Det offentliges brug af Cloud

Speciale i jura ved Aalborg Universitet, maj 2025

Udarbejdet af: Katrine Platon Skyum, studie nr. 20204017

Vejleder: Jan Trzaskowski

Antal tegn: 80.756 (se screen shot s. 44)

Indholdsfortegnelse

Abstract

Denmark is a digital society. Digital solutions are present in almost every aspect of our daily lives. From attending school to studying at university and later in the workplace. We use technology to make our lives easier and more efficient. In Denmark, we primarily use products such as Microsoft's Word, Outlook, Excel and Teams, as well as Google's workplace and education. This technology operates through cloud services to store all the data. Today, the public sector relies heavily on these Cloud- services, which are primarily produced by American companies.

In Denmark, there has been cases such as the "Chromebooksagen" where it has been revealed that municipalities have failed to uphold GDPR by allowing children in elementary schools to use Google products that process data in ways that do not comply with the original purpose. Similar issues have been found in other EU countries, such as Lithuania, where the ministry of Health did not protect its citizen's health care data when developing a covid-app. Furthermore, it has been found in the Bindi vs EU-commission case that even the EU- commission has been lacking in ensuring that data from its own website is not transferred to the USA.

In this master's thesis, the primary focus has been on the public sector as a data controller and its responsibility when using cloud services to ensure compliance with GDPR. To find out how the public sector can use Cloud services in accordance with GDPR, there has also been a focus on the data processor and its reasonability to ensure that the data processing agreement is in compliance with GDPR.

In this master's thesis, it has been concluded that the data controller is responsible for determining the purpose of data processing and ensuring that no data is processed without legitimate grounds. It has also been concluded that the data controller is responsible for following only the instructions laid by the data controller. If a data processor carries out data processing on its own behalf and in its own interest, it will be considered a data controller and therefore the act is illegitimate.

Indledning

Der er et kendt udtryk: *USA innoverer, Kina kopierer og EU regulerer*. Om der er en sandhed i påstanden, kan selvfølgelig diskuteres. Virkeligheden er, at teknologi og AI udvikling i de fleste tilfælde skabes af bl.a. amerikanske virksomheder. AI teknologien er de seneste år blevet styrket, og systemer som generativ AI kan skabe tekst, billeder og videoer, der er tæt på menneskabt indhold. Dette har skabt en offentlig debat med alt fra muligheder, effektivisering af arbejdspladser til trusler om spredning af desinformation. De mange juridiske, etiske og politiske perspektiver, der rejser sig om spørgsmålet af brug af AI er noget, der diskuteres af politikere verden over[1].

Danmark er kendt for at være frontløber på digitalisering, og den danske offentlige sektor siges at være verdens mest digitaliserede.[2] Fremtidens velfærd kommer til at blive forandret markant de næste 10 år. Danmark står over for store velfærds problematikker i form af demografisk udvikling, manglende arbejdskraft samt det økonomiske råderum til at løse disse problemer. Det gør det i høj grad relevant at tænke i teknologiske løsninger til gavn for både borgerne, for ansatte i det offentlige og samfundets sammenhængskraft[3].

I en digitaliseret verden, hvor AI løsninger skal implementeres, er cloud-løsninger en nødvendighed. I praksis ses cloud-service som lagerplads, software og computerkraft, som kan tilgås på internettet. Leverandøren af disse ydelser står ofte som ansvarlig for hardware og infrastruktur, som kunden kan få adgang til via et abonnement. Cloud-løsninger kan være attraktive for særligt det offentlige, fordi egen udvikling kan være dyr. Derudover kræver det stor ekspertise. Cloud-løsninger giver i stedet offentlige myndigheder bedre mulighed for at få tilgang til hardware og infrastruktur, hvorved de selvstændigt kan køre applikationer, behandle data og lagre. I dag bruger de fleste danske kommuner cloud-løsninger til data opbevaring. Det medfører bl.a., at kommunerne kan reducere it-omkostningerne til vedligeholdelse og drift af egne

[1] Forbrukerrådet, Ghost in the machine: Addressing the consumer harms of generative AI, June 2023
[2] Dataetisk Råd, rapport, Generativ AI og offentlige myndigheder: Pålidelighed og dataetik, 2025
[3] Dataetisk Råd, rapport, Generativ AI og offentlige myndigheder: Pålidelighed og dataetik, 2025

serverløsninger [4]. Cloud-ydelser indebærer i høj grad juridiske og sikkerhedsmæssige risici, som skal adresseres før en Cloud-service tages i brug. Cloud-ydelser baseres oftest på standardkontrakter og bliver derfor sjældent forhandlet. Dette kan medføre juridiske risici bl.a. i form af mindre kontrol over databehandlingen i systemerne.[5] Samtidig ses der geopolitiske uro, hvor kontrol med egen digital infrastruktur bliver en meget vigtig nødvendighed.

Et andet dilemma er manglende eftersyn af datahandler aftaler mellem det offentlige og private aktører. Mange løsninger på det teknologiske område kommer fra store Tech giganter såsom f.eks. Microsoft. Datatilsynets afgørelse i Chromebooksagen viste nødvendigheden af at danske kommuner, der indgår it-kontrakter med private aktører, tydeligt får klargjort hvad indsamlede data bliver brugt til. Datatilsynet påpegede følgende om sagen: "*De fleste it-standardprodukter har i dag et meget komplekst kontraktgrundlag, som ikke bare rummer mange muligheder for variationer i behandlingen af personoplysninger, men også har en relativt høj ændringsfrekvens. Dette gør det sværere end nødvendigt for dataansvarlige virksomheder og myndigheder at leve op til GDPR, fordi man let mister overblikket over, hvad der sker med data. Vi i Datatilsynet opfordrer derfor til, at kontrakterne gøres mere gennemskuelige - ikke bare i forhold til behandlingsstrukturen, men også i forhold til konsekvenserne, når forhold omkring leverancen ændres*"[6].

Med det offentliges/kommuners stigende forbrug af private kommercielle løsninger ses en større risiko for kommerciel brug af de indsamlede data til gavn for private cloud-aktørers egne interesser f.eks. brug af borgeres data til forbedring af egne produkter og markedsposition[7].

Specialets hovedformål er at undersøge regulering af kommuners deling af data med private cloud-aktører, og hvordan man balancerer det offentliges interesse med de private virksomheders

[4]Kommunernes Landsforening: Cloud. KL
Videncenter. https://www.kl.dk/videncenter/teknologier/teknologioversigt/cloud
[5] Digitaliseringsstyrelsen, Vejledning i anvendelse af cloudservices version 1.1, juli 2020
[6]Datatilsynet. (2024, januar). Datatilsynet giver påbud i Chromebook-sag
[7] Datatilsynet. (2024, januar). Datatilsynet giver påbud i Chromebook-sag

kommercielle interesser. For når det offentlige tilbyder it-løsninger til sine borgere, må ansvaret for datasikkerhed overholdes i overensstemmelse med GDPR-reglerne.

Problemformulering

Min problemformulering bliver på baggrund af ovenstående: **I hvilket omfang kan private virksomheder, der får adgang til personoplysninger i forbindelse med levering af ydelser som databehandler til det offentlige, lovligt anvende oplysningerne til egne formål, og hvilket ansvar har den offentlige myndighed for at sikre, at den private leverandør overholder GDPR?**

Afgræsning

I specialet vil der ikke blive fokuseret meget på tredjelandes overførsler og regler herfor. Der vil få steder blive nævnt udtræk af domme og litteratur om situationer, hvor tredjelands overførsler har skabt dataretlige problemstillinger. I disse tilfælde vil fokuset være på selve databeskyttelsesforordningens behandlingsregler for cloud baserede løsninger.

Specialet vil sondre mellem oplysninger, der behandles på vegne af den dataansvarlige (myndighed) og de oplysninger, som Cloud-aktøren/virksomheden får adgang til udover, hvad der er nødvendigt for den dataansvarliges behandling.

Databeskyttelsesforordningen er fra 2018 og harmoniserer fælles europæiske standarder for databeskyttelse. Databeskyttelsesforordningen indeholder en række regler om datasubjektets rettigheder såsom indsigt i de registrerede data, berigtigelse, indsigelse og sletning. Disse rettigheder kan gøres til krav mod den dataansvarlige og databehandleren. I besvarelsen af specialets problemformulering vil det ikke blive taget op.

Konsekvensanalyse vil ikke blive inddraget. En konsekvensanalyse skal udarbejdes, hvis der er databehandling, som indeholder høj risiko for svækkelse af individers rettigheder. Det kan være en situation, hvor der foreligger profilering af personlige forhold. Ligeledes skal en konsekvensanalyse

laves, hvis databehandlingen har mængder af særlig personoplysninger[8]. Nye teknologier som hjælper til at effektivisere myndighedsopgaver, vil også ofte kunne indebære, at en konsekvensanalyse er påkrævet. Retspraksis fra EU-domstol og administrativ praksis vil kun blive inddraget, når det findes relevant for specialets problemformulering.

EU-data Act bliver heller ikke gennemgået i specialet. EU-data Act ville kunne have bidraget til en forbedret analyse omkring datadeling, f.eks. om de nye bestemmelser for, hvordan forbrugere af cloud-ydelser vil kunne påkræve nemmere adgang til skift af leverandør og medtage deres data.

Metode

Specialet tager afsæt i juridisk metode ved at fastlægge gældende ret på området vedrørende specialets dataretlige problemstilling. Den juridiske metode ses i specialet ved, at der fastlægges relevant faktum, fastlæggelse af relevant regel og afslutningsvis fastlæggelse et givent resultat[9].

Juridisk metode er en bred definition, der dækker mange forskellige midler til at finde den juridiske løsning. Den juridiske metode i specialet vil anvende den retsdogmatiske metode.
I opgaven vil der blive redegjort for og analyseret relevante retsregler. Der vil også blive systematiseret og beskrevet retskilders værdi og hierarki. Desuden analyseres retspraksis, der skal hjælpe til give indsigt og svar på specialets problemformulering. Afslutningsvis vil der i diskussionen blive givet nye perspektiver og faktuel eller hypotetisk retlig undren[10].

Metodisk problem

Grundet databeskyttelsesforordningen er fra 2018 og dermed ”kun” 7 år gammel, kan det give problemer med manglende retspraksis. Dette kan gøre det sværere at fastlægge, hvordan reglerne skal fortolkes.

[8] Digitaliseringsstyrelsen, Vejledning i anvendelse af cloudservices version 1.1, juli 2020
[9] Munk-Hansen, C. (2017). Den juridiske løsning: Introduktion til den juridiske metode. (1. udg.) Djøf Forlag s. 11
[10] Munk-Hansen, C. (2017). Den juridiske løsning: Introduktion til den juridiske metode. (1. udg.) Djøf Forlag s. 13-14

Retskilder

I Danmark er der konsensus om, at der er 4 grupper af retskilder: Loven, Retspraksis, Sædvanen og Forholdets natur. Denne tilgang, også kaldet den nordiske retstradition, bygger på, at afgørelser skal være med udgangspunkt i retlig bedømmelse af kilder og ræsonnementer uden egen personlig værdiopfattelse[11].

I specialet vil der blive taget udgangspunkt i EU-retten. EU-retten består af 2 retskilder: Primær og Sekundære retskilder. Hierarkisk er de primære retskilder placeret med forrang til de sekundære retskilder. Dette betyder, at sekundære retskilder altid skal fortolkes i overensstemmelse med de primære retskilder[12]. De primære retskilder i EU-retten er: Traktaten om Den Europæiske Union også forkortet TEU, EU Charter om Grundlæggende rettigheder, Traktaten om Den Europæiske Unions funktionsmåde (TEUF), samt EU retlige grundprincipper, der ses afspejlet i case Law[13].
De sekundære retskilder i EU-retten er: internationale aftaler, direktiver (som enten kan ses ved implementering eller have indirekte virkning), forordninger som medfører direkte virkning (ses blandt andet ved databeskyttelsesforordningen som harmoniserer fælles europæiske standarder for databeskyttelse og derfor ikke skal implementeres, da reglerne er direkte anvendelige). Afgørelser afsagt af EU domstolen og national lovgivning kan ligeledes ses som sekundære retskilder[14].

Som nævnt ovenfor er databeskyttelsesforordningen en sekundær retskilde, som skal ses i overensstemmelse med de primære retskilder. Dette vil sige, at reglerne i databeskyttelsesforordningen altid skal afspejle TEUF og EU's Charter om grundlæggende rettigheder. Databeskyttelsesforordningen har forrang over national lovgivning, hvilket vil sige, at reglerne i forordningen tillægges prioritet over national lovgivning i situationer med modstridende lovgivning[15]. Udgangspunktet er dermed, at databeskyttelsesforordningen har direkte virkning, og

[11] Munk-Hansen, C. (2017). Den juridiske løsning: Introduktion til den juridiske metode. (1. udg.) Djøf Forlag s. 14 til 15
[12] Tvarnø, C. D., & Nielsen, R. (2021). Retskilder og retsteorier. (6. udg.) Djøf Forlag. s. 139
[13] Neergaard, U., & Nielsen, R. (2020). EU-ret. (8. udg.) Karnov Group.s.140
[14] Neergaard, U., & Nielsen, R. (2020). EU-ret. (8. udg.) Karnov Group.s. 141-142
[15] Munk-Hansen, C. (2022). Retsvidenskabsteori. (3. udg.) Djøf Forlag., s. 292

er den primære retskilde i europæisk databeskyttelsesret. Til at fastlægge gældende ret skal databeskyttelsesforordningen være udgangspunktet[16].

Til at forstå databeskyttelsesforordningen kan præambler, der indeholder formålsbetragtninger, være en hjælp. Præambler har stor lighed med det, vi fra dansk ret kalder forarbejder. Præambler til direktiver og forordninger er fortolkningsbidrag, der kan danne forståelse for en given regel[17]. Databeskyttelsesforordningen giver undtagelser til forrang i form af delegerede beslutninger. Disse undtagelser ses ved tildeling af kompetence til selvbestemmelse på de områder, hvor databeskyttelsesforordningen ikke har fastlagt specifikke rammer. Dette giver mulighed for at præcisere forordningens anvendelse generelt eller specifikt[18]. I dansk ret er de generelle præciseringer blevet anvendt i databeskyttelsesloven. De specifikke kan ses i bekendtgørelser, hvor det ønskværdige behandlingsformål fremgår. Et tydeligt eksempel findes i artikel 6 stk. 1, litra e, hvor en myndigheds udøvelse kræver sektorspecifik hjemmel. Ligeledes i artikel 9 stk. 2, fremgår det i betænkningen også, at der skal være et påkrav til national lovhjemmel for at kunne aktivere bestemmelsen. Nationale særregler har således forrang på visse områder.

Principperne om lex specialis og lex generalis tilsiger, at særregler har forrang over for generelle regler. I konteksten til databeskyttelsesforordningen ses dette ved, at særlige bestemmelser i e-databeskyttelsesdirektivet, der specificerer reglerne i databeskyttelsesforordningen, anses som ” lex specialls” i forhold til databeskyttelsesforordningens generelle bestemmelser [19].

Fortolkningsprincippet

Der vil blive fortolket på retsreglerne inden for databeskyttelsesforordningen, og derfor vil særligt direktivkonform fortolkning blive anvendt. Dette betyder, at nationale domstole skal fortolke EU-direktiver i overensstemmelse med EU-retten. I situationer, hvor den nationale domstol er i tvivl om en retlig tvist, skal denne tvist forelægges for EU-domstolen. EU-domstolen træffer ikke selv

[16] Blume, P. (2020). Retssystemet og juridisk metode. (4 udg.) Djøf Forlag. s. 56
[17] Neergaard, U., & Nielsen, R. (2020). EU-ret. (8. udg.) Karnov Group.s.136
[18] Blume, P. (2020). Retssystemet og juridisk metode. (4 udg.) Djøf Forlag. s. 36-38
[19] European Data Protection Board. (2019). Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR

afgørelser i konkrete sager, men tager stilling til den retlige tvist[20]. EU-domstolen udvikler retspraksis ved anvendelse af den dynamiske fortolkningsstil, hvilket indebærer at tidligere domme ikke automatisk binder Domstolen i sine senere afgørelser[21].

Vejledninger

I specialet vil der blive taget vejledninger i brug, der er udgivet af bl.a. Datatilsynet og Det Europæiske databeskyttelsesråd (EDPB). Vejledninger er ikke bindende retsregler, men fungerer ofte som detaljerede beskrivelser af, hvordan regler skønnes at skulle anvendes. Det er vigtigt at have for øje, at vejledninger kan bruges som supplement til lovgivning, lovforarbejder og retspraksis, men de udgør ikke i sig selv de facto juridiske løsninger, da skøn under regel er forbudt uden andre gældende elementer[22].

Det Europæiske beskyttelsesråd og Datatilsynet

Det Europæiske databeskyttelsesråd (EDPB) er et organ, der har til formål at harmonisere anvendelsen af reglerne i databeskyttelsesforordningen ved at fastlægge vejledninger, anbefalinger og udtalelser[23]. EDPB har ingen lovgivningsmæssig kompetence, men nationale datatilsyn vægter EDPB's vejledninger, anbefalinger og udtalelser højt, da disse er bindende for dem[24].

Datatilsynet er en forvaltningsmyndighed, der administreres af et råd og et sekretariat. Datatilsynet har kompetence til at føre tilsyn med, at GDPR-reglerne bliver overholdt, med undtagelse af tilsyn med domstolene jf. GDPR-artikel 51. Datatilsynet er uafhængige. Dette betyder, at intet andet organ har instruktionsbeføjelser over datatilsynets arbejde[25]. Datatilsynets arbejde består i behandling af klager og tilsyn. Hvis der ikke er tilstrækkelige oplysninger, kan datatilsynet kræve disse belyst. Klager kan afvises, hvis der f.eks. er tale om konkurrerende sektortilsyn jf. GDPR-artikel 54, stk. 4 og artikel 27, stk. 1. Datatilsynet kan pålægge bødeforlæg,

[20] Munk-Hansen, C. (2017). Den juridiske løsning: Introduktion til den juridiske metode. (1. udg.) Djøf Forlag. 48
[21] Tvarnø & Nielsen, 2021, s. 178
[22] Bog: Den juridiske løsning, Introduktion til den juridiske metode side 78, 2017 Carsten Munk- Hansen
[23] Tasks and duties | European Data Protection Board. (n.d.).
[24] Blume, 2020, s. 64-65
[25] Justitsministeriet. (2017). Betænkning nr. 1565 – Databeskyttelsesforordningen og de retslige rammer

hvis overtrædelsen afspejler en klar retspraksis på det givne område. Derudover har datatilsynet beføjelser til at pålægge kritik, advarsler og påbud. Datatilsynet er den øverste klageinstans, og der sker ingen rekurs af afgørelser truffet af datatilsynet. Dog kan der ske domsafprøvelse vedrørende disse afgørelser jf. GDPR-artikel 78.[26]

Administrativ praksis har i dansk ret en begrænset retskildeværdi og ville kunne tilsidesættes af retspraksis jf. Grundloven § 63. Databeskyttelsesforordningen styrker Datatilsynets betydning og indflydelse, idet forordningens legalitet er forankret i artikel 8 i EU's Charter om Grundlæggende Rettigheder[27]. Det medfører, at Datatilsynets afgørelser anses for betydningsfulde og har stor retskildeværdi. Det skyldes, at Datatilsynet træffer afgørelser med udgangspunkt i EU-domstolen og EDPB, der som tidligere nævnt har forrang i forhold til GDPR.

Retslitteratur

I specialet vil retslitteratur i form af videnskabelige artikler og bøger, der relaterer sig til specialets emne blive anvendt. Retslitteraturen vil bidrage til inspiration for retlige diskussioner og argumentation. Retslitteratur vil også kunne bidrage til forståelsen af retskilder og retspraksis på en pædagogisk måde. Retslitteratur anses dog ikke for at være en egentlig retskilde, og det er derfor vigtigt at udvise kildekritik en forfatteres tilkendegivelser, da disse kan indeholde bias[28].

Retspolitik

Jura og politik hænger sammen. For at forstå, hvorfor en given regel er blevet til, er det nødvendigt at have indsigt i de politiske hensigter og mål, der ligger bag. I juridiske termer anvendes de latinske udtryk de lage ferenda, som kan oversættes til "hvordan loven burde være" og de lege lata, som kan oversættes til "hvordan loven er"[29]. Illustrativt kan det skitseres, at lovgivning er en dynamisk proces, og den lovgivende magt frit kan ændre, hvordan dommere skal dømme i retssager ved at ændre lovgivningen. I specialet vil der blive rejst juridiske diskussion og retlige overvejelser omkring dataretlige dilemmaer.

[26] Justitsministeriet. (2017). Betænkning nr. 1565 – Databeskyttelsesforordningen og de retlige rammer
[27] Blume, 2020, s. 22 og 48-49
[28] Munk-Hansen, C. (2017). Den juridiske løsning: Introduktion til den juridiske metode. (1. udg.) Djøf Forlag. s. 74
[29] Munk-Hansen, C. (2017). Den juridiske løsning: Introduktion til den juridiske metode. (1. udg.) Djøf Forlag. s. 11

Jeg vil analysere Chromebook-sagen for at illustrere, hvordan danske kommuner møder dataretlige dilemmaer, når de anvender cloud-løsninger til folkeskoler. Danmark er et foregangsland inden for teknologi, hvilket ses i den udbredte anvendelse af teknologier til dagligdagen. Arbejdspladser, skoler og den offentlige kommunikation med borgere er digitaliserede. Politisk set har hensigterne, været at Danmark skal være et digitalt samfund. De juridiske regler på dataområdet et teknologi neutrale, men det ses stadig, at reglerne kan være svære at anvende i praksis. Dette afspejles i Chromebook-sagen.

Databeskyttelsesforordningens hensigt og formål

I dette afsnit vil der blive redegjort for databeskyttelsesforordningens hensigt og formål. Dette vil danne et overblik af de juridiske rammer og fastlægge, hvilke bestemmelser der har særlig relevans for besvarelsen af problemformuleringen. Der vil blive set nærmere på personoplysningskategorier og deres behandlingsgrundlag. Derudover vil der blive set nærmere på rollefordelingen mellem den dataansvarlige og databehandleren.

Brug af private cloud-aktørers/virksomheders platforme og services er ikke omkostningsfrie for de brugere, der benytter sig af dem. De data, som virksomhederne indsamler, anvendes til målrettet reklame og profilering med økonomisk gevinst for øje. Dette kan ofte foregå uden brugerens viden[30]. Kommuners dataetiske overvejelser ved anvendelse af it-løsninger fra private cloud-aktører/virksomheder bør sikre borgernes mulighed for gennemsigtighed omkring konsekvenserne af at bruge de pågældende it-løsninger. I EU's Charter om Grundlæggende Rettigheder, artikel 17 (1) fremgår det, at en registreret person ikke i juridisk forstand betragtes som "ejer" af sine persondata, men at der i stedet anvendes udtrykket "respekten for privatheden" samt beskyttelse af personoplysninger[31].

[30]Trzaskowski, J., Savin, A., Lindskoug, P. L., & Lundqvist, B. (2023). Introduction to EU Internet Law. Ex Tuto Publishing. S. 95

[31] Trzaskowski, J., Savin, A., Lindskoug, P. L., & Lundqvist, B. (2023). Introduction to EU Internet Law. Ex Tuto Publishing, s. 95

Persondata er allerede blevet integreret som en rettighed, og i alle situationer, hvor data indsamles kan det i princippet være i modstrid med den grundlæggende rettighed til privatlivets fred. I EU's Charter om Grundlæggende Rettigheder, artikel 8, præciseres det " *Everyone has the right to protection of personal data concerning him or her and that such data must be protected fairly for specified purpose and on the basis of the consent of the person concerned or some other legitimate basis laid down by law*". Bestemmelsen statuerer, at der kan ske lovlig indsamling af personoplysninger med eller uden samtykke fra den registrerede. Dette forudsætter gyldigt behandlingsgrundlag. Bestemmelsen regulerer derudover krav til dataansvarlige databehandlere samt rettigheder til den registrerede[32].

Databeskyttelsesforordningen fra 2018, også kaldet GDPR, udgør i dag den generelle forordning med fokus på databeskyttelse i det indre marked. I Artikel 1 skitseres fordringens genstand og formål:

1. I denne forordning fastsættes regler om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og regler om fri udveksling af personoplysninger.
2. Denne forordning beskytter fysiske personers grundlæggende rettigheder og frihedsrettigheder, navnlig deres ret til beskyttelse af personoplysninger.
3. Den frie udveksling af personoplysninger i Unionen må hverken indskrænkes eller forbydes af grunde, der vedrører beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger[33].

Databeskyttelsesforordningens formål er at fastsætte en fælles europæisk standard for udveksling af personoplysninger. Dermed har EU besluttet at harmonisere databeskyttelsesreglerne. De harmoniserede regler er til gavn for virksomhederne, der har de samme ensartede forpligtelser. De harmoniserede GDPR-regler styrker ligeledes borgernes datasikkerhed på tværs af landegrænser [34].

[32] Trzaskowski, J., Savin, A., Lindskoug, P. L., & Lundqvist, B. (2023). Introduction to EU Internet Law. Ex Tuto Publishing side 98.
[33] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
[34] Pedersen, A. Á., & Vandrup, K. D. (2022). It-sikkerhed i praksis – En introduktion. Samfundslitteratur. S. 401

GDPR forordningen lister 6 grundlæggende principper op som både virksomheder og organisationer er forpligtet af:

1. Formålsbegrænsning
2. Dataminimering
3. Lovlighed, rimelighed og gennemsigtighed
4. Rigtighed
5. Integritet og fortrolighed
6. Opbevaringsbegrænsning[35]

Disse principper kan ses afspejlet i GDPR artikel 4(11*): "consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her' (emphasis added)"*[36]. Den dataansvarlig har til opgave at sikre, at de 6 principper i forordningen efterleves jf. artikel 5 stk. 2. De 6 principper udgør en hjørnesten i forordningens ide om at principperne fungerer som pejlemærker til vurdering af, om en given behandling er i overensstemmelse med GDPR[37].

Forordningen har materiel anvendelse på alle oplysninger, der kan identificere en given person. Forordningens territoriale anvendelse omfatter enhver behandling af data vedrørende en EU-borger og enhver virksomhed etableret i EU med databehandlingsaktiviteter. Definitionen af en behandling præciseres i forordningens art. 4, nr. 2, som siger "*enhver aktivitet eller række af aktiviteter med eller uden brug af automatisk behandling som personoplysninger eller en samling af personoplysninger gøres til genstand for, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring,*

[35] Bog it-sikkerhed i praksis en introduktion 2022 side 403
[36] Trzaskowski, J. (2024). Manipulation by design
[37] Henrik Udsen, "Databeskyttelsesret, s.126

begrænsning, sletning eller tilintetgørelse". For at en behandling kan gøres lovlig, er det et påkrav, at de 6 overnævnte principper i forordningen er overholdt jf. artikel 5 stk. 1[38].

Personoplysningers kategorier og deres behandlings-grundlag

Almindelige personoplysninger defineres i artikel 4 som data, der typisk gives i almindelighed, såsom navn, adresse, e-mailadresse og telefonnummer. Disse oplysninger betragtes ikke som følsomme oplysninger og kan som udgangspunkt ikke bruges til ulempe for den registrerede. Følsomme personoplysninger, der præciseres i artikel 9, udgør modsætningsvis data, der kan bruges negativt mod den registrerede, hvis de indsamlede oplysninger bruges i ond vilje. Her er der tale om oplysninger om etnisk tilhørsforhold, politiske overbevisning, helbredoplysninger, generiske data, seksuel orientering eller biometriske data[39]. Følgende tre sager viser, hvordan information kan skabe nok viden til at identificere en person:
I Sag C-582/14 blev det belyst, at dynamiske IP-adresser i nogle tilfælde vil kunne identificere en person, hvis disse IP-adresser også kombineres med yderligere persondata jf. præmis 49[40]. I en anden Sag C-434/16 blev belyst, at kommentarer på eksamensbesvarelser kan være tilstrækkelig information til at fastslå en identificerbar person jf. præmis 33-35[41]. Også navne på deltagere til møder blev i sag C-28/08 belyst som oplysninger, der kan forbindes med en identificerbar person jf. præmis 63[42].

Almindelige personoplysningers behandlingsgrundlag

Behandlingsgrundlaget for almindelige personoplysninger fremgår af databeskyttelsesforordningens artikel 6, der tilskriver følgende kriterier omkring lovlig behandling:
1. Behandling er kun lovlig, hvis og i det omfang mindst ét af følgende forhold gør sig gældende:

[38] Udsen, H. (2022). Databeskyttelsesret, s,14
[39] Pedersen, A. Á., & Vandrup, K. D. (2022). IT-sikkerhed i praksis: En introduktion. Samfundslitteratur s. 402
[40] Den Europæiske Unions Domstol. (2016). Patrick Breyer v Bundesrepublik Deutschland, C-582/14. EUR-Lex
[41] Den Europæiske Unions Domstol. (2017). Peter Nowak v Data Protection Commissioner, C-434/16. EUR-Lex
[42] Den Europæiske Unions Domstol. (2010). European Commission v The Bavarian Lager Co. Ltd., C-28/08 P. EUR-Lex

a) Den registrerede har givet samtykke til behandling af sine personoplysninger til et eller flere specifikke formål.
b) Behandling er nødvendig af hensyn til opfyldelse af en kontrakt, som den registrerede er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en kontrakt.
c) Behandling er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige.
d) Behandling er nødvendig for at beskytte den registreredes eller en anden fysisk persons vitale interesser.
e) Behandling er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.
f) Behandling er nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger, går forud herfor, navnlig hvis den registrerede er et barn.
Første afsnit, litra f), gælder ikke for behandling, som offentlige myndigheder foretager som led i udførelsen af deres opgaver.
2. Medlemsstaterne kan opretholde eller indføre mere specifikke bestemmelser for at tilpasse anvendelsen af denne forordnings bestemmelser om behandling med henblik på overholdelse af stk. 1, litra c) og e), ved at fastsætte mere præcist specifikke krav til behandling og andre foranstaltninger for at sikre lovlig og rimelig behandling, herunder for andre specifikke databehandlingssituationer som omhandlet i kapitel IX[43].

Et eksempel på, hvordan artikel 6 anvendes som behandlingsgrundlag, kan være følgende: En forbruger shopper på en online shopping platform. For at forbrugeren kan få tilsendt sine ønskede varer, skal han udlevere sine personoplysninger, såsom hjemmeadresse og kreditkortoplysninger. Detailhandleren skal for at kunne opfylde kontrakten behandle forbrugernes oplysninger navnlig kreditkort, hjemmeadresse og eventuelle kontaktoplysninger. Hjemlen til disse behandlingsaktiviteter findes i artikel 6, StK 1, litra b. Hvis situationen i stedet var, at forbrugeren

[43] Europa-Parlamentet & Rådet. (2016). Forordning (EU) 2016/679 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger

vælger at afhente sine varer på et afhentningssted frem for at få dem leveret til sin hjemmeadresse, kan hjemlen ikke findes i artikel 6 stk. 1 litra b. Dette skyldes, at kontraktens opfyldelse ikke kræver oplysninger om forbrugerens bopæl.

Offentlig myndighedsudøvelse fremgår af artikel 6, stk. 1, litra e. Denne hjemmel gør det muligt for f.eks. kommuner, som dataansvarlige, at behandle personoplysninger, når det er nødvendigt for udførelsen af en samfundsinteresse, der er dem pålagt.

Særlige følsomme personoplysningers behandlingsgrundlag

Behandlingsgrundlaget for særligt følsomme personoplysninger fremgår af databeskyttelsesforordningens artikel 9, hvor reglerne for behandling af særlige kategorier af personoplysninger præciseres:

1. Behandling af personoplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering er forbudt.

2. Stk. 1 finder ikke anvendelse, hvis et af følgende forhold gør sig gældende:

a) Den registrerede har givet udtrykkeligt samtykke til behandling af sådanne personoplysninger til et eller flere specifikke formål, medmindre det i EU-retten eller medlemsstaternes nationale ret er fastsat, at det i stk. 1 omhandlede forbud ikke kan hæves ved den registreredes samtykke.

b) Behandling er nødvendig for at overholde den dataansvarliges eller den registreredes arbejd-, sundheds- og socialretlige forpligtelser og specifikke rettigheder, for så vidt den har hjemmel i EU-retten eller medlemsstaternes nationale ret eller en kollektiv overenskomst i medfør af medlemsstaternes nationale ret, som giver fornødne garantier for den registreredes grundlæggende rettigheder og interesser.

c) Behandling er nødvendig for at beskytte den registreredes eller en anden fysisk persons vitale interesser i tilfælde, hvor den registrerede fysisk eller juridisk ikke er i stand til at give samtykke.

d) Behandling foretages af en stiftelse, en sammenslutning eller et andet organ, som ikke arbejder med gevinst for øje, og hvis sigte er af politisk, filosofisk, religiøs eller fagforeningsmæssig art, som led i organets legitime aktiviteter og med de fornødne garantier, og på betingelse af at behandlingen alene vedrører organets medlemmer, tidligere medlemmer eller personer, der på

grund af organets formål er i regelmæssig kontakt hermed, og at personoplysningerne ikke videregives uden for organet uden den registreredes samtykke.

e) Behandling vedrører personoplysninger, som tydeligvis er offentliggjort af den registrerede.

f) Behandling er nødvendig, for at retskrav kan fastlægges, gøres gældende eller forsvares, eller når domstole handler i deres egenskab af domstol.

g) Behandling er nødvendig af hensyn til væsentlige samfundsinteresser på grundlag af EU-retten eller medlemsstaternes nationale ret og står i rimeligt forhold til det mål, der forfølges, respekterer det væsentligste indhold af retten til databeskyttelse og sikrer passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser.

h) Behandling er nødvendig med henblik på forebyggende medicin eller arbejdsmedicin til vurdering af arbejdstagerens erhvervsevne, medicinsk diagnose, ydelse af social- og sundhedsomsorg eller -behandling eller forvaltning af social- og sundhedsomsorg og -tjenester på grundlag af EU-retten eller medlemsstaternes nationale ret eller i henhold til en kontrakt med en sundhedsperson og underlagt de betingelser og garantier, der er omhandlet i stk. 3.

i) Behandling er nødvendig af hensyn til samfundsinteresser på folkesundhedsområdet, f.eks. beskyttelse mod alvorlige grænseoverskridende sundhedsrisici eller sikring af høje kvalitets- og sikkerhedsstandarder for sundhedspleje og lægemidler eller medicinsk udstyr på grundlag af EU-retten eller medlemsstaternes nationale ret, som fastsætter passende og specifikke foranstaltninger til beskyttelse af den registreredes rettigheder og frihedsrettigheder, navnlig tavshedspligt.

j) Behandling er nødvendig til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, på grundlag af EU-retten eller medlemsstaternes nationale ret og står i rimeligt forhold til det mål, der forfølges, respekterer det væsentligste indhold af retten til databeskyttelse og sikrer passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser.

3. Personoplysninger som omhandlet i stk. 1 kan behandles til de formål, der er omhandlet i stk. 2, litra h), hvis disse oplysninger behandles af en fagperson, der har tavshedspligt i henhold til EU-retten eller medlemsstaternes nationale ret eller regler, der er fastsat af nationale kompetente organer, eller under en sådan persons ansvar, eller af en anden person, der også har tavshedspligt i

henhold til EU-retten eller medlemsstaternes nationale ret eller regler, der er fastsat af nationale kompetente organer.
4. Medlemsstaterne kan opretholde eller indføre yderligere betingelser, herunder begrænsninger, for behandling af genetiske data, biometriske data eller helbredsoplysninger.[44]

Et eksempel på, hvordan artikel 9 anvendes som behandlingsgrundlag, kan være følgende: En patient skal modtage behandling, der er tillagt sundhedsvæsenet at udføre. Databeskyttelsesloven § 7 stk. 3 tilskriver: "hvis behandling af oplysninger er nødvendig med henblik på forebyggende sygdomsbekæmpelse, medicinsk diagnose, sygepleje eller patientbehandling eller forvaltning af læge- og sundhedstjenester, og behandlingen af oplysningerne foretages af en person inden for sundhedssektoren, der efter lovgivningen er undergivet tavshedspligt". Den danske bestemmelse er i overensstemmelse med databeskyttelsesforordningens artikel 6, stk. 1 litra e, idet sådan behandling begrundes i samfundsinteresser[45].

Sag C-77/21 illustrerer, hvordan formålsbegrænsning og opbevaringsprincipperne for et behandlingsgrundlag kan fortolkes i vurderingen af lovlig databehandling. I sagen skulle EUD (EU-domstolen) tage stilling til, om en ungarsk internet- og tv-leverandør overholdt databeskyttelsesforordningens artikel 5, stk. 1 litra b og e. Den ungarske internet og tv-leverandør, Digi, havde opbevaret og registreret sine kunders personoplysninger til brug for testformål og fejlfinding i testdatabase. EU-Domstolen skulle på baggrund af dette vurdere, om Digi lovligt kunne behandle disse oplysninger, når personoplysningerne var oprindeligt indsamlet til andet formål, samt hvorvidt principperne om formålsbegrænsning og opbevaringsbegrænsning var overholdt.

EUD konkluderede, at videregivelse af personoplysninger kan være legitimt, hvis det sker med udgangspunkt i det oprindelige formål. Data, der anvendes til test og fejlfinding, må ikke opbevares længere end nødvendigt. Det er de nationale domstole i medlemsstaterne, der skal vurdere, hvorvidt testformålet er i overensstemmelse med det oprindelige formål samt sikre, at tidsbegrænsning af opbevaring overholdes. På baggrund af dommen kan det konkluderes, at

[44]Europa-Parlamentet & Rådet. (2016). Forordning (EU) 2016/679 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger
[45]Justitsministeriet. (n.d.). Databeskyttelsesloven § 7. Danske Love.

databehandling er underlagt begrænsninger, når personoplysninger anvendes til egne formål, hvis formålet ikke er i overensstemmelse med det oprindelige behandlingsgrundlag.

Dataansvarliges og databehandleres rollefordeling

Vigtigheden af at få præciseret den og afgrænset rollefordelingen mellem den dataansvarlige og dens databehandler er for tilsikre forudsigelighed og gennemsigtighed. Dette er med til at sikre, at virksomheder og kommuner opfylder deres databeskyttelsesforpligtelser. Forudsigelighed og gennemsigtighed er ligeledes med til at skabe en tillid for den registrerede og gøre datasubjektet i stand til at gøre krav på sine rettigheder. Virksomheder og kommuners opfyldelse af forudsigelighed og gennemsigtighed kan medvirke til et godt omdømme udadtil. Nedenunder beskrives definition af henholdsvis dataansvarlig og databehandler

Dataansvarlig - definition og forpligtelser

Den dataansvarlige bliver i artikel 4, nr. 7 tydeliggjort som en "*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*". Det er den dataansvarliges forpligtelse at sikre, at der udarbejdes en kontrakt med databehandleren, der regulerer behandlingen af personoplysninger jf. artikel 28, stk. 3. Hvis den dataansvarlige også fungerer som databehandler, skal denne selv fastlægge formål og rammer for behandlingen af persondata jf. artikel 28, stk. 10.

Den dataansvarlig er også forpligtet til at sikre, at videregivelse af data kun må ske, hvis der er hjemmel til dette. Behandlingen fra databehandleren må kun finde sted, hvis den ikke er uforenelig med det oprindelige formål, som den dataansvarlige fastsatte. Derudover skal den dataansvarlige sikre, at databehandlerens behandling overholder GDPR-reglerne jf. artikel 24.

Databehandler - definition og forpligtelser

Artikel 4, nr. 8, fastslår, at en databehandler er *"en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den*

dataansvarliges vegne[46]*"*. Hvis en databehandleren anvender en underdatabehandler, omfattes denne også af artikel 4, nr.8. Underdatabehandler har ingen selvstændig legal definition. Det er databehandlerens pligt at sikre, at en given underdatabehandler behandler personoplysninger fortroligt jf. artikel 28, stk.3. Derudover skal databehandleren sørge for, at de organisatoriske og tekniske foranstaltninger er tilstrækkelige jf. GDPR-artikel 32[47].

Afslutningsvis skal det tilføjes, at der kan opstå situationer, hvor der er fælles dataansvarlig. Dette vil sige, at flere aktører i fællesskab fastlægger formålet med databehandlingen samt hvordan denne skal udføres jf. GDPR. artikel 26. Når der er tale om fælles dataansvarlige, skal disse også informere den registrerede om dette jf. artikel 26, stk. 2. Desuden kan den samme aktør indtræde i forskellige roller, såsom både at være dataansvarlig og databehandler i visse behandlinger og ikke i andre. Disse forhold skal reguleres af den kontraktuelle ramme[48]. Datatilsynet har i sin vejledning om dataansvarlige og databehandlere fra 2017 defineret rollefordelingen på følgende måde: "Af databeskyttelsesforordningens definitioner kan det udledes, at der kun vil foreligge en databehandlerkonstruktion, hvis en aftale eller en del af en aftale mellem dig og en anden part (en databehandler) går ud på, at denne anden part skal behandle (f.eks. indsamle, registrere, opbevare, videregive eller slette) personoplysninger efter instruks fra dig som dataansvarlig. Det afgørende for, om der foreligger en instruks, og dermed en databehandlerkonstruktion, er, om en behandling af personoplysninger foretages af en anden part, mens du som dataansvarlig fortsat bestemmer over formålet og over de væsentligste behandlingsskridt, herunder indsamling, sletning, videregivelse og brug af eventuelle underdatabehandlere[49]."

Det Europæiske Databeskyttelsesråds udtalelse vedrørende artikel 28 kan være et vigtigt fortolkningsbidrag til de dataansvarliges forpligtelser i forhold til tilsyn med databehandlere og underdatabehandlere. Den 7. oktober 2024 vedtog Det Europæiske Databeskyttelsesråd en

[46] Bog it-sikkerhed i praksis en introduktion 2022 side 407 til 408

[47] Europa-Parlamentet og Rådet. (2016). Forordning (EU) 2016/679 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse)

[48] Europa-Parlamentet og Rådet. (2016). Forordning (EU) 2016/679 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse)

[49] Datatilsynet. (2017.). Dataansvarlige og databehandlere.

vejledning på foranledning af Datatilsynets spørgsmål vedrørende de dataansvarliges forpligtelser i forhold til tilsyn med databehandler og underdatabehandlere. Denne vejledning skal ses som et bidrag til et hjælpeværktøj for de 27 EU-lande i deres fortolkning af GDPR. Vejledningen viser, at de dataansvarlige bør have informationer om alle databehandlere og underdatabehandlere, uanset om forskelle i størrelsesorden i forhold til den givne risiko ved behandling. Disse informationer omfatter blandt andet navn, kontaktperson og adresse. Informationerne skal sikre, at den dataansvarlige overholder sine forpligtelser jf. Databeskyttelsesforordningen artikel 28. En databehandler bør også sørge for, at den dataansvarlige løbende modtager oplysninger og sikrer de registreredes rettigheder[50]. Vejledningen tillægger også databehandleren forpligtelser. Databehandleren bør sørge for, at underdatabehandlere kan sikre tilstrækkelige garantier. Vejledningen påpeger samtidig, at det i sidste ende er den dataansvarlige, der står for det overordnede ansvar, og skal beslutte, om underdatabehandlere kan opfylde forpligtelserne ved at demonstrere tilstrækkelige garantier. Jo mere risikobaseret databehandlingen er, jo større krav bør stilles til den dataansvarlige, om at stille øgede krav til dokumentation for, at der ydes tilstrækkelige garanti, der kan sikre den dataansvarliges compliance[51].

Vejledningen tilvejebringer ligeledes information om, hvordan den dataansvarlige skal forholde sig til videregivelse af data til databehandleren. Databeskyttelsesforordningens artikel 28, stk. 3, fastlægger en forpligtelse til, at den dataansvarlige og databehandleren indgår en kontrakt om databehandling. Dette gælder i alle tilfælde, hvor der er tale om behandling af personoplysninger. I artikel 28 stk. 3 litra a, statueres det nærmere: ”*instrukser vedrørende databehandling eller behandling til andre tredjelande pålægges af den dataansvarlige. Dette skal fremgå af kontrakten for at sikre gennemsigtighed og tydeliggøre forpligtelser*”[52].

I sag 683/21 blev det illustreret, hvordan rollefordelingen mellem den dataansvarlige og databehandleren samt deres forpligtelser ikke var tydeliggjort nok i kontrakten. I sagen var der

[50]European Data Protection Board. (2024, October). Opinion 22/2024 on certain obligations following from the reliance on processors and sub-processors

[51] European Data Protection Board. (2024, October). Opinion 22/2024 on certain obligations following from the reliance on processors and sub-processors

[52] European Data Protection Board. (2024, October). Opinion 22/2024 on certain obligations following from the reliance on processors and sub-processors

tale om en aftale indgået mellem det offentligt og det private om udvikling af en sundhedsapp til borgere. CJEU (Den Europæiske Unions Domstol) traf denne principale afgørelse den 5. december 2023. I sagen blev der taget stilling til, hvorvidt en dataansvarlig skal defineres i databeskyttelsesforordningen i en situation, hvor det offentlige har udviklet mobilapplikationer til et it-produkt, der skulle bruges i forbindelse med Covid. Det litauiske sundhedsministerium havde tilkøbt en app fra en privat virksomhed til registrering og monitorering af personoplysninger om borgere, der havde haft Covid. Formålet med dette var epidemiologisk opfølgning. I 2020 blev appen downloadet af over 3.000 brugere via Apple app store og Google Play Store. Mens brugerne havde appen på deres enhed, blev der videregivet personoplysninger herunder oplysninger om isolationsforhold og helbredstilstande. Senere på året blev appen lukket ned på grund af manglende finansiering[53]. Grundet den store mængde indsamlede data iværksatte det Litauiske databeskyttelsesinspektorat en undersøgelse. Undersøgelsen konkluderede, at Covid-appen havde videregivet de registrerede data om borgerne til en anden litauisk virksomhed. Denne virksomhed administrerede et it-system til kontrol og overvågning af smitsomme sygdomme og havde anvendt data fra appen. Derudover var der leveret fiktive data med det specifikke formål at teste appen[54]. Ovenstående forhold medførte, at det litauiske sundhedsministerium i afgørelsen fandt, at det havde medvirket til udvikling af appen ved at klargøre formålet med dataindsamlingen samt midlerne til databehandlingen. Det litauiske sundhedsministerium var således dataansvarlig jf. artikel 4, stk.7, da selve appen blev leveret på ministeriets vegne. At ministeriet ikke udtrykkeligt havde givet samtykke til datastrømme igennem appen eller selv havde stået for egen databehandling, og kontakt til virksomheden bag appen, var ikke nok til fralæggelse af ansvaret. Domstolens vurdering omkring anonymiserede data til test til videreudvikling afhænger af, om dataene kan spores tilbage til en identificerbar person. Hvis dette er tilfældet, er der tale om behandling i henhold til databeskyttelsesforordningen[55]. Det principale i afgørelsen er, at CJEU vurderede, at det offentlige godt kan defineres som dataansvarlig, hvis der iværksættes en udvikling. Ligeledes i de situationer, hvor der ikke sker en direkte databehandling, kan begrebet dataansvarlig anvendes, så længe de involverede partnere har haft indflydelse på formål og midler for databehandling. Afgørelsen viste også, at der er situationer, hvor fælles dataansvar er en

[53] Den Europæiske Unions Domstol. (2023). CJEU - C-683/21.
[54] Den Europæiske Unions Domstol. (2023). CJEU - C-683/21.
[55] Den Europæiske Unions Domstol. (2023). CJEU - C-683/21.

mulighed, selv uden en formel aftale. Det afgørende beror på, at de tilsammen har haft indflydelse på databehandlingen. Fælles dataansvarlige er forpligtet til at overholde lovgivningen i forhold til deres respektive ansvar. I situationer, hvor databehandleren har handlet efter instruks fra den dataansvarlige, kan den ansvarlige også pålægges administrative bøder. Overtrædelsen skal enten have været forsætlig eller uagtsom. Afgørelsen viser også, at en eventuel fraskrivelse af ansvaret som dataansvarlig kræver udtrykkelig afvisning af ansvaret[56].

Delkonklusion - den dataansvarlig og databehandlerens rollefordeling og forpligtelser

Det essentielle er at undersøge, hvordan databehandlerkonstruktionen er opbygget. Der skal afklares, hvem der er databehandler, og om der er underdatabehandlere. Ligeledes skal det afklares, om databehandlerkonstruktionen indebærer en selvstændig dataansvarlig eller fælles dataansvarlige.

Det er ligeledes afgørende at identificere, hvilke kategorier af personoplysninger, der behandles samt klarlægge datastrømmen og fastsætte formålet med dataindsamlingen. Derudover skal databehandlerkonstruktionen kunne dokumenteres og dermed tilsikre, alle parter overholder disse krav i kontrakten. Tilsynet med, om reglerne bliver overholdt, skal afhænge af en individuel vurdering. Der skal dog være en proportional afvejning. Kort sagt: jo større risiko, der er for den registrerede, desto flere tilsyn skal forekomme.

Kommunernes brug af Cloudløsninger

I det kommende afsnit vil der være en analyse af hovedelementerne i Chromebooksagen. Chromebook-sagen startede i Helsingør kommune med en far til en dreng i folkeskolen, som havde fået oprettet en YouTube- konto med drengens personoplysninger uden faderens vide. Faderen rejste spørgsmålet om, hvorvidt dette var lovligt, til Datatilsynet. Datatilsynet fandt frem til, at sagen ikke kun vedrører Helsingør kommune, men også andre folkeskoler fordelt på 53

[56] Den Europæiske Unions Domstol. (2023). CJEU - C-683/21.

kommuner. Derudover konkluderede Datatilsynet, at flere af kommunerne havde forsømt deres ansvar ved at godkende Googles Cloud-standardkontraker[57]. Analysen vil bidrage til forståelse af dataretlige problemstillinger i forbindelse med offentlige myndigheders brug af cloud-ydelser leveret af private aktører. Databeskyttelsesforordningen skal ses i en teknologineutral kontekst. Dette betyder, at enhver databehandling skal ske inden for de dataretlige rammer, uanset hvilket system, der tages i brug.

For at kunne undersøge de retlige problemstillinger ved offentlige myndigheders brug af cloud-ydelser leveret af private aktører er det essentielt at forstå begrebet "Cloud". Begrebet vil derfor kort blive beskrevet nedenunder.

Cloudbegrebet og dens funktion

Cloud-ydelser kan være alt fra simple, standardiserede it-løsninger forbundet med decentrale systemer til netværk af servere, der kan tilgås via internettet. Cloud-løsninger kan også være tjenester med komplette applikationer. Disse mange forskellige Cloud-leverancer medfører også, at der kan opstå en række dataretlige dilemmaer. Dette kan f.eks. vedrøre ansvarsfordeling mellem kunden og leverandøren i forhold til overholdelse af GDPR-reglerne. Datatilsynet har udarbejdet et illustrativt eksempel: En kommune benytter et tekstbehandlingsprogram, hvor funktionaliteten skabes på en server i Irland og vises på brugernes skærme. Kommunen gemmer og opbevarer alle skabte dokumenter på kommunens egen server, men tekstbehandlingsprogrammet, herunder login, opsætninger, brug af orddeling, stavekontrol og al anden funktionalitet, afvikles på serveren i Irland[58]. I cloud-løsninger har kunden som oftest kun kontrol over mængden og typen af ressourcer. Dette indebærer blandt andet processer-kraft, lagring og netværkstopografi, som en potentiel kunde ønsker at få leveret. Cloud-leverandøren har derimod den fulde administration over, hvilke ressourcer der vil tilvejebringes, samt hvor de skal tilvejebringes[59].

[57] Datatilsynet. (2024, januar). Datatilsynet giver påbud i Chromebook-sag
[58] Datatilsynet, Vejledning om Cloud, 2022
[59] Datatilsynet, Vejledning om Cloud, 2022

Datatilsynet har kategoriseret følgende tre cloud-infrastrukturer:

1. Cloud Infrastruktur som en service (IaaS):

   Er kendt for at være en enkel løsning. Kunden får adgang til de grundlæggende ressourcer såsom lagring. netværk og processor-kraft. Kundens ansvar er at drive og installere den tildelte software. Driften skal kunden stå for. Drift kan omfatte sikring, etablering og operativsystemer samt kontrol over lagring af data og forretningsapplikationer.

2. Platform som en service (PaaS):

   Ved PaaS får kunden ikke kun adgang til infrastruktur, men også adgang til de centrale API'er (Grænseroverflade), databaser samt operativsystemer. Kunden har også mulighed for selv at udvikle og tilkøbe alternative applikationer, der kan implementeres i infrastrukturen. Ved PaaS er kunden ansvarlig for eventuelle egen implementerede applikationer og konfigurationsindstillinger i applikationens driftsmiljø. Leverandøren har derimod ansvar for og kontrol med den leverede software, infrastruktur og operativsystemer. PaaS Cloud-tjenester kan i visse situationer også give mulighed for avancerede funktioner til standardværktøjer, hvor kundens egen applikationer spiller sammen med kundens egne features. Dette kan eksempelvis være algoritmer til AI chatbots, big dataanalyser og kunstig intelligens. Leverandøren vil ofte have ansvaret for operativsystemer og infrastrukturen samt drift og udvikling af det, der ikke vedrører kundens egne forretningsapplikationer.

3. Software as a service (SaaS):

   SaaS-software er en løsning, hvor leverandøren har færdigudviklede, cloudbaseret forretningsapplikationer, som kunden kan få adgang til. Kunden har også mulighed for ekstra service, ved at leverandøren sørger for driften af servicen. I modsætning til de to ovenstående cloud-løsninger giver SaaS-løsninger ofte ikke kunden mulighed for at tilpasse produktet. Leverandøren er den ansvarlige for drift og vedligeholdelse af det samlede produkt [60].

Der er obligatoriske forpligtelser for den dataansvarlige til at sikre tilsyn med cloud-leverandøren. Det kan siges, at jo mere komplekse opgaver, der bliver overladt til cloud-leverandøren og jo

[60] Datatilsynet, Vejledning om Cloud, 2022

højere risiko, databehandlingen indebærer for de registrerede, desto større ansvar har den dataansvarlige for at sikre, at de databeskyttelsesretlige regler overholdes, samt at kunne dokumentere, at dette sker[61].

Cloud-løsninger kan leveres på forskellige måder, og datatilsynet har skitseret disse 3 typer af leverancemodeller:

1. Privat cloud:
   Cloud-servicen er til eksklusiv brug af og i en enkelt organisation. Den kan ejes, forvaltes og drives af organisationen selv, en tredjepart eller en kombination af dem, og den kan være etableret i eller uden for organisationens egne faciliteter.
2. Fælles (shared) cloud. Cloud-servicen er til eksklusiv brug af en veldefineret gruppe af organisationer. Den kan ejes, forvaltes og drives af en eller flere af organisationerne i fællesskabet, en tredjepart eller en kombination af dem, og den kan være etableret i eller uden for organisationernes egne faciliteter. En fælles cloud-service tilgodeser typisk de deltagende organisationers fælles behov. Samtidig vil governancestrukturerne (aftalerne og styringsmekanismerne) for en fælles cloud-service typisk give hver organisation større indflydelse på styring og udvikling, end det er tilfældet ved en mere generisk offentligt tilgængelig cloud-service.
3. Offentligt tilgængelig (public) cloud:
   Cloud-servicen udbydes typisk på generelle kommercielle vilkår. Den kan ejes, forvaltes og drives af en virksomhed, en akademisk eller en statslig organisation eller en kombination af dem. Den er etableret i cloud-leverandørens faciliteter og cloud-leverandøren fastsætter egenhændigt politikkerne for servicen. De offentligt tilgængelige cloud-services tilbyder typisk den største kapacitetsmæssige fleksibilitet, den bredeste vifte af services og den hurtigste udvikling af nye services.
4. Hybrid cloud:
   Cloud-servicen er en sammensætning af to eller flere forskellige cloud-services (privat, fælles eller offentlig). Hver cloud-service forbliver en unik enhed, men de er forbundet på

[61] Datatilsynet, Vejledning om Cloud, 2022

en måde, der muliggør, at data og applikationer kan flyttes rundt imellem hver enhed (fx til balancering af belastning). En hybrid-cloudservice er altså ikke det samme som at have flere individuelle, ukoordinerede cloud-services[62].

Viden om de forskellige leverandørmodeller er essentiel for at danne sig et overblik over de sikkerhedsmæssige og tekniske kompleksiteter samt rolle- og ansvarsfordeling. Disse overvejelser skal adresseres i databehandleraftalen for at sikre, de databeskyttelsesretlige regler overholdes. Derudover bør disse forhold belyses ved tilsyn af cloud-leverandøren og eventuelle underdatabehandlere, herunder databehandlere i tredjelande. Dokumentation skal sikre, at personoplysninger behandles til det rette formål, samt der er tilsyn med systemet kun giver adgang til de rette personer[63].

Overførsel af personoplysninger til USA

Når der er tale om en fælles eller private cloud-leverandør kan en kundetilpasset databehandleraftale være en løsning for det offentlige at indgå med leverandøren af cloud-ydelsen. Modsætningsvis er offentlige tilgængelige cloud-ydelser leverandørens ansvar. Dette kan skabe juridiske dilemmaer, hvis leverandøren kommer fra et land uden for EU/EØS-land. Risikoen for juridiske dilemmaer mindskes, hvis leverandøren er fra EU/EØS, da de er forpligtet til at følge databeskyttelsesforordningen. Det er den offentlige myndigheds ansvar at sikre, deres leverandører forpligter sig på at overholde de lovgivningsmæssige krav[64].

Databeskyttelsesforordningen stiller supplerende krav til overførsel af personoplysninger, når det gælder lande uden for EU. Pædagogisk kan man sige, at der findes to zoner for opbevaring og behandling af data:

1. Sikker zone, der ikke kræver specielle aftaler (EU/EØS-lande)

[62] Datatilsynet, Vejledning om Cloud, 2022
[63] Datatilsynet, Vejledning om Cloud, 2022
[64] Digitaliseringsstyrelsen, Vejledning i anvendelse af cloudservices version 1.1, juli 2020

2. Usikker zone (Lande uden for EU/EØS), Hvor EU-kommissionen skal godkende, at et givent lands databeskyttelsesniveau er tilstrækkeligt[65].

EU og USA havde tilbage i 2015 en persondataaftale, der gjorde, at amerikanske virksomheder befandt sig i en sikker zone. Dette blev imidlertid ændret i 2015, da Maximillian Schrams ved de irske domstole vandt en sag mod Facebook Ireland Limted. EU-domstolen fandt blandt andet, at Facebook i strid med databeskyttelsesforordningen kunne indsamle data, som - på grund af deres amerikanske ophav, de amerikanske myndigheder kunne få adgang til. Afgørelsen medførte, at hvis der skal ske udveksling af personoplysninger mellem EU/EØS og USA, skal der være en databehandleraftale, der bygger på EU- kommissionens standardkontraktbestemmelser[66].

Chromebooksagens dataretlige hovedelementer

Den 30. januar 2024 traf Datatilsynet en betydningsfuld afgørelse, som har resulteret i øget opmærksomhed på kommunernes brug af cloud-ydelser fra private tech giganter. Afgørelsen vedrørte 53 danske kommuner, der benyttede Chromebooks i folkeskoler. Datatilsynets afgørelse viste, at kommunerne havde forsømt at sikre, at deres databehandleraftaler indeholdt den nødvendige lovhjemmel til at videregive børns personoplysninger i forbindelse med folkeskolernes brug af Chromebooks, når oplysningerne blev anvendt til forbedring og produktudvikling af Microsoft egne produkter. Ydermere blev kommunerne kritiseret for, at de som offentlige myndigheder havde forsømt at leve op til deres særlige ansvar for borgeres, herunder særlig børns datasikkerhed.

I afgørelsen blev retsgrundlaget for persondatabehandling skitseret i overensstemmelse med databeskyttelsesforordningen: ”Personoplysninger kan behandles på baggrund af et af flere behandlingsgrundlag, som findes i databeskyttelsesforordningens artikel 6, stk. 1. For offentlige myndigheder vil behandling af personoplysninger oftest ske, fordi det er nødvendigt for at overholde en retlig forpligtelse, jf. artikel 6, stk. 1, litra c, eller fordi behandlingen er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig

[65] Pedersen, A. Á., & Vandrup, K. D. (2022). It-sikkerhed i praksis – En introduktion. Samfundslitteratur. s. 421
[66] Pedersen, A. Á., & Vandrup, K. D. (2022). It-sikkerhed i praksis – En introduktion. Samfundslitteratur. s.423

myndighedsudøvelse, jf. artikel 6, stk. 1, litra e. Behandlingen skal i begge tilfælde have et såkaldt supplerende retsgrundlag, som forpligter eller berettiger myndigheden til at udføre en bestemt myndighedsopgave. Det følger af databeskyttelsesforordningens artikel 6, stk. 3".
For at benytte sig af artikel 6, stk. 3 1.pkt skal der være nedsat et supplerende retsgrundlag enten af EU-retten eller i national ret.

Datatilsynet inddrog ligeledes præambelbetragtning nr. 45 og nr. 41 i deres afgørelse for at bidrage til forståelsen af artikel 6, stk. 1, litra e: "*Det fremgår af præambelbetragtning nr. 45, at databeskyttelsesforordningen ikke indebærer, at der kræves en specifik lov til hver enkelt behandling efter artikel 6, stk. 1, litra e. Det kan være tilstrækkeligt med en lov som grundlag for adskillige databehandlingsaktiviteter. Der stilles dog krav om, at behandling efter bestemmelsen sker på baggrund af EU-retten eller national ret. Endvidere følger det af præambelbetragtning nr. 41 til databeskyttelsesforordningen, at det pågældende retsgrundlag ikke nødvendigvis kræver en lov, men at retsgrundlaget dog bør være klart og præcist, og anvendelsesområdet bør være forudsigeligt for personer omfattet af retsgrundlagets anvendelsesområde*".
Af Justitsministeriets betænkning nr. 1565/2017, s. 132f., fremgår følgende om forordningens artikel 6, stk. 1, litra e. "*Datatilsynet pegede på, at selve behandlingen ikke i sig selv antager udtrykkelig beskrivelse i lov. Brugen af artikel 6, stk. 1, litra e, kræver heller ikke nødvendigvis, at opgaven, som kræver behandling af personoplysninger, udtrykkeligt i lovgivningen er pålagt myndigheden. Der kan i den forbindelse henvises til [Datatilsynets udtalelse i sagen med j.nr. 2004-54-1394], hvor tilsynet fandt det naturligt, at Undervisningsministeriet, som den centrale myndighed på området, løste en opgave vedrørende digital tilmelding til og ansøgning om optagelse på uddannelser, selvom der ikke var en udtrykkelig lovhjemmel, der pålagde ministeriet opgaven. Ministeriet kunne derfor bruge bl.a. § 6, stk. 1, nr. 5, i persondataloven om behandling, der er nødvendig af hensyn til udførelsen af en opgave i samfundets interesse*."

Datatilsynet valgte også at lægge vægt på betænkningens s. 160 om forordningens artikel 6, stk. 3 for at kunne bidrage til fortolkningen af, hvad der menes med offentlig myndighedsudøvelse, når behandling sker i samfundets interesse og er pålagt myndigheden at udfører: "*Det følger*

derudover af forordningens artikel 6, stk. 3, 2. pkt., specifikt vedrørende behandling, der er omhandlet i artikel 6, stk. 1, litra e – dvs. af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse – at behandlingen skal være "nødvendig for udførelsen af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse". Det må også her være tilstrækkeligt for opfyldelse af dette nødvendighedskrav, at det kan udledes af den pågældende nationale lov med dens forarbejder, under forudsætning af at behandlingen rent faktisk er "nødvendig". I artikel 6, stk. 3, sidste led, er der et yderligere krav til den lovgivning, som tilpasses anvendelsen af databeskyttelsesforordningen. Der er et krav om, at medlemsstaternes nationale ret skal opfylde et formål i samfundets interesse og stå i rimeligt forhold til det legitime mål, som forfølges. Databeskyttelsesforordningen fastsætter således et krav om proportionalitet og iagttagelse af samfundets interesse i forbindelse med national ret og EU-ret, der tilpasser anvendelsen af databeskyttelsesforordningen[67].

Et andet afgørende hovedelement, når kommuner behandler data er, at proportionalitetsprincippet skal inddrages. Dette vil betyde, at jo mere indgribende en behandling af personoplysninger er, desto klarer lovhjemmel skal der være. Dette afspejles i sagen C-175/20, hvor EUD udtalte følgende: *"I denne henseende bemærkes ikke desto mindre, at den lovgivning, som danner grundlag for behandlingen, for at opfylde det krav om proportionalitet, som artikel 5, stk. 1, litra c), […] er udtryk for […], skal fastsætte klare og præcise regler, der regulerer rækkevidden og anvendelsen af den omhandlede foranstaltning, og som opstiller mindstekrav, således at de personer, hvis personoplysninger er berørt, råder over tilstrækkelige garantier, der gør det muligt effektivt at beskytte disse oplysninger mod risikoen for misbrug. Denne lovgivning skal være retligt bindende i national ret og navnlig angive, under hvilke omstændigheder og på hvilke betingelser der kan vedtages en foranstaltning om behandling af sådanne oplysninger, hvorved det sikres, at indgrebet begrænses til det strengt nødvendige*"[68].

[67] Datatilsynet. (2024, januar). Datatilsynet giver påbud i Chromebook-sag
[68] Datatilsynet. (2024, januar). Datatilsynet giver påbud i Chromebook-sag

Det offentliges brug af cloud-løsninger er ofte en behandling af data til eget formål. I Chromebooksagen påpegede Datatilsynet, at cloud-ydelser, ud over det produkt, de leverer, også indsamler data til eget formål herunder til forbedring af egne produkter. Denne indsamling anses ikke altid for lovlig, når de anvendte oplysninger bruges til private aktørers egne kommercielle formål: "*funktionaliteten af de løsninger, der ønskes anvendt, eller markedspositionen af den leverandør, der ønskes valgt, ikke kan begrunde en manglende overholdelse af databeskyttelsesreglerne. En standardiseret opbygning af løsningerne eller den blotte anvendelse af et standardprodukt kan ligeledes ikke begrunde en manglende overholdelse af databeskyttelsesreglerne*[69]".

Dermed påvises det, at kommuner skal kunne kortlægge, afklare og vurdere, når der sættes it-system i drift ved Cloud. I Chromebookafgørelsen blev der lagt vægt på 3 forhold:

1. Selve hjemlen til videregivelsen.
2. Hvorvidt videregivelsen sker med henblik på forbedring af de leverede tjenester
3. Udvikling af nye tjenester og funktioner.

Dette resulterede i, at selve videregivelsen af personoplysninger til Microsoft Cloud-løsningen, hvor formålet var at forbedre produktet f.eks. øget sikkerhed og funktionalitet, var i overensstemmelse med Databeskyttelsesforordningen. Modsat var der ikke hjemmel til videregivelse af personoplysninger med henblik på forbedring og vedligeholdelse af Microsofts egen tjenester samt produktudvikling. Det fastlægger derfor, at den dataansvarlig skal sikre, hvordan behandling af data skal foregå samt til hvilket formål. En kommune er hermed forpligtet til at undersøge, om databehandleren bruger de indsamlede personoplysninger, og om der er lovhjemmel til dette[70].

Datatilsynet præciserer derimod, at videregivelsen af anonymiserede personoplysninger kan ske frit, da disse ikke er underlagt GDPR-reglerne. Det er hermed lovligt at bruge anonymiserede data til videreanvendelse. Dette rejser dog et principielt spørgsmål om, hvorvidt sådanne data

[69] Datatilsynet. (2024, februar). Region Syddanmarks påtænkte brug af Microsoft 365

[70] Datatilsynet. (2024, februar). Region Syddanmarks påtænkte brug af Microsoft 365

overhovedet kan anonymiseres, da de er bygget på reelt identificerbare data. Datatilsynet henviser til 2 eksempler:

1. Hvor den dataansvarlige selv har anonymiseret data inden videregivelse
2. Hvor det er databehandleren, som står for at anonymisere data.

I andet eksempel bliver det vurderet som videregivelse af personoplysninger.

Chromebooksagens relevans ift. til andre offentlige cloud-løsninger

Efter datatilsynets afgørelse om påbud til 53 skolers brug af Chromebook, er der blevet et skærpet fokus på samarbejdet mellem kommunale og private virksomheder i forbindelse med databehandling. Afgørelsen har rejst et principalt spørgsmål om, hvorledes det offentlige skal håndtere brugen af cloud-løsninger samtidig med at det sikres, at den private leverandør overholder GDPR.

Afgørelsen har givet anledning til at undersøge, om der vil ske et påbud i enhver brug af cloud-løsninger. Som svar på spørgsmål fra region Syddanmark om deres brug af Cloud leveret af Microsoft, udtalte Datatilsynet sig følgende om at kortlægge, afklare og vurdere:

- Hvilke kategorier af personer vil regionen behandle personoplysninger om, herunder f.eks. medarbejdere, patienter mv., som led i brugen af M365?
- Hvilke personoplysninger vil regionen behandle om disse kategorier af personer, og i hvilket omfang vil der blive indsamlet og behandlet metadata om disse personer?
- Hvilket retsgrundlag vil danne baggrund for regionens behandling af de pågældende personoplysninger?
- Hvilke specifikke formål vil Microsoft konkret behandle oplysninger til som led i at holde ”*produkter opdateret og ydende samt forbedre brugernes produktivitet, pålidelighed, effektivitet, kvalitet og sikkerhed*”, og i hvilken rolle?
- Hvordan genereres den ovennævnte aggregerede statistik konkret, herunder navnlig om aggregeringen eller anonymiseringen sker, inden oplysninger videregives til Microsoft?

- Vil det pågældende retsgrundlag kunne danne baggrund for videregivelse af de pågældende personoplysninger til Microsoft til brug for de formål, der er beskrevet ovenfor?

Dette ansvar pålægges af den dataansvarlig jf. §§ artikel 24 stk.1 og 5 stk. 2. Det er Datatilsynets opfattelse, at standardiserede it-løsninger godt kan benyttes, men at disse ikke kan begrunde en manglende overholdelse af GDPR-reglerne[71].

Bindi vs commission T-354/22

Den 8. januar 2025 faldt der er en principal dom fra EUD. Afgørelsen vedrører databeskyttelse af personoplysninger, der behandles af EU-unionens institutioner, kontorer og agenturer og videregives til tredjelande. Sagen blev appelleret af en tysk statsborger, som havde en retlig interesse i informationsteknologi og dens samspil med beskyttelse af personlige data. Den tyske statsborger havde besøgt en hjemmeside, der administreres af EU-kommissionen, kaldet "*Conference on the future of Europe*". Her mente han, at han som datasubjekt ulovligt havde fået videregivet personoplysninger, heriblandt IP-adresse og andre oplysninger fra sin browser til aktører i USA via EU-hjemmesiden. Denne videregivelse skete via Amazon CloudFront og ved klik på funktionen "Log ind med Facebook".[72] Der blev rejst to retlige krav, som EUD skulle tage stilling til:

1. Kompensation på 400 euro for ulovlig videregivelse af personoplysninger til tredjelande, som ikke overholder databeskyttelsesforordningens regler jf. 46 samt annullering af disse data jf. 48 stk. 1 og 2 litra b.[73]
2. Kompensation på 800 euro for manglende ret som datasubjektet til indsigt i, hvilke data, som var blevet videregivet til USA jf. artikel 14 stk. 3 og 4 samt for manglende overholdelse af gennemsigtighed jf. 4 stk. 1 litra a.[74]

EU-domstolen konkluderede, at videregivelsen til Amazon CloudFront ikke var i strid med databeskyttelsesforordningen, idet disse data blev indenfor EU. Vedrørende spørgsmålet om

[71] Datatilsynet. (2024, februar). Region Syddanmarks påtænkte brug af Microsoft 365
[72] Den Europæiske Unions Domstol. (2025). GC - T 354/22 - Bindl v Commission.
[73] Den Europæiske Unions Domstol. (2025). GC - T 354/22 - Bindl v Commission.
[74] Den Europæiske Unions Domstol. (2025). GC - T 354/22 - Bindl v Commission.

hyperlinket ”log på med Facebook” var resultatet, at videregivelsen af personoplysninger til Meta Platforms var i strid med databeskyttelsesforordningen. Her lagde EUD vægt på, at der på daværende tidspunkt ikke var nogen sikkerhedsgaranti for, at USA kunne sikre tilstrækkelige sikkerhedsforanstaltninger i form af standarddatabeskyttelsesklausuler eller andre påviste kontraktklausuler. Desuden påpegede EUD, at funktionen ”Log ind med Facebook” var administreret af Meta og dermed på Metas vilkår. EUD konkluderede, at EU-kommissionen som EU-Institution havde tilsidesat de krav, der er for videregivelse til tredjelande jf. Databeskyttelsesforordningens artikel 46 og 49. Kravet på de 400 EUR blev hermed anerkendt[75].

Hvad er kravene til leverandørstyring af cloud ydelser?

Chromebooksagen og Bindl vs. Commission T-354/22 viser bl.a. hvilke personoplysninger i forbindelse med levering af ydelser som databehandler til det offentlige, lovligt anvende oplysningerne til egne formål. De 2 afgørelser viser også en praksis for, hvilket ansvar den offentlige myndighed har for at sikre, at den private leverandør overholder GDPR. Hvad der kan opsummeres ud fra de 2 sager, fremgår af nedenstående diskussionsafsnit.

Diskussion

EU-charter art. 8 (1) – ”*Enhver har ret til beskyttelse af personoplysninger, der vedrører den pågældende.*” Dette princip er ligeledes forankret i hensigterne bag databeskyttelsesforordningen. I dag bliver retten til beskyttelse af personoplysninger stadig mere kompliceret, især når amerikanske Tech-giganter ikke følger kravene i reglerne for den Europæiske digitale infrastruktur. Den digitale virkelighed, som kommunerne befinder sig i, gør det både kompliceret og uigennemsigtigt, idet de fleste digitale løsninger leveres ved cloud ydelser med uigennemsigtig databehandling. I dag er det sådan, at det i praksis er det offentlige, som dataansvarlig, der har det overordnede ansvar for, at borgernes data behandles i overensstemmelse med GDPR-reglerne. Det er hermed også det offentlige, der risikerer bøder, hvis der sker brud på reglerne. Dette ansvar kan være svært og næsten umuligt at håndtere i nutidens Tech landskab, hvor de største aktører ikke ligefrem er kendte for gennemsigtighed i deres databehandling.

[75] Den Europæiske Unions Domstol. (2025). GC - T 354/22 - Bindl v Commission

Som nævnt fremgår det af EU-charter art. 8 (1) at: "*Enhver har ret til beskyttelse af personoplysninger, der vedrører den pågældende*." Det er en vigtig og fundamental rettighed, som understreger, at databeskyttelsesreglerne har til formål at afveje risikoen for datasubjektets rettigheder i forbindelse med behandling af sine personoplysninger. Momenter som forskelsbehandling, skade på omdømme, krænkelse af sin menneskelig værdighed og kontrol over sin egen personoplysninger er elementer, der tages med i vurderingen. Derfor bør risikoen for disse følgevirkninger i forbindelse med overholdelse af GDPR-reglerne ikke tage udgangspunkt i Tech-giganters eller andre kommercielle virksomheder interesser. Frem for alt må der stilles følgende spørgsmål: Hvad ønsker vi at beskytte datasubjektet imod? Er det uautoriseret adgang til personoplysninger, beskyttelse mod utilsigtet videregivelse eller risikoen for hacking?

Europa står over for et digitalt infrastruktur problem. Siden 2000'erne er de europæiske lande blevet stadig mere afhængige af cloud-løsninger fra især amerikanske virksomheder såsom Meta og Microsoft. Dette gælder både private aktører samt kommuner og andre statslige institutioner. Dilemmaet ligger i, at de amerikanske virksomheder er underlagt en anden lovgivning, der ofte ikke harmonerer med databeskyttelsesforordningen. Dette er blevet påvist af Maximilian Schrems, databeskyttelse aktivist, som har rejst søgsmål mod EU-USA-data aftaler ved EU-domstolen. Dette har blandt andet resulteret i sagerne Safe Harbour og Privacy Shield, der begge har afsløret manglende lovhjemmel til videregivelse af europæiske data, når amerikanske lovgivninger ikke imødekommer samme sikkerhedsgarantier som databeskyttelsesforordningen[76]. Med den stigende usikkerhed efter Donald Trump tiltrædelse, er der opstået et reelt spørgsmål om, hvorvidt USA vil overholde den nuværende aftale mellem EU og USA kaldet TDPF (Transatlantic Data Privacy Framework). Aftalen er udformet som et værn mod amerikanske virksomheder, hvis disse bliver pålagt pligt til at adlyde den føderale stat om videregivelse af udenlandske personoplysninger. I dag estimeres det, at hele 90% af europæiske virksomheder videregiver data til USA[77]. Dette har skabt et kolossalt dilemma og kan i sidste ende føre til, at danske virksomheder

[76] DR Podcast: Genstart: kan USA slukke skyen? 16/4 2025

[77] Euractiv (2025, April 16). Deafening Commission silence, with no credible EU-US data oversight left

og kommuner ikke lovligt kan bruge ydelser fra Microsoft herunder f.eks. co-pilot, OneNote, Word og Excel etc.

I Danmark er der ligeledes blevet rejst bekymring, blandt andet af digitaliseringsminister Caroline Stage, der understreger nødvendigheden af, at Danmark og Europa gør sig mindre afhængige af amerikanske Tech-giganter. I stedet bør der skabes mere Europæisk teknologi på bedre konkurrencevilkår, så det bliver nemmere og billigere at skifte leverandør af Cloud-løsninger.[78] Man kunne fristes til at tro, at den øgede europæiske skepsis og bekymring for datasikkerheden ville påvirke de store Tech-giganters vilje til at imødekomme datakrav. Det største problem for store aktører som Microsoft er, hvis forbrugerne vænner sig til alternative produkter. Dette kan blive en realitet med den øgede bevågenhed og de igangværende samtaler fra europæiske side om EU's muligheder for at gøre sig uafhængige af amerikanske cloud-ydelser. Den 30. april 2025 erklærede Microsoft, at virksomheden vil beskytte Europæiske borgeres data, hvis amerikanske myndigheder vil have indsigt i dem. Microsofts direktør erklærede, at han ikke fandt situationen sandsynlig, men hvis det skete, ville Microsoft kompensere forbrugerne. Selvom Microsoft ikke forventer et amerikansk føderalt påkrav om adgang til europæiske borgeres data, lover virksomheden at etablere datacentre på europæisk grund, en såkaldt ”Europæisk Cloud”, som lokale virksomheder så skal administrere i overensstemmelse med lokal lovgivning[79]. Europæiske databeskyttelsesråd (EDPB) har i sin opinion fra oktober 2024 udtrykt, at selvom virksomheder vælger, at databehandling skal ske i et EU-land, kan der stadig opstå juridiske problemstillinger. Disse kan inkludere krav fra virksomhedens hjemland om at udlevere europæiske data i strid med databeskyttelsesforordningen.[80]

Databeskyttelsesforordningen bygger på etiske principper. Manglende overholdelse af beskyttelsen af individets personoplysninger udgør en trussel mod privatlivet. Skarpt formuleret kan det siges, at det er uetisk manipulation fra det offentliges side, når de indkøber licenser til Cloud-løsninger uden viden om, hvordan borgernes data bliver lagret, og til hvilket formål. Databeskyttelsesforordningen har styrket sikkerheden ved at harmonisere og fastsætte

[78] (2025, april 25). Minister vil bekæmpe tech-afhængighed: Arbejder på exit-plan fra amerikansk cloud | Version2
[79] (2025, April 30). Microsoft pledges to take legal action if governments try to seize EU data.
[80] Opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s)

minimumskrav til databehandling[81]. Alligevel ses der afgørelser såsom Chromebooksagen og Bindl vs mod Comission, som viser, at borgerne kan have svært ved at få kontrol over sine personoplysninger. Så længe det offentlige, herunder kommuner, benytter sig af amerikanske Tech giganters cloud-løsninger, må der ske aktiv handling med at sikre regelmæssigt tilsyn med, hvorvidt private leverandør overholder GDPR, og disse virksomheder ikke ulovligt kan anvende personoplysninger til egne formål. Det er det eneste etisk forsvarlige i den digitale verden, vi lever i.

Konklusion

I specialet er det blevet tydeliggjort, at det er det offentlige som dataansvarlig, der har det primære ansvar for, at databehandlingen er i overensstemmelse med databeskyttelsesforordningen. Dette betyder, at den dataansvarlige har pligt til at undersøge, om databehandleren opfylder de kontraktlige krav i den givne databehandleraftale jf. artikel 28, stk. 3. Det offentlige skal have bedre overblik over implementering af cloud-løsninger og sikre, at de er i overensstemmelse med GDPR. Derudover skal der forhandles, hvis standardkontakter ikke lever op til kravene.

Specialet har vist, at manglende fastlæggelse af rollefordeling i databehandleraftaler, har ført til juridiske dilemmaer, f.eks. hvor det offentlige er blevet fælles dataansvarlig uden en formel kontrakt. I den litauiske dom blev det konkluderet, at det litauiske sundhedsministeriums deltagelse i fastlæggelsen af covid-appens formål og midler til databehandling, var tilstrækkeligt til at statuere dataansvarlig. Det offentlige har som dataansvarlig ansvaret for at tydeliggøre og fastlægge rammerne for databehandling over for databehandleren. Dette skal sikre, at der er behandlingshjemmel til alle databehandlingsaktiviteter. Databehandler har ligeledes pligt til at underrette og følge de instrukser, som den dataansvarlige giver. Derudover skal databehandleren sikre, at den lever op til kravene i GDPR ved ikke anvende personoplysninger til andre end de oprindelige formål. I Chromebooksagen blev det tydeliggjort, at private virksomheder, der - som databehandlere - får adgang til personoplysninger i forbindelse med levering af ydelser til det

[81] Pedersen, A. Á., & Vandrup, K. D. (2022). It-sikkerhed i praksis – En introduktion. Samfundslitteratur. S 433

offentlige, ikke lovligt kan anvende oplysningerne til egne formål uden en klar instruks i databehandleraftalen og datasubjektets viden om, at deres data bliver videregivet. Det er blevet fremhævet, at databehandleraftaler skal adressere håndteringen af dataoverførelser til tredjelande. I Bind vs Commission T-354/22 blev det konkluderet, at EU-kommission ikke havde styr på GDPR på sin egen hjemmeside i forbindelse med funktionen "Log ind med Facebook". Dette medførte, at en tysk statsborgers personoplysninger blev videregivet til USA uden samme sikkerhedsgaranti, som databeskyttelsesforordningen kræver.

Specialet har tydeliggjort det offentliges problemer med at sikre, at registreredes databeskyttelsesrettigheder i den digitale verden ikke overholdes tilstrækkeligt.
EU-charter art. 8 (1): "Enhver har ret til beskyttelse af personoplysninger, der vedrører den pågældende", er en rettighed, som ofte står i skarp kontrast til Tech-giganternes daglige virke. Specialet blev indledt med: "USA innoverer, Kina kopierer og EU regulerer". Sandheden er, at EU i høj grad har reguleret, særligt inden for databeskyttelsesområdet. Regulering kan også være en nødvendighed. Databeskyttelsesforordningen er til for, at europæiske borgere ikke mister deres datarettigheder blot på grund af komplicerede datastrømme med uigennemsigtig databehandling. Dette kan være databehandling, der sker i strid med det oprindelig formål og dermed gør, at der sker overførsel af europæiske data til tredjelande som USA. Databeskyttelsesforordningen stiller krav til hele kæden af dataansvarlige, databehandler og underdatabehandlere for at sikre reel dokumentation for, at reglerne bliver overholdt. Dette er fundamentet for, at retten til beskyttelse af personoplysninger sker fyldest.

Litteraturliste

Lovgivning

Europa-Parlamentet & Rådet. (2016). Forordning (EU) 2016/679 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.

Justitsministeriet. (n.d.). Databeskyttelsesloven § 7. Danske Love.

Betænkninger

Justitsministeriet. (2017). Betænkning nr. 1565 – Databeskyttelsesforordningen og de retslige rammer.

Domme

Den Europæiske Unions Domstol. (2010). European Commission v The Bavarian Lager Co. Ltd., C-28/08 P. EUR-Lex.

Den Europæiske Unions Domstol. (2016). Patrick Breyer v Bundesrepublik Deutschland, C-582/14. EUR-Lex.

Den Europæiske Unions Domstol. (2017). Peter Nowak v Data Protection Commissioner, C-434/16. EUR-Lex.

Den Europæiske Unions Domstol. (2023). CJEU - C-683/21. EUR-Lex.

Den Europæiske Unions Domstol. (2025). GC - T 354/22 - Bindl v Commission. EUR-Lex.

Litteratur

Blume, P. (2020). Retssystemet og juridisk metode (4. udg.). Djøf Forlag.

Munk-Hansen, C. (2017). Den juridiske løsning: Introduktion til den juridiske metode (1. udg.). Djøf Forlag.

Munk-Hansen, C. (2022). Retsvidenskabsteori (3. udg.). Djøf Forlag.

Neergaard, U., & Nielsen, R. (2020). EU-ret (8. udg.). Karnov Group.

Pedersen, A. Á., & Vandrup, K. D. (2022). It-sikkerhed i praksis – En introduktion. Samfundslitteratur.

Tvarnø, C. D., & Nielsen, R. (2021). Retskilder og retsteorier (6. udg.). Djøf Forlag.

Trzaskowski, J., Savin, A., Lindskoug, P. L., & Lundqvist, B. (2023). Introduction to EU Internet Law. Ex Tuto Publishing.

Udsen, H. (2022). Databeskyttelsesret, s. 14.

Rapporter

Dataetisk Råd. (2025). Generativ AI og offentlige myndigheder: Pålidelighed og dataetik.

Datatilsynet. (2024, januar). Datatilsynet giver påbud i Chromebook-sag.

Digitaliseringsstyrelsen. (2020, juli). Vejledning i anvendelse af cloudservices version 1.1.

Forbrukerrådet. (2023, juni). Ghost in the machine: Addressing the consumer harms of generative AI.

Kommunernes Landsforening. (n.d.). Cloud. KL Videncenter.

Opinion og vejledninger

Datatilsynet. (2017). Dataansvarlige og databehandlere.

Datatilsynet. (2022). Vejledning om Cloud.

Datatilsynet. (2024, februar). Region Syddanmarks påtænkte brug af Microsoft 365.

Digitaliseringsstyrelsen. (2020, juli). Vejledning i anvendelse af cloudservices version 1.1.

European Data Protection Board. (2019). Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR.

European Data Protection Board. (2024, oktober). Opinion 22/2024 on certain obligations following from the reliance on processors and sub-processors

Hjemmesider

European Data Protection Board. (n.d.). Tasks and duties.

Artikler

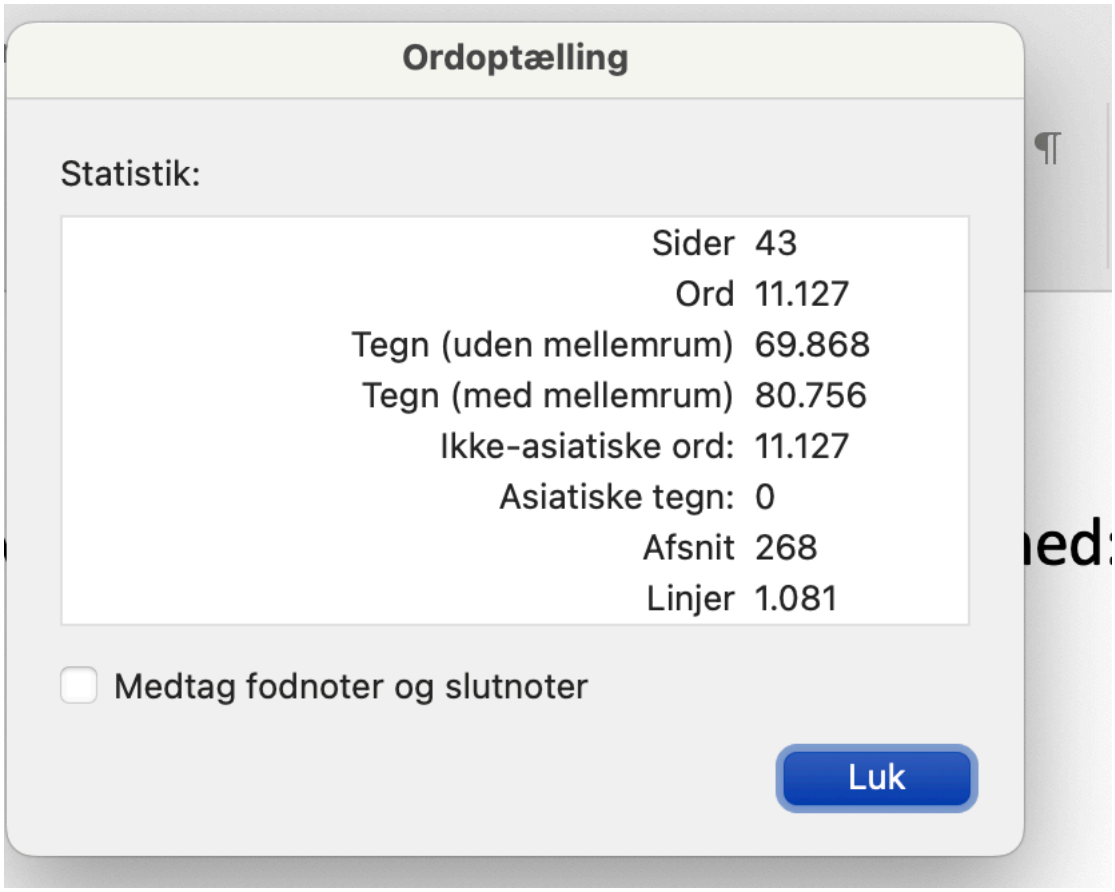
Trzaskowski, J. (2024). Manipulation by design.

Euractiv. (2025, April 16). Deafening Commission silence, with no credible EU-US data oversight left.

Version2. (2025, April 25). Minister vil bekæmpe tech-afhængighed: Arbejder på exit-plan fra amerikansk cloud.

Podcast

DR. (2025, April 16). Genstart: Kan USA slukke skyen? [Podcast]. DR.


Ordoptælling
Statistik:
Sider 43
Ord 11.127
Tegn (uden mellemrum) 69.868
Tegn (med mellemrum) 80.756
Ikke-asiatiske ord: 11.127
Asiatiske tegn: 0
Afsnit 268
Linjer 1.081
Medtag fodnoter og slutnoter
Luk