AALBORG UNIVERSITET

Kandidatafhandling

Beskyttelsen af børns personoplysninger gennem samtykkereglerne i GDPR og databeskyttelsesloven

The protection of children's personal data through the governing consent rules in GDPR and the Danish Data Protection Act

Anne-Sofie Kaldahl Andersen

Studienr: 20204151

15. maj 2025

Titelblad

Titel: Beskyttelsen af børns personoplysninger gennem samtykkereglerne i GDPR og databeskyttelsesloven

Engelsk titel: The protection of children's personal data through the governing consent rules in GDPR and the Danish Data Protection Act

Uddannelsessted: Aalborg Universitet

Uddannelse: Cand. Merc. Jur.

Projektart: Kandidatspeciale

Retsområde: Persondataret

Vejleder: Ulla Steen

Afleveringsdato: 15. maj 2025

Anslag i alt: 113.117

Antal fysiske sider: 66

Forfatter: Anne-Sofie Kaldahl Andersen

Studienr: 20204151

Forkortelsesafsnit

DBL: databeskyttelsesloven

GDPR: databeskyttelsesforordningen (forordningen)

EDPB: Det Europæiske Databeskyttelsesråd (Rådet)

COPPA: Children's Online Privacy Protection Rule (USA)

GDPD: The Italian Data Protection Authority (Italien)

DPC: Data Protection Commission (Irland)

FTC: Federal Trade Commission (USA)

Abstract

The technological development and the increasing online presence among children and young people put pressure on the protection of children's personal data when they use social media, online games and various entertainment apps. These services collect and process large amounts of personal data about their users, which raises significant questions about how children's personal data is protected by these services. This is especially relevant given that children are often less informed about the consequences of what it means when they consent to services collecting and processing information about them. As children are characterized as a particularly vulnerable group of people who need more protection, the processing of their personal data requires additional legal protection.

With the adoption of the Data Protection Regulation, article 8 was introduced. This regulation concerns children's competence to give consent when using information society services and sets the age limit for a child to give consent to the processing of their data at 16 years. In addition, the regulation allows member states to utilize national discretion to set a different age limit down to 13 years. The regulation does, however, not provide further regulation for the protection of children's personal data, as their data is otherwise only regulated in the general provisions of the regulation, which apply to all groups.

Since the online services often use other processing bases than consent for the collection and processing of personal data, this raises the question of whether article 8 of the GDPR and the corresponding §6 section (2) and (3) of the Danish Data Protection Act are sufficient for the protection of children's personal data.

Therefore, the purpose of the thesis is to analyze how children's personal data is protected through the consent rules in Article 8 of the GDPR and §6, section (2) and (3) in the Danish Data Protection Act, when using online services.

By analyzing how the consent rules are enforced in practice, including verification of the child's age, the thesis looks at decisions from European data protections authorities, such as the Irish DPC and the Italian GPDP. These decisions show a tendency of non-compliance with the regulation, as effective systems were not implemented to verify the age of children and did also not use methods to obtain valid parental consent.

The thesis therefore concludes, that the current legal situation and regulation in the GDPR and DPA do not provide children's personal data with the sufficient protection that the GDPR aims to provide in preamble recital 38. Therefore, it is the opinion of this thesis that a more concrete regulation in this area and a uniform standard for age verification should be introduced.

Indholdsfortegnelse

Kapitel 1- Introduktion til projektet

1.1 Indledning

Den teknologiske udvikling og den stigende online tilstedeværelse blandt børn og unge lægger et pres på beskyttelsen af børns personoplysninger, når de benytter sociale medier, spil og diverse underholdningsapps. De pågældende tjenester indsamler og behandler store mængder af personoplysninger om deres brugere, hvilket rejser væsentlige spørgsmål om, hvordan børnenes personoplysninger beskyttes på de online tjenester. Dette er særligt i betragtningen af, at børn ofte er mindre oplyste omkring konsekvenserne af, hvad det betyder, når de accepterer, at tjenesterne må indsamle og behandle oplysninger om dem. Da børn er kendetegnet ved at være en særligt sårbar persongruppe, som har behov for mere beskyttelse, kræver behandling af deres personoplysninger en ekstra retlig beskyttelse.[1]

Implementeringen af databeskyttelsesforordningen[2] (herefter forordningen eller GDPR) i 2018 tildelte netop børn særlig beskyttelse, som den første regulering, der tog stilling til børnenes personoplysninger. Forordningen indførte artikel 8, som angår børns kompetence til at give samtykke i forbindelse med brug af informationssamfundstjenester. Samtidig fastsætter bestemmelsen en aldersgrænse på 16 år for, hvornår et barn kan give samtykke til behandling af sine oplysninger. Hertil tillader forordningen at medlemsstaterne kan udnytte et nationalt råderum til at fastsætte en anden aldersgrænse ned til 13 år[3]. Yderligere regulering for beskyttelsen af børns personoplysninger, indeholder forordningen imidlertid ikke, da beskyttelsen af børns personoplysninger i øvrigt kun er reguleret i de generelle bestemmelser i forordningen, som angår alle persongrupper. Eftersom online tjenester ofte benytter andet behandlingsgrundlag end samtykke til indsamlingen og behandlingen af personoplysninger, lægger dette op til spørgsmålet om, hvorvidt artikel 8 i forordningen og den tilhørende

[1] Europa-Parlamentets og Rådets forordning af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (2016/679) (herefter Forordningen 2016/679), pr. 38

[2] Forordningen 2016/679

[3] Forordningen 2016/679, art.8, stk.1

paragraf 6, stk.2 og stk.3 i databeskyttelsesloven[4], er tilstrækkelig i beskyttelsen af børns personoplysninger.

Specialets formål er derfor at fastlægge, hvordan GDPR samt databeskyttelsesloven beskytter børns personoplysninger gennem samtykkereglerne og vurdere om denne beskyttelse er tilstrækkelig ved børns benyttelse af informationssamfundstjenester. I sammenfald med dette undersøges det, hvordan reglerne håndhæves i praksis med fokus på de problemstillinger, som opstår i relation til aldersverifikation og kontrol af samtykke. Dette sker på baggrund af en gennemgang af samtykkereglerne, en analyse af praksis på området samt en diskussion om aldersverificering.

1.2 Problemformulering

Hvordan sikrer GDPR og databeskyttelsesloven børns personoplysninger samtykkereglerne i GDPR art.8 og DBL §6, stk2 & stk.3. Er beskyttelsen tilstrækkelig ved brug af online tjenester, og hvordan håndhæves samtykkereglerne i praksis?

1.3 Metode

For at besvare specialets problemformulering benyttes retsdogmatisk metode. Metoden anvendes til at undersøge og fastlægge retstilstanden for samtykkereglerne i GDPR samt databeskyttelsesloven, og hvordan børns personoplysninger er beskyttet gennem reglerne.[5] Specialet fokuserer herfor på at beskrive og analysere GDPR art.8 og DBL §6, stk2 & stk.3 samt betingelserne for, hvornår der foreligger et gyldigt samtykke fra børn, og hermed et behandlingsgrundlag til at behandle oplysninger om dem. På baggrund af mangel på retspraksis fokuserer specialet på at beskrive rammebetingelserne gennem en analyse af lovgrundlaget og en undersøgelse af, hvordan håndhævelse af lovgivningen sker i praksis gennem aldersverificering. Til dette benyttes administrativ praksis fra europæiske datatilsyn.

[4] Lov 2018-05-23 nr.502 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (herefter Databeskyttelsesloven)

[5] Carsten Munk-Hansen, Retsvidenskabsteori (Djøf Forlag, 2022), s.211-212

1.4 Retskilder

Som grundlag for specialets analyse, inddrages en række retskilder, både fra dansk ret, EU-ret og i et begrænset omfang også fremmede retskilder. Hertil er det væsentligt at beskrive, hvilke retskilder, der tages udgangspunkt og sammenspillet mellem dem. Derfor vil de følgende afsnit identificere de relevante retskilder, som benyttes til at besvare specialets problemformulering og beskrive retskildeværdien af de anvendte retskilder.

Nedenfor indledes der med en beskrivelse af den anvendte EU-retlige retskilder, herefter de danske retskilder, de fremmede retskilder og slutteligt fortolkningsbidrag fra udvalgte EU-medlemsstater.

1.4.1 EU-ret

Den mest centrale retskilde i afhandlingen, *er Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelsen af fysiske personer i forbindelse med behandling af personoplysninger og fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF* (GDPR). GDPR udgør en del af national ret i alle EU-medlemsstater jf. Traktaten om Den Europæiske Unions Funktionsmåde (TEUF) artikel 288, stk.2. Særligt forordningens artikler 4,6,7, 8 og 25 findes relevante til at besvare specialets problemformulering om beskyttelsen af børns personoplysninger.

På traktatniveau anvendes endvidere *''FN's Konvention om Barnets Rettigheder''* (Børnekonventionen) af 20. november 1989. Konventionen benyttes primært som fortolkningsbidrag til begrebet ''*barn''* som led i analysen af beskyttelsen af børns personoplysninger. Hertil inddrages *''Den Europæiske Unions Charter om grundlæggende rettigheder (2010/C83/02)''* (Chartret) i beskrivelsen af udviklingen af beskyttelsen af børns personoplysninger og GDPR's udformning. Analysen beskriver primært Chartrets artikel 24, som bidrog til udformningen af GDPR's artikel 8.

De tilhørende præambelbetragtninger til forordningen inddrages undervejs i afhandlingen. Disse præambelbetragtninger udgør et vigtigt fortolkningsbidrag til forordningen, da de uddyber og præciserer formålet samt rækkevidden af de enkelte bestemmelser.[6] Særligt

[6] Peter Blume, Persondatarettens kilder og metode (Djøf Forlag, 2020), s.62

præambelbetragtning 38 benyttes i analysen, da denne præciserer den særlige beskyttelse, som tildeles børn, når deres personoplysninger behandles. Endvidere inddrages forarbejder til forordningen, som anvendes til at belyse lovgivers intentioner med bestemmelserne. Det bemærkes, at forarbejder, ligesom præambelbetragtninger, ikke er bindende retskilder, men udgør et fortolkningsbidrag som understøtter forståelse af de anvendte bestemmelser. Af forarbejder findes Europa-Kommissionens *''forslag til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger''* særligt relevant i fortolkningen af forordningen.

Undervejs inddrager specialet også vejledninger fra Det Europæiske Databeskyttelsesråd (herefter EDPB), som har erstattet den forhenværende Artikel 29-gruppe. Disse udtalelser udgør *soft law* og er herfor ikke en bindende retskilde, men har stor betydning for, hvordan reglerne skal forstås. Specielt i databeskyttelsesretten udgør EDPB-udtalelser en vigtig kilde, da Rådet er sammensat af repræsentanter fra de enkelte nationale tilsynsmyndigheder, og derfor tillægges udtalelserne en betydelig værdi.[7] Selvom Artikel 29-gruppen nu er blevet erstattet af EDBP, er de forhenværende udtalelser fra Artikel 29-gruppen blevet godkendt af EDPB, hvorfor disse udtalelser stadig betragtes og anvendes som relevante fortolkningsbidrag.[8] Særligt anvender specialet Artikel 29-gruppens vejledning *''Retningslinjer 5/2020 vedrørende samtykke i henhold til forordning 2016/679"* til begrebsafklaring samt EDPB's *''Statement 1/2025 on Age Assurance af den 11. februar 2025''.*

Endvidere inddrager specialet afgørelser fra europæiske datatilsyn, herunder det italienske datatilsyn Garante per la protezione dei dati personali (herefter GDPD) og det irske datatilsyn Data Protection Commission (herefter DPC). Afgørelserne anvendes som fortolkningsbidrag til belysning af praksis vedrørende aldersverifikation og beskyttelse af børns personoplysninger. Disse udgør vigtige bidrag til fastlæggelsen af, hvordan reglerne håndhæves og fortolkes i praksis i EU-medlemsstaterne. Ligeledes anvendes afgørelserne til at identificere og analysere mulige udfordringer, som kan være relevante i forhold til vurderingen af, om det eksisterende beskyttelsesniveau af børns personoplysninger kan vurderes tilstrækkelig.

[7] Peter Blume, Persondatarettens kilder og metode (Djøf Forlag, 2020), s.63-65
[8] Peter Blume, Persondatarettens kilder og metode (Djøf Forlag, 2020), s.65-66

Specialet benytter derudover vejledninger fra de europæiske datatilsyn. Særligt vejledningen benævnt *''Fundamentals for a Child Oriented Approach to Data Processing*'' af 2021 udstedt af de irske datatilsyn (DPC) findes interessant i analysen af, hvordan artikel 8 og beskyttelsen af børns personoplysninger sker i praksis i forhold til samtykke og aldersverifikation. Vejledninger fra europæiske datatilsyn, er ikke bindende retskilder, men bidrager som fortolkningsbidrag i relation til, hvordan reglerne skal overholdes i praksis. Som følge af GDPRs formål om harmonisering af medlemslandenes fortolkning og anvendelse af forordningens regler, illustrerer både vejledninger og afgørelser fra europæiske datatilsyn, hvordan fortolkning og håndhævelse ligeledes ville realiseres i Danmark jf. præambelbetragtning 10.

1.4.2 Dansk ret

Databeskyttelsesloven (DBL) er en supplering til forordningen jf. DBL §1 og tildeler Danmark et nationalt råderum, til at fastsætte egne regler. Nogle har til formål at uddybe forordningens regler, og andre har ikke en direkte forbindelse til forordningen[9]. Interessant for dette speciale, er netop artikel 8, stk.1 i forbindelse med indhentning af samtykke fra børn til brug af informationssamfundsstjenester, hvor der er tildelt nationalt råderum til medlemslandene til at fastsætte en lavere aldersgrænse. Hertil er DBL §6, stk.2 og stk.3 netop indsat.

Forarbejder til DBL som lovforslag og lovbemærkninger, inddrages undervejs i specialets arbejde, som et fortolkningsbidrag til forståelsen af lovbestemmelserne, da disse forarbejder har betydning i forhold til fastlæggelsen af reglernes mening. [10] Herudover, belyser og anvender specialet administrative forskrifter i form af betænkninger fra Justitsministeriet, navnlig ''*Justitsministeriets Betænkning om databeskyttelsesforordningen (2016/679*)''. Betænkningen anvendes som supplement til forståelsen af databeskyttelsesloven og databeskyttelsesforordningen, da den indeholder bemærkninger og overvejelser hertil. Det

[9] Kristian Korfits Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer (Jurist- og Økonomforbundets Forlag, 2020), s.961-964
[10] Peter Blume, Persondatarettens kilder og metode (Djøf Forlag, 2020), s.41

bemærkes, at betænkninger ikke er lovforarbejder, men en vigtig retskilde i fastlæggelsen af gældende ret.[11]

I Danmark er afgørelser truffet af Datatilsynet en vigtig kilde til persondataretten, da tilsynet er den primære fortolker og anvender af forordningen samt databeskyttelsesloven, hvorfor deres afgørelser viser hvordan reglerne skal forstås og anvendes i praksis.[12] Da der på området for børns samtykke til behandling af personoplysninger, endnu ikke foreligger meget dansk praksis, analyserer specialet afgørelser fra europæiske datatilsyn.

Det danske Datatilsyn har endvidere udgivet en række vejledninger, som også vil blive inddraget i løbet af specialet. Vejledningerne er ikke forpligtende over for borgerne, men angiver hvordan Datatilsynet fortolker og anvender retsreglerne. Derfor peger vejledningerne i retningen af, hvordan Datatilsynet vil træffe afgørelser i sager på de enkelte områder. Vejledningerne ændres løbende, hvis der skulle opstå nye fortolkninger på et givent retsområde. [13] Særligt Datatilsynets *''Vejledning om Samtykke*'' af maj 2021 benyttes i analysen af samtykkereglerne.

Udvalgt retslitteratur vil blive anvendt i specialet. Af relevant litteratur, vil faglitteratur i særdeleshed anvendes. Retslitteratur udgør ikke en egentlig retskilde i sig selv, men bidrager til forståelsen og fortolkningen af reglerne på området, og udgør derfor et væsentligt bidrag til den juridiske metode.[14]

1.4.3 Fremmed ret

Specialet inddrager inspiration fra den amerikanske *Children's Online Privacy Protection Rule* (COPPA), som blev vedtaget i USA i 1998, og angår beskyttelsen af børns privatliv online. Selvom COPPA ikke har nogen retskildeværdi for fortolkningen af forordningens regler om børns samtykke, fremgår det af forarbejder til forordningen, at artikel 8 om børns samtykke i forbindelse med informationssamfundstjenester, er inspireret af COPPA, og herfor vil COPPA benyttes til fortolkningsbidrag og overvejelserne i forbindelse med artikel 8. [15]

[11] Peter Blume, Persondatarettens kilder og metode (Djøf Forlag, 2020), s.43-44
[12] Peter Blume, Persondatarettens kilder og metode (Djøf Forlag, 2020), s.107
[13] Peter Blume, Persondatarettens kilder og metode (Djøf Forlag, 2020), s.43-44
[14] Peter Blume, Persondatarettens kilder og metode (Djøf Forlag, 2020), s.55
[15] Commission Staff working paper Impact Assessment SEC (2012) 72 final, s.68

COPPA administreres af det amerikanske tilsyn Federal Trade Commission (FTC), hvorfor eksempler på metoder til verificering af alder og kontrol af samtykke fra tilsynet inkluderes. Tilsynets praksis har ligeledes ikke bindende retsvirkning i Danmark, men udgør en inspirationskilde til, hvordan kravene til eksempelvis forældresamtykke kan implementeres i praksis.

1.5 Afgræsning

Følgende afsnit beskriver hvilke til- og fravalg, som er foretaget som led i besvarelsen af specialets problemformulering.

Specialet tager udgangspunkt i GPDR-forordningen, med fokus på samtykkebestemmelserne i artikel 4, artikel 6, artikel 7 og artikel 8, men anvender også artikel 25 om databeskyttelse gennem design og standardindstillinger. Herudover beskrives nogle af de grundlæggende principper i GDPR for behandling af personoplysninger. Enkelte andre artikler fra forordningen, nævnes i forbindelse med at fastlægge rammerne for GDPR og anvendelsesområdet, men uddybes ikke yderligere i specialet.

Specialet inddrager i begrænset omfang de registreredes rettigheder. Rettighederne beskrives kort i afsnit 2.4.5. i begrebsafklaringen, og benævnes i relation til samtykkereglerne, men rettighederne uddybes som udgangspunkt ikke yderligere.

Herudover henviser specialet til den amerikanske Children's online Privacy Protection Act (COPPA), samt den tilhørende tilsynsmyndighed Federal Trade Commission (FTC) med fokus på retsgrundlaget vedrørende aldersgrænsen for at kunne afgive et gyldigt samtykke i forbindelse med udbud af informationssamfundstjenester og metoder til verificering af samtykke. Specialet afgrænses udelukkende til dette, og beskriver ikke forordningen eller tilsynets praksis yderligere.

I besvarelsen af specialets problemformulering anvendes afgørelser fra europæiske datatilsyn, herunder det irske og italienske datatilsyn. Afgørelserne er relevante i analysen af, hvordan reglerne fortolkes samt håndhæves i praksis, og benyttes eftersom der ikke eksisterer afgørelser fra det danske datatilsyn, hvor reglerne fortolkes. Til trods for, at der kan forekomme nationale variationer i implementeringen af forordningen, og at medlemsstaterne

i nogle tilfælde kan have forskellige retlige tilgange, anvendes afgørelserne som et væsentligt fortolkningsbidrag, da forordningen tilsigter en ensartet anvendelse på tværs af medlemsstaterne, jf. præambelbetragtning 10.

Specialet fokuserer på problemstillingen angående beskyttelsen af børns personoplysninger ved brug af informationssamfundstjenester, hvorfor specialet afgrænses til ikke at behandle eksempelvis forældres brug eller misbrug af børnenes personoplysninger. I stedet fokuseres på den dataansvarliges behandling af personoplysningerne.

Kapitel 2- Databeskyttelsesforordningen og databeskyttelsesloven

2.1 Indledning

GDPRs artikel 8 regulerer kravene til børns samtykke i forbindelse med udbud af informationssamfundstjenester. Det findes herfor relevant først at fastlægge de overordnede rammer for GDPR, herunder formålet og anvendelsesområdet af forordningen samt en gennemgang af relevante begreber og principper for behandling af personoplysninger.

2.2 Forordningens formål og anvendelsesområde

Forordningen blev vedtaget i 2016 med virkning fra den 25. maj 2018. Hertil blev databeskyttelsesloven også vedtaget i Danmark, som et nationalt supplement til forordningen, og erstattede derfor den tidligere Persondatalov.[16]

Forordningen tjener principielt to formål. For det første, er formålet at fastsætte en regulering, som sikrer beskyttelse af den enkelte persons privatliv i forbindelse med behandling af deres personoplysninger, herunder beskyttelsen af børns personoplysninger jf. GDPR art. 1, stk.1 og 2. For det andet, skal forordningen sikre fri udveksling af personoplysninger i EU, jf. GDPR art. 1 stk. 2 og 3. Det ene formål vægter ikke højere end det andet, men der skal foretages en afvejning af formålene alt efter den konkrete situation.[17]

Forordningen tilsigter derudover harmonisering af EU-medlemslande ved at sikre, at personoplysninger behandles med samme integritet og på samme niveau på tværs af alle EU-medlemsstaterne.[18]

Det materielle anvendelsesområde fremgår af databeskyttelsesforordningens artikel 2, stk.1, hvor det fastlægges, at forordningen finder anvendelse på behandling af personoplysninger, der helt eller delvist foretages ved hjælp af automatisk databehandling og på en anden

[16] Lov 2000-05-31 nr.429 om behandling af personoplysninger
[17] Kristian Korfits Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer (Jurist- og Økonomforbundets Forlag, 2020), s.203
[18] Peter Blume, Persondatarettens kilder og metode (Djøf Forlag 2020), s.23

ikkeautomatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register jf. art. 2

Det territoriale anvendelsesområde er reguleret i forordningen artikel 3, hvor den geografiske udstrækning af GDPR er defineret. Artikel 3 stk.1 omhandler situationen, hvor der sker behandling af personoplysninger, som led i aktiviteter, og som udføres for en dataansvarlig eller databehandler, der er etableret inden for unionen. Stk. 2 omhandler derimod den situation, hvor databehandleren eller den dataansvarlige ikke er etableret inden for unionen, men der sker behandling af personoplysninger af en registreret, som er i unionen gennem udbud af varer/tjenester eller overvågning af den registreredes adfærd.

GPDR finder også anvendelse på behandling af personoplysninger, som foretages af en databehandler, som dog ikke er etableret i EU, men hvor medlemslandenes nationale ret gælder i medfør af folkeretten jf. art. 3, stk.3.

2.3 Børns retstilling i GDPR

I forordningen er det udtrykt, at børn bør nyde en særlig beskyttelse af deres personoplysninger, idet de er kategoriseret som en sårbar persongruppe. Dette er begrundet i, at børn ofte mangler den nødvendige modenhed til at forstå de risici og konsekvenser, som er forbundet med databehandlinger jf. præambelbetragtning 38. Derfor kan børn have vanskeligere ved at varetage og udnytte deres rettigheder. Det anerkendes imidlertid også, at børn skal anses som en persongruppe, der kan varetage beskyttelsen af egne personoplysninger gennem et samtykke, forudsat at betingelserne for et gyldigt samtykke er opfyldt.[19]

Beskyttelsen af børns personoplysninger er reguleret i de bestemmelser, som generelt vedrører hvordan personoplysninger lovligt kan behandles og hvilke rettigheder, som den registrerede har i forbindelse med behandlingen af deres personoplysninger. Herunder retten til oplysning (artikel 13-14), indsigt (artikel 15), berigtigelse (artikel 16), sletning (artikel 17) og indsigelse (artikel 21). De pågældende rettigheder skal udøves under hensyntagen til barnets alder,

[19] Forordning 2016/679 art.8

hvorfor retten til oplysning blandt andet skal varetages med fokus på letforståelig og lettilgængelig formidling.[20]

Derudover er beskyttelsen af børns personoplysninger fremhævet i forbindelse med rettigheden i artikel 22, som angår automatiske individuelle afgørelser, herunder profilering. Hertil fremhæver præambelbetragtning 71, at automatiserede afgørelser ikke bør omfatte børn.

På baggrund af den teknologiske udvikling og en større online tilstedeværelse blandt børn, var der i overvejelserne til udformningen af forordningen, fokus på en særlig beskyttelse af børns personoplysninger samt regulering af børns samtykke i forbindelse med informationssamfundstjenester.[21] Herfor blev artikel 8 indsat i forordningen.

Et andet centralt element i beskyttelsen af børns personoplysninger, er artikel 25, som indebærer et princip om databeskyttelse gennem design og standardindstillinger, der benævnes *privacy by design og by default*. Denne bestemmelse pålægger den dataansvarlige en pligt til at integrere databeskyttelseseretlige principper allerede i udformningen af systemet/tjenesten, der udbydes. Dette er med henblik på, at behandlingen af personoplysninger begrænses til det nødvendige i forhold til formålet med behandlingen. Bestemmelsen er central i relation til beskyttelsen af børns personoplysninger, da de til trods for deres manglende modenhed og forståelse for konsekvenserne af databehandling, stadig ydes en beskyttelse gennem reglens pligt til at den dataansvarlige indretter tjenesten med fokus på dataminimering, gennemsigtighed og indhentning af et lovligt samtykke ved eksempelvis aldersverifikation. [22]Artikel 25 udgør i visse tilfælde derfor en forudsætning for at samtykke efter artikel 8 kan indhentes lovligt, eftersom den tekniske udformning af tjenesten kan være afgørende for vurderingen om, at der er indhentet lovligt samtykke fra barnet eller forældremyndighedsindehaveren.

For at kunne analysere, hvordan forordningens regler beskytter børns personoplysninger, findes det nødvendigt at fastlægge betydningen af blandt andet begrebet ''*barn''*, og andre relevante begreber i databeskyttelsesretten.

[20] Forordning 2016/679, art.12, stk.1
[21] Commission Staff working paper Impact Assessment SEC (2012) 72 final
[22] EDPB Retningslinjer 4/2019 om artikel 25 Databeskyttelse gennem design og standardindstillinger (2020)

2.4 Begrebsafklaring af relevante databeskyttelsesretlige begreber

De følgende afsnit har til formål at redegøre for relevante persondataretlige begreber, som specialet behandler, og som er vigtige for forståelsen af lovgrundlaget. GDPR artikel 4 indeholder legaldefinitionerne på alle de centrale databeskyttelsesretlige begreber, hvorfor begrebsafklaringen tager udgangspunkt i denne. Begrebet ''*barn*'' er imidlertid ikke indeholdt i legaldefinitionerne i artikel 4, hvorfor dette begreb defineres ud fra forarbejder i form af lovforslaget til forordningen (forslaget) samt udtalelser fra den tidligere Artikel 29-gruppe. Begrebet ''*samtykke*'' defineres i et senere kapitel.[23]

2.4.1 Personoplysninger

I GDPR artikel 4, nr.1, findes definitionen på begrebet *personoplysninger*, hvorved det beskrives, at personoplysninger er *''enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede)*''. Tilsvarende definition findes i databeskyttelsesloven §3, nr.1. Eftersom oplysningerne skal vedrøre en identificeret eller identificerbar fysisk person, omfatter GDPR herfor ikke anonyme oplysninger. Ved udtrykket *''identificerbar person''*, forstås en person, der enten ved direkte eller indirekte identifikatorer, kan identificeres. Identifikatorer kan blandt andet være navn, adresse, identifikationsnummer som eksempelvis CPR-nummer eller andet, som kan fastslå den fysiske persons identitet. Herudover omfattes også billeder, videoer og biometrisk data som værende en personoplysning.[24]. Ved personoplysninger skelnes der mellem tre typer af personoplysninger, henholdsvis almindelige personoplysninger, særlig kategori af personoplysninger og oplysninger om strafbare forhold. Derudover findes også fortrolige oplysninger, som dog ikke udtrykkeligt nævnes i databeskyttelsesreglerne. Hver kategori indebærer forskellige procedurer for behandling, men specialet fokuserer primært på behandlingen af almindelige personoplysninger samt følsomme oplysninger. [25] Til

[23] Samtykkebegrebet defineres i afsnit 3.3

[24] Kristian Korfits Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelseloven med kommentarer (Jurist- og Økonomforbundets Forlag 2020), s.237-240

[25] https://www.datatilsynet.dk/Media/637647832459647592/Personoplysninger%20-%20f%C3%A5%20et%20hurtigt%20overblik.pdf hentet 14-05-2025

behandlingen af de almindelige oplysninger kræver dette, at der findes et behandlingsgrundlag i artikel 6, stk.1, litra a-f. Behandlingen af følsomme oplysninger kræver imidlertid dobbelthjemmelsgrundlag, da der udover et behandlingsgrundlag i artikel 6, stk.1, litra a-f, også skal findes behandlingsgrundlag i artikel 9.

I konteksten med børn og deres brug af informationssamfundstjenester, er de personoplysninger, som behandles, ofte adfærdsmæssig data og præferencerelaterede data.[26] Denne behandling kan være problematisk, hvis barnets oplysninger behandles, selvom der ikke er afgivet gyldigt samtykke efter artikel 8, fordi der eksempelvis ikke er foretaget aldersverifikation. Præambelbetragtning 38 fastslår, at børn er en særlig sårbar gruppe, da de ofte ikke modne nok til at forstå konsekvenserne af databehandling, hvorfor der skal tages særligt hensyn, når der behandles personoplysninger om børn.

2.4.2 Behandling

GDPR artikel 4, nr. 2 definerer det databeskyttelsesretlige begreb ''*behandling*'', der forlyder: "*enhver aktivitet eller række af aktiviteter – med eller uden brug af automatisk behandling – som personoplysninger eller en samling af personoplysninger gøres til genstand for*". Også dette begreb er defineret med en tilsvarende ordlyd i persondatalovens § 3, nr. 2. Begrebet *''behandling''* omfatter alle former for håndtering af personoplysninger, herunder opbevaring, registrering, arkivering, systematisering mv. Hvor artikel 4, nr.2 opremser en række eksempler på behandlinger, er denne liste ikke udtømmende, hvorfor andre former for håndtering af personoplysninger, ligeledes vil være omfattet af begrebet. GDPR tillader dermed en bred fortolkning af begrebet, men inddeler det imidlertid efter automatisk behandling og ikke automatisk behandling, hvor den automatiske behandling er alt behandling foretaget ved hjælp af EDB. [27] I henhold til specialets fokus på beskyttelsen af børns personoplysninger ved brug af informationssamfundstjenester, fokuserer specialet primært på automatisk behandling.

26 Fundamentals for a child-oriented approach to data processing, December 2021, sektion 5.8

[27]Kristian Korfits Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelseloven med kommentarer (Jurist- og Økonomforbundets Forlag 2020), s.253

2.4.3 Dataansvarlig

Definitionen af begrebet ''*dataansvarlig*'' findes i GDPR artikel 4, nr. 7, hvori bestemmelsen beskriver en dataansvarlig som: "*en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger''.* Som følge heraf, pålægges den dataansvarlige ansvaret for, at alt databehandling overholder og opfylder kravene i GDPR. Dette skyldes at den dataansvarlige fastlægger til hvilket formål, personoplysningerne skal behandles, samt hvordan oplysningerne skal behandles, og hvem der må behandle dem. Det pålægges hermed den dataansvarlige at sikre, at der er hjemmel til behandlingen, at de registreredes rettigheder til hver en tid efterleves, og at behandlingssikkerheden overholdes i forbindelse med fastlæggelsen af formålet og de anvendte hjælpemidler som benyttes i forbindelse med behandlingen. Dette følger princippet om ansvarlighed, som den dataansvarlige skal overholde jf. GDPR artikel 5, stk. 2. Begrebsdefinitionen indeholder ikke nogen begrænsninger i forhold til hvem, der kan være dataansvarlig. Listen opremser udelukkende eksempler på dataansvarlige, som imidlertid kan være både fysiske personer, private virksomheder, foreninger mv.[28] Når der behandles personoplysninger om børn, pålægges den dataansvarlige særlige forpligtelser, herunder at sikre et gyldigt samtykke i relation til artikel 8. Desuden skal den dataansvarlige tage hensyn til, at de klassificeres som en særlig sårbar persongruppe, ved at tilpasse kommunikation og information til aldersgruppen.[29]

2.4.4 Informationssamfundstjeneste

Begrebet ''i*nformationssamfundstjeneste"* er defineret i artikel 1, stk. 1, litra b i Europa-Parlamentets og Rådets direktiv (EU) 2015/1535, hvorved der ved begrebet skal forstås enhver tjeneste, der normalt ydes mod betaling, og som teleformidles ad elektronisk vej på individuel anmodning fra en tjenestemodtager. De tjenester som er omfattet af definitionen, er eksempelvis online platforme som sociale medier, søgemaskiner, cloudtjenester og digitale

[28] Kristian Korfits Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelseloven med kommentarer (Jurist- og Økonomforbundets Forlag 2020), s.271
[29] Forordningen 2016/679 art.12, stk.1

markedspladser.[30] Specialet fokuserer primært på sociale medier som TikTok og Meta samt tjenesten ChatGPT, da netop disse platforme er lettilgængelige for og hyppigt benyttet af børn, hvilket taler for behovet for en særlig beskyttelse af deres personoplysninger.

I løbet af specialet, benyttes begrebet *online tjeneste* som synonym for informationssamfundstjeneste. Ligeledes benyttes begreberne *sociale medier* og *digitale tjenester*, som hører under kategorien informationssamfundstjenester.

2.4.5 De grundlæggende principper – artikel 5

I GDPR artikel 5, stk.1, litra a-f fremgår de grundlæggende principper for behandling af personoplysninger. Principperne udgør fundamentet for al behandling af personoplysninger inden for EU, hvorfor disse principper hidrører under den dataansvarliges ansvar, som altid skal sørge for at principperne overholdes jf. artikel 5, stk.2.

Principperne i litra a-f indeholder krav om lovlighed, rimelighed, gennemsigtighed, formålsbegrænsning, rigtighed, opbevaringsbegrænsning, integritet og fortrolighed. Specialet har primært fokus på principperne om lovlighed, rimelighed og gennemsigtighed samt dataminering, da disse principper fastsætter en standard om god behandlingsskik fra den dataansvarlige. Dette findes særligt relevant, når der behandles personoplysninger om børn, hvorfor behandlingen og information til den registrerede skal tilpasses aldersgruppen jf. art.12. Princippet om lovlighed, rimelighed og gennemsigtighed indebærer at information kommunikeres på en lettilgængelig og letforståelig måde, samt at det tydeliggøres, hvad formålet med behandlingen er. [31] Dataminimeringsprincippet indebærer, at behandlingen af personoplysninger begrænses til, hvad der er nødvendigt i forhold til formålet med behandlingen. Dette bidrager til at begrænse risikoen for misbrug og sikre unødvendig dataophobning.[32] Princippet er særligt relevant i relation til indsamling og behandling af personoplysninger om børn, hvor den dataansvarlige i forbindelse med verifikation af barnets

[30] Datatilsynets Vejledning om samtykke, maj 2021, s.18
[31] Kristian Korfits Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelseloven med kommentarer (Jurist- og Økonomforbundets Forlag 2020), s.314
[32] Kristian Korfits Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelseloven med kommentarer (Jurist- og Økonomforbundets Forlag 2020), s.328

alder, skal vælge den mindst indgribende metode til at opnå formålet, som er at kontrollere alderen på barnet.[33]

2.4.6 Barn

Som nævnt i kapitlets introduktion, findes der ikke en legaldefinition på begrebet ''*barn*'' i forordningen. Begrebet er dog anvendt i flere artikler, herunder artikel 8. Dog fremgår det imidlertid uklart, hvornår en person er et barn ifølge forordningen, hvilket kan have konsekvenser i forhold til beskyttelsesniveauet for børns personoplysninger.

I forarbejderne til forordningen, indeholdt EU-kommissionens forslag til forordningen, oprindeligt en generel definition af begrebet barn, som definerede alle personer under 18 år som værende børn.[34] Kommissionens intention med denne definition var, at det skulle stemme overens med FN's Børnekonventions definition på børn, som i artikel 1 definerer børn ved følgende:

> ''*I denne konvention forstås ved et barn ethvert menneske under 18 år, medmindre barnet bliver myndigt tidligere efter den lov, der gælder for barnet*''[35]

Denne definition tillader et nationalt råderum, i tilfælde af at nogle lande har en lavere myndighedsalder. Definition kom dog ikke med i den videre lovgivningsproces, på grund af uenigheder mellem medlemsstaterne om, hvorvidt der burde indsættes en fælles definition i GDPR. [36]

Artikel 29-gruppen (nu EDPB) har dog under det tidligere persondatadirektiv ligeledes defineret børn som alle personer under 18 år, hvorfor det antages at denne definition umiddelbart udgør den generelle forståelse af begrebet barn. Begrebet skal dog samtidig forstås fleksibelt, eftersom der kan være hensyn og forhold, som taler for en anden definition.

---

[33] EDPB Retningslinjer 4/2019 om artikel 25 Databeskyttelse gennem design og standardindstillinger, oktober 2020

[34] Proposal for a Regulation of the European Parliament and of the Councils on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Bruxelles januar 2012, COM (2012) 11 final, s..43

[35] FN's konvention af 20. november 1989 om Barnets Rettigheder, artikel 1

[36] Det fremgår ikke direkte hvorfor begrebet udgik, men begrebet kom ikke med i den endelig version af forordningen.

Dette kan eksempelvis være landendes individuelle opfattelse af modenhed samt den krævede mængde beskyttelse af deres personoplysninger.[37]

GDPRs artikel 8 og den tilhørende §6 stk.2 og stk.3 i databeskyttelsesloven definerer ikke direkte, hvad et barn er, men fastsætter en aldersgrænse i forhold til børns evne til at give samtykke i databeskyttelsesretlig forstand. Hvor GDPR fastsætter den aldersgrænse til 16 år, tildeler forordningen ligeledes et nationalt råderum til at fastsætte en aldersgrænse ned til 13 år. Her fastslår databeskyttelsesloven, at børn har kompetence til at give et gyldigt samtykke i Danmark, når de er 15 år.

[37] Artikel 29-gruppen nr.2/2009 om beskyttelse af børns personoplysninger, 11 februar 2009, WP 160

Kapitel 3 - Den retlige beskyttelse af børns personoplysninger

De følgende afsnit beskriver udviklingen i beskyttelsen af børns personoplysninger, og hvor hensynet til beskyttelse af deres oplysninger stammer fra. Herefter analyseres hvor beskyttelsen af børn er reguleret i forordningen. Eftersom den primære beskyttelse af børns personoplysninger fremgår i reglerne om samtykke til behandling af personoplysninger i forbindelse med udbud af informationssamfundstjenester, fokuseres der på samtykkebegrebet og det undersøges nærmere, hvordan et barn kan afgive et samtykke inden for databeskyttelsesretten. Herfor analyseres det generelle samtykkebegreb, og efterfølgende betingelserne for hvornår et barn kan give et gyldigt samtykke i artikel 8 og DBL §6, stk.2 og stk.3.

3.1 Den historiske udvikling i beskyttelsen af børns personoplysninger

Selvom beskyttelsen af personoplysninger har været reguleret i en del år i Danmark, er det dog nyt, at der er særskilt regulering af beskyttelsen af børns personoplysninger. Denne retsbeskyttelse kom med vedtagelsen af databeskyttelsesforordningen i 2018.

3.1.1 Persondatadirektivet

Før databeskyttelsesforordningen, var beskyttelsen af personoplysninger reguleret i persondatadirektivet, (Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger om fri udveksling af sådanne oplysninger), som blev vedtaget af EU-kommissionen i 1995 og implementeret i Danmark med persondataloven (Lov nr.429 af 31. maj 2000 og om behandling af personoplysninger) i 2000. Persondatadirektivet havde til formål at beskytte personoplysninger og sikre et højt niveau af sikkerhed i forbindelse med udvekslingen af personoplysninger på tværs af EU-landene.[38]

Der blev dog ikke taget nogle særskilte hensyn til børn og beskyttelsen af deres personoplysninger i persondatadirektivet. Dette kom blandt andet til udtryk ved at ordet

[38] Henrik Udsen, Databeskyttelsesret (www.databeskyttelsesret.dk, 2022), s.37

''*barn*'' ikke blev anvendt i direktivet, og beskyttelsen af børns personoplysninger blev derfor ikke særskilt reguleret i direktivet. Efterfølgende opstod der imidlertid overvejelser angående børns rettigheder, beskyttelsen af deres personoplysninger, og hvordan reglerne skulle fortolkes og anvendes i forhold til børn. Disse overvejelser gav anledning til en ændring af Den Europæiske Unions Charter om grundlæggende rettigheder (Chartret) ved indsættelsen af artikel 24 i Chartret, som angår beskyttelsen af børns rettigheder og har følgende ordlyd:

''Børn har ret til den beskyttelse og omsorg, der er nødvendig for deres trivsel. De kan frit udtrykke deres synspunkter. Der tages hensyn hertil i forhold, der vedrører dem, i overensstemmelse med deres alder og modenhed.

1. *I alle handlinger vedrørende børn uanset om de udføres af offentlige myndigheder eller private institutioner, skal barnets tarv komme i første række.*
2. *Ethvert barn har ret til regelmæssigt at have personlig forbindelse og direkte kontakt med begge sine forældre, medmindre dette er i modstrid med dets interesser''*[39]

Bestemmelsen afspejler de grundlæggende principper i Børnekonventionen, som er princippet om barnets bedste (artikel 3) og princippet om barnets ret til at blive hørt (artikel 12).

Som følge af vedtagelsen af Lissabontraktaten i 2009[40], blev Chartret juridisk bindende på traktatniveau, som betød, at EU-medlemsstaterne blev forpligtede til at beskytte rettighederne fra Chartret gennem EU-lovgivning.[41] På baggrund af denne udvikling og det generelle større politiske fokus på børns rettigheder, udkom Artikel 29-gruppen blandt andet også med en udtalelse, som specifikt vedrørte beskyttelsen af børns personoplysninger. I Artikel 29-gruppens udtalelse nr.2 af 2009, udstedte gruppen nogle retningslinjer for fortolkningen af persondatadirektivet i forhold til behandlingen af børns personoplysninger. I udtalelsen opfordrede gruppen blandt andet til at begrebet barn skulle defineres som alle personer under 18 år, således der var overensstemmelse i begrebets anvendelse på tværs af internationale regler. Herudover fastslog gruppen, at børn bør anses som en særlig persongruppe, eftersom

[39] Den Europæiske Unions Charter om grundlæggende rettigheder (2010/C83/02), art.24
[40] Lissabontraktaten om ændring af traktaten om Den Europæiske Union og traktaten om oprettelse af Det Europæiske Fællesskab, underskrevet i Lissabon den 13. december 2007
[41] Betænkning over Forslag til lov om ændring af lov om Danmarks tiltrædelse af de Europæiske Fællesskaber og Den Europæiske Union (Danmarks ratifikation af Lissabontraktaten), 14 marts 2008

de har brug for mere beskyttelse, da de endnu ikke har opnået den modenhed, som det kræver for at beskytte dem selv. [42]

På baggrund af dette, anførte Artikel 29-gruppen, at persondatadirektivets regler skulle fortolkes ud fra tre principper, som er princippet om barnets tarv, princippet om barnets ret til privatliv og princippet om retlig repræsentation. Det er gruppens overbevisning, at anvendelsen af principperne, vil sikre den nødvendige beskyttelse af børns personoplysninger. Princippet om barnets tarv, eller barnets bedste, er ifølge gruppen det vigtigste princip i fortolkningen af persondatadirektivet, når en behandling af personoplysninger angår et barn. Dette er på baggrund af princippets formål, som er at sikre, at der altid tages højde for, hvad der er bedst for barnet, og at der foretages en konkret vurdering i hver situation som omhandler beskyttelsen af et barns personoplysninger. Dette skal styrke barnets position i databeskyttelsesretten, således at der tages et skærpet hensyn til dataretlige principper, når behandlingen angår et barn.

I forhold til andet princip om barnets ret til privatliv, skal denne ret udøves af forældrene på barnets vegne, men selve retten til databeskyttelse angår imidlertid barnet.

Som følge af de ovenstående bemærkningerne fra Artikel 29-gruppen, anbefalede gruppen, at alle situationer, som udløser anvendelsen af persondatadirektivets regler, og som omhandler børn, bør inddrage de tre principper i fortolkningen af reglerne. Herved sikres, at der foretages en afvejning af barnets sikkerhed og behov.

Udtalelsen fra Artikel 29-gruppen satte gang i udviklingen af beskyttelsen af børns personoplysninger, da de anerkendte børn som en særlig persongruppe, som krævede ekstra beskyttelse.[43]

3.1.2 Persondataloven

Persondataloven blev implementeret sammen med persondatadirektivet i 2000.[44] Direktivet havde tildelt et råderum til at indføre nationale særregler, men Persondataloven udnyttede imidlertid ikke dette råderum til at indføre nogle regler vedrørende børn og beskyttelsen af

[43] Artikel 29-gruppen nr.2/2009 om beskyttelse af børns personoplysninger, 11 februar 2009, WP 160
[44] Lov 2000-05-31 nr.429 om behandling af personoplysninger

deres personoplysninger. Datatilsynet udgav dog en vejledning angående registreredes rettigheder i samme år, som loven blev vedtaget, hvor de blandt andet behandlede spørgsmålet om børns ret til indsigt i deres personoplysninger. Efterfølgende er denne rettighedsvejledning blevet brugt i afgørelser fra Datatilsynet, hvor det er blevet vurderet, at et barn kan samtykke til behandling af deres personoplysninger, når de var modne nok til at forstå konsekvenserne af et afgivet samtykke. Herved kan det konstateres, at vejledningen gav anledning til et øget fokus på børns samtykke i forbindelse med behandling af deres personoplysninger, selvom der endnu ikke eksisterende regler, som eksplicit regulerede beskyttelsen af børns personoplysninger i persondataloven.[45]

3.1.3 Databeskyttelsesforordningen

Som anført i afsnit 2.2, blev databeskyttelsesforordningen vedtaget den 25. maj 2018, og blev suppleret i Danmark med databeskyttelsesloven. I forordningen blev det anført, at børn bør nyde en særlig beskyttelse af deres personoplysninger, da de er kategoriseret som en særligt sårbar persongruppe[46]. Som anført i begrebsafklaringen, var forordningen den første regulering af børns personoplysninger, og den første til at anvende begrebet ''*barn*''. Begrebet er imidlertid ikke defineret i forordningen, men i forslaget til forordningen, er begrebet barn defineret som ''alle personer under 18 år'' jf. artikel 4 nr.18. Denne definition kom dog ikke videre med i lovgivningsprocessen på grund af uenighed omkring nødvendigheden af databeskyttelse for børn og omfanget heraf. Datatilsynet var af den overbevisning, at det ikke var muligt med en præcis definition af begrebet barn, da definitionen kan varierer fra medlemsstat til medlemsstat alt efter, hvornår børn opfattes som modne. Definitionen blev i forslaget derfor angivet som, at et barn var alle personer under 18 år. Forslaget indeholdt ligeledes også en regel om børns kompetence til at give samtykke, da det blev anført, at børn kunne samtykke til informationssamfundstjenester, som var udbudt direkte til børn, når de var fyldt 13 år.

I forslaget var der imidlertid også uenighed omkring, hvorvidt forordningen skulle indeholde to regler i forbindelse med databeskyttelse for børn. Udover reglen at børn kunne samtykke

[45] Datatilsynets Vejledning om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger (historisk og findes kun på retsinformation nu)
[46] Forordning 2016/679 pr.38

til benyttelse af informationssamfundstjenester når de var 13 år, blev det endvidere diskuteret, om forordningen skulle indeholde en ekstra regel, som definerede begrebet barn. Men da begrebet barn skulle defineres som alle personer under 18 år, ville dette ikke harmonere med samtykkereglen, som gav kompetence for børn til at samtykke, når de var 13 år.[47] Det bemærkes herefter, at definitionen af begrebet barn udgik af forslaget efter førstebehandlingen, og aldersgrænsen for hvornår et barn kan give samtykke ligeledes blev slettet, hvorfor der blev indført en formulering, som gav medlemsstaterne rum til at indføre national lovgivning for aldersgrænsen.

Generelt kan det udledes fra forarbejderne til lovforslaget, at der var uenighed omkring emnet om databeskyttelse for børns personoplysninger. Både definitionen af begrebet barn, samt nødvendigheden for regler på området. Selvom forordningen blev vedtaget med artikel 8, angående børns kompetence til at give samtykke i forbindelse med informationssamfundstjenester udbudt direkte til børn, fremgår det ikke af forarbejderne, hvorfor artiklen er udformet således, og ligeledes giver ordlyden anledning til spørgsmål, omkring anvendelsesområdet. Efterfølgende er der ligeledes blevet rejst kritik omkring beskyttelsen af børns personoplysninger. Dette afspejles eventuelt i den manglende praksis på området, da forvirring omkring reglens anvendelsesområde, har gjort reglen utilstrækkelig.

3.2 Børns samtykke og beskyttelsen af deres personoplysninger ved brug af onlinetjenester

Børn skal ifølge præambeltragtning nr.38 nyde en særlig beskyttelse i forhold til behandling af deres personoplysninger, da de er mindre bevidste om de risici og konsekvenser, som kan være forbundet med behandlingen af deres personoplysninger. Denne beskyttelse skal særligt være til stede, når der sker behandling af personoplysninger i forbindelse med markedsføring og ved indsamling af oplysninger på tjenester, der er rettet mod og tilbydes direkte til børn. Det er dog ikke yderligere præciseret, hvordan denne beskyttelse skal sikres, og som tidligere nævnt, er der heller ikke i forordningen taget stilling til, hvornår man er et barn efter forordningens forstand, udover i artikel 8 om børns samtykke ved brug af

[47] Commission Staff working paper Impact Assessment SEC (2012) 72 final, s.71

informationstjenester. Her fastlægges det, at et barn ikke kan give samtykke til brug af informationstjenester, før det er 16 år. Brug af informationstjenester før barnet er 16 år, vil være betinget af et samtykke fra indehaveren af forældremyndigheden. [48]

Det findes hertil relevant at undersøge, hvad samtykkebegrebet indebærer, og hvordan et barn kan afgive samtykke.

Eftersom den primære beskyttelse af børns personoplysninger er reguleret i denne artikel, vil analysen tage udgangspunkt i artikel 8, og de øvrige samtykkebestemmelser. For at kunne vurdere, hvordan og hvornår et barn kan afgive et gyldigt samtykke efter artikel 8, er det nødvendigt at klarlægge, hvad der forstås ved et samtykke som behandlingsgrundlag. Det er herfor en forudsætning, for at kunne forstå kravene, der stilles til et barns samtykke til brug af informationssamfundstjenester, at samtykkebegrebet analyseres nærmere.

3.3 Samtykket i databeskyttelsesretten

3.3.1 Definition af samtykke

Samtykke er defineret i forordningens artikel 4, nr.11, som forbinder et samtykke med enhver frivillig, specifik, informeret og utvetydig viljestilkendegivelse fra den registrerede, hvorved den registrerede ved erklæring eller klar bekræftelse indvilliger i, at personoplysninger, der vedrører den pågældende, gøres til genstand for behandling. Et samtykke er hermed et lovligt grundlag for en behandling af personoplysninger jf. artikel 6, stk.1, litra a.

3.3.2 Samtykket som behandlingsgrundlag

For at kunne påbegynde behandling af personoplysninger, skal en hjemmel til behandlingen findes. I forordningen, defineres denne hjemmel som et behandlingsgrundlag. Artikel 6, stk.1, litra a-f opremser de 6 behandlingsgrundlag, som giver adgang til at starte behandling af personoplysninger, alt efter hvad formålet med behandlingen er. Behandling er derfor kun lovlig, såfremt der foreligger et gyldigt behandlingsgrundlag. Er der tale om følsomme oplysninger, også kaldet særlige kategorier af oplysninger, er der et dobbelthjemmelskrav, og

[48] Marie Jull Sørensen og Tanja Kammersgaard Christensen, Samtykke i databeskyttelsesretten (Ex Tuto Publishin A/S, 2024) s.193

der skal udover et behandlingsgrundlag i artikel 6, stk.1, litra a-f, også findes behandlingsgrundlag i artikel 9

I artikel 6, stk.1, litra a er samtykke angivet som et gyldigt behandlingsgrundlag, og fastlægger at behandlingen er lovlig, hvis *''den registrerede har givet samtykke til behandling af sine personoplysninger til et eller flere specifikke formål*''. Udover at samtykket skal opfylde kravene i definitionen af samtykke i artikel 4, nr.11 som listet ovenfor, skal den, der afgiver samtykket også være retlig i stand til at afgive samtykket. Hermed forstås, at vedkommende skal være af en bestemt alder, og tillige skal vedkommende have mandat til at afgive samtykket. Når der behandles oplysninger på baggrund af et samtykke fra den registrerede, er det herudover, også en betingelse, at de grundlæggende principper i artikel 5 er opfyldt, herunder at behandling skal være i overensstemmelse med god databehandlerskik jf. artikel 5, stk.1, litra a. [49]

3.3.3 Betingelser for et gyldigt samtykke – artikel 5

Bestemmelsen opstiller fire krav til et gyldigt samtykke, navnlig at det skal være *frivilligt, specifikt, informeret* og *utvetydigt*.

Formålet med samtykket er således at give den registrerede frihed til at vælge, om de vil give samtykke til at deres oplysninger behandles eller ej, samt kontrol over hvilke oplysninger der behandles om vedkommende. En vigtig forudsætning er derfor, at samtykket er afgivet frivilligt. Det fremgår af EDPBs retningslinjer for samtykke, at samtykke ikke kan anses for at være givet frivilligt, hvis den registrerede reelt ikke har et valg i afgivelsen af samtykke, eller at den registrerede ikke kan nægte et samtykke, uden at det har negative konsekvenser. Ligeledes er der tale om et ufrivilligt samtykke, såfremt at det er knyttet til vilkår eller betingelser, og at det ikke kan forhandles.[50] Såfremt den registrerede ikke kan afvise behandlingen af deres personoplysninger, eller får vedkommende ikke muligheden for at trække deres samtykke tilbage uden skade, er der heller ej tale om et frivilligt samtykke.[51]

[49] Kristian Korfits Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelseloven med kommentarer (Jurist- og Økonomforbundets Forlag 2020), s.351-352

[50] EDPB Retningslinjer 5/2020 vedrørende samtykke i henhold til forordning 2016/679, s.6

[51] Datatilsynet Vejledning om samtykke, maj 2021, s.5

Ønsker den dataansvarlige at behandles oplysninger til flere forskellige formål, skal den registrerede have muligheden for at vælge, hvilke formål de samtykker til. Dette kaldes granularitet, da det samtykket opdeles. Såfremt proceduren for indhentning af samtykket ikke giver den registrerede mulighed for at give særskilt samtykke, kan samtykket ikke anses for at være givet frivilligt. [52]

I kravet om at samtykket skal være specifikt, indebærer dette, at det præcist skal fremgå, hvad den registrerede samtykker til. Samtykket skal derfor være konkretiseret, så det tydeligt fremgår, hvilket oplysninger der behandles, samt formålet med behandlingen. Samtykket må således ikke være udformet generelt og uklart. [53] Er der tale om forskellige formål med behandlingen, skal disse specificeres, således den registrerede er klar over, hvilke personoplysninger der behandles til hvert formål. Dette er knyttet til princippet om formålsbegrænsning i artikel 5, som angiver at personoplysninger skal indsamles til udtrykkeligt angivne og legitime formål.

Samtykket skal endvidere være informeret, hvilket hænger sammen med princippet om gennemsigtighed, og at den registrerede skal have mulighed for at træffe et valg om at afgive samtykke på et informeret grundlag. Herved pålægges den dataansvarlige således en oplysningspligt, da den registrerede skal have de nødvendige informationer på tidspunktet for anmodningen om samtykket. Dette indebærer, at den registrerede blandt andet bliver informeret om, hvad der gives samtykke til. Denne information skal fremgå letforståelig, lettilgængelig og i et klart og enkelt sprog, uden at indeholde urimelig vilkår jf. præambelbetragtning 42 og art.12.

Det er ligeledes et krav, at samtykket er en utvetydig viljestilkendegivelse fra den registrerede. Af præambelbetragtning 32 fremgår det, at viljestilkendegivelsen kan ske ved enten erklæring eller handling, som eksempelvis at afkrydse et felt på en hjemmeside. Forudafkrydsede felter anses dog ikke som en afgivelse af et gyldigt samtykke, da dette ikke kan anses som en utvetydig viljestilkendegivelse. Det afgørende er, at handlingen klart og tydeligt tilkendegiver

[52] Datatilsynets Vejledning om samtykke, maj 2021, s.6
[53] Datatilsynets Vejledning om samtykke, maj 2021, s.9

den registreredes samtykke og accept af den pågældende behandling. [54]

3.3.4 Yderligere betingelser til et gyldigt samtykke – artikel 7

I artikel 7 fremgår det blandt andet, at den dataansvarlige til hver en tid, skal kunne påvise, at den registrerede har afgivet samtykke til behandlingen af deres personoplysninger. Samtykket kan afgives både mundtlig og skriftligt, men eftersom et mundtligt samtykke er svært at dokumentere, bør en skriftlig erklæring altid indhentes af den dataansvarlig, da bevisbyrden for, at behandlingen er lovlig og behandlingsgrundlaget er til stede, pålægges den dataansvarlige jf. art.7, stk.1. Derudover skal samtykket kunne skelnes fra andre forhold, dvs. at samtykket ikke må gemmes blandt en lang kontrakt eller andet, samtykket skal være fremhævet eller præsenteret særskilt. [55]

Angår behandlingen følsomme oplysninger, skal samtykket endvidere være udtrykket jf. art. 9 stk. 2, litra a. Dette understreger vigtigheden af, at der ikke skal være tvivl om, hvorvidt den registrerede har givet samtykke til den pågældende behandling.

3.3.5 Tilbagekaldelse af samtykke

Den registrerede kan til hver tid trække sit samtykke tilbage, og den dataansvarlige skal sørge for, at dette kan gøres på en enkel og lettilgængelig måde, da det skal være lige så let at trække sit samtykke tilbage, som det er at give det. Lige så snart at den registrerede har trukket sit samtykke til tilbage, skal behandling af den registreredes oplysninger stoppe. Det påvirker dog ikke lovligheden af den behandling, som er sket inden tilbagekaldelsen, men alt behandling efter at den registrerede har trukket sit samtykke tilbage, anses for ulovlig behandling. Tilbagekaldelsen vedrører dermed kun den fremtidige behandling af den registreredes personoplysninger. [56]

[54] Kristian Korfits Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelseloven med kommentarer (Jurist- og Økonomforbundets Forlag 2020), s.269
[55] Kristian Korfits Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelseloven med kommentarer (Jurist- og Økonomforbundets Forlag 2020), s.409

[56] Kristian Korfits Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelseloven med kommentarer (Jurist- og Økonomforbundets Forlag 2020), s.410

Når samtykke er tilbagekaldt, har den registrerede ret til at få alle oplysninger om sig selv slettet, og uagtet at den registrerede anmoder om det, bør den dataansvarlige altid tage stilling til om oplysningerne bør slettes, i overensstemmelse med princippet om dataminimering. I enkelte tilfælde kan behandling fortsætte, til trods for et tilbagekaldt samtykke fra den registrerede. Dette kunne eksempelvis være i tilfælde, hvor den dataansvarlige kan finde et andet lovligt behandlingsgrundlag end samtykke, som opbevaring af oplysningerne i forbindelse med overholdelse af reglerne om bogføring. Fortsætter den dataansvarlige behandlingen af den registreredes oplysninger, skal den registrerede informeres om det nye behandlingsgrundlag samt formålet for behandlingen mv. [57] EDPB påpeger dog, at den dataansvarlige ikke kan skifte fra samtykke til andet behandlingsgrundlag, og at det vil være urimeligt over for den registrerede, at benytte samtykke som behandlingsgrundlag, hvis et andet grundlag alligevel kunne retfærdiggøre behandling. [58]

Efter specialets gennemgang af det databeskyttelsesretlige samtykkebegreb, fremstår det herefter nærliggende at fokusere på de særlige forhold, der gør sig gældende i forbindelse med børns afgivelse af samtykke. Den særlige status som en sårbar persongruppe i forordningen indebærer, at der opstilles skærpede krav til, hvordan og hvornår et barn kan give et gyldigt samtykke til behandling af personoplysninger. Dette gør sig særligt gældende i forbindelse med brugen af informationssamfundstjenester. De følgende afsnit vil herfor analysere de retlige rammer for børns samtykke, med fokus på artikel 8 i forordningen.

[57] Datatilsynets Vejledning om samtykke, maj 2021, s.16
[58] EDPB Retningslinjer 5/2020 vedrørende samtykke i henhold til forordning 2016/679, 2020 s.27

Kapitel 4 - Børns samtykke

Forordningen regulerer, hvornår et barn kan afgive et samtykke både offline og online. Hvor artikel 8 i forordningen regulerer det online, er det de ordinære samtykkeregler i artikel 4 og 7, som regulerer børns offlinesamtykke. Artikel 8 har derfor et begrænset anvendelsesområde, som ofte udløses af, at et barn opretter en profil på en social tjeneste, hvorved de kan give samtykke til behandlingen af deres personoplysninger såsom fødselsdato og mailadresse. Det online samtykke indebærer flere risici for barnet, da online tjenester potentielt indsamler flere oplysninger om barnet, end de selv er klar over, hvor et offline samtykke umiddelbart ikke behandler flere oplysninger, end barnet har kendskab til.

De oplysninger som udbyderen kan indsamle ved det onlinesamtykke uden at barnet er opmærksom på dette, er eksempelvis oplysninger om barnets adfærd og interesser, som barnet via deres handlinger på den pågældende tjeneste, udviser. Det er disse digitale spor, også kendt som adfærdsdata, som udbyderen kan indsamle om barnet. Denne form for data kan eksempelvis anvendes til profilering og målrettet markedsføring, hvilket understøtter behovet for en effektiv beskyttelse af børns personoplysninger. [59]

De følgende afsnit vil derfor undersøge barnets online samtykke i forbindelse med informationssamfundstjenester, som findes i forordningens artikel 8.

4.1 Indhentning af samtykke i forbindelse med informationssamfundstjenester

Den primære regulering og beskyttelse af børns personoplysninger, findes som nævnt i samtykkereglerne for indhentning af samtykke i forbindelse med informationssamfundstjenester, der udbydes direkte til børn. Som beskrevet i afsnit 2.4.4 omfatter informationssamfundstjenester eksempelvis platforme som Meta og TikTok.

[59] Fundamentals for a child-oriented approach to data processing, December 2021, sektion 5.8

Betingelserne for et barns samtykke i forbindelse med informationssamfundstjenester er reguleret i forordningens artikel 8. Bestemmelsen har følgende ordlyd:

Databeskyttelsesforordningen artikel 8

1. *Hvis artikel 6, stk.1, litra a), finder anvendelse i forbindelse med udbud af informationssamfundstjenester direkte til børn, er behandling af personoplysninger om et barn lovlig, hvis barnet er mindst 16 år. Er barnet under 16 år, er sådan behandling kun lovlig, hvis og i det omfang samtykke kan gives eller godkendes af indehaveren af forældremyndigheden over barnet. Medlemsstaterne kan ved lov fastsætte en lavere aldersgrænse til disse formål, forudsat at en sådan aldersgrænse ikke er under 13 år.*
2. *Under hensyntagen til den tilgængelig teknologi skal den dataansvarlige gøre sig rimelig bestræbelser på i sådanne tilfælde at kontrollere, at indehaveren af forældremyndigheden over barnet har givet eller godkendt samtykket.*
3. *Stk.1 berør ikke medlemsstaternes generelle aftaleret, som f.eks. bestemmelser om gyldighed, indgåelse eller virkning af en kontrakt, når der er tale om et barn.* [60]

Udover formålet med bestemmelsen, som er beskyttelsen af børns privatliv online, tager bestemmelsen imidlertid også højde for barnets modningsproces, da bestemmelsen fastslår, hvornår barnet har kompetence til at afgive et samtykke. Der var i det tidligere persondatadirektiv ikke indeholdt nogen bestemmelse om børns samtykke, så dette er en ny bestemmelse, som er direkte inspireret af den amerikanske COPPA-lovgivning. Det fremgår af forarbejder til forordningen, at der i udformningen af bestemmelsen, var uenighed om hvorvidt bestemmelsen skulle medtages i forordningen, da medlemsstaterne havde forskellige opfattelser af behovet for beskyttelse af børns personoplysninger. [61]Derfor blev bestemmelsen vedtaget som et kompromis, der ikke indeholder yderligere forklaring eller begrundelse for den endelige udformning, hvorfor nogle aspekter af bestemmelsen fremgår uklare. Dette omfatter blandt andet uklarhed omkring hvordan ''*informationssamfundstjenester*'' skal fortolkes, og hvornår sådan en tjeneste udbydes direkte til børn. Dette undersøges derfor nærmere efterfølgende.

[60] Forordning 2016/679 art.8
[61] Commission Staff working paper Impact Assessment SEC (2012) 72 final

4.1.1 Informationssamfundstjeneste udbudt direkte til børn

Informationssamfundstjenester er som beskrevet ovenfor, et bredt begreb, som omfatter de fleste kommercielle online-tjenester i informationssamfundet. Artikel 8 gælder dog kun for tjenester, som er udbudt direkte til børn, og hermed begrænses bestemmelsens materielle anvendelsesområde. Det fremgår imidlertid uklart af bestemmelsen, hvornår en informationssamfundstjeneste per definition udbyder direkte til børn, hvilket skaber uklarhed omkring, hvem der forpligtes af bestemmelsen.

Formuleringen kan forstås således, at der fastsættes krav til, at den pågældende tjeneste er indrettet specifikt til børn gennem eksempelvis indhold, sprog mv. og et alderskrav, som tydeligt illustrerer, at tjenesten henvender sig til børn. Denne fortolkning vil betyde, at bestemmelsen udelukkende forpligter udbydere, som har en målgruppen, der er børn eller personer under 18 år. Det vil imidlertid betyde, at flere udbydere af onlinetjenester, som indsamler personoplysninger om børn, ikke vil være omfattet og hermed forpligtet af bestemmelsen, da de netop ikke udbyder direkte til børn gennem deres indhold, sprog mv. I praksis udbydes der sjældent til målgruppen børn, hvorfor mange tjenester ikke vil være omfattet af forpligtelsen i artikel 8, hvis bestemmelsen fortolkes således. Dette betyder dog ikke, at børnene ikke benytter sig af de pågældende tjenester. Selvom eksempelvis Facebook og Instagram ikke udbyder direkte til børn, benytter mange børn helt ned til 13 år disse tjenester.[62] Derfor bør bestemmelsen ligeledes omfatte tjenester, som i princippet udbyder til voksne, da der kan forekomme brugere, som er børn. Dette pålægger udbyderen ansvaret for, at børns oplysninger bliver tilstrækkeligt beskyttet. Formuleringen direkte til børn bør derfor ikke fortolkes restriktivt, da formålet med bestemmelsen netop er at beskytte børns oplysninger, når de bruger onlinetjenester. Derfor bør udbyderen pålægges ansvaret for, at børns oplysninger blive behandlet med den fornødne sikkerhed, uagtet om tjenesten er designet med børn som målgruppe.

Dette understøttes af Artikel 29-gruppen, som anfører, at der bør lægges vægt på de faktiske omstændigheder og ikke blot udbyderens intention, når det vurderes, hvordan den pågældende hjemmeside opfattes fra brugerens side ud fra indholdet og markedsføringen. Når de faktiske

[62] https://www.ncbi.nlm.nih.gov/books/NBK594761/pdf/Bookshelf_NBK594761.pdf hentet 14-05-2025

omstændigheder viser, at brugere både er voksne og børn, forpligtes udbyderen derfor af online-tjenesten af samtykkekravet i artikel 8.[63]

Hertil opstår spørgsmålet så, hvorledes den dataansvarlige skal kontrollere, at brugeren af tjenesten er over aldersgrænsen jf. art. 8 og derfor kan give et gyldigt samtykke. Svaret på dette kan ikke findes i bestemmelsen, men forudsætter formentlig en aldersverifikation. (Uddybes i afsnit ''4.6. Verifikation af barnets alder''. Er tjenesten og indholdet imidlertid indrettet således, at det tydeligt fremgår, at tjenesten udelukkende udbydes til voksne, er udbyderen af tjenesten ikke omfattet af bestemmelsen. Dette støttes af EDPB, som udtaler:

''Formuleringen ''tilbydes direkte til et barn'' angiver, at artikel 8 er beregnet på nogle, men ikke alle informationssamfundstjenester. I denne forbindelse gælder det, at hvis en udbyder af informationssamfundstjenester gør det klart for potentielle brugere, at han eller hun kun tilbyder sin tjeneste til personer på 18 år eller derover, og dette ikke drages tvivl i anden dokumentation, opfattes tjenesten ikke som en tjeneste, der ''tilbydes direkte til børn'', og artikel 8 finder ikke anvendelse.'' [64]

Fra udtalelsen kan det udledes, at den dataansvarlige bliver pålagt en omvendt bevisbyrde, eftersom den dataansvarlige aktivt skal demonstrere, at tjenesten ikke henvender sig til børn. Dette bekræfter yderligere, at bestemmelsen skal fortolkes udvidende og ikke indskrænkende.

4.2 Regulering af børns samtykke i databeskyttelsesloven

Barnets samtykke er yderligere reguleret i DBL, som supplement til GDPR, hvor det i §6, stk.2 fremgår, at behandling af personoplysninger af børn, er lovlig hvis barnet har samtykket til behandlingen og er mindst 15 år. Når barnet har denne alder, kan barnet dermed selv give samtykke til at anvende informationssamfundstjenester. [65]

Er barnet under 15 år, er behandlingen kun lovlig, hvis samtykke er givet eller godkendt af indehaveren af forældremyndigheden over barnet jf. §6, stk.3. Bestemmelsen er en direkte implementering af det nationale råderum, som GDPR tillader i forhold til at fastsætte en

[63] Artikel 29-gruppen Retningslinjer vedrørende samtykke i henhold til forordningen 2016/679, 28. november 2017, vedtaget 10. april 2018, WP 259
[64] EDPB Retningslinjer 5/2020 vedrørende samtykke i henhold til forordningen 2016/679, 4 maj 2020, s.29
[65] Kristian Korfits Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelseloven med kommentarer (Jurist- og Økonomforbundets Forlag 2020), s.1015

national aldersgrænse mellem 13 og 16 år. I Danmark blev aldersgrænsen til at afgive et samtykke først sat til 13 år, men senere hævet til 15 år. Årsagen hertil uddybes afsnit 4.4 *''Forhold der blev lagt vægt på i fastsættelsen af aldersgrænsen*''.

Det fremgår dog af præambelbetragtning 38, at samtykke fra indehaveren af forældremyndigheden ikke er nødvendigt, såfremt der er tale om forebyggende eller rådgivende tjenester, som tilbydes direkte til et barn. Et eksempel på dette, er BørneTelefonen, hvor samtykket fra forældremyndighedsindehaveren heller ikke er nødvendigt, selvom barnet er under 13 år. Dette demonstrerede Datatilsynet allerede i en afgørelse fra 2014.[66]

I afgørelsen fra den 8. januar 2014, foretog Datatilsynet en vurdering af Børns Vilkårs behandling af personoplysninger om børn, som de indsamlede, når børn benyttede sig af BørneTelefonen og organisationens e-mailrådgivning. Oplysningerne som blev behandlet omfattede blandt andet i begrænset omfang almindelige personoplysninger som navn, alder og telefonnummer samt følsomme oplysninger (særlig kategori af personoplysninger), som helbredsoplysninger og oplysninger om seksuelle og familiemæssige forhold. Dermed skulle Datatilsynet vurdere, om behandling af særligt de følsomme personoplysninger kunne ske uden samtykke fra forældrene, da formålet med indsamlingen var at yde rådgivning og hjælp til børnene.

Datatilsynet konkluderede i afgørelsen, at Børns Vilkår gerne måtte behandle følsomme oplysninger om børn uden et forældresamtykke, når oplysningerne blev indhentet med et formål om rådgivning, som skete i barnets tarv. Hertil henviste Datatilsynet til det daværende databeskyttelsesdirektiv og principperne om barnets tarv og proportionalitet, og fastslog, at den behandling, som Børns Vilkår foretog, var nødvendig for at kunne yde effektiv støtte og rådgivning, hvorfor behandling skete på baggrund af et grundlag, som ikke krævede samtykke. Datatilsynet fastslog ligeledes, at et barn, som er i stand til selv at søge rådgivning hos Børns Vilkår, og dermed selv afgiver personoplysninger, umiddelbart også er i stand til at give et gyldigt samtykke til behandling af deres personoplysninger.

Selvom denne afgørelse er afsagt før GDPR's og den nuværende databeskyttelseslovens ikrafttræden, findes den relevant i forhold til præambelbetragtning 38 til GDPR. Denne fastslår ligeledes at samtykke fra forældremyndighedsindehaverens ikke er nødvendigt, når

[66] https://www.datatilsynet.dk/afgoerelser/historiske-afgoerelser/2014/jan/behandling-af-personoplysninger-hos-boerns-vilkaar hentet 14-04-2025

behandling sker med et rådgivende eller forebyggende formål. Præambelbetragtningen og afgørelsen udgør herfor en undtagelse til GDPR's artikel 8 og DBL §6, stk.3. Af dette kan det udledes, at reglerne om samtykke til behandling af børns personoplysninger ikke må fortolkes restriktivt, hvis formålet med behandlingen er rådgivning eller beskyttelse af barnet, eftersom dette fjerner barnets adgang til hjælp og/eller beskyttelse.

4.3 Børns habilitet til at give samtykke og kontrol af forældresamtykke

Når en dataansvarlig skal behandle personoplysninger om et barn baseret på et samtykke, skal den dataansvarlige tage stilling til, om barnet selv kan give samtykke til behandlingen, eller om der skal indhentes samtykke hos forældremyndighedsindehaveren.

Når samtykket indhentes i forbindelse med udbud af en informationssamfundstjeneste direkte til børn, skal barnet være mindst 15 år for at kunne give samtykke i Danmark jf. DBL §6, stk.2. Såfremt barnet er under denne aldersgrænse, skal den dataansvarlige indhente et samtykke fra forældremyndighedsindehaveren jf. DBL §6, stk.3.

Det fremgår endvidere af forordningens artikel 8, som fastslår, at den dataansvarlige har pligt til at kontrollere, at der er givet eller godkendt samtykke fra indehaveren af forældremyndigheden, og at dette er foretaget med rimelige bestræbelser og under hensyn til den tilgængelige teknologi. Artiklen uddyber dog ikke yderligere, hvad dette indebærer. Det pålægger derfor den dataansvarlige at vurdere, hvornår denne indsats fremgår tilstrækkelig, hvorfor det overlades til den dataansvarlige at foretage et skøn. Forordningen angiver heller ikke hvilke metoder, som den dataansvarlige skal benytte til at verificere samtykket.

Artikel 29-gruppen anfører hertil, at indsatsen skal være forholdsmæssig og proportional, hvilket betyder, at den dataansvarlige kun skal indsamle de oplysninger, som er nødvendige for at verificere forældresamtykket, og indsatsen skal være proportional med risikoen for barnets databeskyttelse. [67] Kravene til indsatsen afhænger samtidig med de tilgængelige teknologiske løsninger, hvorfor den nødvendige indsats løbende kan ændre sig ifølge med den teknologiske udvikling. Endvidere kan der være store forskelle i tjenesteudbyderes ressourcer og kapacitet, hvilket kan resultere i differentiation i den benyttede teknologi.

[67] EDPB Retningslinjer 5/2020 vedrørende samtykke i henhold til forordningen 2016/679, 4 maj 2020, s.30

Selvom der således sættes visse krav til indsatsen i at verificere et samtykke, så er kravene formuleret vagt og udbydere kan have forskellige indsatsformer til verificeringen, som løbende kan ændre sig i takt med teknologiens udvikling. Dette gør det svært at vurdere, hvornår den dataansvarlige har opfyldt sin pligt til at kontrollere samtykket og opfyldt kravet om at foretage rimelig bestræbelser for denne verificering.

Datatilsynets *''Vejledning om samtykke''* og GDPR overlader det i høj grad til den enkelte udbyder at vurdere, hvordan alder og samtykke kontrolleres, og opstiller ikke nogen konkrete metoder for, hvordan dette skal gøres. Derimod angiver eksempelvis den amerikanske COPPA-lovgivning og det amerikanske tilsyn Federal Trade Commission (FTC) en liste med specifikke og accepterede metoder til at kontrollere alder og samtykke, herunder indtastning af kortoplysninger, underskrevet samtykkeerklæring, telefonisk samtykke mv. Hertil påpeges det, at den valgte metode skal være passende i forhold til risikoen ved benyttelsen af den enkelte tjeneste. Hvis tjenesten eksempelvis giver mulighed for offentlig deling af personoplysninger, vil dette kræve en mere sikker verifikationsmetode. Tilsynet fortager ligeledes løbende evalueringer af, om nye teknologier kan anvendes til verificeringen af gyldigt samtykke. [68]

4.4 Forhold der blev lagt vægt på i fastsættelsen af aldersgrænsen på 13 år i DBL

I vedtagelsen af databeskyttelsesloven i 2018, udnyttede Danmark som tidligere nævnt, dette nationale råderum, som GDPR tillader, ved at sætte aldersgrænsen til 13 år, som er det laveste, alderen kan fastsættes til. Dette blev begrundet med, at danske børn allerede var meget medievante, og at adgangen til tjenester som Snapchat og Instagram har en stor social og samfundsmæssig betydning for børnene og dannelsen af sociale fællesskaber. Man lagde vægt på, at en højere aldersgrænse kunne medføre, at nogle børn blev udelukket fra fællesskabet, hvis adgangen til en tjeneste var betinget af et samtykke fra forældremyndighedsindehaveren, som potentielt ikke ville give samtykke til barnets adgang. Dette kunne have den konsekvens,

[68] https://www.ftc.gov/business-guidance/privacy-security/verifiable-parental-consent-childrens-online-privacy-rule hentet 14-05-2025

at børn ville udgive sig for at være ældre, end de egentlig var, for at få adgang til sociale tjenester. [69]

I fastsættelsen af aldersgrænsen på 13 år, var fokus på barnets frihed, da man ikke vil begrænse barnets frihed, ved at sætte en højere aldersgrænse, eller kræve godkendelse fra forældremyndighedsindehaveren. Da forældre principielt kan nægte barnet adgang til diverse tjenester, ville dette fratage barnets frihed. Det danske justitsministerium foreslog derfor aldersgrænsen skulle være 13 år, da det mentes, at børnene ville nyde høj beskyttelse i forordningen uanset aldersgrænsen. [70]

4.4.1 Hævelse af aldersgrænsen fra 13 til 15 år

I juni 2022 nedsætter den danske regering en ekspertgruppe af folk fra erhvervslivet om tech-giganter (udbydere som Meta og TikTok), med det formål at understøtte regeringens arbejde i forhold til at håndtere problemstillinger forbundet med tech-giganternes forretningsmodeller. Hertil skulle gruppen afrapportere om tech-giganternes ansvar over for børn med anbefalinger om eventuelle tiltag i forhold til beskyttelse af børn på internettet. En af de anbefalinger, som gruppen fremsætter, er blandt andet at aldersgrænsen for et barns samtykke i forbindelse med udbud af informationssamfundstjenester, skal hæves fra 13 år til 16 år. Ekspertgruppen påpeger, at tech-giganterne i tilfælde af at barnet er under 16 år, vil skulle indhente samtykke fra forældrene for at kunne behandle oplysninger om børn, og at flere mindreårige herfor vil kunne nyde den beskyttelse, som databeskyttelsesforordningen tildeler dem.

I deres anbefalinger henviser ekspertgruppen fra erhvervslivet blandt andet til at den nuværende aldersgrænse på 13 år følger den amerikanske Children's online Privacy Protection Act, COPPA, som på daværende tidspunkt også forsøgtes hævet til 16 år. Dette blev imidlertid ikke vedtaget, hvorfor aldersgrænsen til at give samtykke til brug af informationssamfundstjenester i USA stadig ligger på 13 år.

Desuden lægger ekspertgruppen også vægt på, at en række EU-lande som Tyskland, Holland og Irland har fastsat en aldersgrænse på 16 år. Samtidig lægges der vægt på, at den øgede

[69] Marie Jull Sørensen og Tanja Kammersgaard Christensen, Samtykke i databeskyttelsesretten (Ex Tuto Publishin A/S, 2024) s.196
[70] Betænkning 79 over Forslag til lov om ændring af databeskyttelsesloven og lov om Det Centrale Personregister, 2023/1

online tilstedeværelse, kan være skadelig for børn, da visse former for indhold kan have negative konsekvenser for blandt andet trivsel. [71]

På baggrund af ekspertgruppens konklusioner, vælger den danske regering at fremsætte et lovforslag, hvori de foreslår af hæve aldersgrænsen for, hvornår et barn kan give samtykke til behandling af deres personoplysninger i forbindelse med brug af informationssamfundstjenester. Det danske justitsministerium henviser til, at børn og unge har et særligt behov for beskyttelse, som GDPR også foreskriver, og navnlig i forhold til indhold, som ikke er aldersvarende til børn, og som kan påvirke deres adfærd. Med en højere aldersgrænse, skal forældremyndighedsindehaveren godkende barnets samtykke eller selv samtykke til barnets brug af informationssamfundstjenester i tilfælde af, at barnet er under den påkrævende aldersgrænse. Justitsministeriet pointerer at formålet med at hæve aldersgrænsen, er at øge bevidstheden hos børnene og forældrene i forhold til de risici, som kan være forbundet med at give informationssamfundstjenesterne adgang til at behandle deres personoplysninger som risiko for profilering og overvågning. Ligeledes var formålet at øge eftertænksomheden vedrørende børns færden på online tjenester. På baggrund af dette, foreslog Justitsministeriet af hæve aldersgrænsen til 15 år, som harmonerer med øvrige aldersgrænser, der gælder i Danmark for blandt andet den kriminelle og seksuelle lavalder.[72]

Lovforslaget blev generelt positivt modtaget blandt danske organisationer, da et høringssvar blev sendt ud til relevante aktører og myndigheder med en interesse i lovforslagets indhold. I et svar fra IT-Politisk Forening stiller de sig imidlertid kritisk ved, om hævelse af aldersgrænsen reelt vil give børn den særlige beskyttelse som GDPR foreskriver at børn skal nyde. Foreningen mener, som den danske regering også lagde vægt på i 2018 da aldersgrænsen blev fastsat til 13 år, at en højere aldersgrænse blot vil øge risikoen for at børn udgiver sig for at være ældre end de reelt er, og at det er tvivlsomt om en høj aldersgrænse vil medføre en øget integritetsbeskyttelse. IT-Politisk Forening pointerer endvidere, at ekspertgruppens argument med at flere mindreårige vil nyde den særlige beskyttelse som GDPR giver, ikke er afhængig af, om barnet selv eller barnets forældre har givet samtykke til behandling af barnets oplysninger. Foreningen vurderer, at lovforslaget reelt kan resultere i en dårligere beskyttelse

[71] https://www.em.dk/Media/638314161358806766/anbefalinger-fra-tech-ekspertgruppe.pdf hentet 14-05-2025

[72] Forslag til lov om ændring af databeskyttelsesloven og lov om Det Centrale Personregister, L79, 2023/1

af børns personoplysninger. [73] Lovforslaget blev imidlertid vedtaget i december 2023, og trådte således i kraft 1. januar 2024. Om hævelsen af aldersgrænsen for at give samtykke til 15 år, har medført en bedre eller dårligere beskyttelse af børns personoplysninger, er endnu ukendt, men i medfør af den nye aldersgrænse, er der blevet sat spørgsmålstegn ved, om sociale medier overholder reglerne om børns samtykke.

4.4.2 Sociale medier som Facebook og TikToks behandling af oplysninger om børn

I et brev til Datatilsynet har Børns Vilkår henvendt sig i forbindelse med aldersgrænsen for samtykke og børns adgang til sociale medier. I brevet oplyser Børns Vilkår, at sociale platforme som Facebook og TikTok ikke overholder reglerne omkring aldersgrænser for brugen af sociale medier og det samtykke, som børn afgiver for at få adgang til pågældende medier. I henvendelsen anføres Børns Vilkår:

''at de sociale medier ikke overholder de nationalt fastsatte aldersgrænser, herunder aldersgrænsen i den danske databeskyttelsesloven, som gælder for samtykke i forbindelse med informationssamfundstjenester direkte til børn''

Datatilsynet bekræfter, at sociale medier, som er informationssamfundstjenester, er omfattet af databeskyttelseslovens § 6, stk. 2, hvorefter behandling af personoplysninger baseret på samtykke forudsætter, at barnet er mindst 15 år. Dog er det Datatilsynets vurdering, at de sociale medier typisk ikke behandler oplysninger om børnene baseret på samtykke, men derimod på kontraktgrundlag i henhold til databeskyttelsesforordningens artikel 6, stk. 1, litra b. Dette indebærer, at aldersgrænsen for at afgive et samtykke ikke nødvendigvis har betydning for børnenes adgang til sociale medier. Spørgsmålet om, hvorvidt børn kan indgå en gyldig kontrakt, reguleres ikke af databeskyttelsesretten, men af aftaleretlige regler, hvilket falder uden for Datatilsynets kompetence. [74]

Af Datatilsynets svar kan det udledes, at et samtykke som udgangspunkt ikke anvendes som det primære behandlingsgrundlag, når et barn opretter en profil på en

[73] https://www.ft.dk/samling/20241/lovforslag/l22/bilag/2/2920934.pdf hentet 14-05-2025
[74] https://www.datatilsynet.dk/Media/638501550348383386/Brev%20til%20b%C3%B8rns%20vilk%C3%A5r.pdf hentet 14-05-2025

informationssamfundstjeneste som Facebook og TikTok, og tjenesten herefter behandler oplysninger om barnet. Det behandlingsgrundlag som oftest benyttes, er, at oplysningerne indsamles som led i et kontraktforhold. Hvorvidt barnet kan indgå en gyldig kontrakt, er således ikke noget som GDPR og Datatilsynet kan tage stilling til, og her ses begrænsningerne i GDPR og databeskyttelseslovens beskyttelse af børns personoplysninger.

I et samrådsspørgsmål fra Folketingets udvalg for Digitalisering og IT, er Justitsministeriet blevet anmodet om at svare på, hvad der netop skulle forstås ved at brugeroprettelsen på sociale medier ofte sker på andet grundlag end samtykke, som mediet Snapchat eksempelvis henviser til, når de fraviger det danske lovgrundlag med en aldersgrænse for at afgive samtykke på 15 år.

Hertil svarer det danske justitsministerium, at en brugeroprettelse på mange sociale medier sker på baggrund af en kontrakt mellem platformen og brugeren, og at aldersgrænsen på 15 år ikke nødvendigvis forhindrer et barn under 15 år i at oprette en profil på en social platform. Juridisk set er der forskel på at afgive et ''*ja*'' i en kontaktmæssig sammenhæng og at afgive et samtykke.

Derfor fremhæver Justitsministeriet også, at de vil undersøge, om det er muligt at nedlægge et forbud mod at sociale medier kan indgå kontrakter med børn under en bestemt alder, således de udelukkes fra at kunne oprette profiler på sociale medier. Om dette er muligt, har Justitsministeriet endnu ikke fundet en konklusion på.[75]

4.5 Det irske datatilsyns praksis i forhold til beskyttelsen af børns personoplysninger og håndhævelse af artikel 8

Det følgende analyseafsnit vil sammenligne den danske regulering og håndhævelse af reglerne vedrørende beskyttelsen af børns personoplysninger i forbindelse med afgivet samtykke til informationssamfundstjenester med den irske regulering og håndhævelse. Den irske tilgang findes relevant, da mange udbydere af informationssamfundstjenester har hovedsæde i Irland,

[75] https://www.ft.dk/samling/20231/almdel/diu/spm/174/svar/2052175/2873347/index.htm hentet 14-05-2025

hvorfor det er den irske tilsynsmyndighed, som primært håndterer håndhævelsen af reglerne. Herfor fokuseres på tilsynsmyndighedernes praksis og vejledninger.

Det danske datatilsyns praksis i forhold til overholdelse af forordningens artikel 8, og DBL §6, stk.2 og stk.3, fremgår primært som udbud af vejledninger frem for afgørelser. Der foreligger endnu ikke meget praksis i Danmark, hvor online tjenester er blevet sanktioneret for manglende overholdelse af bestemmelserne, eller ulovlig behandling af børns personoplysninger på baggrund af et ugyldigt samtykke efter DBL §6, stk.3. En væsentlig årsag hertil, er, at mange af de hyppigst benyttede informationssamfundstjenester, er etableret i andre EU-lande, hvorfor det ligger uden for det danske datatilsyns myndigheds kompetence at træffe afgørelser i sager mod disse tjenester. Nogle af de mest benyttede informationssamfundstjenester er netop sociale medier som Facebook (Meta), som har hovedsæde i Irland, hvorfor det irske datatilsyn er den primære tilsynsmyndighed. Dette betyder imidlertid, at børn i Danmark, som benytter de pågældende tjenester, er afhængige af håndhævelse af reglerne i landet, hvor tjenesten udbydes.

I Irland har de implementeret GDPR med den nationale Data Protection Act 2018[76], hvori de har fastsat en aldersgrænse på 16 år til at give samtykke i forbindelse med udbud af informationssamfundstjenester. Denne aldersgrænse differentierer sig herfor med et år fra den danske på 15 år. Beslutningen om en aldersgrænse på 16 år i Irland blev truffet på baggrund af, et ønske om at styrke beskyttelsen af børn i forhold til kommerciel udnyttelse, såsom profilering og målrettet markedsføring.[77]

Det irske datatilsyn, the Data Protection Commission (DPC) offentliggjorde efterfølgende i 2021 vejledningen *''Fundamentals for a Child-Oriented Approach to Data Processing''* om behandling af børns personoplysninger. Heri introducerer tilsynet 14 principper, som de anbefaler, at organisationer følger, når de behandler børns personoplysninger. Formålet med vejledningen er at fremme lovlig databeskyttelsespraksis, som tager hensyn til og respekterer børns sårbarhed i den digitale verden.

Det irske datatilsyn påpeger, at aldersverifikation ikke er valgfrit, men en pligt for den dataansvarlige at kontrollere, når der skal behandles oplysninger om børn. Endvidere fastslår

[76] Data Protection Act, 25 maj 2018 (Irland)
[77] https://www.dataprotection.ie/sites/default/files/uploads/2023-04/DPC_ChildrensData_ParentalConsent.pdf hentet 14-05-2025

tilsynet, at udbyderen skal behandle alle brugere som børn, hvis de ikke har implementeret et system til at verificere brugerens alder. I sådanne tilfælde, skal udbyderen benytte standardindstillinger, som tager højde for alle brugere behandles som børn. Dette følger princippet, som vejledning kalder *floor of protection*.

Yderligere fremhæver vejledningen i princippet om parental *consent & child's evolving capacity*, at et samtykke fra en forælder ikke fritager den dataansvarlige for ansvaret i tilfælde af, at barnet ikke forstår behandlingen af deres personoplysninger. Gyldigheden af et samtykke forudsætter herfor, at informationen er formildet på en sådan måde, at barnet også kan forstå det.

I forbindelse med aldersverifikation af barnets alder, fastslår princippet *proportionality in verifation* imidlertid, at aldersverifikationen skal være effektiv, men ikke uforholdsmæssigt indgribende, hvorfor der foretrækkes indikatorbaserede metoder til at verificere alderen frem for identifikatorer som et upload af eksempelvis kørekort eller pas.

Vejledningen konkretiserer således, hvordan udbydere i praksis kan respektere børns særstilling i GDPR ved at sætte nogle skærpede krav til samtykke, aldersverifkation og standardindstillinger. Selvom DPC's anbefalinger ikke er juridisk bindende i Danmark, har de alligevel en betydelig værdi i forhold til fortolkningen af reglerne vedrørende beskyttelse af børns personoplysninger gennem eksempelvis privacy by design i artikel 25. Derudover er Irland, som nævnt indledningsvis, også hovedsæde for mange af de største tech-giganter, som Facebook (Meta), hvorfor den irske tilsynsmyndigheds fortolkning og håndhævelse af GDPR reglerne overfor disse virksomheder, fungerer som en retningsgiver i vurderingen af, hvordan reglerne anvendes i forhold til børn. [78]

4.6 Verifikation af barnets alder

EDPB (tidligere Artikel 29-gruppen) anbefaler ligeledes i ''*Retningslinjer 5/2020 vedrørende samtykke i henhold til forordning 2016/679''*, at der indføres aldersverifikation af børn, i overensstemmelse med princippet om beskyttelse af børns personoplysninger samt hensynet til børns ret til privatliv og selvbestemmelse. Herved kan den dataansvarlige identificere børn

[78] Fundamentals for a child-oriented approach to data processing, December 2021

under 15 år, som ikke selv er i stand til at give samtykke til behandling. Derudover understøtter princippet om ansvarlighed, at det kontrolleres, om brugerne af en onlinetjeneste, er gamle nok til at benytte tjenesten. I Datatilsynets vejledning om samtykke, anfører de, at

''*Udbydere af informationssamfundstjenester direkte til børn skal sikre beskyttelse ved at indbygge mekanismer, så børn under den fastsatte aldersgrænse udelukkes fra at give samtykke i forbindelse med f.eks. oprettelse af en profil. Kontrol af brugerens alder eller samtykke fra indehaveren af forældremyndigheden bør ske under inddragelse af de risici, der er forbundet med behandlingen og den tilgængelige teknologi*.''[79]

Datatilsynet anfører således, at udbyderen af tjenesten, skal inkorporerer tekniske foranstaltninger i tjenesten, som kan udelukke børn under 15 år fra at benytte tjenesten. Det er dog uklart, hvorvidt den dataansvarlige har en pligt til at kontrollere barnets alder, da ikke umiddelbart fremgår af artikel 8. Ligeså er der ikke udarbejdet en fælles teknisk løsning, som kan benyttes af alle dataansvarlige til at verificere alderen, hvorfor det kan være uforholdsmæssigt at pålægge den dataansvarlige en pligt, som ikke kan opfyldes i praksis.

Denne uklarhed synes netop at have haft praktiske konsekvenser. Flere afgørelser, herunder en afgørelse fra det irske datatilsyn om TikTok (TikTok-sagen) og to afgørelser fra det italienske datatilsyn om ChatGPT (ChatGPT-sagen) og en AI-chatbot (Replika-sagen), har påpeget manglen på effektive aldersverifikationsmekanismer, som en væsentlig overtrædelse af forordningen, hvilket kunne indikere tegn på et hul i den nuværende lovgivning.

Til trods for vejledningerne fra tilsynsmyndigheder, viser praksis betydelige mangler i implementeringen af aldersverifikation. Dette illustreres gennem en nærmere analyse af disse centrale afgørelser fra europæiske datatilsyn.

4.6.1 ChatGPT-sagen

I en afgørelse fra december 2024 af det Italienske Datatilsyn (GPDP), kritiserer tilsynet OpenAI's ChatGPT for ulovlig indsamling af personoplysninger og manglende verificering af mindreåriges alder, hvorfor de blev pålagt en bøde på 15 millioner Euro for overtrædelse af GDPR. Tilsynet konkluderer i afgørelsen, at OpenAI ikke har indført en effektiv

[79] Datatilsynet, Vejledning om samtykke, maj 2021, s.18

aldersverificerende kontrol, som kan udelukke børn under 13 år for at få adgang til upassende indhold på tjenesten. Her blev der lagt vægt på, at ChatGPT tillod at børn under 13 år kunne udsætte for svar, som ikke tog højde for deres alder og udviklingsniveau.

GDPD anførte, at websiden havde overtrådt flere bestemmelser i GDPR, herunder princippet om lovlighed, rimelighed og gennemsigtighed i artikel 5, stk.1, litra a samt artikel 25 om databeskyttelse gennem design og standardindstillinger, ved ikke at udelukke mindreårige fra siden ved aldersverifikation.

Tilsynet forbød herfor adgangen til ChatGPT i Italien og gav virksomheden en frist på 20 dage til at dokumentere overholdelse af lovgivningen. Forbuddet blev ophævet, da OpenAI gennemførte en række ændringer i systemet, som blandt andet sikrede brugerne detaljeret information om, hvilke personoplysninger de indsamler, og hvordan de behandles. Endvidere skulle brugere, som allerede havde en konto på tjenesten bekræfte at de var myndige for at fortsat kunne benytte tjenesten. Derimod skal nye brugere nu angive deres fødselsdato ved oprettelsen af en bruger, hvorfor brugere under 13 år automatisk bliver udelukket fra tjenesten, medmindre der gives samtykke fra forældremyndighedsindehaveren. Endeligt blev OpenAI, med henblik på at sikre effektiv gennemsigtighed, også pålagt at skulle gennemføre en seks måneders informationskampagne i tv, aviser og på internettet som den italienske nationale implementering af forordningen (Italien Privacy Code) tillader. Denne kampagne skulle godkendes af tilsynsmyndigheden, og have fokus på at fremme forståelsen for, hvordan ChatGPT virker, særligt i forhold til hvilke oplysninger, som tjenesten indsamler og behandler og samt brugerens rettigheder, herunder retten til indsigelse og sletning. [80]

4.6.2 Replika-sagen

Det italienske datatilsyn traf ligeledes også afgørelse i en lignende sag fra februar 2023 mod den amerikanske AI-chatbot app, Replika, som havde overtrådt flere bestemmelser i GDPR i forbindelse med behandling af børns personoplysninger.

Replika blev udbudt og markedsført som en virtuel og følelsesmæssig assistent, som tilbød terapeutisk støtte og kunne agere som en ven for brugeren. Appen blev klassificeret som egnet

[80] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10085432 hentet 14-05-2025

for brugere over 17 år, men havde i praksis hverken implementeret aldersverifikation eller adgangsbegrænsning, da brugereoprettelsen blot krævede en indtastning af navn, e-mail og køn. Replika blev herudover kritiseret for at udbyde upassende indhold til børn, hvilket for en app som skulle agere som pædagogisk støtte og forbedre humøret på brugeren, fandtes kritisabelt da dette sandsynligvis vil påvirke personens humør og øge risiciene for sårbare personer. Dette kan anses som et brud på den særlige beskyttelse, der skal ydes til børn på grund af deres kategorisering som en særlig sårbar persongruppe jf. præambelbetragtning 38.

Tilsynet fandt, at Replika ikke havde implementeret effektiv alderskontrol, og foretog endvidere ikke kontrol af samtykke fra forældremyndighedsindehaveren for brugere under 18 år, som udbyderens hjemmeside ellers krævede for brugere under den fastsatte aldersgrænse. Dette fandtes i strid med artikel 8 i GDPR samt artikel 5 og 6, da der således heller ikke forelå et gyldigt behandlingsgrundlag til at behandle personoplysningerne om brugerne. Tilsynet konkluderede også, at appens privatlivspolitik var uforenelig med kravene om gennemsigtighed i GDPR's artikel 13, eftersom appen ikke gav tilstrækkelig og gennemsigtig information om behandlingen af børnenes personoplysninger. Dette blev ligeledes vurderet til at være i strid med artikel 25 om databeskyttelse gennem design og standardindstillinger, da appen ikke havde indbygget nogen form for beskyttelse af mindreårige ved eksempelvis at udelukke dem fra systemet via aldersverifikation.

På baggrund af appens overtrædelser af GDPR, traf tilsynet en beslutning om en midlertidig begrænsning af alt databehandling relateret til italienske brugere jf. art. 58, stk.2, litra f. Replika blev pålagt at dokumentere overholdelse af GDPR inden for 20 dage. [81]

4.6.3 TikTok-Sagen

I september 2023 pålagde det irske datatilsyn (DPC) TikTok en bøde på 345 millioner euro for overtrædelse af GDPR. Tito-appen tillod børn under 13 år at oprette en konto uden at sikre et verificerbart samtykke fra forældrene. Tilsynet konkluderede på baggrund af dette, at appen ikke havde en effektiv aldersverifikation, da børn nemt kunne omgå registreringskravene. Derudover gav TikTok ikke børnene tilstrækkelig information om, hvordan deres data blev

[81] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9852214 hentet 14-05-2025

behandlet og anvendt. Desuden behandlede appen flere oplysninger end nødvendigt ift. formålet med behandlingen. Dette var problematisk i forhold til den særlige beskyttelse, som børn er tildelt jf. præambelbetragtning 38, hvilket indebærer at information fra appen til brugeren, skal tilpasses brugerens alder og forståelsesniveau. Udover det irske datatilsyn, berørte sagen også det italienske og det tyske datatilsyn, som havde indsigelser i afgørelsen fra det irske datatilsyn. Derfor blev sagen forelagt EDPB, som traf bindende afgørelse om, at TikTok ikke overholdt reglerne om databeskyttelse gennem design og standardindstillinger ved at udelukke brugere under 13 år gennem tilstrækkelig aldersverifikation. I afgørelsen tog EDPB blandt andet stilling til TikToks designpraksis med pop-up notifikationer ved registrering. Rådet vurderede, at disse notifikationer ikke præsenterede valgmuligheder til brugeren på en objektiv måde, men lagde op til at brugeren ved anvendelse af knappen ''skip'', fjernede muligheden for at indstille en privat konto, hvorfor kontoen som standard ville være offentlig tilgængelig. Dette fandt EDPB at være i strid med blandt andet artikel 25 i GDPR, som omhandler kravet om databeskyttelse gennem design og standardindstillinger. [82]

Det er bemærkelsesværdigt, at den irske tilsynsmyndighed imidlertid påpeger, at artikel 24 og 25 ikke præcist angiver, hvilke foranstaltninger, der bør træffes for at sikre alderskontrol og dermed udelukke mindreårige fra at benytte sig af TikTok-appen, da alderskontrol stadig er et område under udvikling. Endvidere anfører de, at der endnu ikke er fastsat nogle branchemæssige eller reguleringsmæssige standarder, hvorfor det må være op til tilsynsmyndigheden at foretage en individuel vurdering af, om de indførte foranstaltninger er passende med hensyn til det aktuelle tekniske niveau samt omkostninger for implementering af sådanne alderskontrolsystemer.

4.6.4 Delkonklusion:

Selvom artikel 8 i GDPR udgør den centrale bestemmelse vedrørende børns samtykke til databehandling, findes der i praksis ikke mange afgørelser, hvor netop denne artikel direkte anvendes som hjemmelsgrundlag. I Replika afgørelsen kom det italienske datatilsyn frem til, at tjenesten ikke overholdte artikel 8, eftersom der ikke blev indhentet et forældresamtykke ved brugere under 18 år. Eftersom tjenesten ikke havde andet lovligt behandlingsgrundlag,

[82] https://www.edpb.europa.eu/system/files/2024-11/edpb_bindingdecision_202302_ie_sa_ttl_children_da_0.pdf hentet 14-05-2025

skulle der indhentes et lovligt samtykke fra forældremyndighedsindehaveren, hvilket tjenesten ikke havde implementeret. Herfor illustrerer denne afgørelse en overtrædelse af artikel 8.

Der ses imidlertid en tendens i andre afgørelser, herunder TikTok-sagen og ChatGPT-sagen, hvor kravene om aldersverifikation og beskyttelse af børns personoplysninger begrundes i artikel 25 om databeskyttelse gennem standardindstillinger og design. Dette kan tolkes som et udtryk for, at artikel 8's formål om beskyttelse af børns personoplysninger i praksis gennemføres i de tekniske krav, der stilles til tjenesteudbydernes systemer. Det rejser spørgsmålet, om samtykkebestemmelsen i artikel 8 i sig selv er tilstrækkelig – eller om en reel beskyttelse forudsætter, at kravene til aldersverificering implementeres som standardmekanismer, uafhængigt om der er givet et samtykke.

4.7 Fokus på dataminimering og databeskyttelse gennem design og standardindstillinger

De foregående analyser har belyst nogle af de udfordringer, der opstår i praksis i beskyttelsen af børns personoplysninger på online tjenester som TikTok og ChatGPT. Afgørelserne fra de europæiske datatilsyn har vist en tendens til udbyderes manglende implementering af effektive systemer, som kan aldersverificere og indhente gyldigt samtykke. I afgørelserne anfører tilsynsmyndighederne, at udbyderne ikke overholder principperne om dataminimering og databeskyttelse gennem design og standardindstillinger. Herfor findes det relevant at analysere, hvordan udbyderne kan overholde disse principper i praksis med henblik på beskyttelsen af børns personoplysninger.

Princippet om dataminimering indebærer, som kort nævnt i begrebsafklaringen, at personoplysninger skal være ''tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles'' jf. art. 5, stk.1, litra c. Dette betyder i praksis, at udbydere af online tjenester til børn, skal være særligt opmærksomme på at begrænse indsamlingen af data om børnene, og at den dataansvarlige bør foretage en nødvendighedsvurdering af, hvilke data, der er nødvendige at indsamle i forhold til formålet. Hvis det er muligt, bør den dataansvarlige også anvende anonymisering eller pseudonymisering således, at oplysningerne ikke kan henføres til et specifikt barn. Derudover

bør oplysninger om børnene kun opbevares så længe, at det er nødvendigt i forhold til formålet med behandlingen. Herefter bør oplysningerne slettes.

I forhold til bestemmelsen om databeskyttelse gennem design og standardindstillinger i artikel 25, indebærer denne bestemmelse, at udbyderen af en tjeneste skal integrere databeskyttelse ind i designet af tjenesten fra starten. Intentionen med denne bestemmelse er at forebygge databeskyttelsesretlige problemer, før de opstår. Derfor bør udbyderen af en tjeneste, som udbydes til børn, indtænke beskyttelsen af børns personoplysninger ind i designet af tjenesten. Bestemmelsen sætter ikke krav til, at der anvendes nogle specifikke foranstaltninger, men blot at de valgte foranstaltninger skal være robuste og effektive. Dette kan eksempelvis være via foranstaltninger som kryptering af data, alderskontrol og brugerkontrol samt via gennemsigtighed i kommunikationen. [83]

Som tilsynene i afgørelserne også anfører, er disse principper essentielle i behandlingen af personoplysninger om børn og bør indgå allerede i udarbejdelsen af online tjenester.

I forlængelse af dette, har EDPB for nyligt vedtaget en udtalelse om, hvordan alderskontrol skal medvirke til beskyttelsen af børns personoplysninger ved at implementere tekniske systemer, som kan verificere børns alder og sikre et lovligt samtykke.

4.8 EDPB's udtalelse om alderskontrol i forbindelse med beskyttelsen af børns personoplysninger

EDPB vedtog i februar 2025 en udtalelse om alderskontrol som led i Rådets og GDPRs øgede fokus på beskyttelsen af børn og deres rettigheder samt personoplysninger (EDPB Statement 1/2025 on Age Assurance). Rådets formål med udtalelsen er at skabe en ensartet tilgang til efterlevelse af reglerne omkring behandling af børns personoplysninger i EU. I erklæringen vedtog EDPB brugen af aldersverificering, og opremser blandt andet ti principper for lovlig behandling af personoplysninger gennem verificering af en persons alder.

Gennem de ti principper pålægger Rådet den dataansvarlige at sikre overholdelse af artikel 8 ved at præciserer, hvordan dette skal foregå i praksis. I udtalelsen fastslår EDPB blandt andet,

[83] https://www.edpb.europa.eu/system/files/2024-11/edpb_bindingdecision_202302_ie_sa_ttl_children_da_0.pdf hentet 14-05-2025

at børn skal ses som en persongruppe, der kræver en særlig beskyttelse, og at det herfor er afgørende at kunne verificere, om barnet har den fornødne alder til at kunne give et samtykke, eller om der kræves forældresamtykke. Hertil fremhæver Rådet, at de valgte aldersverificeringsmekanismer, som dataansvarlig vælger, skal være nødvendige, proportionelle og samtidig udformes med hensyn til at sikre overholdelse af principperne om dataminimering (artikel 5, stk.1, litra c) og databeskyttelse gennem design og standardindstillinger (artikel 25).

Rådet understreger dog, at det særlige hensyn til børn og indførslen af disse aldersverificerende mekanismer ikke skal føre til overvågning af brugere og ej heller unødvendig behandling af deres personoplysninger. Rådet anfører hertil:

''The processing of personal data for age assurance should not provide additional means to fulfil purposes unrelated to the age assurance itself'' [84]

Med dette pålægger Rådet den dataansvarlige at implementere foranstaltninger og garantier, der forhindrer at processen med aldersverificering ikke medfører unødvendige risici for databeskyttelsen, som at brugeren udsættes for profilering eller at brugeren kan spores på en sådan måde, som ikke er nødvendig i forhold til formålet om aldersverificering. Dette betyder ligeledes, at behandlingen af personoplysninger i forbindelse med denne aldersverificering, ikke må benyttes til andre formål end den pågældende alderskontrol. For at efterleve dette, skal den valgte aldersverificeringsmetode leve op til kravene om databeskyttelse gennem design og standardindstillinger jf. art. 25. Systemet skal således fra start designes med henblik på at minimere databehandling og beskytte de personoplysninger, der behandles.

Rådet anfører dog, at udbyderen bør inkorporere alternative metoder til at bekræfte alder i tilfælde af, at en bruger ikke ønsker eller ikke kan benytte en bestemt metode. Dette skal sikre, at der ikke opstår, hvad Rådet refererer til som *''power imbalance''*, hvor brugeren, især børn, bliver presset til at indgå i løsninger, som ikke respekterer retten til privatliv, og tvinger brugeren til at dele flere personoplysninger end nødvendigt. Dette er særligt relevant i forhold til diskussionen om, hvorvidt det er muligt at indføre en ensartet løsning i alle lande, som eksempelvis verificering af alder via upload af identitetskort og i Danmark eksempelvis MitID, da Rådet hertil pointerer at:

[84] EDPB Statement 1/2025 on age assurance, s.4.

'' *When certain categories of individuals are at risk of being discriminated against by a specific age assurance method, for example because they do not own a suitable identity document or mobile phone or because of a disability, alternative methods for age assurance should be made available, when reasonably possible, with adequate levels of privacy, safety and security. Age assurance solutions should also comply with any applicable legislation on accessibility.''*[85]

Dette betyder, at aldersverificeringsmetoden ikke må diskriminere mod bestemte persongrupper i tilfælde af, at de ikke har gyldigt ID eller ejer en telefon. Herfor skal udbyderen stille alternative verifikationsmetoder til rådighed. Endvidere kommer EDPB frem til, at aldersverifikation skal være en indikator men ikke en identifikator:

''*..the service provider may only need to know whether the user is over or under an age threshold. This could be implemented by a tokenized approach based on the participation of a third-party provider…*'' [86]

Verifikation gennem eksempelvis upload af identifikationspapirer som standardløsning kan derfor være for indgribende og muligvis i strid med princippet om dataminimering.

Udtalelsen understøtter således også forudsætningerne i artikel 8 om implementering af effektive aldersverificerende systemer, som kan kontrollere, at brugeren er gammel nok til at give samtykke. Udtalelsen har derfor betydning for den praktiske implementering af artikel 8, og sætter krav til den dataansvarliges rolle i beskyttelsen af børns personoplysninger. Ligeledes påpeger Rådets udtalelser problematikken i den afvejning, som skal foretages i forhold til behovet for beskyttelsen af børns personoplysninger og overdreven databehandling.

[85] EDPB Statement 1/2025 on age assurance, s.6
[86] EDPB Statement 1/2025 on age assurance, s.5

Kapitel 5 - Diskussion – Om aldersverificering med identifikationssystemer kan være fremtiden

Som de foregående analyser og afgørelser har belyst, har den nuværende regulering vedrørende beskyttelsen af børns personoplysninger på onlinetjenester været mangelfuld, særligt i relation til aldersverifikation. Trods GDPRs intention om at yde en særlig beskyttelse til børn, fremgår det blandt andet ikke entydigt af forordningens artikel 8, hvordan den dataansvarlige skal sikre, at der udelukkende gives samtykke fra personer over den fastsatte aldersgrænse. Dette åbner op for spørgsmålet, om hvorvidt der bør indføres nogle ensartede tekniske standarder i EU til aldersverificering, for at forbedre retssikkerheden for børn og sikre overholdelsen af artikel 8. En ny udtalelse fra EDPB peger imidlertid på, at implementeringen af et ensartet system for alle EU-medlemslande, kan være i strid med forordningens øvrige bestemmelser og principper.

Som belyst i specialet, kræver artikel 8, at der ved behandling af personoplysninger om børn i forbindelse med udbud af informationssamfundstjenester, skal indhentes et gyldigt samtykke fra barnet eller indehaveren af forældremyndigheden, hvis barnet er under 16 år (i Danmark 15 år). I praksis benytter mange udbydere imidlertid blot en selverklæring ved oprettelsen af en profil på en informationssamfundstjeneste, hvor brugeren forholdsvist nemt kan erklære, at brugeren er ældre end brugeren reelt er, hvorfor det samtykke, som brugeren giver til behandling af sine personoplysninger, er ugyldigt. Dette peger på et behov for en teknisk løsning, som effektivt og præcist kan verificere brugens alder således, at børn under den fastsatte aldersgrænse udelukkes fra at afgive et ugyldigt samtykke til behandling af deres personoplysninger.

En sådan teknisk løsning kan eksempelvis være en implementering af nationale identifikationssystemer som det danske MitID, der kan anvendes til at verificere brugerens alder, når brugeren opretter en profil på en online tjeneste. En sådan løsning vil formentlig sikre en højere beskyttelse af børn, og udelukke brugere under den fastsatte aldersgrænse i af give samtykke til, at deres personoplysninger behandles. Eftersom de fleste børn i Danmark

får adgang til MitID når de fylder 15 år[87], og systemet allerede er teknisk stærkt, virker det umiddelbart som en oplagt løsning.

Brugen af MitID rejser imidlertid også nogle væsentlige problemstillinger. Først og fremmest, er det ikke alle lande, som har lignende online identifikationssystemer som MitID. Derfor vil sådanne systemer først skulle implementeres og tilsluttes blandt alle borgere, hvilket er omfattende og omkostningsfuldt.

En anden problemstilling med implementeringen af sådanne systemer, er spørgsmålet om proportionalitet, da brugen af løsninger som MitID kan anses for værende for indgribende en metode at benytte, når man ''blot'' vil oprette en bruger på en online tjeneste. I så fald skal det jf. GDPRs proportionalitetsprincip og artikel 25 om privacy by design dokumenteres, at der ikke findes en mindre indgribende metode til at opnå formålet. Dette understøttes af EDPB's udtalelse fra februar 2025, hvor EDPB, som nævnt i et tidligere afsnit, mener, at aldersverifikation bør ske ved indikatorer og ikke identifikatorer. En yderligere problematik ved benyttelsen af MitID som verifikation, er, som Rådet i udtalelsen af 2025 også pointerer, at der skal være mulighed for, at brugeren kan vælge en anden metode til verificere sin alder, da systemet ikke må diskriminere. I så fald, skal der indføres en alternative metode til at brugeren kan verificere sin alder.

Der eksisterer imidlertid allerede et system, *EU Digital Identity Wallet (EUDI Wallet)*[88], som er en digital ID-tegnebog, der kan tilsluttes af alle EU-borgere. EUDI-Wallet er oprettet i led med forordningen om den europæiske digitale identitet, som blev vedtaget i 2024[89]. Denne løsning giver borgere mulighed for at bevise deres identitet, og kan konfigureres til udelukkende at videregive alderen på brugeren, uden at dele eksempelvis navn og CPR-nummer. Et sådant system imødekommer umiddelbart EDPBs anbefalinger fra udtalelsen af februar 2025, om aldersverificering ved indikator og ikke identifikator, og er herfor ikke i strid med princippet om dataminimering jf. artikel 5, stk.1, litra c.

Der kan derfor argumenteres for, at en løsning som EUDI-Wallet har potentiale til at være en effektiv aldersverificeringsmetode, som yder den nødvendige sikkerhed og samtidig

[87] https://www.mitid.dk/hjaelp/hjaelpeunivers/15-aarige/?language=da-dk hentet 14-05-2025
[88] https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/What+is+the+Wallet hentet 14-05-2025
[89] Regulation (ER) 2024/1183 of the European Parliament and of the Council of April 11 2024 amending Regulation No 910/2014 as regards establishing the European Digital Identity Framework

respekterer principperne om dataminimering og proportionalitet, som EDPBs ligeledes sætter krav til. Det kræver dog, at systemet implementeres blandt alle EU-medlemslande, hvortil der formentlig kommer udfordringer af både teknisk, praktisk og strukturel karakter. Tjenesteudbyderne skal derfor først integrere løsningen frivilligt, da der på nuværende tidspunkt ikke er et påbud om brugen af sådanne aldersverifikationssystemer. Derudover kan der forekomme nationale forskelle i, hvornår man efter et EU-medlemslands opfattelse, kan opnå identitet og adgang til EUDI Wallet'en. Endvidere vil implementeringen kræve en stor del IT og investering i teknisk infrastruktur.

Udover EUDI-Wallet har den Europæiske Kommission offentliggjort et udkast til retningslinjer under Digital Services Act (DSA)[90] for at styrke beskyttelsen af mindreårige på internettet. I retningslinjerne opfordrer Kommissionen blandt andet til at online tjenester implementerer aldersbekræftende værktøjer for at begrænse mindreåriges eksponering for skadeligt indhold.[91] Endvidere har EU Kommissionen medfinansieret en aldersvalideringsapp, som allerede er i test-fasen af udviklingen, og det forventes at testfasen kan afsluttes i løbet af nogle måneder. Appen skal gøre det muligt at verificere alder uden at afløsere yderligere oplysninger, hvorfor denne app lever op til EDPB's krav om aldersverificering ved indikator og ikke identifikator. Denne løsning anses derfor umiddelbart som værende mere fordelagtig end EUDI-Wallet, eftersom Kommissionens app er designet med henblik på dataminimering, og er udviklet med formålet om at beskytte børns personoplysninger. Derudover forventes det, at appen er færdigudviklet inden for nærmeste fremtid, hvis den består testfasen. Derimod er EUDI-Wallet umiddelbart en langsigtet løsning, da denne applikation ikke er designet med henblik på beskyttelsen af børns personoplysninger, hvorfor EUDI-Wallet først skal konfigureres og tilpasses til formålet om beskyttelse af børns personoplysninger. [92] Det er på nuværende tidspunkt uvist, om appen bliver lovpligtig for udbydere at implementere. Det kan imidlertid udledes, at en lovpligtig implementering af appen i EU, vil sikre en tilstrækkelig beskyttelse af børns personoplysninger, eftersom

[90] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)

[91] Commission guideline on a measure to ensure a high level of privacy, safety and security for minors online pursuant to Article 28(4) of Regulation (EU) 2022/2065

[92] EU Commission to launche test of age verification app - CADE – Civil Society Alliances for Digital Empowerment Hentet 14-05-2025

aldersverificeringen vil medføre, at mindreårige udelukkes fra at kunne tilgå online tjenester, hvorved behandlingen af deres personoplysninger undgås.

Kapitel 6 - Konklusion

Specialet har haft til formål at analysere, hvordan børns personoplysninger er beskyttet gennem samtykkereglerne i GDPR's artikel 8 samt databeskyttelseslovens §6, stk.2, og stk.3 ved brug af onlinetjenester.

Det er på baggrund af analysen blevet klargjort, at der i forarbejder til forordningen var stor uenighed omkring vedtagelsen af artikel 8, og om der overhovedet var behov for en særregel, der eksplicit reguleredе beskyttelsen af børns personoplysninger. Denne uenighed i lovgivningsfasen, kan have haft indflydelse på den endelig udformning af artikel 8, som nu fremgår upræcis, hvilket skaber tvivl om bestemmelsens anvendelsesområde. Denne tvivl har endvidere resulteret i manglende praksis på området. Det er herfor specialets opfattelse, at den upræcise formulering i bestemmelsen ikke yder den fornødne beskyttelse af børns personoplysninger, som ellers tilsigtes i præambelbetragtning 38 til forordningen. Årsagen hertil skyldes blandt andet, at ordlyden i artikel 8 udelukkende omhandler samtykket som behandlingsgrundlag, hvilket herfor ikke dækker de situationer, hvor den dataansvarlige behandler personoplysninger om børn på et andet behandlingsgrundlag, som eksempelvis ved en kontrakt. Uagtet om kontrakten er lovligt indgået, regulerer artikel 8 altså ikke beskyttelsen af børns personoplysninger, når et andet behandlingsgrundlag end samtykke benyttes. Dette er problematisk da mange online tjenester netop behandler oplysninger om børn baseret på et kontraktforhold, og dermed ikke et samtykke. Det kan herfor anføres, at samtykkereglen i mange situationer, hvor der indsamles personoplysninger om børn, ikke kan anvendes til at sikre tilstrækkelig beskyttelse af børnenes personoplysninger, hvorfor beskyttelsen må dækkes af øvrige bestemmelser i GDPR.

Der findes ligeledes problematikker i forbindelse med håndhævelsen af samtykkereglerne i praksis, blandt andet i forhold til verifikation af barnets alder. Der er ikke blevet indført én ensartet og anerkendt standard, som udbydere kan benytte til at verificere alderen på brugerne, hvilket har resulteret i manglende overholdelse af forordningen samt forskelle i landendes praksis på området. Herfor er det også svært for den dataansvarlige at overholde kravene om at indhente et gyldigt samtykke fra barnet eller forældremyndighedsindehaveren, hvis barnet er under den fastsatte aldersgrænse. Dette har specialet illustreret eksempler på i ChatGPT-sagen, TikTok-sagen og Replika-sagen, hvor der ikke var implementeret effektive systemer

til at verificere alder på barnet og/eller et gyldigt forældresamtykke. Som følge af udbyderes manglenende overholdelse af reglerne om beskyttelse af børns personoplysninger gennem blandt andet databeskyttelse gennem design og standard i artikel 25, udkom EDPB i februar 2025 herfor med en udtalelse om, hvordan netop denne beskyttelse skulle inkorporeres i udbydernes systemer ved at implementere effektiv aldersverificering. Af denne grund diskuterer specialet, om EUDI-Wallet eller den nye aldersverifikationsapp fra EU-Kommissionen kunne være en lovpligtig standardløsning, som udbydere i EU-medlemslandene skulle implementere til aldersverificering. Dette ville fordelagtigt skabe en ensartet tilgang, som ville sikre beskyttelsen af børns personoplysninger ved at udelukke brugere under den fastsatte aldersgrænse, eller i så fald kræve et forældresamtykke. Derudover skal systemet konfigureres således, at der benyttes metoder som har fokus på dataminimering og gennemsigtighed. Afhængigt af resultaterne af testfasen af aldersverifikationsappen, kan en lancering af denne måske være nærtstående. Implementeringen af denne vil dog kun løse problemet vedrørende alderskontrol i forbindelse med børns samtykke, men ikke de underliggende problemer med artikel 8 og bestemmelsens udformning.

Specialet kan herfor på baggrund af analysen og diskussionen konkludere, at den nuværende retstilstand og de gældende regler i GDPR og DBL ikke yder børns personoplysninger den tilstrækkelige beskyttelse, som GDPR ellers tilsigter i præambelbetragtning 38. Herfor er det specialets opfattelse, at der bør indføres en mere konkret regulering på området og en ensartet standard til aldersverificering. Såfremt den nye aldersverificeringsapp og den tilhørende lovgivning ikke bliver vedtaget, vil en alternativ implementering formentlig have lange udsigter endnu.

Litteraturliste

Bøger

Blume, Peter. *Samtykke i persondataretten.* Djøf Forlag, 1.udgave, 1.oplag, 2023

Blume, Peter. Persondatarettens kilder og metode. Djøf Forlag, 1. udgave, 2020

Hansen, Carsten-Munk. Retsvidenskabsteori. Djøf Forlag, 3.udgave, 2022

Nielsen, Kristian Korfits og Lotterup, Anders. *Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer*. Jurist- og Økonomforbundets Forlag, 1.udgave, 1.oplag, 2020

Sørensen, Marie Jull og Christensen, Tanja Kammersgaard. *Samtykke i databeskyttelsesretten*. Ex Tuto Publishing A/S, 1.udgave, 1.oplag, 2024

Udsen, Henrik. *Databeskyttelsesret*. www.databeskyttelsesret.dk. Version 0.1, 2022

Lovgivning

Databeskyttelsesforordningen: ''Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse)''

Lovforslag til databeskyttelsesforordningen: Forslag til Europa-Parlamentet og Rådets Forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, Bruxelles, 25. januar 2012, COM(2012) 11 final

COMMISSION STAFF WORKING PAPER Impact Assessment SEC (2012), 0072 final

Databeskyttelsesloven: ''Lov 2018-05-23 nr.502 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger''

Lovforslag til databeskyttelsesloven: ''Lovforslag nr. L 68, fremsat den 25. oktober 2017 af justitsministeren''

Traktaten om Den Europæiske Unions funktionsmåde, TEUF.

Europa-Parlamentets og Rådets forordning (EU) 2024/1183 af 10. april 2024 om rammerne for en europæisk digital identitet, EUDI-forordningen

Persondatadirektivet: '' EUROPA-PARLAMENTET OG RÅDETS DIREKTIV 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger'' (historisk)

Persondataloven: ''Lov 2000-05-31 nr.429 om behandling af personoplysninger'' (historisk)

Børnekonventionen: FN's konvention af 20. november 1989 om Barnets Rettigheder

Chartret: Den Europæiske Unions Charter om grundlæggende rettigheder (2010/C83/02)

COPPA: Children's Online Privacy Protection Rule, Act of 1998, 15. U.S.C. 6501-6505

EMRK: Den Europæiske Menneskerettighedskonvention af 4. november 1950, (Lovbekendtgørelse nr.750 af 19. oktober 1998)

Data Protection Act, 25 maj 2018

Regulation (ER) 2024/1183 of the European Parliament and of the Council of April 11 2024 amending Regulation No 910/2014 as regards establishing the European Digital Identity Framework

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)

Vejledninger, betænkninger og udtalelser

Artikel 29 gruppen: Retningslinjer vedrørende samtykke i henhold til forordning 2016/79, vedtaget den 28. november 2017, vedtaget den 10. april 2018, WP 259

Artikel 29 gruppen: nr.2/2009 om beskyttelse af børns personoplysninger (Generelle retningslinjer og særtilfældet skoler), vedtaget den 11. februar 2009, WP 160

Artikel 29 gruppen: nr.15/2011 om definitionen af et samtykke, vedtaget den 11. februar 2009, WP 160

EDPB: Statement 1/2025 on Age Assurance, vedtaget den 11. februar 2025

EDPB: Retningslinjer 4/2019 om artikel 25. Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, version2.0, vedtaget den 20. oktober 2020.

EDPB: Retningslinjer 5/2020 vedrørende samtykke i henhold til forordning 2016/679, version 1.1, vedtaget den 4. maj 2020

Justitsministeriet: Udkast til tale til brug for besvarelsen af samrådsspørgsmål H fra Folketingets Udvalg for Digitalisering og It, den 22. maj 2024

Datatilsynet: Vejledning om samtykke, maj 2021

Datatilsynet: Vejledning om registreredes rettigheder efter reglerne i kapitel 8-10 i lov om behandling af personoplysninger, juli 2000 (historisk)

DPC: Fundamentals for a child-oriented approach to data processing, December 2021

Folketinget: Betænkning nr.79 over Forslag til lov om ændring af databeskyttelsesloven og lov om Det Centrale Personregister, den 6. december 2023

Justitsministeriet: Betænkning nr. 1565 om Databeskyttelsesforordningen 2016/679 – og de retlige rammer for dansk lovgivning, del 1, bind 1

Commission guideline on a measure to ensure a high level of privacy, safety and security for minors online pursuant to Article 28(4) of Regulation (EU) 2022/2065

Betænkning over Forslag til lov om ændring af lov om Danmarks tiltrædelse af de Europæiske Fællesskaber og Den Europæiske Union (Danmarks ratifikation af Lissabontraktaten), 14 marts 2008

Afgørelser fra det danske datatilsyn

https://www.datatilsynet.dk/afgoerelser/historiske-afgoerelser/2014/jan/behandling-af-personoplysninger-hos-boerns-vilkaar

Afgørelser fra EU

Sagsnr: IN-21-9-1: https://gdprhub.eu/index.php?title=DPC_(Ireland)_-_IN-21-9-1

https://www.edpb.europa.eu/system/files/2024-s11/edpb_bindingdecision_202302_ie_sa_ttl_children_da_0.pdf

Sagsnr:10085432: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10085432

Sagsnr: 9852214: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9852214

Hjemmesider

https://digital-strategy.ec.europa.eu/da/policies/eudi-resgulation senest hentet 14-05-2025

https://www.datatilsynet.dk/Media/637647832459647592/Personoplysninger%20-%20f%C3%A5%20et%20hurtigt%20overblik.pdf senest hentet 14-05-2025

https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business#step4 senest hentet 14-05-2025

https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business#step4 senest hentet 14-05-2025

https://www.em.dk/Media/638314161358806766/anbefalinger-fra-tech-ekspertgruppe.pdf senest hentet 14-05-2025

https://www.ft.dk/samling/20231/almdel/diu/spm/174/svar/2052175/2873347/index.htm senest hentet 14-05-2025

https://www.dataprotection.ie/sites/default/files/uploads/2023-04/DPC_ChildrensData_ParentalConsent.pdf senest hentet 14-05-2025

https://ec.europa.eu/digital-building blocks/sites/display/EUDIGITALIDENTITYWALLET/What+is+the+Wallet senest hentet 14-05-2025

Bilag

Skærmprint af antal anslag