For det første for ikke at gøre lovgivningen alt for belastende for virksomhederne og for det andet at det, på baggrund af den hurtige teknologiske udvikling, vil være for besværligt at foretage ændringer på EU niveau, som kan blive nødvendigt ved udviklingen af vores teknologier, hvormed det er blevet et nationalt anliggende at specificere lovgivningen yderligere. Et eksempel på den hurtigt voksende teknologi er smartphones, som ifølge Danmarks Statistik er vokset fra 33% af befolkningen havde en smartphone i 2011 til 83% i 2016.[5] Det smarte ved smartphones er, at man har mulighed for stort set alt, uanset hvor man er, fordi det er muligt at tilgå sig internettet fra denne lille mobile enhed. Derudover er der apps tilgængeligt til smartphones, som kan gøre alt, lige fra informationssøgning til indkøb til underholdning, meget lettere. Dette medfører imidlertid også et stort dataflow. Selvom der ikke aktivt skal betales for mange af disse apps, betales der indirekte med data. Der er altså tale om databetaling. Nogle af disse data er bl.a. kontakter og fotos, som er lagret på telefonen. Et andet problem ved apps er, at folk ikke tænker over, hvad der bliver spurgt om adgang til ved installationen af apps. Herudover er de oplysninger, som apps henter ned fra de registreredes smartphones, oplysninger som de registrerede oftest ikke vil give ud, såfremt de blev spurgt direkte af en fysisk person. Et eksempel er Forbrugerrådet Tænks kampagne i 2014 for bedre digitale rettigheder, hvor de forsøgte at få samme oplysninger som apps spørger om, ud fra fysisk tilstedeværende personer, ved at en bager spurgte om disse

[4] Forordning 2016/679 art. 5, stk. 1, litra c).
[5] Bilag 1.

data, når kunderne betalte for deres varer.[6] Siden 2014 er der dog kommet mere fokus på datasikkerhed og derudover træder den nye EU-forordning også i kraft i 2018. Spørgsmålet er imidlertid, om apps overholder disse regler, som forordningen indeholder.[7]

Der vil i dette kandidatspeciale blive set på dette spørgsmål, hvor der bliver taget udgangspunkt i Facebook appen. Grunden til at der bliver taget udgangspunkt i denne app er, at den udover at være populær, som gør at en stor del af befolkningen har denne app installeret på deres smartphone, kræver appen informationer om mange forskellige ting, som kan være krænkende for den registrerede. Dette er bl.a. kontakter, kamera, fotos, placering m.m. Dette er også informationer som kan bruges til overvågning af den registrerede og dermed krænkende i forhold til privatlivets fred. F.eks. Kan appen se hvor den registrerede er og hvor han har været. Facebook kan derudover også profilere personer gennem deres interesser (både likes og artikler/links man har klikket på), ens tætte venner og deres interesser m.m. Appen vil altså blive undersøgt i forhold til den nye persondataforordning, fordi de har elementer som umiddelbart kan virke krænkende og fortrolige, men på den anden side også er nødvendige for disse apps virke, hvorfor det er interessant at se på netop denne app for at finde ud af, om de er ulovlige eller stadig er i overensstemmelse med den nye forordning på trods af deres store indhentning af fortrolige data. Det er lige præcis dette som gør det interessant at se på apps i forhold til persondata, fordi de pågældende appudviklere får mange forskellige persondata gennem deres apps. Disse data kan blive brugt til at fortælle hvem den registrerede er, hvilke interesser personen har, hvor personen (oftest) befinder sig. Disse data kan bruges til at lave en profil på personen som andre personer, specielt inden for erhvervslivet, kan være meget interesseret i, da de på denne måde kan specificere deres reklamer eller andre ydelser til de registrerede personer. Grunden til at apps vil være interessant at se på i forbindelse med den nye forordning er, at man stort set altid har apps på sig, som indhenter data gennem ens smartphone.

En anden grund til, at det netop er Facebook der bliver taget udgangspunkt i, er at det var med udgangspunkt i Facebooks videregivelse af persondata til USA, at Safe-Harbour ordningen blev anset som ugyldig. Der er her tale om dom C-362/14, Maximillian Schrems. Der blev her lagt vægt på, at hvis offentlige instanser, i dette tilfælde FBI, NSA og andre sikkerhedsbureauer, kan anskaffe sig adgang til unionsborgernes persondata på et generelt niveau og ikke på et objektivt grundlag om national sikkerhed, ville Det Europæiske Charter (2000) artikel 7 om privatliv, ikke have nogen rækkevidde. Der bliver her bl.a. sagt:

[6] https://taenk.dk/aktiviteter-og-kampagner/tidligere-kampagner/har-dine-apps-frit-spil-beskyt-dine-personlige
[7] Blume, P. (2016), s. 29-49.

"Navnlig skal en lovgivning, der gør det muligt for de offentlige myndigheder på generel vis at få adgang til indholdet af elektronisk kommunikation, anses for at udgøre et indgreb i det væsentligste indhold af den grundlæggende ret til respekt for privatlivet..."[8]

Det bliver altså fastlagt, at en generel automatiseret indsamling af persondata er en krænkelse af privatlivet, og dermed imod EU-lovgivningen.[9] Der bliver her også sagt i præmis 96, at Kommissionen kræver, at EU-borgernes grundrettigheder som minimum bliver overholdt, ved videregivelse af persondata til tredjelande.

[8] C-362/14, Maximillian Schrems, præmis 94.
[9] C-362/14, Maximillian Schrems, præmis 34 og 91 – 95.

3 AFGRÆNSNING

Der vil i dette speciale blive set på, hvorvidt Facebooks mobilapp er lovlig rent persondataretligt, med udgangspunkt i nogle af de mere generelle regler som f.eks. indhentning af samtykke, gennemsigtighed, oplysninger til den registrerede m.m. Dette bliver forsøgt svaret på gennem problemstillinger, som står i afsnit 4.1. Andre dele af persondataforordningen, end dem der er relevante i forhold til besvarelse af problemformulering og problemstillinger, vil ikke blive behandlet i dette speciale. De vil dog stadig kunne blive nævnt, såfremt dette findes relevant. Der vil ikke blive set på eventuelle speciallovgivninger, som kunne tænkes at være relevante ved lovlighedsbedømmelsen. Da der kun bliver set på en privat virksomheds app, vil der ikke blive set på lovgivning, som udelukkende gælder for den offentlige sektor.

Der vil også kun blive set på Facebooks app, som hvordan den dataretligt bliver behandlet som en app. Med dette menes der, at der ikke bliver set på de andre virkeområder end som app til mobilenheder (smartphone og tablet), som f.eks. hjemmesider og smartwatch, medmindre dette er direkte foreneligt med appen. Da dette er et juridisk speciale, vil fokus primært være på juraen, hvormed der kun vil blive taget fat i de nødvendige tekniske elementer, som f.eks. dataflow, uden at dette bliver for stor en del af specialet. Dette vil dermed blive gjort kort og præcist uden at det bliver et teknisk speciale. Det er dog nødvendigt i persondataretten at komme ind på de relevante tekniske elementer, da dette er en del af de fakta, som skal bruges til at belyse problemstillingen gennem den juridiske metode, hvorfor det ikke kan afgrænses helt ud af specialet.

Selvom Facebook er et amerikansk selskab, som dermed sender data til et usikkert tredjeland, vil der ikke blive set på Facebooks overholdelse af EU-US Privacy Shield. Grunden hertil er, at dette vil blive for omfattende for specialet og at EU-US Privacy Shield i sig selv ikke er direkte relevant i forbindelse med indhentning af samtykket, som dette speciale omhandler. Videregivelse til tredjelande er efter samtykkets indhentning, når behandlingen er startet.

4 PROBLEMFORMULERING

Som nævnt er der kommet et større fokus på det persondataretlige område, hvilket også har resulteret i den nye forordnings tilblivelse. Dette skyldes den hurtigt voksende tekniske udvikling, samt befolkningens større behov for teknologi. Vi bliver altså teknologiseret i større og større grad. Selv vores hvidevarer bliver "smart".[10] Dette medfører imidlertid også at befolkningen bliver overvåget i større grad af virksomheder, hvormed privatlivet er i fare. Specielt brugen af apps på enheder, som der altid er tændt og befinder sig på den registrerede, som f.eks. smartphones, kan blive problematiske for privatlivet. Forordningen forsøger at beskytte de registrerede, uden at blive for stor en byrde for virksomhederne.

Der vil i dette speciale blive taget udgangspunkt i Facebooks app. Grunden til at der vil blive taget udgangspunkt i denne app er, at det er er en populær app, som indhenter store mængder data, herunder også fortrolige og følsomme data. Appen indhenter både data lagret på smartphonen, dette kan f.eks. være billeder, kontakter m.m. og data som smartphonen indhenter løbende, som f.eks. den registreredes placering. Dette speciale vil se på, om Facebooks app krænker privatlivet i en sådan grad, at det er ulovligt ifølge den nye forordning, hvilket gøres gennem følgende problemformulering:

Overholder Facebooks mobilapp den nye EU persondataforordning 2016/679, ved indsamling af samtykke til behandling af persondata?

4.1 PROBLEMSTILLINGER

- Lever Facebooks app op til de forøgede krav om indhentning af samtykke?
- Hvordan indhentes der samtykke for behandling af persondata om børn under 13-16 år?
- Bliver der oplyst om alle de lovpligtige oplysninger ved indsamling af persondata?
- Bliver de generelle principper for behandling af persondata i artikel 5, herunder specielt litra c) om dataminimering, overholdt?
- Bliver reglerne om gennemsigtighed i artikel 12, stk. 1 overholdt?

[10] http://www.samsung.com/us/explore/family-hub-refrigerator/

5 METODE OG OPBYGNING

Til besvarelsen af den valgte problemformulering og de underliggende problemstillinger, vil forordning 2016/679 blive analyseret i forhold til de faktiske omstændigheder, som Facebook pålægger dets brugere. Dette vil også blive belyst på baggrund af nuværende retspraksis og principper, såfremt de findes relevante i forhold til den nye forordning. Denne fremgangsmåde kaldes den retsdogmatiske metode, som overordnet set stræber efter at beskrive, fortolke, analysere og systematisere gældende ret. Der vil altså blive benyttet gældende (og fremtidig) jus i forhold til gældende fakta, som Facebooks app præsenterer, bl.a. gennem Facebooks privatlivspolitik, dataindsamling m.m. Denne analyse af jus i forhold til fakta, vil derefter blive benyttet til at komme med en konklusion på den valgte problemformulering, herunder også problemstillinger. I henhold til den retsdogmatiske metode, vil dette blive gjort ud fra et objektivt synspunkt, således at konklusionen så vidt muligt bestræbes på at være i overensstemmelse med, hvad lovgivningen (EU) har haft som intention med forordningen, samt hvad de dømmende institutioner har haft med deres afgørelser og udtalelser.[11]

Den juridiske teori siger, at den gode juridiske tekst, som forsøger at klarlægge gældende ret, er karakteriseret ved korrekt benyttelse af retskilder, her både ved at alle relevante kilder er inddraget samt analyseret på en sådan måde, at den argumentation som teksten fremstiller, virker overbevisende for læseren. Når man taler om retsdogmatisk metode, er dette vigtigt at holde sig for øje, da retsdogmatikken har til formål at beskrive gældende ret, hvormed det at argumentere for sine synspunkter omkring denne ret på en korrekt og analytisk måde bliver vigtig, da ens tekst ellers bliver ubrugelig i den forstand, at den ikke kan benyttes af andre. Specielt i dette tilfælde når der er tale om en kommende lovgivning, som ikke er noget retspraksis på endnu, bliver det vigtigt at udforme teksten korrekt efter de juridiske teorier og metoder. Grunden hertil er, at der ved gældende lov vil være retspraksis som kan hjælpe med at fortælle hvordan man skal fortolke en lovtekst, mens dette ikke er tilfældet ved kommende lovgivning, da der ikke er noget retspraksis.[12]

Der vil på denne baggrund blive inddraget relevante domme og afgørelser samt lovtekst, hvorpå der vil blive lavet en sproglig- og fortolkningsanalyse, til forståelse af den pågældende teksts benyttelse i praksis. I denne anledning vil forordning 2016/679 blive analyseret, men også set i forhold til direktiv 95/46/EF, for at se de ændringer, som der er i forordningen. Fortolkningsanalysen vil bl.a. blive gjort på baggrund af hidtidige domme og afgørelser fra retsinstanser, såfremt at denne retspraksis ikke findes at være blevet forældet med

[11] Munk-Hansen, C (2014), s. 85 - 98 og 189 -204.
[12] Blume, P. (2009), s. 159 – 161.

den nye forordning, men også på baggrund af de overvejelser, som er blevet gjort i anledning af forordningens tilbliven og eventuelt også på baggrund af persondatarettens retshistorie, hvis dette bliver relevant, hertil specielt grunden til datarettens tilbliven, som er beskyttelse af privatlivets fred.

Opbygningen af dette speciale vil efterfølgende starte med at præsentere de vigtige elementer af persondataforordningen i forhold til den valgte problemformulering og de underliggende problemstillinger. Der vil her også blive set på, hvad forskellen er på den nye forordning og det hidtil gældende direktiv, for at se i hvor stor grad forordningen skærper datasikkerheden for den registrerede, herunder også belastningen for de dataansvarlige. Derefter bliver der set på, hvordan Facebooks app forsøger at imødekomme de krav, som forordningen opstiller, hvorefter der vil blive set på, om det, som der bliver gjort, er tilstrækkeligt for at overholde forordningen. Efter denne analyse af Facebooks overholdelse af forordningen, kommer konklusionen, som vil forsøge at svare på den valgte problemformulering ved hjælp af de foregående afsnit. Sidst i specialet er en perspektivering til andre relevante emner inden for dette emne samt et kort afsnit om Facebook of persondataforordningens fremtid, efterfulgt af et engelsk resumé.

6 PERSONDATAFORORDNINGEN

I dette afsnit bliver de områder i forordning 2016/679 forklaret, som der er relevante for besvarelsen af problemformuleringen og videre vil blive behandlet i forbindelse med analyse i forhold til Facebooks vilkår og privatlivspolitik.

6.1 SAMTYKKE

For at der kan behandles persondata, skal der være en hjemmel herfor. Denne hjemmel findes hhv. I forordningens artikel 6 for almindelige personoplysninger og artikel 9 for særlige personoplysninger. Dette kan ses i artiklernes ordlyd som siger:

"Behandling er kun lovlig, hvis og i det omfang mindst ét af følgende forhold gør sig gældende: (...)",[13]

"Behandling af personoplysninger om (...) er forbudt".[14]

I begge tilfælde er det muligt at behandle oplysninger, såfremt den registrerede har givet samtykke til behandlingen, udtrykkeligt hvis der er tale om oplysninger under artikel 9. Betingelser for samtykke kan findes i artikel 7. Denne artikel er en udvidelse af behandlingssikkerheden i forhold til persondatadirektivet, hvor der ikke er en specificering af samtykkebegrebet, men hvor dette udelukkende er implementeret i artiklerne om behandlingsformer (direktivets artikel 7 og 8). Resultatet af denne nye artikel er et skærpet behandlingskrav for de dataansvarlige. Bl.a. er det op til den dataansvarlige at påvise, når han har fået et samtykke fra den registrerede, at dette samtykke er i et enkelt og klart sprog, samt at samtykket er givet frit, hvormed forstås om de indhentede data er nødvendige i forhold til kontrakten mellem dataansvarlig og den registrerede. Herudover bliver det også fastlagt ved lov, at den registrerede har ret til at trække samtykket tilbage.

Der er altså en væsentlig udvidelse af samtykkebegrebet, som øger sikkerheden for den registrerede. Forordningens artikel 7 gælder for både almindelige og særlige kategorier af personoplysninger. Artikel 9 har krav om *udtrykkelig samtykke*. Grunden hertil er, at behandling af samtykke om følsomme oplysninger som f.eks. helbredsoplysninger, kan have konsekvenser for den registrerede, som denne ikke er klar over. Det er derfor vigtigt, at samtykket ikke er tvetydigt i forhold til, hvad der bliver indhentet samtykke til. Der må dermed være krav om at samtykket klart, tydeligt og eksplicit siger, hvad og hvorfor sådanne oplysninger er

[13] Forordning 2016/679 art. 6, stk. 1.
[14] Forordning 2016/679 art. 9, stk. 1.

nødvendige at behandle. Det er dog ikke sikkert at det er lovligt at behandle følsomme oplysninger på baggrund af samtykke, da det i artikel 9, stk. 2 siger:

"... medmindre det i EU-retten eller medlemsstaternes nationale ret er fastsat, at det i stk. 1 omhandlede forbud ikke kan hæves ved den registreredes samtykke".[15]

Samtykkehjemlen er dermed ikke gældende i sådanne tilfælde, som er omhandlet af ovennævnte citat. Dette er en af forskellene på almindelig samtykke og udtrykkelig samtykke. En anden er, at det almindelige samtykke krav skal have den registreredes *"… erklæring eller klar bekræftelse…"* [16] på behandlingen. Derudover skal samtykket selvfølgelig også overholde artikel 7. Spørgsmålet er imidlertid her, om det er muligt at indhente et indirekte samtykke. Der kan her f.eks. ses ved brugen af cookies, hvor nogle hjemmesider giver information omkring deres cookies (en såkaldt cookiepolitik) og indhenter samtykket hertil, ved at brugeren fortsat bruger siden eller bare orienterer om, at websiden bruger cookies, som ses på billede 1.

Billede 1

Ved udtrykkeligt samtykke vil dette ikke være muligt, da samtykket i givet fald vil være indhentet indirekte og dermed ikke udtrykkeligt.[17]

Det er dog ikke kun et samtykke der gør det muligt at behandle persondata. Artikel 6 opstiller seks hjemler til behandling af data, hvor samtykke kun er en enkelt af disse. Det vil dog næppe være muligt for disse apps at behandle data på baggrund af de andre bestemmelser i den indledende fase, hvor en bruger bliver oprettet. Problemet med behandling efter de andre hjemmelsregler er, at disse i stor grad kræver, at der er en anden legitim grund til behandlingen, at der allerede er et forhold mellem den registrerede og den dataansvarlige eller at et sådan forhold vil blive indgået i fremtiden. F.eks. kan det ses i art. 6, stk. 1, litra b), at der kan behandles data med hensigt til gennemførelse af foranstaltninger som den registrerede træffer, forud for indgåelsen af en kontrakt. Men da der ikke foreligger en kontrakt mellem den dataansvarlige og de registrerede i forhold til Facebooks app og at der ingen hensigt er til at indgå en sådan kontrakt, vil denne hjemmel til behandling næppe være mulig at benytte. Samtykket er altså den mest optimale hjemmel til behandling af data for apps. Grunden hertil er, at det er sikkert og nemt at indhente et samtykke, hvilket i de

[15] Forordning 2016/679 art. 9, stk. 2, litra a).
[16] Forordning 2016/679 art. 3, nr. 11.
[17] Waaben, H. og Nielsen, K. K. (2015), s. 288 – 289.

fleste tilfælde ved brugeraktivering sker ved at klikke en boks, hvor brugerne tilkendegiver at de har læst og accepteret de linkede privatlivsvilkår og politikker, hvormed de bliver registreret og deres data vil blive behandlet.

Definitionen af samtykke findes i forordningens artikel 4, nr. 11. Her står der at samtykket skal gives frivilligt, specifikt, informeret og utvetydigt. Ved indhentning af samtykket skal der altså specificeres hvilke formål og behandlingsformer den registrerede samtykker til, hvilket også betyder at den registrerede skal informeres om, hvilke data der behandles samt grunden til behandlingen. Dette skal gøres på et utvetydigt fundament, hvilket vil sige at der ikke må være tale om bl.a. indirekte indhentning af samtykket. Det skal altså være udtrykkeligt. Samtykket skal herudover også være frivilligt. Hvis der er tale om at samtykket er givet i forbindelse med tvang eller magtudøvelse er der ikke tale om frivilligt afgivelse af samtykket. Hvis der derimod er tale om, at samtykket er givet i forbindelse med en modydelse, hvor der er krav om samtykke, er der dog stadig tale om at samtykket er givet frivilligt. Resultatet heraf er at persondata bliver til et betalingsmiddel i sig selv, f.eks. ved at afgive samtykke til behandling af persondata ved at tilkomme sig en vare eller ydelse. Hertil siger kommissionen dog i forordningens præambel betragtning 43:

"Med henblik på at sikre, at der frivilligt er givet samtykke, bør samtykke ikke udgøre et gyldigt retsgrundlag (…) hvis der er en klar skævhed mellem den registrerede og den dataansvarlige (…) hvis det ikke er muligt at give særskilt samtykke til forskellige behandlingsaktiviteter (…) eller hvis opfyldelsen af en kontrakt (…) gøres afhængig af samtykke, selv om et sådant samtykke ikke er nødvendigt for dennes opfyldelse."[18]

Som eksempel på denne "skævhed" gives det offentlige i forhold til den registrerede, hvor det offentlige klart er større end den registrerede og dermed skævvrider forholdet imellem dem. Så snart at samtykket får en stor negativ konsekvens for den registrerede i forhold til den modydelse den registrerede får herfor, vil det kunne være til diskussion om samtykket er blevet givet frivilligt. Et andet eksempel herpå er, hvis en arbejdstager skal afgive samtykke til en arbejdsgiver. Hvis konsekvensen af ikke at give samtykket er, at arbejdstageren bliver fyret, vil der være en negativ konsekvens som gør, at samtykke næppe kan anses som værende afgivet frivilligt. Resultatet heraf vil dermed være, at arbejdsgiveren må finde en anden hjemmel til behandling end samtykke.[19]

I forbindelse med videregivelse kan det i nogle tilfælde virke absurd og modstridende at indhente samtykke i forhold til videregivelsens formål. Hertil kan nævnes højesteretsdommen U2011.2343H. Dommen handler

[18] Forordning 2016/679 præambel, betragtning 43.
[19] Blume, P. (2016), s. 63 – 67.

om to medarbejdere H og S, hvor H i en telefonsamtale til S videregav oplysning om mistanke om at A havde et alkoholmisbrug. A fik ikke ansættelse hos S, hvorfor A anlagde sag for overtrædelse af bl.a. persondataforordningen. Resultatet blev at der var tale om behandling af følsomme oplysninger, som krævede samtykke til behandling af den registrerede. Det som kan anses at være et problem ud fra dette er, at referencepersoner ikke kan videregive følsomme oplysninger, selvom det er relevant at vide for den ansættende part. Omvendt skal det dog også siges, at dette selvfølgelig er beskyttelse af den registrerede, specielt når der er tale om "en mistanke". Dette afbilleder imidlertid igen den balance som persondataretten forsøger at gå mellem beskyttelse af individer på den ene side og funktionalitet for erhvervslivet på den anden, hvor persondataretten har tendens til at hælde mere mod beskyttelse af den registrerede frem for erhvervslivet. Herudover kommer dommen også frem med den konklusion, at følsomme oplysninger, på trods af at være udtømmende, skal fortolkes bredt. Dette ses ved at alkoholmisbrug i denne dom fastlægges som værende en helbredsoplysning. Et andet eksempel er medlemskaber, da man ud fra nogle medlemskaber eller abonnementsoplysninger kan uddrage følsomme oplysninger om en person som f.eks. religion.[20]

6.2 DATABEHANDLING AF BØRN

Ved behandling af børn gælder samme regler som ved voksne, medmindre hjemlen til databehandlingen er samtykke. Ved samtykke er der skærpede regler for behandling af børn under 16 år, som står i forordningens artikel 8. Ved "børn" forstås personer under 16 år, men det er muligt for medlemsstaterne at ændre dette ned til 13 år ved national lovgivning. I dette speciale vil der dog blive taget udgangspunkt i forordningens hovedregel, som er 16 år. Det er vigtigt at holde sig for øje, at artikel 8, stk. 1 ikke har virkning på medlemsstaternes generelle aftaleret som omhandler børn.

Artiklens stykke ét siger, at der ved udbud af informationssamfundstjenester til børn under 16 år, skal samtykket godkendes af en med forældremyndighed. Da der er valgt "informationssamfundstjenester" i stedet for "behandling", må dette også betyde, at ikke al behandling falder inden for artikel 8 stk. 1's virkeområde. Informationssamfundstjenester defineres som:

"… denne definition omfatter enhver tjeneste, der normalt leveres mod betaling, og som teleformidles ved hjælp af elektronisk databehandlingsudstyr (…) og dataoplagringsudstyr på individuel anmodning af en tjenestemodtager…"[21]

[20] Waaben, H. og Nielsen, K. K. (2015), s. 283 - 287
[21] Direktiv 2000/31/EF præambel, betragtning 17.

I forbindelse med apps vil dette altid blive formidles elektronisk og på afstand. Herudover bliver de oftest også downloadet på baggrund af brugerens egen anmodning. Spørgsmålet er imidlertid hvorvidt de services der bliver tilbudt "normalt leveres mod vederlag". Underholdning bliver altid leveret mod vederlag, da de firmaer der står bag disse programmer, skal have en indkomst. Men ved gratis apps som f.eks. Facebook er der ikke tale om direkte betaling fra brugeren. Denne betaling finder primært sted gennem de informationer Facebook får fra brugeren, hvorefter de kan præcisere reklamer fra deres sponsorer bedre. I forhold til om Facebooks app falder under artikel 8 stk. 1's anvendelsesområde, kommer an på hvor bredt "normalt leveres mod vederlag" skal fortolkes. At komme med en decideret konklusion på dette kan være svært, men som udgangspunkt må Facebook være underlagt denne bestemmelse. Grunden hertil er, at der sker betaling gennem informationer (informationsbetaling), som Facebook tjener penge på. Resultatet heraf er, at appen skal overholde artikel 8 ved indhentelse af samtykke fra børn under 16 år.

Der er imidlertid en lempelse til kravet om forældregodkendt samtykke i stk. 2, som siger at den dataansvarlige skal:

> *"… gøre sig rimelige bestræbelser på i sådanne tilfælde at kontrollere, at indehaveren af forældremyndigheden over barnet har givet eller godkendt samtykke".*[22]

Der skal altså kun foretages en bestræbelse efter at sikre sig et samtykke givet af en persondataretlig myndig person. Hvorvidt Facebooks app overholder dette, vil blive diskuteret i "Forordningen i praksis".

6.3 OPLYSNINGSPLIGT

Forordningens artikel 13 og 14 omhandler oplysningspligt fra den dataansvarliges side overfor den registrerede. Artikel 13 omhandler oplysningspligt ved indhentning af data direkte fra den registrerede, mens artikel 14 omhandler oplysningspligt overfor den registrerede, såfremt data om denne er indhentet andetstedsfra end den registrerede. Da apps kommunikere direkte med den registrerede, vil den relevante artikel herfor være artikel 13, dog vil Facebook også indhente data gennem andres oplysninger om den registrerede, bl.a. gennem venners oplysninger om denne, hvormed artikel 14 også er relevant ved Facebooks behandling.

Den artikel som svarer til forordningens artikel 13 i direktivet er artikel 10. Artiklerne ligner overordnet hinanden i de to lovtekster med nogle få fravigelser, herunder specielt forordningens stk. 1, litra f) om oplysninger om videregivelse til tredjeland. Direktivets artikel stopper imidlertid der, hvorimod forordningens har yderligere krav til oplysninger i stk. 2. Der er her bl.a. krav om at oplyse den registrerede

[22] Forordning 2016/679, art. 8, stk. 2.

om behandlingens tidsrum samt indsigts-, berigtigelse-, klage- og sletningsret. Igen er forordningen altså mere krævende for den dataansvarlige end direktivet er. Ud over de i artikel 13 og 14 nævnte krav til oplysningspligten, er der også artikel 12, stk. 1 som siger, at disse oplysninger skal være gennemsigtige, klare og letforståelige.

I forhold til oplysningspligten der er fremlagt i direktivet, fokuserer forordningen i større grad på, at den registrerede skal kunne beskytte sig selv ud fra de oplysninger han får. Hermed menes der, at der i direktivet var krav om at den registrerede skulle kunne få oplysninger til selv at kunne søge informationer om den pågældende behandling, mens der i forordningen er krav til at den registrerede får den fornødne information at vide til at kunne foretage en velinformeret beslutning om afgivelse af samtykket. Grunden til denne ændring må til dels være på grund af det kraftigt stigende forbrug af specielt internettet, gennem mange forskellige enheder, som gør, at forbrugerne lader sig registrerer i langt større grad end for blot 10 år siden. Dette stærkt stigende forbrug medfører et marked for persondata og dermed en nødvendighed om, at forbrugerne (de registrerede) bliver bekendt med de konsekvenser behandlingen har for dem, hvilket de øgede krav om oplysningspligt forsøger at imødegå.

6.4 GENERELLE PRINCIPPER

I forordningens artikel 5 findes de generelle principper om behandling af persondata. Ud over de principper der er oplistet i artiklens stk. 1 bliver der givet et yderligere princip i artiklens stk. 2. Dette princip er ”ansvarlighed”. Den dataansvarlige er ansvarlig for at overholde de i stk. 1 listede principper, samt kunne påvise at disse bliver overholdt. Der er altså tale om at den dataansvarlige er ansvarlig for at overholde forordningen og dermed være i stand til at påvise denne overholdes i tilfælde af stridigheder.

Artikel 5, stk. 1 nævner seks forskellige principper som skal overholdes ved behandling af persondata. Den første der bliver nævnt i litra a), er princippet om god databehandlingsskik. Behandlingen skal være ”lovlig, rimelig og udføres gennemsigtigt”. Dette er meget bredt, særligt kravet om ”rimelighed”, hvilket også er grunden til, at Datatilsynet benytter sig af artiklen om god databehandlingsskik som en generalklausul, hvormed de kan afvise en ellers lovlig behandling, hvis behandlingen anses som urimeligt bebyrdende for den registrerede. Litra b) omhandler formålsbegrænsning, eller formålsbestemthedsprincippet, som betyder at den dataansvarlige skal behandle de indsamlede data i overensstemmelse med den hjemmel, som de er indhentet efter. Dette vil sige, at hvis data er blevet indsamlet efter samtykkehjemlen, må der kun foretages behandling efter samtykkets givne område, altså de data som den behandlede kender til og har accepteret behandling af, jf. artiklerne 6-9, 12 stk. 1, 13 og 14. Derudover skal det være klart hvorfor der bliver indsamlet data. Der skal altså være en nærliggende sammenhæng mellem den aktivitet den dataansvarlige udøver og behovet for at indsamle de pågældende data. Dette kaldes også saglighedsprincippet. Litra c) komme ind på

proportionalitet og relevans, herunder også forbud mod unødvendig dataophobning. Tilsammen også kaldet dataminimering. Når den dataansvarlige indsamler data, må han kun indsamle data der er tilstrækkelige og nødvendige til behandling af det formål, som han har hjemmel til. Såfremt der er data som kan blive nødvendige på et senere tidspunkt, men ikke er det på indsamlingstidspunktet, må disse data dermed ikke blive indhentet, da det vil skabe dataophobning. Derudover må der også kun indsamles data i en proportionel størrelse, som er forenelig med dataindsamlingens formål. Dette er specielt et problem i forhold til Big Data, som netop indsamler store mængder data til fremtidig brug, som ofte ikke vil kunne anses som proportionel i forhold til et specifikt givent formål. Dataminimering medfører også at den dataansvarlige skal tage stilling til, om det overhovedet er nødvendigt at indsamle persondata til et givent formål. Dataminimeringen forsøger altså at komme væk fra den selvfølgelighed det er at indsamle data til behandling ved løsning af forskellige opgaver.

Litra d) omhandler datakvalitet, som specielt kan være problematisk for Facebook. Grunden hertil er, at litra d) siger, at de data der behandles skal være korrekte og ajourførte. Dette giver et problem i forhold til profilering, som skaber en profil ud fra de oplysninger man har om den registrerede. Problemet i forhold til Facebook er, at de oplysninger Facebook får om den registrerede ikke nødvendigvis er korrekte, eller siger det om den registrerede som profileringen konkluderer. Derudover siger reglen også, at der skal foretages "ethvert rimeligt skridt" til berigtigelse eller sletning af urigtige personoplysninger. Dette er princippet om rigtighed. Dette princip skal dog ses i forhold til den dataansvarlige, sådan at alle de indsamlede data ikke skal efterses dagligt, da dette vil være en alt for stor ressourcemæssig byrde for den dataansvarlige, men med passende mellemrum. I forhold til litra e) og f) omhandler disse tidsbegrænsning og sikkerhed. Som kort siger, at den dataansvarlige behandler data med tilstrækkelig sikkerhed, samt at de indsamlede data kun opbevares i et nødvendigt tidsrum i forhold til det formål, som de er blevet indhentet til. [23]

6.5 GENNEMSIGTIGHED

I forlængelse af oplysningspligten i artiklerne 13 og 14 i forordningen, siger artikel 12, stk. 1 at disse oplysninger skal meddeles *"… i en kortfattet, gennemsigtig, letforståelig og lettilgængelig form og i et klart og enkelt sprog…"*[24] Dette gælder specielt hvis der er tale om mindreårige børn. Det er altså ikke muligt for de store virksomheder at lave en lang indviklet juridisk tekst, som kun de færreste vil kunne forstå, da dette ikke vil være et klart sprog eller gennemsigtigt. Ved kortfattet må forstås at teksten skal fremstille de nødvendige krav til oplysningspligt på en klar og kortfattet måde, så den registrerede uden komplikationer

[23] Blume, P. (2016), s. 69-76.
[24] Forordning 2016/679 art. 12, stk. 1, 1. pkt.

kan forstå hvilke persondata den dataansvarlige indsamler, hvorfor de bliver indsamlet samt i hvor lang en periode, så den registrerede kan tage en beslutning omkring behandlingen på et oplyst grundlag. Det samme gælder for kravet om gennemsigtighed og letforståelig tekst. Det skal altså ikke være muligt for den dataansvarlige at gemme sig bag ved et uforståeligt juridisk dokument på uproportionelt mange sider, som den registrerede ikke ville være i stand til at have overblik over. På baggrund af artikel 12, stk. 1, samt artiklerne 13 og 14 kan det ses, at forordningen forsøger at skærpe sikkerheden til den registrerede på en sådan måde, at der ikke bliver gemt eller på anden måde skjult nødvendige oplysninger for den registrerede, som er nødvendige for at tage beslutningen omkring behandlingen. I forhold til Facebook resulterer dette i, at de tydeligt skal fortælle brugeren, den registrerede, hvad de gør med de persondata de indhenter ved brug af deres apps, hvem de sender dem til osv. Dette gør de på nuværende tidspunkt ved at refererer til deres privatlivspolitik og vilkår hvor den registrerede krydser af i en boks for at bekræfte, at disse betingelser er blevet læst.

Et problem dette kan give for de dataansvarlige er i forhold til børn. Enten skal de dataansvarlige lave et dokument hvor de oplyser om alt det, der kræves af dem i forhold til artiklerne 13 og 14, som er forståeligt for et barn. Dette vil imidlertid være umuligt, da dette vil kræve at børnene som minimum kan læse de sprog som privatlivspolitikkerne er skrevet i, hvilket ikke er givet ved installation af apps, som delvist henvender sig til børn. En anden mulighed er, at de dataansvarlige forsøger kun at tillade personer over 16 år, så de registrerede ikke forbindes som værende børn rent persondataretligt efter forordningens ikrafttrædelse. Dette vil imidlertid mindske de dataansvarliges økonomiske resultat, da de vil hindre en stor gruppe fra at benytte deres apps. Den bedste løsning til problematikken omkring indhentning af oplysninger hos børn, må dermed være at indhente samtykke fra forældre eller værge til behandling af barnets persondata ved brugen af appen. Dette giver dog et nyt problem: hvordan indhentes sådan et samtykke rent elektronisk og hvor sikker skal de dataansvarlige være på, at den der giver samtykket er forælder eller værge eller overhovedet er over 16 år? Mange steder skal man f.eks. skrive ens fødselsdato ind eller afkrydse en boks som siger at man er over et bestemt år for at lave en bruger. Der er imidlertid ingen beviser for dette, hvormed det principielt kan være et barn, der siger at personen selv er over 16 år. Vil dette være gyldigt indhentet samtykke til behandling af barnets persondata? Dette vil blive behandlet yderligere under afsnittet ”indhentning af samtykke fra børn under 16 år”.

7 FACEBOOKS DATAPOLITIK OG VILKÅR

I dette afsnit vil Facebooks app blive gennemgået så den kan blive analyseret på baggrund af persondataforordningen i punktet "Forordningen i praksis". Der skal dog gøres opmærksom på, at der bliver taget udgangspunkt i de oplysninger der er blevet offentliggjort på nuværende tidspunkt, ét år før forordningens ikrafttræden. Resultatet heraf kan være, at der er nye privatlivsvilkår under udarbejdelse, som modsvar til forordningens nye krav.

7.1 DEN DATAANSVARLIGE

Når der er tale om et socialt medie, er det ikke udelukkende det sociale medie som er den dataansvarlige, men også brugerne af dette medie. Grunden hertil er, at det er brugerne selv der lægger persondata ud på mediet. Der skal i dette henseende ses på bl.a. forordningens art. 9, stk. 2 litra e) som siger, at art. 9, stk. 1 ikke gælder på personoplysninger, som den registrerede selv har offentliggjort. Hvis den registreredes Facebookprofil er offentlig, er det, som bliver lagt herpå (både af venner og af den registrerede selv), offentligt tilgængeligt.

> *"Hvis en person har en profil på Facebook som er så åben at det ikke kun er de brugere som er hans eller hendes 'venner' på Facebook, der har adgang til oplysningerne, men alle brugere på Facebook (…) er de oplysninger der ligger om personen på hans eller hendes Facebook, efter min opfattelse offentligt tilgængelige. Det gælder både de oplysninger personen selv har lagt ud på sin åbne Facebook, og de oplysninger andre har lagt om ham eller hende på den åbne Facebook. De oplysninger der ligger om personen på Facebook, kan på den baggrund som udgangspunkt frit behandles i persondatalovens forstand."*[25]

Der er dermed en sandsynlighed for, alt efter hvordan brugerens profil er sat op, at de data som brugerne lægger ud på Facebook er offentligt tilgængelig og dermed kan behandles frit af andre. Dette bliver imidlertid begrænset af forordningens artikel 5 om generelle principper for behandling, herunder formålsbegrænsning og rimelighed. Herudover kan art. 5, stk. 1, litra d) om rigtighed blive vanskelig, alt efter hvordan de pågældende data bliver brugt, da ikke alle oplysninger, der bliver sat ud på Facebook, er korrekte.

Det er dermed ikke Facebook der er den direkte dataansvarlig, men dette betyder imidlertid ikke, at Facebook er fritaget for at overholde forordningens regler i forbindelse med persondata. Grunden hertil er, at Facebook

[25] Folketingets ombudsmands beretning for 2011, sag nr. 2011 15-1.

må anses som værende databehandler i de tilfælde, hvor persondata bliver lagt ud på profilen. Dette kan ses i datatilsynets afgørelse af myndigheders brug af Facebook, hvor der i punkt 3 står:

"Hvis myndigheden får en indbakke på f.eks. Facebook, vil myndigheden efter Datatilsynets umiddelbare vurdering være dataansvarlig (…) Det er samtidig tilsynets umiddelbare vurdering, at Facebook vil være databehandler for myndigheden i forhold til personoplysningerne i indbakken, som jo er lagret hos Facebook, og ikke hos myndigheden selv."[26]

Det er dog vigtigt at understrege, at dette kun gælder de persondata som bliver offentliggjort på en tilstrækkelig offentlig profil, hvormed det ikke dækker de data, som Facebook derudover indhenter, hvor de her er dataansvarlige.[27] Dette bliver også sagt i Datatilsynets vejledning til persondataloven og sociale netværk.[28]

For persondata, som ikke er blevet offentliggjort af den registrerede eller dennes venner på Facebook, men derimod indhentet på anden måde, bl.a. gennem ikke offentlige profiler, genne profil indstillinger eller andre dataindsamlingsmetoder, er Facebook dataansvarlig for disse oplysninger, og skal dermed overholde de krav en dataansvarlig er underlagt i disse tilfælde.

7.2 FACEBOOKS INDSAMLING AF OPLYSNINGER

Facebook indsamler mange forskellige data gennem brug af deres service. Dette er bl.a. enhedsplacering, og når der er tale om apps som bliver brugt på en smartphone, som man stort set altid har på sig, vil dette betyde ens placering hele døgnet kan blive lagret, såfremt man er på Facebook. IP-adresse, betalingsoplysninger, netværk, billeder m.m bliver også lagret. Disse oplysninger indhentes delvis gennem den registreredes brug af Facebook, som f.eks. ved at lægge billeder ud på ens profil, tilføje venner, skrive opslag eller lignende. Der bliver imidlertid også indhentet persondata gennem tredjeparter som Facebook tilbyder en service i samarbejde med, eller hvis tredjeparten benytter sig af Facebook til deres eget brug. Dette kan f.eks. være spil som kan logges ind på gennem Facebook. I disse tilfælde får Facebook de oplysninger som appudgiveren oplyser til Facebook. Hvad der præcist ligger i dette, oplyser Facebook ikke, men som udgangspunkt kan der være tale om alle oplysninger som tredjeparten kommer i besiddelse af.

Facebook indhenter ikke kun persondata om den registrerede gennem hvad denne person lægger op på sin profil, men også data om den registreredes enheder, som f.eks. fysisk placering via GPS og IP-adresser, som EU-domstolen har sagt er persondata i sag C-582/14. Der bliver i denne dom fastlagt, at IP-adresser er

[26] Datatilsynet journalnummer 2013-321-0173.
[27] Dall, N. P., Langemark, J. og Langebæk, A. (2016), s. 213 – 217.
[28] https://www.datatilsynet.dk/borger/sociale-netvaerk/persondataloven-og-sociale-netvaerk/

personoplysninger, såfremt det er muligt at identificere den registrerede igennem disse. Det er tidligere blevet fastlagt at statiske IP-adresser er personoplysninger, jf. her C-70/10 præmis 51. I dom 582/14 bliver det imidlertid fastlagt, at også en dynamisk IP-adresse er en personoplysning, såfremt det er muligt for den dataansvarlige lovligt at kunne finde den registreredes identitet:

"… en dynamisk internetprotokoladresse, som en udbyder af online-medietjenester registrerer i forbindelse med en søgning foretaget af en person på en internetside (…) udgør en personoplysning (…) når udbyderen råder over lovlige hjælpemidler, der gør det muligt for denne at få identificeret den registrerede…"[29]

Alle former for IP-adresser er altså personoplysninger, såfremt det er muligt på lovligt vis at tilkomme sig disse data. Såfremt det ikke er muligt for den dataansvarlige at tilkomme sig disse data på en lovlig måde, udgør en dynamisk IP-adresse dermed ikke en personoplysning, jf. dommens præmis 38. Herudover bliver det også sagt i generaladvokatens udtalelse i præmis 68, at der også må tages en betragtning om ressourceomkostninger samt tid til at tilkomme sig denne yderlige viden – altså en rimelighedsbetragtning. Det skal dog her bemærkes, at Facebook automatisk kan identificere en person på IP-adressen. Med dette menes der, at det er muligt for Facebook at tilkoble IP-adresser til de registreredes profiler og gennem denne profilering se, hvem en given bruger er ved genkendelse af IP-adressen.

Grunden til at Facebook indhenter persondata omkring den registreredes placering og andre data, der som udgangspunkt ikke er relevant for Facebooks virke som en social netværksudbyder er, at disse data bliver brugt til at forbedre den registreredes brugeroplevelse. Dette kan f.eks. være i forbindelse med placering, hvor Facebook kan vise den registrerede annoncer, som på baggrund af placeringen har større sandsynlighed for at være relevant for den registrerede. Dette forbedrer dog ikke kun den registreredes brugeroplevelse, men også Facebooks ydelse til sponsorerne, hvormed Facebooks indkomst kan blive forøget. Dette kan f.eks. være gennem indhentning af data til spil, hvor Facebook ser tendenser i benyttelse af spil, hvormed reklamer for andre lignende spil kan blive vist for den registrerede. Dette kan f.eks. være gennem indhentning af data til spil, hvor Facebook ser tendenser i benyttelse af disse spil, hvormed reklamer for andre lignende spil kan blive vist for den registrerede for større chance for at den registrerede vil prøve det pågældende spil.

Som sagt bliver disse data indhentet til at forbedre den registreredes brugeroplevelser, hvilket Facebook forsøger at understrege i deres privatlivspolitik, hvilket kan ses i deres første linje om, hvordan de bruger de persondata de indsamler:

"Vi er dybt engagerede i at give folk interessante og personligt tilpassede oplevelser"[30]

[29] C-582/14, præmis 61 om første præjudicielle spørgsmål.
[30] Facebooks privatlivspolitik, *"Hvordan bruger vi oplysningerne?".*

I og med at konkurrencen inden for sociale netværk omhandler den bedste brugeroplevelse, er det meget forståeligt, at Facebook vil indsamle så mange persondata som muligt, for at forbedre brugeroplevelsen og dermed øge deres konkurrenceevne. Ud over dette kan man også se at Facebook forsøger at formidle deres privatlivspolitik på en positiv måde. Et problem der kan komme ved at formidle politikken på en sådan ens synet måde er, at det kan gå ud over gennemsigtigheden for den registrerede.

7.3 FACEBOOK OG DEN REGISTRERERE

Overordnet set giver Facebook en letforståelig kommunikation til den registrerede omkring deres behandling af persondata. Dette er både i forhold til hvilke informationer de indhenter, hvorfor persondataene indhentes samt hvordan den registrerede selv kan administrere og komme i besiddelse af disse data, som Facebook har om den registrerede. Denne vejledning til indhentning af Facebooks data er letforståelig og kort, som gør den gennemskuelig for den almindelige Facebookbruger. Derudover er vejledning også simpel at finde, da man skal gå ind på Facebooks privatlivspolitik, hvorefter denne er struktureret på en sådan måde, at den er nem at navigere rundt i, på grund af den opsætning som Facebook har lavet. Alt er inddelt i overskrifter og underoverskrifter. Trods denne letforståelige kommunikation til den registrerede, er der ikke noget der tyder på, at der er muligt at begrænse Facebooks indhentning af persondata, medmindre den registrerede helt sletter sin konto. Den vejledning Facebook har i forbindelse med begrænsning af oplysninger er i forhold til deling af data med andre, f.eks. begrænse et opslag til en bestemt gruppe venner. I forhold til begrænsning af deling af data til Facebook, er dette muligt i appens indstillinger, hvorfra man kan nægte eller give adgang til automatisk indhentning af data om kontakter og placering, men bliver ikke kommunikeret til brugeren gennem politikken.

De oplysninger man kan nedhente fra Facebook omhandler bl.a. venner (og deres kontaktinformation som f.eks. telefonnummer), beskeder sendt gennem Facebook og Messenger appen, enheder der har forbundet sig til den pågældende konto, herunder også deres IP-adresser m.m.

Perioden hvorpå persondata bliver gemt i Facebooks database er fra kontoens begyndelse indtil dens sletning. Dette vil altså sige, at den registreredes data, rent teoretisk, kan blive gemt for evigt (eller indtil Facebook lukker ned), hvis den registrerede ikke sletter sin konto. Sletteprocessen kan tage op til 90 dage, mens Facebook sletter data fra deres backupsystemer. Det er imidlertid ikke alle data der bliver sletter sammen med ens konto.

"Nogle af de aktiviteter, du foretager dig på Facebook, lagres ikke på din konto. En ven kan f.eks. måske stadig se beskeder fra dig, selv efter du har slettet din konto. Disse oplysninger findes stadig, efter du har slettet din konto."[31]

Facebook beholder altså data om den registrerede, selvom den registrerede har bedt om at få de pågældende data slettet. I forhold til den danske lovgivning anno 2017, kan dette anses som værende imod Datatilsynets forståelse af, hvad konsekvenserne er ved en sletning af en konto. Der bliver her sagt, at der ved sletning af bruger-profiler bør slettes enhver oplysning og indhold, som er blevet offentliggjort.[32] Ved sletning af alt offentligt tilgængeligt indhold og tilbagekaldelse af samtykke er der dermed ikke hjemmel til videre behandling af brugerens personoplysning. Problemet er her, at det er svært at forstå, hvad der præcist bliver lagt i ordene "nogle af de aktiviteter". Da denne formulering er meget overordnet, kan det være svært at gennemskue hvilke data den registrerede ikke længere har rådighed over, hvilket er et problem, da det ikke er til at vide, hvilke data Facebook beholder om den registrerede, efter denne har slettet sin konto. Dette bliver ikke et mindre problem af, at beskeder mellem to eller flere personer kan omhandle fortrolige eller følsomme data. Dette er specielt et problem i forhold til forordningens artikel 17, stk. 1, som omhandler "retten til at blive glemt". Især litra b) i dette tilfælde, som omhandler situationer, hvor den registrerede tilbagekalder samtykke til behandling af persondata, hvilket må være tilfældet ved anmodning om sletning af ens konto.

Et problem ved persondatasikkerheden er, at det kan hæmme brugeroplevelsen for den registrerede. Selvom Facebook "kun" er databehandler for nogle oplysninger, skal love og regler stadig overholdes, som medfører, at Facebook i realiteten bliver tildelt ansvar som ved en dataansvarlig. Der kan her nævnes, at det ifølge IT-sikkerhedskomiteen er sagt, at sociale netværk skal fremme god brug af billeder på tjenesten. Dette medfølger bl.a. at Facebook skal opfordre brugeren til, at indhente samtykke fra personer på billedet, før det bliver lagt ud, samt at Facebook som et eksempel kan forhindre billeder med tags i at blive offentliggjort indtil de taggede personer har accepteret tagget.[33] Hvis brugeren skal acceptere en masse juridiske dokumenter hver gang der bliver lagt et billede ud på profilen, eller skal vente flere dage før et billede bliver offentliggjort, vil dette hæmme brugernes oplevelse af tjenesten. Facebook har imidlertid foretaget nogle persondatasikrende initiativer i deres vilkår, hvor de bl.a. opfordrer til ikke at offentliggøre oplysninger af en vis karakter. Se nærmere om dette i afsnit 7.5 Facebooks vilkår.

[31] https://www.facebook.com/help/250563911970368?helpref=hc_global_nav
[32] https://www.datatilsynet.dk/erhverv/sociale-netvaerkstjenester/anbefalinger-til-beskyttelse-af-privatlivets-fred-i-sociale-netvaerkstjenester/
[33] https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Persondatalovspjece/It-sikkerhedskomiteens_kodeks_om_god_adfaerd_paa_online_sociale_netvaerkstj__FINAL.pdf

7.4 FACEBOOK SOM APP

Facebook har som sagt en app, som tilbyder det samme som deres hjemmeside, dog ikke chatmeddelelser, da dette kræver appen "Messenger". Appen er underlagt samme privatlivsvilkår og politikker som andre Facebook tjenester, som f.eks. deres hjemmeside. Dette kan ses i deres privatlivsvilkår:

"Med "Facebook" eller "Facebook-tjenester" mener vi de funktioner og tjenester, vi gør tilgængelige, herunder via (a) vores website på www.facebook.com og ethvert andet Facebook-brandet website eller fællesbrandede websites (herunder underdomæner, internationale versioner, widgets og mobilversioner)…"[34]

Mobilversioner må her tale om bl.a. deres app. En forskel på Hjemmesiden og appen er, at appen også indhenter data omkring placering og kontakter automatisk, medmindre man slår dette fra i indstillinger. Dette medfører også, at Facebook får oplysninger om registrerede gennem andre registrerede. For eksempel hvis en registreret ikke har angivet sit mobilnummer til Facebook, kan de stadig have dette i deres database gennem en ven til den pågældende, som har nummeret på sin telefon og samtidig har givet Facebook adgang til kontaktbogen. Ud over dette minder Facebooks hjemmeside og appen meget om hinanden i opsætning, muligheder for begrænsninger osv. Det er dog primært kun muligt at begrænse sig i forhold til om det man foretager sig på Facebook er offentligt eller privat, og dermed ikke i forhold til Facebooks indhentning af persondata. Derudover står det også i vilkårene, at den registrerede giver sit samtykke til at andre kan synkronisere deres enheder, med alt der er synligt for dem på Facebook om den pågældende registrerede.

"Du giver dit samtykke og alle de nødvendige rettigheder, for at brugerne skal kunne synkronisere (herunder via en applikation) deres enheder med enhver oplysning, der er synlig for dem på Facebook."[35]

Et eksempel herpå kan bl.a. være, hvis en registreret ændrer profilfoto, ændres dette for alle på andre platforme, som er tilkoblet Facebook, som f.eks. Spotify (hvis den registrerede er logget på via Facebook). Resultatet er dermed, at billedet bliver delt af Facebook. I forhold til appen kan dette også ske modsat, hvilket kan ses ved kontaktsynkronisering, hvor Facebook indhenter og gemmer oplysninger, som er lagret på telefonen omkring kontakterne. Dette kan være telefonnumre, kontaktoplysninger og andre oplysninger som er gemt, kontaktbillede m.m. Denne tjeneste er dog mulig at deaktivere i appens indstillinger.

Billede 2

[34] Facebooks vilkår, afsnit 17. *Definitioner*, punkt 1.
[35] Facebooks vilkår, afsnit 6. *Mobilenheder og andre enheder*, punkt 3.

Som det fremgår af billede 2, er det alle ens kontakter som Facebook får oplysninger omkring, også selvom man ikke tager kontakt til disse. Denne form for synkronisering medfølger, at der bliver givet navn og telefonnummer, muligvis e-mail og billede gennem denne synkronisering. Disse data bliver brugt til at give forslag til venner på Facebook. Dette gælder imidlertid ikke kun for den registrerede som lader disse data overføre til Facebooks servere. Det gælder også for andre brugere, hvor disse persondata kan være relevante.

Billede 2

> *"… Facebook vil bruge de oplysninger, som du har overført om dine kontakter, til at komme med venneforslag til dig og andre, og du vil hjælpe os med at yde bedre service for alle".*[36]

Dataene bliver dermed også brugt til at forbedre Facebooks service, uden at dette bliver specificeret yderligere med udgangspunkt i, at dette hjælper andre brugere med at finde venner, må dette dog forstås som en bred benyttelse af persondata, hvormed der menes, at de indhentede data fra telefonen hjælper Facebook med at forbedre deres services generelt og ikke udelukkende på tjenesten "find venner". Der bliver altså delt persondata med Facebook, uden at der er samtykke til denne deling mellem brugeren og Facebook. Derudover bliver de andre brugere heller ikke oplyst om, at deres persondata er indhentet i forbindelse med den pågældende synkronisering af kontakter.

7.5 FACEBOOKS VILKÅR

Den mest normale måde at oprette en Facebook konto på, er gennem deres hjemmeside, hvilket kan ses gennem deres guide til kontooprettelse, hvor det kun er hjemmesiden der bliver refereret til.[37] Her accepteres Facebooks vilkår uden aktiv handling, da man blot accepterer vilkårene, samt cookie- og datapolitik, ved at oprette kontoen, som ses på billede 3. Disse vilkår fortæller om det

Billede 3

[36] Facebooks app, *Administrer invitationer og importerede kontakter.*
[37] https://www.facebook.com/help/570785306433644/?helpref=hc_fnav

juridiske ved brug af Facebook, herunder også at der bliver givet samtykke til, at Facebook må videregive oplysninger til bl.a. sponsorer, som bliver sagt i vilkårenes afsnit 9, første punkt. Det er altså vigtigt for den registrerede at læse disse vilkår, for dermed at få indsigt i, hvad Facebook reelt gør med de data, som de indhenter og får oplyst. Derfor kan det være et problem, at der ikke er en decideret aktiv handling ved accept af vilkår og politikker. Hvis brugeren opretter sin konto gennem appen, er det dog anderledes. Den første side man skal forbi for at oprette sin konto her, er accept af vilkår og politikker. Der bliver dermed gjort en aktiv handling her, da man ved at fortsætte accepterer alt det, som denne side refererer til. På trods af, at man i appen skal skrive sin fødselsdato i forbindelse med kontoregistreringen, er der intet i forbindelse med indsamling af accept om, at man er over 16 år. Afsnit 13, punkt 5 i Facebooks vilkår siger dog, at man accepterer ikke at bruge Facebook, hvis man er under 13 år.

Vilkårene er præget af en tendens fra Facebooks side, til at skrive i eventuelle handlinger, som bl.a. kan ses i afsnit 1:

"… og hvordan vi indsamler og muligvis bruger dit indhold og dine oplysninger."[38]

Dette stemmer ikke overens med, hvad de senere skriver i vilkårenes afsnit 9 og afsnit 9 første punkt om videregivelse af persondata i forbindelse med annoncering på Facebook. Der bliver her sagt, at persondata bliver delt med bl.a. sponsorer. Klarheden i vilkårene bliver mindsket ved at benytte sig af eventualis-sætninger, når de reelt set gør det pågældende. I forhold til forordningens artikel 12, stk. 1, som siger, at sproget skal være klart når der bliver givet oplysninger til den registrerede, samt gennemsigtigheden af vilkårene vil det være bedre hvis vilkårene blev skrevet i et sprog, som fastlagde hvad Facebook gør, når der er tale om noget der bliver gjort og ikke "muligvis" bliver gjort.

I vilkårene beskriver Facebook som sagt deres juridiske grundlag. Herudover bliver der også opfordret i, hvordan man skal benytte sig af Facebook og passe på andres rettigheder, som IT-sikkerhedskomiteen har sagt er god adfærd i Danmark. F.eks. bliver der i vilkårenes afsnit 5 sagt, at Facebook forventer, at brugerne respekterer andre brugeres privatliv, hvor der også i punkt 9 bliver sagt, at der ikke må tagges brugere, hvis der ikke er blevet givet samtykke hertil. Derudover er det også muligt at fjerne tags på billeder, som andre har lagt op om én, og helt få billedet slettet, enten ved at bede personen der har lagt billedet ud om at slette det, eller tage kontakt til Facebook. Facebook siger dog selv, at selvom persondata bliver slettet fra profiler, kan de stadig være lagret på deres servere. Herudover er det muligt for Facebook at scanne billeder der bliver lagt ud, med hensigt på at identificerer personerne på billedet. Resultatet heraf er, at selvom brugeren ikke har tagget en person på et billede, er det muligt for Facebook at tilføje billedet til profileringen af den anden

[38] Facebooks vilkår, afsnit 1.

bruger, og derved også videregive dette til tredjeparter i anledning af bl.a. annoncer. Facebook skriver, at de ikke danner personskabeloner ud fra billeder hvor tagget er blevet fjernet, dette betyder imidlertid ikke, at billedet ikke fortsat er på Facebooks profilering af brugeren, selvom brugeren (ved at fjerne tagget) tilkendegiver, at han ikke ønsker at blive genkendt på det pågældende billede.[39]

[39] https://www.facebook.com/help/122175507864081?helpref=faq_content

8 FORORDNINGEN I PRAKSIS

På baggrund af de ovenstående afsnit, vil der her blive analyseret, hvordan Facebook forsøger at overholde EU's persondataret med fokus på indhentning af samtykke og om disse tiltag er nok til ikke at være i modstrid med persondataforordningen, som træder i kraft i maj 2018.

8.1 INDHENTNING AF SAMTYKKE

Reglerne om samtykke er hjemlet i forordningens artikel 6, stk. 1, litra a), hvis der er tale om almindelige oplysninger og artikel 9, stk. 2, litra a) ved særlige kategorier af personoplysninger. Herudover handler artikel 7 om, hvordan et samtykke indhentes. Et samtykke er kun gyldigt for de områder, som er blevet oplyst den registrerede. Hvis der er tale om indhentning af persondata, som ikke er blevet oplyst den registrerede, gælder artikel 6, stk. 4, hvor der her bl.a. bliver set på, om der er forbindelse mellem de indsamlede data og det formål der er blevet givet samtykke til.

Den måde som Facebooks app indhenter samtykke til behandling af persondata på, er ved at henvise til Facebooks datapolitik samt vilkår ved oprettelsen af Facebookkontoen. Ved at trykke "fortsæt", og starte kontooprettelsen, gives samtykket til databehandlingen. Spørgsmålet er her, om dette er en tilstrækkelig aktiv handling fra den registrerede, til at samtykket kan håndhæves. Der står i forordningens præambel i betragtning 32, at samtykke skal gives:

> *"… i form af en klar bekræftelse, der indebærer en frivillig, specifik, informeret og utvetydig viljetilkendegivelse (…) Dette kan f.eks. foregå ved at sætte kryds i et felt ved besøg på et websted (…) Tavshed, forudafkrydsede felter eller inaktivitet bør derfor ikke udgøre samtykke."*[40]

Da oprettelse af kontoen kræver, at den registrerede trykker "fortsæt" for at starte sin konto, og at det eneste der står på den pågældende side er, at vilkår og datapolitikken accepteres, må dette have samme effekt som ved afkrydsning af en boks. Grunden hertil er, at der i begge tilfælde bliver taget en aktiv handling i forbindelse med samtykkeerklæringen. På den anden side kan det også minde om et forudafkrydset felt, da det er muligt at gå videre, muligvis ved tilfældigvis at trykke fortsæt og dermed accepterer de pågældende vilkår uden at have lagt mærke til dem. Spørgsmålet er altså, om samtykket er afgivet "utvetydigt". Her skal der ses på, at der ikke må herske tvivl om, at den registrerede har afgivet sit samtykke til behandling af persondata. Problemet med afrydningsfelter som er afkrydset automatisk, frem for at den registrerede selv aktivt afkrydser feltet er, at samtykket i så fald bliver givet gennem en inaktiv handling, altså et passivt

[40] Forordning 2016/679 præambel, betragtning 32.

samtykke. Et passivt samtykke kan ikke bruges som et hjemmelsgrundlag, da det i så fald ikke er utvetydigt, hvorvidt den registrerede reelt set er klar over, hvad behandlingen omhandler. Gyldigt samtykke kræver altså en aktiv handling. Facebooks app kræver denne aktive handling i dets form af indhentning af samtykke i den forstand, at det ikke er muligt at fortsætte med oprettelsen af ens konto, før man fortsætter fra den pågældende side, som ses på billede 4. Knappen "kom i gang" kommer i dette tilfælde til at virke som en "accepter" knap, hvormed der er en aktiv handling i accept af Facebooks vilkår og datapolitik til behandling af persondata. Effekten må dermed anses at være den samme som hvis der var et felt, som man skulle krydse af ved kontoens oprettelse.[41]

Billede 4

I forhold til følsomme persondata, som artikel 9 omhandler, kommer spørgsmålet dog, om samtykket er blevet givet "udtrykkeligt". Hertil bliver der lagt vægt på, om den registrerede har fået alle de nødvendige oplysninger i hænde ved afgivelse af samtykket på en udtrykkelig måde.[42] Herudover også om disse oplysninger er nødvendige for Facebooks virke som et socialt netværk.

Facebook angiver, at der bliver indsamlet data, om den registrerede gennem det, der bliver lagt på Facebook af den registrerede selv, af andre brugere og af andre virksomheder, som samarbejder med Facebook, samt andre måder som de beskriver i deres datapolitik og vilkår. Dette vil sige, at hvis de pågældende persondata bliver delt af en selv eller andre, har Facebook meddelt dette i deres datapolitik. I forbindelse med hvad der bliver lagt på Facebook af brugeren selv, bliver de pågældende data offentlige, hvormed der som udgangspunkt ikke er et problem at behandle disse. Herudover er dette også nødvendigt at behandle oplysninger, som den registrerede selv lægger op på Facebook, for Facebooks funktion som et socialt medie. I forhold til hvis de pågældende data bliver delt af andre, kommer lovligheden her an på, hvorvidt der er samtykke hertil fra den part der deler persondata med Facebook. Grunden hertil er, at Facebook i disse tilfælde må opfattes som en databehandler, som ikke kan stilles bedre end den dataansvarlige. Hvis Facebook

[41] Dall, N. P., Langemark, J. og Langebæk, A. (2016), s. 56 – 58.
[42] Datatilsynet, journalnummer 2006-43-2010, punkt 2.4.

på den måde kommer i besiddelse af persondata, som den dataansvarlige ikke har hjemmel til at videregive, har Facebook dermed heller ingen hjemmel til at behandle de pågældende data.

I forhold til de følsomme data, som Facebook selv indhenter, skriver Facebook ikke direkte at de behandler følsomme data som f.eks. religion eller sundhedsoplysninger. De siger imidlertid, at de behandler de data, som den registrerede angiver ved brugen af deres tjenester. I grundlæggende oplysninger om brugeren på dennes Facebookprofil er det muligt at tilføje både religiøs overbevisning samt politiske synspunkter, som begge er omfattet af artikel 9 om følsomme oplysninger. Måden hvorpå disse er præsenteret må imidlertid være i overensstemmelse med, hvad Facebook siger i deres politik, nemlig at oplysningerne vil blive behandlet hvis brugeren selv angiver disse oplysninger. Derudover kan brugeren anses for at have offentliggjort de pågældende persondata. Hertil skal ses på, hvor mange venner den registrerede har, herunder hvor mange af disse "venner" ikke kan anses som værende venner, tilstrækkeligt tilknyttet til den registrerede. Profilens offentlige status samt deling med andre, herunder gennem venner og venners venner. Folketingets ombudsmand nævner i sin udtalelse herom, at der generelt skal ses på, hvor tilgængelig profilen er for andre.[43]

8.1.1 Delkonklusion af Indhentning af samtykke

Den måde Facebook indhenter persondata på, er overordnet set, på baggrund af ovenstående analyse, tilstrækkelig til behandling af persondata. Samtykket bliver indhentet korrekt, gennem en aktiv handling fra den registrerede. Da det ikke er muligt at oprette en Facebookkonto gennem appen, uden at acceptere Facebooks vilkår og datapolitik, som tydeligt bliver nævnt i denne forbindelse, må det dermed anes som værende afgivet på en aktiv og utvetydig måde. Dette skyldes at deres vilkår og datapolitik er opsat på en ordnet måde, hvormed det er let at finde de informationer man ønsker, bl.a. hvilke kategorier af oplysninger der bliver behandlet. Hertil skal det siges, at dette kun er tilstrækkeligt, fordi vilkårene og datapolitikken accepteres særskilt fra selve kontoopsættelsen. Dette er dog udelukkende omkring den tekniske indhentning af samtykket og om dette er indhentet tilstrækkelig klart, som gør at samtykket ikke er afgivet på en utvetydig måde. Hvorvidt Facebook overholder de juridiske og principielle krav i forordningen i anledning af samtykkets indhold, vil blive analyseret i de efterfølgende afsnit.

[43] Folketingets ombudsmands beretning, sag. 2011 15-1, s. 6.

8.2 INDHENTNING AF SAMTYKKE FRA BØRN UNDER 16 ÅR

Den måde Facebook sikrer sig at der ikke bliver behandlet oplysninger om børn, er ved at skrive i deres vilkår i afsnit 4, at den registrerede kun angiver rigtige oplysninger, samt angiver nogle forpligtelser over for den registrerede, herunder i punkt 5, at Facebook ikke vil blive brugt, hvis den registrerede er under 13 år. Det er dermed ikke muligt at lave en Facebookkonto medmindre man er over 13 år, selvom man får lov hertil af sin værge, da der ikke er noget i vilkårene om muligheden for, at man tilkendegiver, at man har sin værges samtykke til afgivelse af databehandlingssamtykke. Derudover skal der ved oprettelse af Facebookkontoen angives fødselsdato, som virker som en angivelse af, at man er over 13 år, som fungerer i forbindelse med at man kun angiver korrekte oplysninger efter afsnit 4, punkt 1 i Facebooks vilkår. Hertil hjælper Facebook også i deres hjælp side under "hvordan kan jeg anmelde et barn, som er under 13?", hvordan forældre kan hjælpe deres børn med at slette børnenes konti, uden en henvisning til at det er muligt at give samtykke til børnenes videre brug af Facebook. Under denne side skriver Facebook også, at aldersgrænsen kan være højere end 13 i nogle retskredse.

I forhold til at lægge ansvaret for at finde ud af, hvad aldersgrænsen er, for at børn kan anvende Facebook over på den registrerede, er der her ikke indhentet korrekt samtykke til behandling af barnet. Hvis lovgivningen f.eks. siger, at barnet skal være over 16 år, er der i dette tilfælde ikke givet et klart og velinformeret grundlag til indhentelsen af samtykket, som bunder i Facebooks ansvar for at overholde persondataforordningen efter artikel 5, stk. 2.

Ifølge en artikel fra 2012 hvori fire organisationer, herunder bl.a. Børns Vilkår og Red Barnet, siger, at der er mange børn under 13 år, specielt i Skandinavien, som benytter sig af Facebooks tjenester, på trods af Facebooks forbud imod dette.[44] Det må altså på denne baggrund konstateres, at Facebook ikke tager de fornødne tiltag til helt at forhindre børn under 13 år at lave en Facebook konto. Spørgsmålet er imidlertid hvorvidt Facebook, gennem brugerens accept af vilkår og datapolitik, har gjort hvad de kunne i forhold til at forhindre behandling af børn under 13 år. Ifølge forordningens præambel i betragtning 38 skal børn have særlig beskyttelse af deres personoplysninger, specielt når disse persondata bliver brugt med henblik på markedsføring eller til oprettelse af personligheds- eller brugerprofiler. Om der er tale om særlig beskyttelse af børns persondata, når samtykket til denne behandling udelukkende sker på baggrund af en forpligtelse i vilkårene om, at brugeren er over 13 år, er tvivlsom. Grunden hertil er, at der ligesom ved følsomme data er et særligt behov for at tage den registreredes behov i tankerne ved indsamlingen af persondata. Når der er tale om børn vil dette dermed kræve en ekstra hjemmel til denne behandling, som må ske på baggrund af en yderligere aktiv handling, som kan ske ved bl.a. afkrydsning i et afkrydsningsfelt. I forhold til appen ville dette,

[44] http://www.sikkerchat.dk/da-DK/For%C3%A6ldre/Aktuelt/Nyheder.aspx?Action=1&NewsId=133&PID=348

på baggrund af ovenstående analyse om indhentning af samtykke, også kunne blive gjort ved en eksplicit aktiv handling, altså hvis der på siden hvor man accepterer vilkår og datapolitik, også stod at brugeren tilkendegav at denne er over 13 år. Grunden til at det ikke må anses som værende tilstrækkeligt at indhente samtykke om, at den registrerede er over 13 år i vilkårene er, som betragtning 38 i forordningens præambel siger, at børn ofte er mindre bevidste om de medfølgende risici, konsekvenser og rettigheder ved persondatabehandling, hvorfor denne ekstra grad af sikkerhedsstillelse fra den dataansvarlige bør anses som god databehandlingsskik efter artikel 5, stk. 1, litra a).

Herudover må der også blive set på forskellen mellem tilkendegivelse og accept af at man er over 13 år. Facebook indhenter af samtykket gennem vilkårene, hvormed den registrerede på denne måde accepterer at være over 13 år. Der kan imidlertid i denne forbindelse være tale om vanhjemmel, da det ikke er muligt at indhente en accept om noget, som ikke omhandler den pågældende person på baggrund af personens alder. Med dette menes der, at vilkårene ikke gælder for børn under 13 år, da det ikke er muligt for Facebook at behandle disse børns data gennem deres accept af denne, herunder også reglen om urigtige oplysninger i Facebooks vilkår afsnit 4, pkt. 1, som her omhandler børnenes falske fødselsdato. Hvis Facebook i stedet får børnene til at tilkendegive at de er over 13 år, vil Facebook have bestræbt sig på at overholde persondataforordningen.

Det skal dog siges, at Datatilsynet har udtalt følgende:

"… Afgørelsen af, hvorvidt der foreligger et gyldigt samtykke, beror på en konkret vurdering i hver enkelt situation, hvor bl.a. barnets modenhed har betydning."[45]

Herudfra må det dermed forstås, at såfremt vilkår og datapolitik er forståelig og tilstrækkelig oplysende i forbindelse med barnets samtykke, må det accepteres, såfremt barnet kan anses som værende moden nok til at kunne forstå, hvad samtykket bliver givet til, trods at aldersgrænsen bliver "gemt" i vilkårene og datapolitikken.

[45] Datatilsynets journalnummer 2002-219-0139, *Vedrørende logning og opbevaring af kommunikationsdata på Jubii chatten,* afsnit 16.

8.2.1 Delkonklusion på indhentning af samtykke fra børn under 16 år

I forhold til forordningen vil dette sige, at samtykket kan være indhentet korrekt, hvis der er tale om et barn på 15 år, da barnets alder i dette tilfælde muligvis kan medføre, at barnets modenhed burde gøre denne i stand til at overskue konsekvenser ved at forfalske sin alder. Dette er med udgangspunkt i, at Facebooks vilkår ændres til børn under 16 år ved forordningens ikrafttræden. Hvis et barn på 8 år derimod gør det samme som den 15-årige, vil samtykket ikke være indhentet korrekt, da en 8-årig næppe vil være moden nok til at kunne overskue konsekvenserne af behandlingssamtykket.

I forhold til at indhente dette samtykke, når der er tale om børn, kan der dermed være en skillelinje i bedømmelsen af, om informationer er givet tilstrækkeligt oplyst ved Facebooks metode, som afgøres efter barnets alder og modenhed. Hvis Facebook dermed vil sikre sig et korrekt indhentet samtykke, skal de gøre det bedste de kan efter den teknologi der er dem til rådighed, uden uproportionelle høje udgifter. Dette kan f.eks. være ved at brugeren angiver at være over 13 år ved at trykke på "fortsæt" ved oprettelsen af kontoen, frem for at skrive dette i vilkårene. Forskellen her er, at barnet (og eventuelle værger som opretter kontoen til deres børn), udtrykkeligt ser, at der er en aldersgrænse for benyttelse af Facebooks tjenester og dermed er informeret tydeligt herom. Der er dermed gjort en ekstra beskyttelse i forhold til barnets sikkerhed.

8.3 OPLYSNINGSPLIGT

I Persondataforordningens artikel 13 og 14 er der fastsat nogle klare minimumskrav til, hvilke oplysninger den registrerede skal have at vide, når den dataansvarlige behandler persondata om denne. Disse oplysninger bliver i Facebooks tilfælde gjort gennem vilkår og datapolitik, som den registrerede accepterer ved oprettelse af dennes facebookkonto.

Artikel 13 omhandler persondata om den registrerede, som bliver indhentet fra den registrerede selv. Artiklens stk. 1 omhandler de basale informationer, som er et krav den dataansvarlige oplyser den registrerede om. Dette er bl.a. identitet og kontaktinformationer for den dataansvarlige, formålene med behandlingen og eventuelle modtagere, eller kategorier af modtagere, af de pågældende persondata. Facebook oplyser om kontaktinformationer for både Facebook Inc., som er Facebooks hovedsæde i USA, og Facebook Ireland, som er hovedsædet i EU. Dette gøres i deres persondatapolitik. I forhold til formålet med behandlingen af persondata bliver dette også gjort i datapolitikken. Formålet med behandlingen er, ifølge Facebook, at levere, forbedre og udvikle tjenester til den registrerede. Dette giver god mening i den forstand, at et socialt netværk kræver persondata for at kunne fungere som et socialt netværk. Uden Behandling af persondata ville det f.eks. ikke være muligt at finde sine venner på Facebook, da alt identificerbar information, herunder også et navn, udgør en persondata efter forordningens artikel 4, nr. 1). Hele

grundstenen for et socialt netværk ville dermed forsvinde, hvis det ikke var tilladt at behandle persondata i forhold til at levere deres tjenester. Ud over at behandle disse data i direkte forbindelse med de tjenester der bliver tilbudt den registrerede, bliver persondata også brugt til at finansiere Facebook. Dette gøres dog ved at videregive uidentificerbare oplysninger til kunder, herunder virksomheder der benytter sig af Facebook ved annoncering. Dette er også foreneligt med oplysninger om modtagere eller kategorier om modtagere. Her bliver der bl.a. nævnt, at Facebook deler oplysninger med andre virksomheder i Facebook koncernen, hvor der også bliver nævnt at Facebook har certificeret sig til at være omfattet af EU-US Privacy Shield, kunder og andre brugere, samt offentliggørelse af oplysninger, som den registrerede selv udgiver på en offentlig profil, offentlige rum eller lignende. Stk. 1 virker dermed som udgangspunkt at være overholdt på baggrund af, hvad der bliver oplyst den registrerede i datapolitikken.

Artikel 13, stk. 2 omhandler de mere beskyttende oplysningspligtige informationer. Dette er bl.a. tidsrum for opbevaring, retten til indsigt, berigtigelse og sletning af oplysninger, betydning og konsekvenser af profilering m.m. Facebook skriver i deres datapolitik, hvordan det er muligt at administrere sine Facebook data, herunder se hvilke data Facebook har, samt hvordan og hvornår persondata slettes fra Facebook. Facebook behandler data så længe det er nødvendigt i forbindelse med levering af tjenesterne. Spørgsmålet er imidlertid hvor længe "nødvendigt" er. Dette er imidlertid et spørgsmål i forhold til artikel 5 om generelle principper, hvor dette også vil blive analyseret yderligere.

I forbindelse med billeder giver Facebook information om denne behandling, bl.a. ved at indhente tilladelse til at behandle persondata, som brugeren selv lægger ud på Facebook. Der er imidlertid en dataform som Facebook ikke tilkendegiver i deres vilkår og datapolitik. Dette er elektronisk ansigtsgenkendelse, som må anses at være biometrisk data, som er følsom data efter artikel 9. Biometrisk data er fysiske eller adfærdsmæssige karakteristika, som gør indehaveren af disse data i stand til at identificere en person, som f.eks. fingeraftryk og DNA. Elektronisk ansigtsgenkendelse sker typisk ved, at teknologien ser på omkring 80 forskellige karakteristika ved ansigtet, herunder afstanden mellem øjne, kindben og hage.[46] Ifølge Politikken var Facebooks ansigtsgenkendelsesprogram i 2014 bedre end den teknologi, som stod myndigheder til rådighed, herunder bl.a. FBI i USA, med en nøjagtighed på 97,25%.[47] Denne form for behandling er følsom, da den let kan benyttes til overvågning og dermed er i strid med selve grundstenen i persondataforordningen, nemlig sikring af privatlivets fred. I forbindelse hermed, skriver Facebook i deres politik, at der kan foreslås tags, ved at sammenligne billeder med de oplysninger de har fra andre billeder, brugerne er blevet tagget i.

[46] http://www.tekno.dk/wp-content/uploads/2014/12/p10_Biometri_brug_af_biometriske_teknologier_i_det_danske_samfund.pdf, s. 52.
[47] http://politiken.dk/forbrugogliv/digitalt/art5549887/Sociale-medier-udleverer-store-m%C3%A6ngder-brugerdata-til-myndigheder

For at se hvilke oplysninger der her bliver beskrevet, skal man ind på Facebooks "hjælp"-side omkring foreslåede tags. Her bliver det sagt, at foreslåede tags sker ved at scanne og sammenligne billeder. Men da ansigtsgenkendelse ikke bliver nævnt i oplysningerne, som samtykket er baseret på og at der heller ikke er blevet henvist til "hjælp"-siden ved denne oplysning, er spørgsmålet om der er indhentet et gyldigt samtykke til behandling af disse biometriske data. Da der i datapolitikken kun blive sagt at der foreslås tagging på baggrund af at sammenligne "oplysninger" fra brugernes billeder, vil dette næppe kunne blive anset som værende klart, gennemsigtigt eller letforståeligt, som artikel 12, stk. 1 siger er et krav. Herudover er samtykket til denne behandling heller ikke udtrykkelig, som er kravet for persondata omhandlet af artikel 9. Dette er selvom det er nemt at finde ud af, nogle af de oplysninger Facebook refererer til i denne sammenhæng, ved at søge om det i Hjælp. Der er imidlertid tale om, at det i så tilfælde er nødvendigt for den registrerede at lave en aktiv søgning, udover hvad der bliver denne oplyst, for at finde de nødvendige oplysninger til at kunne afgive et velinformeret samtykke. Der vil her være tale om et stilsigende samtykke til behandling af biometrisk persondata i forbindelse med billeder, som efter forordning 2016/679 ikke er lovligt, grundet en generel samtykkeindhentning.[48] Til behandling af biometriske data, ville det dermed kræve, at Facebook klart og utvetydigt oplyste den registrerede om brugen af disse i enten deres vilkår eller persondatapolitik, som den registrerede accepterer gennem en aktiv handling, hvorefter der er samtykket er blevet givet til behandlingen.

Artikel 14 omhandler oplysningspligt ved persondata, som ikke er indhentet fra den registrerede, men fra andre steder. Sådanne data, som bliver lagt ud på Facebook af en anden bruger end den pågældende registrerede selv, bliver meddelt gennem notifikationer, medmindre disse manuelt er slået fra af den registrerede. Her får den registrerede dermed informationer om hvem der er den dataansvarlige og hvilke persondata der er tale om. Gennem denne notifikation bliver kravene om oplysningspligten overholdt i forbindelse med artikel 14, stk. 1. Dette er bl.a. identiteten på den dataansvarlige (her den bruger som lægger persondataene ud på Facebook), kontaktoplysninger (den dataansvarlige brugers konto bliver nævnt i notifikationen) og berørte kategorier af persondata.

Ligesom ved artikel 13 har artikel 14 et stk. 2, som omhandler de mere beskyttende regler for den registrerede. Selvom det er den anden bruger som reelt er dataansvarlig, må Facebook have påtaget sig de krav, som her er stillet. Grunden hertil er, at Facebook som socialt netværk, opfordrer deres brugere til at dele ting om sig selv og hinanden. Hertil bruger de personoplysninger til at forbedre deres tjenester, som forbedrer brugeroplevelsen af de registrerede, som herunder også gælder for minimering af de juridiske nødvendigheder, som f.eks. oplyse de registrerede om nødvendige oplysninger i forbindelse med

[48] Dall, N. P., Langemark, J. og Langebæk, A. (2016), s. 56 – 58.

databehandlingen. Det skal dog understreges, at Facebook ikke har det direkte ansvar som dataansvarlig for de oplysninger der bliver lagt ud på Facebook af brugerne, førend der bliver sagt indsigelse imod behandlingen af de offentliggjorte oplysninger, hvilket f.eks. kan ske gennem sletning af den registreredes facebookkonto.[49] Dette fritager dog ikke Facebook til at varetage brugernes persondata, hvorfor de også oplyser brugerne om behandlingen af deres persondata.[50] I forhold til artikel 14, stk. 2 er problemerne her de samme som i artikel 13, navligt lagringen af de behandlede persondata. Selvom persondata bliver offentliggjort, eller hvis det er en tilstrækkelig lukket profil udelukkende lagt på Facebook, bliver de pågældende persondata lagret på Facebooks server, uden at det er muligt for den registrerede at slette disse, medmindre kontoen slettes. Selv i dette tilfælde vil nogle data blive gemt på Facebooks server til videre behandling. Dette er også gældende hvis de pågældende persondata bliver slettet fra der offentlige Facebook på grund af indsigelser fra den registrerede. I dette tilfælde bliver Facebook dermed dataansvarlig for de persondata, som er blevet slettet fra Facebook, men lagret på deres server.

8.3.1 Delkonklusion af oplysningspligt

I forhold til almindelige oplysninger bliver der nævnt i Facebooks vilkår og datapolitik, hvilke kategorier der bliver behandlet, hvem de videresender oplysninger til, samt oplysning af de andre grupper af oplysningspligtige informationer. Det bliver dog mere gråt når der er tale om de følsomme data, da disse bliver gemt under den generelle indsamling af almindelige oplysninger. Følsomme persondata er underlagt en ekstra grad af sikkerhed for behandling, da der er større konsekvenser ved behandling af disse følsomme oplysninger end ved almindelige. Hertil kommer, at når der behandles følsomme oplysninger, kræver det, at samtykket er blevet givet udtrykkeligt hertil, hvilket er svært at se ud fra Facebooks vilkår og datapolitik. Oplysningspligten er dermed ikke opfyldt når der er tale om følsomme oplysninger. Dette er dog kun i forhold til persondata, som Facebook selv indhenter og ikke som brugeren selv offentliggør på sin profil, som f.eks. religiøs overbevisning i deres profilindstillinger. Hertil gælder, at Facebook har nævnt i deres vilkår og datapolitik, at data, som den registrerede selv sætter på sin profil, bliver behandlet.

Det bliver også nævnt i Facebooks datapolitik at fortrolige oplysninger, som f.eks. placering, bliver indsamlet og behandlet. Dette gøres eksplicit, hvormed oplysningen om denne form for behandling er imødekommet. Problemet ved Facebooks oplysninger til den registrerede, er dermed primært i forhold til de følsomme

[49] https://www.datatilsynet.dk/borger/sociale-netvaerk/persondataloven-og-sociale-netvaerk/
[50] https://www.datatilsynet.dk/erhverv/sociale-netvaerkstjenester/anbefalinger-til-beskyttelse-af-privatlivets-fred-i-sociale-netvaerkstjenester/

oplysninger, som også bør nævnes eksplicit i deres datapolitik eller vilkår, ligesom f.eks. placering er, hvormed behandlingen af de følsomme oplysninger klart og tydeligt bliver oplyst den registrerede.

8.4 DATAMINIMERING, PROPORTIONALITET OG ANDRE GENERELLE PRINCIPPER

Som nævnt tidligere er der nogle problematikker for Facebook i forhold til bl.a. proportionalitet, når det gælder lagring af data. Dette ses bl.a. ved lagringen af beskeder, trods en kontos sletning. Men også andre oplysninger bliver lagret i lange perioder, som f.eks. events som den registrerede har deltaget i og IP-adresser. Ligesom chat-beskeder kan disse være følsomme eller fortrolige, hvilket kræver en større grad af sikkerhed for den registrerede, som bl.a. mindre behandlingstid, hvilket også var tilfældet i sag 2007-42-0049 fra Datatilsynet (se nærmere herom efterfølgende). Det kan tænkes at et event den registrerede har deltaget i, har været af religiøs karakter på en lukket gruppe. Der må i sådanne tilfælde ske en fortolkning af sociale netværks aktiviteter. Grunden hertil er, at de data som den registrerede giver i anledning af de aktiviteter denne benytter på sociale netværk, ikke er underlagt persondataforordningen. Her står der:

"Denne forordning gælder ikke for en fysisk persons behandling af oplysninger under en rent personlig eller familiemæssig aktivitet… Personlige eller familiemæssige aktiviteter kan omfatte (…) sociale netværksaktiviteter og onlineaktiviteter, der udøves som led i sådanne aktiviteter."[51]

Der skal dermed ses på, hvornår en aktivitet ikke længere kan anses som værende i forbindelse med den tjeneste, som Facebook leverer. Herudover skal det dog også nævnes, at forordningen stadig gælder for de informationer, som Facebook indhenter og behandler i forbindelse med deres administration af deres tjenester.[52] Herudover er lagringen af IP-adresser fortrolige, da dette kan benyttes til overvågning af de registrerede. Det er let på baggrund af en IP-adresse at finde frem til individets placering. F.eks. kan hjemmesiden https://www.iplocation.net/ findes gennem en simpel Google søgning, hvorefter det på baggrund af de lagrede IP-adresser, er muligt at finde frem til placeringen det pågældende tidspunkt. F.eks. kan jeg se, at jeg d. 7. november 2011 kl. 09:05 var på Aalborg Universitets internet, via de lagrede data Facebook har om mig.

Som det kan ses af bilag 2, bliver samtaler lagret i minimum op til 7 år.[53] Ved benyttelse af Facebook appen bliver beskeder sendt gennem appen "Messenger", som også ejes af Facebook og refererer til Facebooks vilkår og datapolitik ved installation. Selvom der er tale om to forskellige apps, bliver de her set som værende den sammen, hvormed det er relevant at medtage i specialet. Grunden hertil er, at begge apps ejes og

[51] Forordning 2016/679 Præambel, betragtning 18.
[52] https://www.datatilsynet.dk/borger/sociale-netvaerk/persondataloven-og-sociale-netvaerk/
[53] Dette speciale skrives i 2017 og samtalen i bilag 2 er fra 2010.

kontrolleres af Facebook, samt det faktum, at Facebook appen viderestiller til Messenger, når brugeren ønsker at sende en chat-besked. Messenger er dermed ikke en selvstændig app, men en tillægsapp til fuldførelse af Facebookappen.

Som sagt vil en samtale der strækker sig 7 år tilbage, som muligvis ikke er med en person som den registrerede stadig er i kontakt med, kunne blive anset som værende "nødvendig"? I sag 2002-219-0139 fra Datatilsynet blev det sagt, at lagring af chatbeskeder var i overensstemmelse med det indhentede samtykke, herunder også §5 i persondataloven om god databehandlingsskik. Der blev her lagt vægt på, at formålet til lagringen var at skabe en sikker chat for brugerne samt at kunne hjælpe myndighederne med udlevering af oplysninger i tilfælde af mistanke om lovovertrædelse ved benyttelse af chatten. Dette bliver også sagt i Facebooks datapolitik. I afgørelse 2007-42-0049 blev det imidlertid sagt, at ved lagring af kommunikation skulle slettes efter 6 måneder og 3 måneder ved 1-1 kommunikation. Dette er dog i forhold til børn, hvorfor slettefristen er mindre end det ene år, der blev afsagt i sag 2002-219-0139. Ved sammenholdelse af disse må det dog være tvivlsomt, om 7 år eller mere vil være proportionelt i forhold til Datatilsynets forståelse af dette i Persondatalovens forstand. Grunden hertil er, at forordningen er mere skærpende end Direktiv 95/46/EF, herunder også Persondataloven. Herudover er 7 år også en væsentlig forlængelse af 6 måneder og et år, som blev konstateret var i overensstemmelse med Persondataloven i sagerne 2002-219-0139 og 2007-42-0049. Hermed menes der, at trods den "særlige beskyttelse" af børn under 16 år i forordningens forstand, må 6 måneder i forhold til 7 år forstås som værende væsentligt længere og dermed mere vidtgående end den særlige beskyttelse der gælder ved behandling af børns persondata. Hvor lang den reelle beskyttelse er for behandling af voksnes kommunikation må dermed som udgangspunkt ligge på omkring ét år, som Datatilsynet godkender i forbindelse med Jubiis logning af chatbeskeder.

I Jubiis tilfælde i sag 2002-219-0136, blev det anset som værende proportionelt at lagre samtaler i et år i forhold til eventuelle samfundsinteresser. Hertil kan præamblens betragtning 24 i forlængelse af forordningens artikel 2, stk. 2, litra b) sige, at hvis der foretages behandling af personoplysninger vedrørende registreredes adfærd, gælder forordningen også for dataansvarlige i udlandet. Der er altså en særlig beskyttelse af registrerede, når det gælder overvågning. Hertil er også grundstenen i forordningen, nemlig retten til privatlivets fred, som også medfører en ekstra beskyttelse af individerne, når der er tale om overvågning. På denne baggrund må behandling af mulige fortrolige og følsomme persondata i forbindelse med lagring af meddelelser, placering og andre lignende data, ikke kunne være proportionelt med målet, som er forbedring af Facebooks tjenester eller i forhold til samfundets interesse. I forbindelse med behandling af persondata i samfundets interesse, behøves der ikke samtykke til det, da dette er en hjemmel i sig selv (jf. art. 6, stk. 1, litra e) og art. 9, stk. 2, litra g)).

Et andet problem i forhold til de lagrede data er, at Facebook tilsyneladende gemmer disse persondata, efter en konto bliver slettet. Hvis den registrerede sletter sin konto, må dette være ensbetydende med tilbagetrækning af dennes samtykke, hvormed det ikke længere er muligt at behandle dennes personoplysninger, jf. forordning 2016/679 art. 17, stk. 1, litra b). Når samtykket tilbagekaldes fjernes hjemlen til behandlingen af personoplysninger efter art. 6, stk. 1 litra a) og art. 9, stk. 2, litra a). Såfremt der ikke er en anden hjemmel til behandlingen af personoplysningerne, er selve behandlingen i strid med art. 5, stk. 1, litra a) om lovlighed ved persondatabehandling. Dette vil dermed sige, at behandlingen af disse data er i strid med persondataforordningen, såfremt der ikke er en alternativ hjemmel, som f.eks. behandling i samfundets interesse. Der er altså her tale om det samme, som ved lagring af persondata i lange perioder, nemlig proportionalitet af den pågældende behandling.

En forlængelse af dette er dataminimering. Dette omhandler en minimering af den behandlede data, hvortil der skal ses på, om dataene er *"… tilstrækkelig, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles".*[54] I forhold til lagring af meddelelser og billeder er dette, at de personer som eventuelt er forbundet til de pågældende data, dette kan være modparten i en chat-samtale, fortsat kan se, hvad den pågældende har foretaget sig på det sociale netværk. Lagringen må således i dette tilfælde kunne ses som værende både tilstrækkelig og relevant for et socialt netværks virke. Om det derimod er nødvendigt er en anden sag. Når der er tale om en nødvendighed i forhold til Facebook, må der ses på, om Facebook fortsat kan fungere som et socialt netværk, hvis den pågældende behandling stoppes. Hvis lagringen af placering stoppes, vil dette tvivlsomt hæmme Facebooks funktion af et socialt medie, da dette ikke bliver offentliggjort til andre personer, medmindre den registrerede selv tilføjer dette til et opslag. Når kontoen dermed slettes, eller der er gået tilstrækkeligt lang tid efter indhentningen af placeringen, er der intet behov for fortsat behandling af disse data. Hertil skal det siges, at IP-adressen til dels indhentes og lagres af Facebook, af sikkerhedsmæssige grunde for den registrerede, f.eks. i tilfælde af hacking, hvorfor behandling efter samtykkets tilbagekaldes kan begrundes i en begrænset og proportionel periode. "Nødvendigheds" kriteriet bliver også nævnt i art. 5, stk. 1, litra e) om opbevaringsbegrænsning, som også siger at persondata ikke må behandles i en længere tidsperiode end det er nødvendigt til de formål, som de er blevet indhentet til. Formålet med dataene er, at brugeren kan benytte sig af Facebooks tjenester, hvorved det primære formål hertil fjernes når kontoen slettes.

I forbindelse med nødvendighed og dataminimering, kan der også blive set på, om det overhovedet er nødvendigt for Facebook at indsamle følsomme persondata, som er omhandlet i artikel 9 i forordningen. Her skal der lægges vægt på, at Facebook ikke spørger om følsomme oplysninger ved oprettelse af brugerens

[54] Forordning 2016/679, art. 5, stk. 1, litra c).

konto. De persondata der bliver spurgt om, er udelukkende navn, e-mail eller telefonnummer samt fødselsdato. Profilen kan senere blive ændret, sådan at den indeholder følsomme data som f.eks. religionstilknytninger. Det er dog op til den registrerede selv at tilføje disse persondata efter egen vilje, hvormed det på denne baggrund må forstås på en sådan måde, at den registrerede hermed gerne vil vise andre sin religiøse overbevisning og få henvisninger fra eventuelle tjenester fra Facebook, knyttende sig til dette, som f.eks. annoncer, forslag til venner eller lignende. Oplysningerne bliver altså gjort offentlige af den registrerede selv, såfremt profilen er tilstrækkelig åben. Dette vil dermed også sige, at i sin funktion af at være et socialt netværk, vil behandlingen af følsomme data være nødvendig, såfremt der er tale om persondata, som den registrerede selv offentliggør eller frivilligt sætter på sin profil.

Såfremt der er tale om følsomme data, som den registrerede ikke selv tilsætter profilen, men automatisk sker, kan resultatet være anderledes. F.eks. i forbindelse med automatisk ansigtsgenkendelse kan det siges, at denne funktion er nødvendig for funktionen "foreslåede tags", men er denne funktion en nødvendighed, for at Facebook kan fungere som et socialt netværk? Funktionen forøger brugeroplevelsen ved uploading af billeder, men har ikke en stor funktion i Facebook som en helhed. Derfor skal der ses på, om behandlingen er rimelig i forhold til den registreredes interesser. Rimelighedsvurderingen har hjemmel i artikel 5, stk. 1, litra a) og bliver nævnt i forordningens præambel i betragtning 39, hvor der står:

"Enhver behandling af personoplysninger bør være lovlig og rimelig. 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 personoplysningerne behandles eller vil behandles…"[55]

Da ansigtsgenkendelse kun bliver nævnt på Facebooks hjælp-side, er gennemsigtighedsprincippet næppe overholdt i dette tilfælde. Rimeligheden af behandlingen af de biometriske data, som et ansigtsgenkendelsesprogram benytter, er dermed heller ikke overholdt, da der i dette tilfælde er tale om uinformeret indhentning af følsomme persondata.

[55] Forordning 2016/679 præambel, betragtning 39.

8.4.1 Delkonklusion af de generelle principper

Facebooks har dermed nogle problemer ved overholdensen af de generelle principper i artikel 5. Dette skyldes Facebooks lange behandlingstid af deres informationer, samt et samtykke, som ikke er blevet specificeret nok i forhold til de formål, Facebook ønsker de indhentede data skal hjælpe til at opnå. Resultatet heraf er, at samtykket bliver givet på et generelt grundlag, hvormed nogle af de persondata, som Facebook indhenter, ikke bliver indhentet korrekt. Dette kan f.eks. være biometriske data i forbindelse med deres ansigtsgenkendelsesprogram. Problemet ligger imidlertid i stor stil i princippet om opbevaringsbegrænsning, som har hjemmel i forordningens artikel 5, stk. 1, litra e). Facebook gemmer persondata i en lang årrække tilbage (minimum 7 år), som næppe er relevante i forhold til den registrerede. Der mangler altså en behandlingsfrist fra Facebook, hvor persondata bliver slettet efter en bestemt periode, medmindre der er en særlig grund til en fortsat behandling. Dette gælder for alle oplysninger Facebook indsamler, herunder også eventdeltagelse og interesseoplysninger, som f.eks. hvilke opslag den registrerede har trykket på for at se. En begrænsning af behandling vil imidlertid gå ud over Facebooks tjeneste "tidslinje". Dette kan imidlertid løses, ved at Facebook gør det muligt for den registrerede, selv at forlænge behandlingsperioden i indstillinger. Hertil skal det dog siges, at der i så fald vil være krav til, at behandlingstiden skulle ændres manuelt og ikke automatisk er på den længst mulige behandlingsperiode.

Derudover indhenter Facebook også rigtig mange oplysninger, som muligvis ikke er nødvendige for deres virke som socialt netværk, og dermed vil kunne være i strid med artikel 5, stk. 1, litra c) om dataminimering. De informationer der bliver behandlet er, ifølge Facebooks vilkår og datapolitik, til forbedringer af deres tjenester. Et eksempel herpå kan være, hvis den registrerede har undladt at angive sit telefonnummer, men benytter sig af appen. Ifølge Facebooks datapolitik om enhedsoplysninger, indsamler Facebook forbindelsesoplysninger, herunder bl.a. telefonnummer. I og med det er muligt for den registrerede selv at indtaste sit telefonnummer, må dette fortolkes som en information, som ikke er nødvendig for Facebooks tjenester, men blot vil forbedre dem. Når de samtidig selv indhenter denne oplysning, må der dermed være tale om en behandling, som ikke er nødvendig for deres virke og det formål, som der er blevet den registrerede oplyst.

Problematikken for Facebook i forhold til artikel 5, er i høj grad baseret i artiklens stk. 2 om ansvarlighed. Det er op til Facebook at kunne påvise at stk. 1 (de generelle principper) er overholdt. Når der dermed er tale om uproportionelle behandlingsperioder, indhentning af persondata uden et angivet formål hermed eller bare generelt indhentning af persondata, uden behov for den pågældende behandling, vil behandlingen af persondataene være imod stk. 2. Det er Facebook der skal kunne bevise, at behandlingen sker i overensstemmelse med artikel 5, stk. 1. Til at bevise dette, er det ikke nok med at indhente et samtykke fra

den registrerede til den pågældende behandling, da de generelle principper begrænser behandlingsområdet for den dataansvarlige, til det der er nødvendigt for dennes virke.

8.5 GENNEMSIGTIGHED

Facebook skriver i deres datapolitik, at de sammenligner billeder med de oplysninger Facebook har om den registrerede, til det formål at forbedre brugeroplevelsen gennem bl.a. genveje og forslag. Ved blot at skrive "de oplysninger", er det svært for den registrerede at vide hvilke oplysninger der her er tale om. Dette vil være et problem i forhold til gennemsigtighed, som er omtalt i art. 5, stk. 1, litra a) og art. 12, stk. 1. I forordningens præambel betragtning 39 står der:

"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."[56]

Dette kan sammenholdes med forordningens art. 9, stk. 2, litra a) som siger, at følsomme data må behandles, såfremt den registrerede har givet et udtrykkeligt samtykke til behandlingen af et eller flere specifikke formål. På baggrund af disse to artikler, kan det dermed siges, at når der er tale om følsomme data, skal samtykket som er indhentet til denne behandling, være blevet givet af den registrerede på et oplyst og gennemsigtigt grundlag. Når der blot står "de oplysninger" er det svært at gennemskue, hvilke oplysninger dette er, medmindre den registrerede har en teknisk viden, som gør den registrerede i stand til at vide, at der i forhold til oplysninger indsamlet af billeder, kan være tale om ansigtsgenkendelse. Da der ikke bliver nævnt noget i forhold til indsamlingen af de pågældende biometriske data i dette tilfælde, ud over "de oplysninger" vil det være svært at anse dette som gennemsigtigt, da det kræver en speciel viden fra den registrerede eller en yderligere aktiv informationssøgning fra den registrerede, for at finde ud af, hvilke oplysninger der her bl.a. er tale om. Hvis Facebook derimod blot refererede til deres hjælp-side om tagging, hvor de nævner ansigtsgenkendelse, ville gennemsigtigheden stige, da Facebook i så tilfælde ville have givet de nødvendige informationer omkring deres behandling tilgængelige for den registrerede, i anledning af at samtykket blev indhentet.

Det skal altså være muligt for den registrerede at overskue de informationer, der blive denne tildelt. Såfremt sproget ikke er klart og letforståeligt bliver informeret omkring databehandlingen samt formålet med denne behandling, anses oplysningen af informationen ikke gennemskueligt.

En af grundende til, at det er op til Facebook at være sikker på, at samtykket er indhentet korrekt med en tilstrækkelig gennemsigtighed er, at art. 5, stk. 2 siger, at det er Facebooks ansvar, at art. 5, stk. 1, om bl.a.

[56] Forordning 2016/679 præambel, betragtning 39.

lovlighed og gennemsigtighed, bliver overholdt. Dette vil også sige, at hvis Facebook indhenter persondata, som de reelt har samtykke til, men på grundlag af en svær forståelig tekst, vil behandlingen kunne være i strid med forordningen. Grunden hertil er, at beskyttelsen af den registreredes rettigheder spiller en central rolle i forordningen, da det omhandler beskyttelsen af dennes privatliv, hvorfor det ikke skal være muligt for de dataansvarlige at gemme sig bag indviklede tekster, som giver dem et generelt samtykke til databehandling, hvilket også ses i forhold til dataminimering.[57]

Et princip som er underlagt gennemsigtighedsprincippet, er klarhed. Med dette menes der, at oplysninger der bliver informeret til den registrerede, skal være klart formuleret. Når Facebook i deres vilkår ét sted skriver, at de muligvis bruger indhold og oplysninger, hvor de senere skriver at oplysningerne bliver brugt i forbindelse med forbedringer af brugeroplevelsen, herunder også specificere annoncer. Samme gælder at de skriver, at persondata muligvis bliver delt i forbindelse med ransagningskendelser, hvor faktum er, at hvis den offentlige myndighed har en ransagningskendelse efter retsplejelovens kapitel 73, til indhentning af persondata i forbindelse med beskyttelse af samfundets interesser, skal disse oplysninger udleveres af Facebook. Klarheden af sproget bliver mindsket, når det bliver skrevet på en måde, at selv en behandling, som bliver foretaget, bliver skrevet som en mulig hændelse. Hvis sådanne behandlinger blev beskrevet som faktiske behandlinger, frem for mulige, ville klarheden, og dermed også gennemsigtigheden, blive forøget, hvormed samtykket ville blive indhentet på et bedre og mere sikkert grundlag. Grunden til at klarheden er et vigtigt princip i forbindelse med gennemsigtigheden er, at hvis de oplysninger den registrerede bliver informeret omkring ikke er gennemsigtig og klar, kan hele samtykket være ugyldigt, hvis konsekvenserne af samtykket er for store i forhold til udarbejdelsen af samtykket.

Definitionen af et samtykke er:

"… enhver frivillig, specifik, informeret og utvetydig viljeserklæring fra den registrerede…"[58]

Hvis sproget ikke er klart og gennemsigtigt for den registrerede, er der altså ikke tale om, at informationen er blevet givet i overensstemmelse med forordningens krav. Når Facebook skriver at de "muligvis" behandler persondata i forbindelse med specifikke formål, når disse persondata faktisk bliver behandlet, er dette ikke utvetydigt. Det samme gælder ved behandling af biometriske data i forbindelse med datagenkendelsesteknologier. I og med at der ikke bliver informeret om dette ved indsamlingen af samtykket, er der ikke tale om et gyldigt samtykke til dette specifikke formål. Dette er til trods for, at Facebook nævner det andetsteds end vilkår og datapolitik. Problemet er imidlertid, at samtykket ikke er

[57] Dall, N. P., Langemark, J. og Langebæk, A. (2016), s. 51 - 52 og Blume, P. (2016), s. 69 – 70.
[58] Forordning 2016/679 artikel 4, nr. 11).

blevet givet på baggrund af disse ekstra informationssteder. Dette kan også udledes af forordningens præambel i betragtning 32, hvor der står, at viljeserklæringen (samtykket) indhentes på en sådan måde, at den registrerede accepter behandlingen af dennes persondata. Hvis samtykket dermed ikke er givet informeret og utvetydigt ved indsamlingen af det, er der dermed ikke tale om et gyldigt samtykke. Hvis samtykket ikke er gyldigt må behandlingen ikke finde sted, medmindre der er en anden hjemmel til den pågældende databehandling.

Det er altså vigtigt for dataansvarlige, så som Facebook, at indhente et korrekt samtykke til behandlingen af de persondata, de har behov for til et givent formål. Trods Facebooks datapolitik, som er delt ind i forskellige og overskuelig grupperinger, er dette ikke nødvendigvis tilstrækkeligt til at gøre datapolitikken gennemsigtig. Selve sproget der bliver benyttet i teksten skal være klart og letforståeligt, specielt når der er tale om følsomme oplysninger. Det er ikke muligt for den dataansvarlige at gemme sig bag et samtykke, som den registrerede, ikke har mulighed for at gennemskue.

Et andet eksempel på at der kan være nogle problemer med gennemsigtigheden af Facebooks oplysninger, er i forhold til oplysning omkring kommercielle formål. I IT-sikkerhedskomiteens kodeks om god adfærd på sociale netværk, står der i 3. punkt,[59] at tjenesten (her Facebook) skal oplyse brugen på en utvetydig, tydelig og klar måde, at dennes personoplysninger vil eller kan blive brugt til kommercielt formål. Dette gør Facebook også i deres vilkår i afsnit 9, hvor de klart og tydeligt skriver, at den registreredes oplysninger, så som navn, profilbillede og andet indehold, vil blive brugt til kommercielle formål. Dette gøres bl.a. i forhold til at forbedre annoncørernes brug af tjenesten. I Facebooks vilkår står der imidlertid, at Facebook deler persondata med tredjepartspartnere, så som annonceringstjenester. Disse data kan imidlertid *ikke* bruges til personlig identifikation. Når Facebook dermed i deres vilkårs afsnit 9 skriver, at de kan bruge både navn og profilbilleder til kommercielle formål, herunder til annoncering, men i deres datapolitik skriver, at disse oplysninger ikke er identificerende, er det tvetydigt hvad de reelt gør. Der står i Facebooks vilkår:

"Det betyder, at du f.eks. tillader en virksomhed eller en anden enhed at betale os for at vise dit navn og/eller profilbillede eller dine oplysninger uden betaling til dig."[60]

Der bliver dermed sagt direkte, at Facebook i disse tilfælde kan modtage penge fra tredjeparts virksomheder for den registreredes identificerende personoplysninger i forbindelse med kommercielle situationer, hvilket de i datapolitikken har skrevet, udelukkende er ikke identificerbare personoplysninger. I forhold til IT-sikkerhedskomiteens adfærdskodeks ville dette dermed ikke være optimalt. Herudover bliver

[59] https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Persondatalovspjece/It-sikkerhedskomiteens_kodeks_om_god_adfaerd_paa_online_sociale_netvaerkstj__FINAL.pdf
[60] Facebooks vilkår afsnit 9, punkt 1.

gennemsigtigheden af deres vilkår og datapolitik også mindsket, når de på denne måde er modsigende og tvetydige.

8.5.1 Delkonklusion af gennemsigtighed

På trods af, at både Facebooks vilkår og deres datapolitik er opbygget på en letforståelig måde, hvorpå den registrerede på en nem måde kan finde de oplysninger han leder efter, er vilkårene og datapolitikken ikke gennemsigtig. Grunden hertil er, at Facebook ikke udtrykkeligt fortæller, hvad de indhenter samtykke om i alle tilfælde. Dette er f.eks. ved billeder, hvor ansigtsgenkendelse bliver gemt under oplysning om, at behandling af "oplysninger" sker. Et andet eksempel er, at Facebook giver modstridende oplysninger, omkring bl.a. videregivelse af persondata i forbindelse med kommercielle formål. Selv hvis der i denne situation menes to forskellige ting, vil formuleringen gøre det utvetydigt for den registrerede, hvormed gennemsigtigheden stadig ikke er optimal.

Problemet ved at de oplysninger, som den dataansvarlige giver den registrerede ved indhentning af samtykke, ikke er gennemsigtige er, at samtykke kræver at være velinformeret, for at være et gyldigt samtykke. Når gennemsigtigheden dermed ikke er tilstrækkelig til at kunne sige, at den registrerede har afgivet sit samtykke til den pågældende behandling på et velinformeret grundlag, vil samtykket ikke være gyldigt og behandlingen for de pågældende persondata må ikke finde sted, medmindre der er hjemmel til dette andetsteds i forordningen. Det er dermed yderst vigtigt, at den dataansvarlige formulerer sine vilkår og datapolitik på en gennemsigtig måde, så samtykket bliver indhentet korrekt. Hertil skal der ses på de oplysninger, som der er krav til at den dataansvarlige informerer den registrerede om i artikel 13 og 14 om oplysningspligt. Hvis disse oplysninger ikke er gennemsigtige, er den registrerede ikke blevet oplyst på en korrekt måde. Gennemsigtigheden er til dels en forlængelse af oplysningspligten, hvorfor der er hjemmel til gennemsigtighed to steder i forordningen, nemlig i artikel 5, stk. 1, litra a) og artikel 12, stk. 1. Artikel 12, stk. 1 handler specifikt om oplysninger, der henvender sig til den registrerede, herunder bl.a. artiklerne 13 og 14 om oplysningspligt. Artikel 5, stk. 1, litra a) handler om at de pågældende persondata behandles på en gennemsigtig måde, som ikke udelukkende handler om gennemsigtigheden i de oplyste informationer, men generelt om databehandling.

9 KONKLUSION

På baggrund af ovenstående analyser, kan det dermed konkluderes, at Facebook ikke overholder den nye forordning ved indsamling af samtykke til behandling af persondata på nuværende tidspunkt. Det skal hertil siges, at Facebooks vilkår og datapolitik sandsynligvis bliver ændret i forbindelse med forordningens ikrafttræden i 2018. Ovenstående analyse fremstiller imidlertid nogle af de problemer i forbindelse med indhentningen af samtykket, som Facebook skal have ændret ved denne opdatering af deres vilkår og datapolitik.

Selvom der er problemer i forhold til overholdelsen af forordningen, er der også problemstillinger, som er i overensstemmelse hermed. Dette er bl.a. den tekniske indhentning af samtykket. Ved udelukkende at se på Facebooks app, sker der en aktiv accept af Facebooks vilkår og datapolitik, hvormed den registrerede bliver nødsaget til at foretage sig en aktiv handling til afgivelse af sit samtykke, hvormed Facebook har indhentet dette på en korrekt måde. Problemerne for Facebooks app kommer primært i forbindelse med de informationer som Facebook informerer den registrerede om. I forhold til information om, hvem der er dataansvarlig for data er informationen tilstrækkelig, hvor Facebook i deres vilkår bl.a. skriver, at offentlige oplysninger kan blive brugt af alle.[61] I dette tilfælde kunne Facebook muligvis være mere specifikke i deres formidling af denne oplysning, da de oplysninger den registrerede lægger ud på Facebook kan blive betragtet som offentlig i dansk optik, selvom disse bliver delt inden for en begrænset gruppe, såfremt denne gruppe er tilstrækkelig stor.[62] Informationen er imidlertid blevet givet af Facebook, hvormed den registrerede er blevet informeret herom. Det der ligger heri er, at det er den registrerede selv som er dataansvarlig for de oplysninger, denne lægger ud på Facebook. Hertil hjælper Facebook også de registrerede til at slette ting, som andre lægger op om dem, hvilket bliver linket i datapolitikkens introduktion. Facebook hjælper dermed deres brugere i forhold til persondata, som de er databehandler for. Når Facebook på den anden side oplyser om indhentning af persondata eller videregivelsen af disse, når de selv er dataansvarlig, er der mere tvetydighed at spore eller implicitte behandlinger i deres oplysninger. Hertil kan f.eks. nævnes deres brug af ansigtsgenkendelsesteknologi, som bliver gemt under en generel sproglig formidling, hvor Facebook blot skriver "oplysninger", hvorefter den registrerede selv må lede videre på Facebook, for at finde frem til, hvilke oplysninger der her bl.a. er tale om. Et andet eksempel er lagringen af persondata selv efter en kontos sletning. Her skriver Facebook, at nogle data vil blive gemt efter sletning, hvor der bl.a. er tale om samtaler,

[61] Facebooks vilkår, afsnit 3, punkt 4.
[62] Folketingets ombudsmands beretning for 2011, sag nr. 2011 15-1, s. 6.

som kan være fortrolige eller følsomme oplysninger for den registrerede. Problemerne for Facebook ved deres indhentning af samtykke, er dermed primært deres formidling af oplysninger i forbindelse med behandling af følsomme oplysninger samt minimering af deres databehandling.

Dataminimering og opbevaringsbegrænsning er knyttet tæt sammen, i den forstand, at hvis noget lagres i en for lang periode, vil det ikke længere være relevant for den dataansvarlige at behandle disse persondata. I forhold til indsamlingen af samtykket, er dette vigtigt, fordi der i artikel 13, stk. 2, litra a) og artikel 14, stk. 2, litra a) står, at den dataansvarlige skal oplyse den registrerede om det tidsrum persondataene vil blive behandlet i. Facebook skriver i deres datapolitik, at de gemmer data så længe det er nødvendigt for deres tjenester. I forbindelse med Facebooks tidslinje, vil dette sige alle persondata, som den registrerede lægger ud på sin profil, vil blive gemt, indtil profilen slettes. Hertil kommer dog, at oplysninger som andre brugere har delt om den registrerede ikke bliver slettet, da dette ikke er en del af den registreredes konto, som denne sletter. Grunden til at dette er i overensstemmelse med forordningen er, at det er de andre brugere der er dataansvarlig og ikke Facebook, hvorfor den registrerede, som vil have sig slettet fra Facebooks systemer, skal bede disse andre brugere om at slette alle oplysninger, der har med den registrerede at gøre. Et problem i denne henseende er dog lagringen af samtaler, som også er nævnt i bl.a. Jubii afgørelsen fra datatilsynet. Samtaler kan have karakter af fortrolige eller følsomme oplysninger, hvorfor der skal være yderlige sikkerhed ved behandling af disse, hvilket også kræver større grund til behandling. Når der er gået et tilstrækkeligt tidsrum skal samtalen dermed slettes (i Jubii afgørelsen efter ét år), for at sikre den registreredes interesser. Lige netop chat-beskeder er den type oplysning, som Facebook skriver bliver gemt efter sletning, som stadig kan benyttes til identifikation. Lagringstiden for chat-beskeder bør dermed gøres kortere og informere den registrerede herom ved indsamlingen af samtykket til behandling af persondata. Hvis det ikke er muligt at angive tidsrummet for lagringen af persondata, giver forordningen også mulighed for, at den dataansvarlige kan nøjes med at oplyse om de kriterier, der benyttes til fastlæggelse af tidsrummet. Dette gælder dog også for de andre fortrolige og følsomme persondata, der ikke bliver offentliggjort af den registrerede selv som f.eks. IP-adresser. Lige så snart det er den registrerede der offentliggør dataene selv, som f.eks. ved at deltage i et åbent event, er der tale om offentlig oplysninger, som Facebook kan benytte så længe det er relevant i forhold til deres tjenester og har gyldigt samtykke til behandling af disse oplysninger, hvilket kan ses i forordningens artikel 2, stk. 2, litra c) og hertil også præamblens betragtning 18. Facebook skal dermed være bedre til at oplyse den registrerede om vigtige forhold ved indhentning af samtykke.

Gennemsigtigheden af deres datapolitik og vilkår er dermed ikke optimal, når deres oplysningspligt ikke er opfyldt. Dette gælder specielt når der er tale om børn, hvor Facebook må anses ikke at yde den korrekte form for sikkerhed herfor. Grunden hertil er, at Facebook ikke stiller tilstrækkelig sikkerhed til rådighed, for at børn

under 13-16 år ikke benytter sig af deres tjenester. Facebook skal efter deres bedste mulighed sikre, at børn ikke bruger Facebooks tjenester, da de ellers laver en ulovlig behandling af persondata, fordi de ikke indhenter samtykke fra barnets værge. Ligesom ved afgivelse af samtykke bør dette gøres på en aktiv og klar måde, hvorpå det ikke må være nok at benytte sig af vilkår og datapolitik til at sikre sig, at barnet er over 13-16 år, men at de selv skal angive, at de er over 13-16 år, for at benytte sig af Facebook.

Facebooks app lever dermed ikke op til de krav, som persondataforordningen stiller ved indsamlingen af samtykket. Facebook skal oplyse deres brugere bedre, om hvordan deres data bliver brugt og den risici der er med behandlingen. Dette gælder specielt, når der er tale om fortrolige og følsomme persondata, som placering og biometriske data. Også i forhold til behandling af børn, bør Facebook forøge deres tiltag, for at mindreårige børn ikke får adgang til Facebooks tjenester. Alt dette skal selvfølgelig ses i et proportionelt forhold til udgifter samt de tekniske muligheder, den nuværende teknologi kan gøre for at sikre disse tiltag. I forhold til indsamlingen af samtykket, er det for appens vedkommende kun den tekniske del af indhentningen der er i overensstemmelse med forordningen, mens den baggrund, hvorpå samtykket skal gives, ikke lever op til forordningens krav.

10 PERSPEKTIVERING

Når der dermed bliver konkluderet, at Facebooks app ikke lever op til kravene af den nye persondataforordning, er det dermed også vigtigt at se på, om Facebooks hjemmeside i større grad lever op til disse krav. Når der bliver lavet en konto på Facebooks app, og dermed indhentet samtykke til behandling, refererer appen til de samme vilkår og datapolitik, som hjemmesiden gør ved oprettelse af en konto. Der er dermed de samme problemer i disse for hjemmesiden, som der er ved appen, i forhold til på hvilket grundlag samtykket er givet på og behandlingstiden af persondata. Når der dermed er tale om de mere tekniske dele, er der store forskelle på appen og hjemmesiden. Dette er bl.a. om samtykket bliver indhentet på en gyldig måde. På baggrund af ovenstående analyse, bliver konklusionen for appen, at samtykket bliver indhentet på en gyldig måde, da der er en aktiv handling ved afgivelse af samtykket. For hjemmesiden er dette helt anderledes. Når der bliver lavet en konto fra Facebooks hjemmeside, er der ingen boks der kan afkrydses i forbindelse med accept af vilkår og datapolitik. Derudover står informationen om afgivelse af samtykket med småt under selve registreringsformularen. Hjemmesiden overholder dermed ikke kravet om, at samtykket gives i form af en klar, frivillig, specifik, informeret og utvetydig viljestilkendegivelse, som forordningens præambels betragtning 32 fremstiller. Selvom der heller ikke skal krydses af i en boks i appen, er forskellen, at appen på en klar og tydelig måde fremstiller vilkår og datapolitik for den registrerede, som aktivt skal gå videre fra denne side, for at komme til selve registreringsformularen. Det er denne aktive handling som gør, at appen i dette tilfælde overholder forordningens krav, mens hjemmesiden ikke overholder disse.

En anden forskel på appen og hjemmesiden er, at appen giver adgang til flere begrænsninger ved brug af Facebook. I indstillingerne på appen er det f.eks. muligt at begrænse Facebooks adgang til kontakter og placering. Dette er ikke muligt på hjemmesiden. Dette er dog kun for GPS placering i forhold til de tjenester, som skal bruge placering, da IP-adresser og placering herigennem stadig bliver behandlet af Facebook. Dette bliver gjort for at den registrerede kan se, om andre har logget på hans konto, og i så fald hvor de (cirka) befinder sig.

Ud over de artikler som er nævnt i analysen, er der også andre artikler, som ville kunne benyttes til at komme frem til samme konklusion. Dette er specielt artikel 25 om databeskyttelse gennem design og standardindstillinger. Kort omhandler disse om, at den dataansvarlige skal tage den registreredes interesser i betragtning, og sikre disse gennem teknologi og standardindstillinger. I forhold til databeskyttelse gennem design, artikel 25, stk. 1, kan her f.eks. nævnes sikringen af, at der ikke behandles persondata om børn. Ved at skifte designet på dette, så det ikke i vilkårene står, at man skal være over 13 år, men i et særskilt afkrydsningsfelt (som obligatorisk skal krydses af) erklærer, at man er over 13 år, vil Facebook på denne måde

overholde forordningen. Samme gælder ved databeskyttelse gennem standardindstillinger, artikel 25, stk. 2, hvor den dataansvarlige skal varetage den registreredes interesser, ved bl.a. at minimere datamængden og behandlingstiden til det, som der er nødvendigt.

Når man ser på, om samtykket er indhentet korrekt, er det også vigtigt i Facebooks tilfælde, at se, om samtykket til profilering er indhentet korrekt. Grunden hertil er, at Facebook danner profiler af deres brugere på baggrund af de oplysninger de får. Dette kan ses gennem de oplysninger de skriver de indhenter deres privatlivspolitik under "Hvilken type oplysninger indsamler vi?". I forordningen står der i artikel 22, stk. 2, litra c), at samtykke til profilering skal ske udtrykkeligt. Når der dermed ikke står eksplicit i hverken deres vilkår eller datapolitik, er spørgsmålet om samtykket hertil er indhentet korrekt, selvom Facebook tydeligt skriver, at de indsamler data som medvirker til profilering, samt det faktum, at man danner en Facebook "profil". Der er dermed informationer, som fortæller om profileringen, spørgsmålet er imidlertid, om det er tilstrækkeligt i forhold til de konsekvenser profileringen kan have. Der er altså tale om en proportionalitetsspørgsmål.

I forhold til overholdelse af andre dele af forordningen, end dem som dette speciale har fokuseret på, kan det være en god idé for Facebook, at ansætte en DPO (Data Protection Officer, på dansk databeskyttelsesrådgiver), da Facebook behandler mange persondata, både almindelige, fortrolige og følsomme. En DPO skal sikre, at virksomheden overholder forordningens regler. Der er i forordningens artikel 37, stk. 1 opstillet nogle tilfælde, hvor der er krav om at der bliver ansat en DPO. Hvorvidt det er et krav for Facebook vil der ikke blive taget stilling til, men uanset om det er et krav eller ej, ville det sandsynligvis være godt for Facebook at have en DPO. Dette skyldes, at en DPO ville kunne hjælpe Facebook med de persondataretlige elementer, og i og med at Facebooks virke i stor grad afhænger af indhentning og behandling af persondata, ville dette kunne forbedre Facebooks retlige stilling, og dermed også sikre brugernes persondata på en mere tilfredsstillende måde efter persondataforordningen. Sådan en DPO ville f.eks. være i stand til at vejlede Facebook til at minimere deres dataindsamling, ved at sikre at der kun bliver indhentet det nødvendige data.[63]

Afsluttende skal det dog siges, at dette speciale er skrevet ud fra Facebooks vilkår og datapolitik, som er gældende foråret 2017. Dette vil sige, at den konklusion som specialet er kommet med, ikke nødvendigvis vil være den samme, når forordningen træder i kraft, da Facebook kan have opdateret deres vilkår og politik til at overholde forordningens krav.

[63] Dall, N. P., Langemark, J. og Langebæk, A. (2016), s. 123 – 127.

10.1.1 Persondataforordningen og Facebook i fremtiden

Et problem med forordningen er, at den forsøger at regulere noget, som udvikler og ændrer sig markant meget hurtigt. Som det ses af bilag 1, bliver der mere og mere teknologi i hjemmet, som resulterer i større nødvendighed af sikringen af persondata. Men som det også blev set med persondatadirektivet fra 1995 blev det forældet i takt med, at teknologien og befolkningens behov herfor blev forøget. Hertil også det netværkssamfund som vi ser i dag, hvor mange har behov for ofte at være online på bl.a. Facebook. Resultatet heraf er, at forordningen skal anses som en ramme, som sidenhen bliver udfyldt af retspraksis. Dette medfører usikkerhed for de dataansvarlige, herunder Facebook, i forhold til, hvordan forordningen skal forstås og hvor lang sikkerheden for de registrerede skal gå. Som et eksempel hertil kan f.eks. nævnes dette speciales analyse af behandling af børns persondata. Konklusionen herpå er, at der er en øget sikkerhed, som gør at Facebook skal indhente en aktiv tilkendegivelse af, at den registrerede er over en bestemt alder, hvormed behandling kan foretages. Hvorvidt denne konklusion er korrekt afhænger af, hvad domstolene i fremtiden bestemmer der skal lægges i præamblens betragtning 38 om *"særlig beskyttelse"*. Der kan på denne baggrund ske en voldsom ændring, både i forhold til at gøre dette speciales konklusion mere lempelig, men også strengere, alt efter hvordan domstolene, hertil specielt EU-domstolen, fortolker forordningen. Dette betyder, at de dataansvarlige skal være varsomme med at indskrænke deres vilkår og datapolitik for meget, da dette kan medføre at de alligevel ikke overholder forordningen, på baggrund af en fortolkning, som de ikke havde forudset. Dette er dog ikke anderledes end andre retsområder, forskellen er dog den, at persondataforordningen kommer med nogle store ændringer som vil ramme alle, hvorfor dette er nødvendigt at pointere.

I forhold til Facebook er dette også vigtigt, da Facebooks indhentning af data er så omfattende, at det kan være sammenligneligt med Big Data, som er en stor udfordring for persondataretten og ideen om sikkerhed for den registrerede. Specialet i forhold til Facebooks app, som har mulighed for at indsamle væsentlig flere persondata om den registrerede, end hjemmesiden kan, bl.a. gennem fotos der bliver taget på den mobile enhed og placeringsdata gennem GPS. Herudover kan vi ikke vide på nuværende tidspunkt hvordan vores teknologi ser ud om nogle få år, da udviklingen går stærkt, hvilket kan medføre flere muligheder for indhentning af data gennem smartphone, tablet eller anden enhed som benytter appen. Det er dermed vigtigt for Facebook at overholde de idéer der ligger bag forordningen, da fortolkningen af den ellers vil kunne give problemer for Facebook på et senere tidspunkt, hvor teknologien har udviklet sig yderligere med nye muligheder for dataindsamling.[64]

[64] Blume, P. (2016), s. 195 – 210.

11 SUMMARY

This master thesis is about how Facebook collects consent from the data subject and the compliance with the new privacy regulation from EU, general data protection regulation 679/2016.

To determine the compliance with the way of collecting consent and the compliance with the regulation has been analyzed through Facebooks terms of compliance and the privacy policy, which has been linked to and accepted when creating a Facebook account.

The thesis is primarily about Facebooks application for mobile devices such as smartphones, but as the terms and policy are the same as for the website, most of what is concluded, can also be used on the website and Facebook as a whole. There are some differences between the application and the website, which mainly is the technical part of collecting the consent, for example how the terms and policy is accepted.

The main articles which is worked with is article 5, 6 – 9, 12 (1), 13 and 14. These articles is about the general principles within the regulation, requirements for when personal data can be processed both for children and for grownups. Lastly article 13 and 14 is about what is required for the controller to inform the data subject and article 12(1) is about the transparency of this information. Together these articles determines if the consent is collected correctly with the necessary information. This means that the thesis is not concerned with the other parts of the regulation, such as the controllers' safety regulations or compliance with the regulations' other articles, unless they are relevant for a specific case or argument.

Because there currently are no case law on the subject, as the regulation does not take effect until 2018, the way the analysis is conducted, is by using the appendix of the regulation to help analyze the meaning of the articles, as well as old case law and statements from the Danish supervisory authority.

All this is done to answer the stated problem:

"Is Facebooks' app in compliance with the new EU regulation 2016/679, when collecting consent for processing personal data?"

This is done through five sub questions, which each have a part of the regulation as a focus. The reason this is done, is to give a better overview of Facebooks' current problems regarding the new data protection regulation.

As shown through this thesis' analysis and conclusion, Facebooks main problems when collecting consent for data processing, is with their processing time, which at times can be done even though after the data subject has deleted his or hers account. Besides this, also the information Facebook gives to their users are not as

clear as it should, especially when it comes to the processing of special categories of personal data. Also their attempt to diminish underaged people in using their services are not as secure as it should. These are however only three examples of non-compliance, which has been concluded in this thesis.

Although this may sound as though Facebook does not comply with the regulation at all, they do have areas, in which the application comply. This is for example the way Facebook collects the consent, which requires an active action from the data subject. Which in this thesis has been concluded the app does sufficiently active.

12 KILDELISTE

12.1 BØGER

- Blume, P. (2016), *DEN NYE PERSONDATARET Persondataforordningen*, Jurist- og Økonomforbundets Forlag, 1. Udgave, 2. oplag.
- Blume, P. (2009), *Juridisk metodelære,* Jurist- og Økonomforbundets Forlag, 5. udgave, 1. oplag.
- Waaben, H. og Nielsen, K. K. (2015), *Lov om behandling af personoplysninger*, Jurist- og Økonomforbundets Forlag, 3. Udgave.
- Munk-Hansen, C (2014), *Retsvidenskabs teori,* Jurist- og Økonomforbundets forlag,1. udgave, 1. oplag.
- Dall, N. P., Langemark, J. og Langebæk, A. (2016), *Persondataforordningen – en håndbog for praktikere,* Ex Tuto publishing A/S, første udgave, andet oplag.

12.2 DOMME, AFGØRELSER OG UDTALELSER

- U2011.2343H.
- C-362/14, Maximillian Schrems.
- C-70/10, Scarlet Extended SA.
- C-582/14, Patrick Breyer.
- Forslag til afgørelse C-362/14, Maximillian Schrems.
- Forslag til afgørelse C-582/14, Patrick Breyer.
- Folketingets ombudsmands beretning for 2011, sag nr. 2011 15-1.
- Datatilsynets journalnummer 2013-321-0173*, Myndigheders brug af Facebook*.
- Datatilsynets journalnummer 2006-43-2010, *Advarselsregister hos Rejsekort A/S (II).*
- Datatilsynets journalnummer 2002-219-0139, *Lagring af chat hos Jubii.*
- Datatilsynets journalnummer 2007-42-0049, *Vedrørende monitorering og logning af 1-1 kommunikation på www.arto.com*.

12.3 LOVGIVNING

- Forordning 2016/679, persondataforordningen.
- Direktiv 95/46/EF, persondatadirektivet.
- Direktiv 2000/31/EF, direktiv om elektronisk handel.
- Lov nr. 429 af 31. maj 2000, *Persondataloven*.

12.4 HJEMMESIDER

- http://www.nethistory.info/History%20of%20the%20Internet/web.html
- http://www.sas.com/en_us/home
- https://taenk.dk/aktiviteter-og-kampagner/tidligere-kampagner/har-dine-apps-frit-spil-beskyt-dine-personlige
- http://www.samsung.com/us/explore/family-hub-refrigerator/
- https://www.facebook.com/
- Facebooks privatlivspolitik 1/3-2017: https://www.facebook.com/privacy/explanation
- Facebooks vilkår 1/3-2017: https://www.facebook.com/legal/terms/update

- https://www.datatilsynet.dk/forside/
- http://www.tekno.dk/wp-content/uploads/2014/12/p10_Biometri_brug_af_biometriske_teknologier_i_det_danske_samfund.pdf
- http://www.sikkerchat.dk/da-DK/For%C3%A6ldre/Aktuelt/Nyheder.aspx?Action=1&NewsId=133&PID=348
- https://www.iplocation.net/
- http://politiken.dk/forbrugogliv/digitalt/art5549887/Sociale-medier-udleverer-store-m%C3%A6ngder-brugerdata-til-myndigheder

12.5 Billeder

- Forside billede: https://www.dr.dk/nyheder/indland/din-facebook-vens-vens-ven-kender-maaske-mark-zuckerberg
- Billede 1: http://tv2.dk/
- Billede 2: Om kontaktsynkronisering på Facebooks app.
- Billede 3: https://www.facebook.com/
- Billede 4: Oprettelse af Facebookkonto på Facebooks app.

12.6 Bilag

- Bilag 1: http://www.statistikbanken.dk/VARFORBR
- Bilag 2: Udklip fra eget Facebook dataarkiv.
- Bilag 3: https://www.facebook.com/legal/terms
- Bilag 4: https://www.facebook.com/full_data_use_policy