Lov & Data

Nr. 150
Juni 2022

Nr. 2/2022

Innhold

Leder 2

Artikler 4

Steinar Østmoe, Robin Welhaven Føyen og Thale Marie Bø: Dataportabilitet – får den glemte personvernrettigheten et nytt liv med Digital Markets Act? 4

Ida Thorsrud: Databehandlers adgang til å behandle kundedata til egne formål. 10

Eirin Helen Hauvik, Hanne Pernille Gulbrandsen og Marianne Lie Howard: Hvilken betydning har det at databehandler har et morselskap i et ikke-godkjent tredjeland? 13

JusNytt 17

Halvor Manshaus og Mats Hole: EU-domstolen balanserer opphavsrett og ytringsfrihet i sak om DSM artikkel 17

Rettsinformatisk litteratur 22

Bokomtale
Kevin McGillivray: Government cloud procurement – Contracts, Data Protection, and the Quest for Compliance, ... 22

Arrangementer 2022 25

Nytt om personvern 27

Nytt om immaterialrett 35

Nytt om IT-kontrakter 44

Karnov Lovkommentarer 47

Nytt fra Lovdata 48









Lov&Data

Lov&Data er et skandinavisk tidsskrift for rettsinformatikk og utgis av

Lovdata
Postboks 6688 St. Olavs plass
NO-0129 Oslo, Norge
Tlf.: +47 23 11 83 00
E-post: lovogdata@lovdata.no
Nettside: www.lovdata.no

Lovdata forbeholder seg rett til å bruke artikler og domsreferater i Lovdatas elektroniske systemer.

Ansvarlig redaktør er Jarle Roar Sæbø
Medredaktør er Trine Shil Kristiansen, Lovdata.
Redaktører for Danmark er dr.juris Henrik Udsen ved Center for informations- og innovationsret, Københavns universitet og Tue Goldschmieding, partner i firmaet Gorrissen Federspiel, København.
Redaktør for Sverige er Daniel Westman, uavhengig rådgiver og forsker.
Fast spaltist er Halvor Manshaus, partner i advokatfirmaet Schjødt.

Trykk: ISSN 0800-7853
Elektronisk: ISSN 1503-8289
Utkommer med 4 nummer pr. år.

Abonnementspriser for 2022
Norge: nkr 385,- pr. år
Utland: nkr 468,- pr. år
Studenter, Norge: nkr 182,- pr år
Studenter, utland: nkr 244,- pr. år
Alle fritt tilsendt.

Lov&Data sendes gratis til ordinære abonnenter av Lovdata Pro og er medlemsblad for foreningene Norsk forening for jus og edb, Svenska föreningen för IT och Juridik (ADBJ), Dansk forening for Persondataret og Danske IT-advokater.

Foreningene kan ev. sende låste pdf-er til sine medlemmer.

Abonnenter på papirutgaven av Lov&Data kan ved henvendelse til Lovdata/sin forening få passord som gir tilgang til elektroniske utgaver av tidsskriftet. Disse er tilgjengelige på *http://www.lovdata.no/pro/tidsskrift/*

Trykk og layout: 07 Media – 07.no

Leder

Fremtidens it-kontraktret

Tue Goldschmieding

Der bliver i disse år sat handling bag EU's ambition om digital uafhængighed og visionen om at EU i fremtiden skal være en regulatorisk supermagt. Med introduktionen af ny lovgivning, der adresserer både beskyttelse af den digitale forbruger, platformsøkonomier, digitale rettigheder og nye teknologier, bevæger IT-retten sig for alvor fra at handle om anvendelsen af traditionel lovgivning i det digitale rum til selvstændig lovgivning, der udspringer af de digitale udfordringer. Således er eksempelvis EU-Kommissionens forslag til en ny AI-forordning, Digital Services Act, Platformsordningen og New Deal for Consumers lovgivning, der specifikt er reaktioner på og er rette mod problemstillinger i det digitale rum.

Denne lovgivning får stor betydning for IT-jurister i alle EU's Medlemsstater og i EØS-landene. Dette er ikke mindst tilfældet i de skandinaviske lande, der er gennemdigitaliserede og hvor den private sektor og store dele af den offentlige IT-infrastruktur er afhængig af nationale og internationale IT-leverandører. Med den massive mængde ny lovgivning, der introduceres i et hidtil uset højt tempo, vil IT-juristen i fremtiden indtage en endnu mere central rolle i det digitale rum.

IT-juristens force har alle dage været, at kunne koble den generelle og sektorspecifikke jura med teknologien. Denne evne kommer i endnu højere grad til at være en forudsætning for at kunne navigere i fremtidens IT-ret.

En kompleks og udfordrende fremtid

Et aktuelt eksempel der indvarsler kravene til den tekniske kunden hos fremtidens IT-jurister er den praksis, der er ved at udvikle sig i kølvandet på Schrems II afgørelsen. Sagens kerne, nemlig, at europæiske borgeres personoplysninger ikke er tilstrækkelig juridisk beskyttet over for myndighederne i USA, lader sig i sagens natur ikke let løse. Derfor ser vi også, at både EDPB og de lokale datatilsyn overlade det til teknologien at løse det grundlæggende juridiske problem gennem krav om brug af supplerende foranstaltninger til at afhjælpe konsekvenserne af de juridiske udfordringer.

Det danske Datatilsyn udgav i marts 2022 en vejledning om anvendelse af cloud tjenester i forbindelse med behandling af personoplysninger. Baseret på EDPBs tidligere anbefaling adresserer vejledningen blandt andet de problemstillinger, der knytter sig til overførsel af personoplysninger til tredjelande og særligt USA. Som et eksempel på ovenstående opstiller tilsynet i vejledningen en række scenarier for brug af cloud-tjenester og kommenterer på de forhold, der bør overvejes af myndigheder og virksomheder. Det er i den forbindelse illustrativt, at det ifølge vejledningen er påkrævet, at myndigheder og virksomheder har en meget detaljeret forståelse af de tekniske sikkerhedsforanstaltninger, der kan anvendes i forbindelse med overførsel af personoplysninger, for i praksis at kunne vurdere, hvorvidt myndigheden eller virksomheden faktisk overholder persondataretten. Eksempelvis vil en myndighed eller virksomhed efter omstændighederne skulle have en dyb forståelse af, hvordan de nøgler, der anvendes til kryptering af data håndteres samt hvorvidt myndighederne i et tredjeland må antages at kunne bryde en given form for kryptering.

Tilsvarende tekniske og normbaserede regler gør sig også gældende i meget af EU's kommende regulering af det digitale rum. Eksempelvis indeholder EU-Kommissionens udkast til en ny AI-forordning, krav om risikovurdering, transparens og dokumentation ved markedsføring og idriftsættelse af AI-systemer, der stiller store krav til virksomhedernes tekniske kompetencer. I denne forordning er det også op til myndigheder og virksomheder selv at vurdere i hvilket omfang de tekniske normer, der opstilles i lovgivning og praksis er opfyldt ved brugen af konkrete digitale tjenester og teknologier.

Fra et retspolitisk perspektiv rejser det spørgsmålet om en almindelig borger eller virksomhed med rimelighed vil være i stand til at vurdere egen retsstilling på baggrund af lovgivning, der kræver en så dyb teknisk forståelse. For fremtidens IT-jurist betyder det et behov for endnu dybere teknologisk forståelse for at kunne omsætte juraen til relevant rådgivning, der kan implementeres i praksis.

Behov for nye kompetencer og værktøjer

I en fremtid med langt mere omfattende og kompleks regulering af det digitale rum vil IT-juristens force stadig være at koble juraen med teknikken. Dog vil fremtidens IT-jurist i endnu højere grad skulle navigere i det teknologiske landskab og have en så dyb forståelse af de teknologier, der er genstand for regulering eller udgør de midler hvormed reglerne kan overholdes. Fremtidens IT-ret bygger på dynamiske teknologiske normer og standarder, for hvad der eksempelvis udgør tilstrækkelige sikkerhedsforanstaltninger eller foranstaltninger mod ulovligt indhold. At have fingeren på pulsen i forhold til den teknologiske udvikling er derfor i fremtiden en forudsætning for fortolkning af loven.

Tue Goldschmieding

Dataportabilitet – får den glemte personvernrettigheten et nytt liv med Digital Markets Act?

Av Steinar Østmoe, Robin Welhaven Føyen og Thale Marie Bø

1. Innledning

Europakommisjonen presenterte 15. desember 2020 forslag til europaparlaments- og rådsforordning om åpne og rettferdige markeder i den digitale sektoren i Digital Markets Act (DMA). Forslaget er en del av det rettslige rammeverket som skal muliggjøre målsetningene i EUs datastrategi sammen med blant annet Data Act, Digital Services Act og Data Governance Act. Initiativene skal til sammen øke verdiskapningen i EU gjennom økt tilgang til, gjenbruk og utnyttelse av data. DMA dekker et aspekt ved dataøkonomien ved å bidra til en mer åpen og rettferdig plattformøkonomi, og hindre adferd som er skadelig for konkurransen og forbrukerne.

Som flere av de andre rettsaktene, regulerer DMA digitale markeder og inneholder regler som grenser til og delvis overlapper med personvernforordningen (GDPR). DMA tar særlig sikte på å regulere store internettbaserte plattformer, såkalte portvoktere.

Et område som reguleres i GDPR og DMA er dataportabilitet. Kort fortalt omhandler dataportabilitet retten til å få utlevert sine data slik at man selv kan bruke dem, eller kunne overføre opplysningene fra én virksomhet eller tjeneste til en annen.

Dataportabilitet har blitt omtalt som «den glemte personvernrettigheten». Særlig tre faktorer i DMA kan endre dette bildet. For det første gir DMA rett til dataportabilitet også for virksomheter. For det andre utvider DMA informasjonsgrunnlaget som omfattes av retten til dataportabilitet. For det tredje for portvokterne en utvidet plikt til å tilrettelegge for dataportabilitet. Vil vil derfor sammenligne retten til dataportabilitet i GDPR og DMA, og se om DMA kan føre til en fornyet interesse for dataportabilitet.

2. Dataportabilitet - et uforløst potensial?

Dataportabilitet ble innført som en ny rettighet med GDPR i 2016 (i Norge i 2018), og hadde som uttalt formål å gi de registrerte bedre kontroll over egne opplysninger.[1] Ved ikraftsettelsen av GDPR ble det diskutert om retten til dataportabilitet også kunne medføre konkurransefordeler og bidra til at små virksomheter kunne konkurrere på bedre vilkår.[2] For eksempel kunne en nystartet sosiale medierplattform lettere tiltrekke seg nye brukere hvis brukerne hadde muligheten til å portere bildene og videoene sine direkte fra andre sosiale medier til den nye plattformen.[3] Personer som ønsket å bytte bank, kunne flytte alle opplysningene sine direkte over til den nye banken uten å måtte taste inn disse selv, hvilket ville gjøre det

1 GDPR, fortalens avsnitt 68
2 Diker Vanberg, A. and Ünver, M. B., (2017) s. 5
3 Graef, I., Verschakelen, J., and Valcke, P. (2013) s. 6

Steinar Østmoe

Robin Welhaven Føyen

Thale Marie Bø

enklere for dem å bytte banker og motvirke såkalt «lock-in»-effekt.[4]

Foreløpig ser det ut til at mulighetene for den enkelte, og de samfunnsmessige gevinstene av dataportabilitet man så for seg, ikke har båret frukter i særlig stor grad. EU-kommisjonen konkluderte i sin første evaluering av GDPR med at dataportabilitet har et helt tydelig potensial som ennå ikke hadde blitt fullt ut utnyttet.[5] Videre har det vært få saker og avgjørelser fra tilsynsmyndighetene knyttet til dataportabilitet, særlig hvis man sammenligner med den tilgrensende retten til innsyn.[6]

Ulike årsaker har vært pekt på som mulige til at dataportabilitet har kommet i bakgrunnen.[7] Lav bevissthet blant de registrerte om retten til dataportabilitet kan være en faktor[8], samt at det kan foreligge et digitalt kompetansegap som fører til at de registrerte ikke ser fordelene med dataportabilitet, selv om de skulle være klar over rettigheten.[9] Den behandlingsansvarliges plikt til å informere og legge til rette for dataportabilitet i GDPR skulle bidra til å øke bevisstheten om rettighetene. Plikten slik den er tolket så langt, omfatter ikke en plikt til å konkretisere mulighetene for dataportabilitet, og vil dermed sannsynligvis ha begrenset verdi. Tilsynsmyndighetenes fokus, og registrerte som gjør sin rett gjeldende eller aktivisme på vegne av de registrerte har vært to av de viktigste driverne for rettsutvikling innen GPDR. Dette kan bidra til å forklare hvorfor dataportabilitet har blitt en lite brukt rettighet.

3. Hvilke virksomheter får nye plikter etter DMA?

Digital Markets Act (DMA) får anvendelse på virksomheter som driver store internettbaserte plattformer. Slike virksomheter omtales i forslaget som «gatekeepers» («portvoktere» vil bli brukt i det videre). Plikten om å legge til rette for dataportabilitet påligger portvokterne, jf. artikkel 6 nr. 1 bokstav h[10]. For å oppfylle portvokterkriteriet må virksomheten være tilbyder av en internettplattform, og oppfylle følgende kvalitative krav:

- ha en betydelig innvirkning på det indre marked,
- drive en plattformtjeneste som fungerer som en viktig portal for næringsbrukere for å nå ut til kunder og
- ha en sterk og varig posisjon for sine aktiviteter, eller det kan forventes at den vil få en slik posisjon i nær fremtid.

Internettjenesten vil automatisk anses som en portvokter dersom tjenesten har en markedsverdi på mer enn 75 milliarder euro eller årlig omsetning på over 7,5 milliarder euro, tilbyr tjenesten i minst tre EU-stater, har over 10 000 forretningskunder og månedlig når minst 45 millioner aktive sluttbrukere.[11] Kommisjonen kan også utpeke virksomheter som ikke oppfyller de kvantitative kravene som portvoktere, dersom de mener de ovennevnte kvalitative kravene er oppfylt. Det gir Kommisjonen en viss fleksibilitet til å vurdere hvilke virksomheter som faller inn under regelverket. Kommisjonen har anslått at 10–15 virksomheter kan bli utpekt som portvoktere innenfor disse rammene.[12] Ingen norske selskaper peker seg ut som åpenbare kandidater, og i praksis vil kun virksomheter som Facebook, Google, Amazon m.m. utpekes som portvoktere. Til tross for at plikten til å legge til rette for dataportabilitet kun vil påligge et fåtall virksomheter, vil den i praksis kunne ha stor betydning for både privatpersoner og virksomheter som benytter tjenester fra de store internettplattformene.

Kun et fåtall virksomheter vil ha forpliktelser som portvoktere sammenlignet med antallet behandlingsansvarlige som har plikt til å ivareta den registrertes rett til dataportabilitet etter GDPR. Pliktsubjektene for dataportabilitetsreglene etter GDPR favner dermed en langt større krets av virksomheter enn det som følger av DMA. Portvoktere vil som regel være behandlingsansvarlige og databehandler etter GDPR og må dermed ivareta krav om dataportabilitet i henhold til begge regelverkene.

4 Diker Vanberg, A. and Ünver, M. B., (2017) s. 5

5 EU-Kommisjonen (24.6.2020). Communication from the commission to the European parliament and the council; Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation.

6 Eksempelvis er det kun 7 avgjørelser registrert i GDPR hub på dataportabilitet (art. 20), mens 135 avgjørelser er registrert gjeldende forespørsler om data access.. Dataportabilitet er heller ikke nevnt i Datatilsynets årsrapport for 2021.

7 Exposito-Rosso, Stephanie; Cao, Francois-Xavier; Piquet, Antoine; Medjaoui, Mehdi (2021) s. 32

8 Personvernundersøkelsen 2019/2020 s. 8. Undersøkelsen viser at dataportabilitet var rettigheten færrest av de spurte var klar over.

9 Exposito-Rosso, Stephanie; Cao, Francois-Xavier; Piquet, Antoine; Medjaoui, Mehdi (2021) s. 32

10 Det er mulig at bestemmelsens plassering i lovteksten kan endres før forordningen trer i kraft.

11 Regjeringen.no (2021). Forordning om digitale markeder (Digital Markets Act - DMA).

12 EU-Kommisjonen (15.12.2020). Commission staff working document - executive summary of the impact assessment report accompanying the document proposal for a regulation of the european parliament and of the council on contestable and fair markets in the digital sector (Digital Markets Act). Avsnitt 148

4. Retten til dataportabilitet i DMA – bedre vilkår for forbrukere og virksomheter

Digital Markets Act har til formål om å fremme mer rettferdig konkurranse i den digitale økonomien. Data, inkludert personopplysninger, er en svært verdifull ressurs (ofte beskrevet som «den nye oljen»), og den digitale økonomien domineres av en håndfull giganter med enorm kapasitet til å innhente og bruke personopplysninger – slik som Google, Meta, og Amazon. For mindre eller nystartede virksomheter som ikke har denne fordelen, kan det være vanskelig å konkurrere.

Til forskjell fra GDPR, pålegger DMA portvoktere en plikt til å legge til rette for dataportabilitet både for fysiske og juridiske personer. GDPR gir bare rettigheter til registrerte, det vil si fysiske personer jf. art. 1 og 4 (1), og som en følge av dette har virksomheter og andre juridiske personer ikke rett til dataportabilitet etter GDPR.

Plikten portvoktere har i DMA art. 6 gjelder overfor virksomheter etablert i EU («Business users») og sluttbrukere («End users»). I DMA art. 2 (16) og (17) defineres «End user» som «any natural or legal person using core platform services other than as a business user»; mens «Business user» defineres som «any natural or legal person acting in a commercial or professional capacity using core platform services for the purpose of or in the course of providing goods or services to end users». En «End user» kan derfor omfatte forbrukere og virksomheter som kjøper en tjenester, men «business users» omfatter virksomheter som selger tjenester ved hjelp av portvokternes plattformertjenester.

I tillegg til å utvide virkeområdet for retten til dataportabilitet sammenlignet med GDPR, pålegger DMA portvokterne en utvidet plikt til sikre effektiv portabilitet av data som genereres gjennom aktiviteten på internettplattformen av sluttbrukere, og pålegger portvokterne plikten til å stille til rådighet verktøy for å lette utøvelsen av dataportabilitet. At virksomheter får benytte seg av dataportabilitet, vil antagelig kunne føre til mer rettferdige konkurransebetingelser og bedre balanse i markedet ved at mindre virksomheter kan dra nytte av dataene om brukere av deres tjenester som er samlet inn av portvokterne. Disse vil ofte ha større kapasitet til å samle inn store mengder opplysninger. Dette vil også kunne ha positive effekter for dataøkonomien ved at det legger til rette for større grad av gjenbruk av data.

Kommisjonen har tidligere behandlet spørsmål om dataportabilitet for virksomheter i flere saker i tilknytning til konkurranseretten – for eksempel i Google Search-saken, der Kommisjonen bøtela Google 2,42 milliarder euro for misbruk av dominerende stilling ihht. art. 102 TFEU. Saken ble anket til EU-domstolen, som i all hovedsak opprettholdt Kommisjonens avgjørelse[13]. Saken gjaldt primært at Google fremhevet sine egne tjenester i søkeresultatene i søkemotoren sin, og ga mindre plass til konkurrenter. Imidlertid inkluderte Kommisjonen også et spørsmål om dataportabilitet.[14] Google hadde kontraktuelt begrenset programvareutviklere fra å utvikle verktøy som kunne muliggjøre overføring av reklamekampanjer fra en Google-eid markedsføringstjeneste, Adwords, til konkurrerende markedsføringsplattformer. Det er kostbart å opprette digitale markedsføringskampanjer, og hvis digitale markedsførere må opprette nye kampanjer når de bytter fra én annonseringsplattform til en annen, er det mindre sannsynlig at de bytter plattform.

Ved innføringen av DMA vil portvoktere få en plikt til å tillate overføringer av markedsføringskampanjer fra sine egne plattformer til konkurrenters, og dermed ulovliggjøre en slik praksis som Google hadde. I så fall må ikke portvokterne bare tillate at programvareutviklere utvikler verktøy for overføring av reklamekampanjer til andre plattformer – de vil også selv måtte gi konkurrentene verktøyene for å fasilitere slike overføringer.

DMA vil også styrke forbrukeres rett til dataportabilitet, ettersom portvoktere blir forpliktet til å sørge for en «effektiv» rett til dataportabilitet også overfor sluttbrukere, i tillegg til å stille verktøy til rådighet for å lette utførelsen av dataportabilitet for dem.

Det er mulig at denne utvidede muligheten til dataportabilitet vil føre til nye tekniske løsninger som både vil medføre mer rettferdige konkurransebetingelser og fordeler for forbrukere og virksomheter som sluttbrukere. For eksempel dersom en ny sosiale medier-plattform utvikler en funksjon hvor plattformen selv, med brukerens samtykke, overfører brukeres bilder og videoer fra andre plattformer. Dette ville kanskje være enklere enn om brukeren selv skulle benytte sin egen rett til dataportabilitet og kreve at den gamle sosiale medier-plattformen overførte brukerens bilder og videoer til den nye plattformen.

Det kan også tenkes at virksomheter selv ønsker å benytte seg av dataportabilitet på samme måte som fysiske personer. En liten bedrift som bytter bank vil kanskje dra for-

13 Dom av 10 November 2021 [GC], Google Search, ECLI:EU:T:2021:763

14 European Commission (2017) Press Release - Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service. European Commission Press Release Database. Retrieved from: http://europa.eu/rapid/press-release_IP-17-1784_en.htm

del av å overføre dataene sine til den nye banken for enkelhets skyld, akkurat som en fysisk person ville gjort.[15]

5. Hvilke opplysninger kan porteres – gir DMA en utvidet rett?

Retten til dataportabilitet i GDPR art. 20 har en rekke begrensninger. Den omfatter kun personopplysningene til den registrerte. I tillegg gjelder rettigheten kun for opplysninger som er samlet inn på grunnlag av samtykke eller avtale, og som den registrerte har «gitt til en behandlingsansvarlig». Dette begrenser rettighetens virkeområde.

I veilederen til Article 29 Working Party er det uttalt at uttrykket «gitt til en behandlingsansvarlig» skal omfatte data den registrerte aktivt og bevisst har gitt, samt observerte data (for eksempel rådata som behandles av en smartmåler eller andre typer tilkoblede objekter, aktivitetslogger, historikk for bruk av nettstedet eller søkeaktiviteter). Den registrerte har gitt ved bruken av tjenesten eller enheten. Dermed legger WP29-gruppen opp til en utvidende tolkning der ikke bare data direkte og eksplisitt levert av den registrerte er dekket av retten til dataportabilitet.

Når det gjelder hvilke data som ikke skal betraktes som «gitt til en behandlingsansvarlig» av den registrerte, fremgår det av veilederen at data generert av en behandlingsansvarlig som angår den registrerte, ikke skal være en del av retten til dataportabilitet. Dette inkluderer analyser av den registrertes atferd («metadata»), eller data som er en del av en personlig tilpasnings- eller anbefalingsprosess[16].

Dataportabilitet i DMA gjelder data generert gjennom aktiviteten til en «business user» eller «end user». Denne ordlyden kan tolkes videre enn i GDPR art. 20, hvor det kun gis rett til å portere opplysninger som er «gitt til» behandlingsansvarlig. Business users gis også muligheten til å få tilgang til og bruke personopplysningene til sluttbrukere så lenge disse samtykker til dette. Samtykket må innhentes i henhold til kravene i GDPR, men portvoktere kan få ansvar for å innhente gyldig samtykket i DMA. Gitt at EU-domstolen ofte legger til grunn en formålsrettet tolkning av EU-regelverkene, er det ikke usannsynlig at DMA kan medføre at rett til dataportabilitet kan tolkes utvidende, i form av at mer informasjon vil være omfattet, dersom det kan oppfylle formålet om økt konkurranse.

Denne forskjellen kan for eksempel få betydning på online auksjonsnettsteder som eBay. Auksjonstjenesten legger selv til informasjon slik som tilbakemeldinger fra kjøpere og hvilken «rating» kjøperne har gitt selgeren. Sistnevnte informasjon er data selgeren gjerne kunne ønsket å ta med seg ved et plattformbytte, men faller ikke strengt tatt inn under begrepet «gitt til» i GDPR art. 20. Tilbakemeldinger fra kjøperne og selgers «rating» kan imidlertid regnes for data som er generert gjennom aktiviteten til business users eller end users i henhold til DMA art. 6 (1) (h), slik at portvokterne får en plikt til å portere denne dataen.

Mens GDPR kun gir rettigheter knyttet til den type data som faller inn under definisjonen av personopplysninger, gjelder reglene i DMA også for «data» som ikke kan betegnes som personopplysninger. I DMA art. 2 (19) defineres «Data» som «any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording».

Det at DMA art. 6 (1) (h) gjelder «data» kan i seg selv tilsi at dataportabilitet etter denne bestemmelsen favner videre enn i GDPR, hvor retten kun gjelder for personopplysninger.

På disse måtene kan det tenkes at rekkevidden av dataportabilitet er mer omfattende i DMA enn i GDPR, slik at brukere får rett til å portere flere typer data og en større datamengde enn de tidligere kunne.

6. Portering av opplysninger mellom plattformer når det er teknisk mulig

Det fremgår av art. 20 GDPR at dataportering direkte fra en behandlingsansvarlig til den neste bare kan skje hvis det er «teknisk mulig», noe som setter en grense for omfanget av dataportabilitet. Ordlyden i «teknisk mulig» vil naturligvis forstås i den retningen at behandlingsansvarlig og databehandler må overføre data så langt det er rimelig håndterbart gitt teknologien som kreves.

Dette betyr at en behandlingsansvarlig kan nekte en registrert forespørsel om å overføre data på grunnlag av at deres egen tekniske utvikling ikke tillater direkte overføring av dataene til en annen virksomhet.

Et problematisk aspekt ved denne begrensningen er at det ikke er noen forklaring i GDPR på hva «teknisk mulig» faktisk betyr. Dette kan gi et smutthull for virksomheter som ikke ønsker å portere data, da de ganske enkelt kan hevde at portering ikke er teknisk mulig. Selv om behandlingsansvarlige oppfordres til å utvikle interoperable dataformater i GDPR-fortalen[17], pålegges de ingen bindende forpliktelse til dette.

Til forskjell fra dette, innfører DMA krav om at portvoktere skal «provide tools for end users to facil-

15 Diker Vanberg, A. & , Ünver, MB., 2017, s. 5

16 Article 29 Data Protection Working Party, Guidelines on the right to data portability s. 10. EDPB har sluttet seg til veilederen

17 GDPR, fortalen avsnitt 68

itate the exercise of data portability, in line with Regulation EU 2016/679» jf. art. 6 (1) (h). Dette vil tilsynelatende gjøre det enda enklere for brukere som ønsker å overføre data fra én tjeneste til en annen, og gjøre det vanskeligere for portvoktere å hevde at de ikke kan imøtekomme forespørsler om dataportabilitet.

I tillegg vil reglene i DMA innføre sanntids- og kontinuerlig portabilitet, der dataportabilitet etter GDPR art. 20 kun gjelder personopplysningene behandlingsansvarlig har behandlet frem til forespørselen om portabilitet ble mottatt.

En kritikk som har vært rettet mot GDPR art 20 er at det kan være uforholdsmessig tyngende for virksomheter å imøtekomme registrertes forespørsler om å portere data. Særlig for mindre virksomheter som ikke nødvendigvis har ressursene eller de tekniske fasilitetene til å utføre slike forespørsler, kan forespørsler om utlevering eller overføring av opplysninger være tyngende og vanskelig å gjennomføre. I DMA vil dette ikke utgjøre et like stort problem, ettersom DMA kun kommer til anvendelse for virksomheter som er store nok til å betegnes som portvoktere.

7. Tilsyn og håndheving

Tilsyn og håndheving av GDPR har fått stor oppmerksomhet siden forordningen trådte i kraft, og tilsynsmyndighetens prioriteringer har vært utslagsgivende for hvordan virksomhetene har forholdt seg til regelverket. I motsetning til GDPR, vil de fleste virksomheter få rettigheter under DMA som «business user» eller «end users», og vil kunne melde fra om brudd på forordningen slik de registrerte kan etter GDPR.

Siden det er få virksomheter som blir ansett som portvoktere, og for å sikre harmonisering av tilsynet i det indre marked, er EU-kommisjonen den eneste som kan håndheve DMA. En forutsetning i DMA er imidlertid at det skal foregå et samarbeid på tvers av tilsynsmyndigheter i ulike sektorer og landegrenser. Art. 32 i DMA etablerer f. eks. en rådgivende komité for å bistå og lette arbeidet til EU-kommisjonen. Land vil også kunne gi nasjonale konkurransemyndigheter fullmakt til å starte undersøkelser av mulige overtredelser og rapportere sine funn til EU-kommisjonen.

Når retten til dataportabilitet utvides, er det naturlig at den vies større oppmerksomhet også fra et tilsynsperspektiv. I likhet med økningen i bevissthet rundt personvern vi har sett etter innføringen av GDPR, kan en økning i bevissthet om dataportabilitet føre til større grad av rapportering til tilsynsmyndighetene. De økonomiske insentivene for virksomheter til å hevde rett til bruken av dataportabilitet kan også være større enn for enkeltpersoner.

Dataportabilitet kan både være begrunnet ut fra konkurransehensyn og ut fra personvernhensyn og kontroll med egen data. Samarbeid mellom tilsynsmyndighetene om prioriteringer av tilsyn og sanksjoner vil være viktig for å skape forutsigbarhet både for de som rapporterer inn avvik. I Norge har Datatilsynet allerede fokus på tettere samarbeid med Forbrukertilsynet og Konkurransetilsynet.[18]

8. Konklusjon

Retten til dataportabilitet i GDPR har kanskje ikke fått så stor praktisk betydning som det var antatt da GDPR fremdeles var nytt, og er kanskje heller ikke brukt i like stor utstrekning som andre GDPR-rettigheter. DMA åpner imidlertid nye muligheter som kanskje vil føre til at dataportabilitet blir brukt i større grad enn tidligere, og som kan føre til nye tekniske løsninger og muligheter både for forbrukere og virksomheter både til å ivareta sine rettigheter og til å gjenbruke data som kan skape store samfunnsmessige gevinster. Dataportabilitet er i så fall et av flere viktige tiltak for å legge til for mer forbrukermakt og høyere grad av konkurranse i det europeiske markedet.

Senior Manager/ advokatfullmektig Steinar Østmoe, Manager/ advokatfullmektig Robin Welhaven Føyen og advokatfullmektig Thale Marie Bø i Deloitte Advokatfirma AS.

18 Årsrapport for 2020 – Tall og tendenser fra Datatilsynets virksomhet, side 64

Foto: Shutterstock

Kildeliste

- Diker Vanberg, A. & , Ünver, MB., «The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?», in European Journal of Law and Technology, Vol 8, No 1, 2017.
- Graef, I., Verschakelen, J., and Valcke, P. (2013). Putting the right to Data Portability into a Competition Law Perspective. Law: The Journal of the Higher School of Economics, Annual Review, pp. 53-63, s. 6.
- EU-Kommisjonen (24.06.2020). Communication from the commission to the European parliament and the Council - Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation. URL: *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0264&from=EN*
- EU-Kommisjonen (15.12.2020). Commission staff working document – executive summary of the impact assessment report accompanying the document proposal for a regulation of the european parliament and of the council on contestable and fair markets in the digital sector (Digital Markets Act). URL: *https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2020:0364:FIN:EN:PDF*
- Exposito-Rosso, Stephanie; Cao, Francois-Xavier; Piquet, Antoine; Medjaoui, Mehdi (2021). GDPR Data Portability: The Forgotten Right. URL: *https://cellar-c2.services.clever-cloud.com/alias-code-is-law-assets/static/report/gdpr_data_portability_the_forgotten_right_report_full.pdf*
- Regjeringen.no (2021). Forordning om digitale markeder. URL: *https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2021/juni/forordning-om-digitale-markeder-digital-markets-act-dma/id2860419/*
- Datatilsynet (2020). Personvernundersøkelsen 2019/2020. URL: *https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/personvernundersokelser/personvernundersokelsen-20192020/*
- Dom av 10 November 2021 [GC], Google Search, ECLI:EU:T:2021:763

Databehandlers adgang til å behandle kundedata til egne formål

Av Ida Thorsrud

Leverandører som er databehandlere, har som hovedregel ikke lov å bruke kundens data til sine egne formål. Flere leverandører bruker imidlertid data fra kundene sine til egne formål, for eksempel for å videreutvikle den tjenesten man leverer. Kundedata er ofte personopplysninger, så når er det lov å gjøre dette? Og hvilke plikter har kunden som behandlingsansvarlig og «eier» av dataene i et personvernperspektiv? Det franske datatilsynet kom i januar i år med en veileder[1] for databehandleres gjenbruk av personopplysninger. Veilederen gir oss et metodisk utgangspunkt for når leverandører kan gjøre dette på en lovlig måte.

Problemstillingen og Microsoft som eksempel

Som et utgangspunkt kan en databehandler bare behandle personopplysninger på instruks fra behandlingsansvarlig.[2] En slik instruks er typisk en databehandleravtale. Fordi leverandører kun skal behandle personopplysninger på instruks, foreligger det samtidig et forbud mot å behandle personopplysninger til egne formål. Det er imidlertid svært utbredt at leverandører forbeholder seg retten til å gjøre akkurat dette: behandle kundedata til egne formål. Særlig større leverandører gjør det ofte til en forutsetning for å ta i bruk den tjenesten de selger at kundene må godta en standard databehandleravtale. I denne databehandleravtalen godtar kunden også at leverandøren behandler deres personopplysninger til egne formål.

Microsoft har i sin standard databehandleravtale[3] for eksempel fastslått at de skal kunne behandle personopplysninger til egne formål knyttet til a) «å levere produkter og tjenester til kunden», og b) «forretningsvirksomhet som skyldes levering av produktene og tjenestene til kunden». Microsoft presiserer at levering av tjenester omfatter også «levering av funksjonsegenskaper» (det vil si funksjonalitet), «feilsøking» (forhindre, oppdage og

Ida Thorsrud

reparasjon av problemer i tjenesten eller programmet), «kontinuerlig forbedringer» for eksempel ved «installasjon av nye oppdateringer og forbedring av brukerproduktivitet, pålitelighet, effektivitet, kvalitet og sikkerhet». Selv om dette er formål som er nært knyttet til de produkter og tjenester Microsoft leverer, er det ikke tydelig hvilke kundedata Microsoft faktisk behandler for eksempel for å forbedre effektiviteten i tjenestene de tilbyr sine kunder. Dette gjør det vanskelig for virksomheter egentlig å forstå omfanget av behandlingen til Microsoft, og dermed også hva man faktisk godtar ved å inngå en standard databehandleravtale med Microsoft.

Alternativet til å inngå en standard databehandleravtale er også utfordrende. Det skal mye til før større skyleverandører som Microsoft godtar å inngå i en forhandling med behandlingsansvarlige for å tilpasse databehandleravtalen. Det franske datatilsynets veiledning prøver å bøte på dette ved å skissere en fremgangsmåte hvor behandlings-

1 https://www.cnil.fr/fr/sous-traitants-la-reutilisation-de-donnees-confiees-par-un-responsable-de-traitement

2 GDPR artikkel 28 nr. 3 bokstav a)

3 Tillegg om databeskyttelse for produkter og tjenester fra Microsoft (Microsoft Products and Services Data Protection Addendum (DPA)), sist oppdatert 15. september 2021

ansvarlig likevel kan oppnå noe kontroll med behandlingen til databehandler.

En konkret og skriftlig godkjennelse

Det franske datatilsynet foreslår i sin veiledning en modell der en leverandør ikke kan gjenbruke kundens data til sine egne formål uten at dette er uttrykkelig godkjent fra den behandlingsansvarlige. Denne godkjennelsen må oppfylle visse vilkår: den må være konkret, skriftlig og den må inneholde en kompatibilitetstest. Hva betyr dette i praksis?

For at godkjennelsen skal være konkret, må den være *spesifikk* og *tydelig;* det må være klart at den behandlingsansvarlige gir databehandler en eksplisitt tillatelse til å behandle kundedata til databehandlerens egne formål. En godkjennelse som ligger innbakt i en standard databehandleravtale vil som hovedregel ikke oppfylle kravet til å være konkret. Godkjennelsen må videre være skriftlig. Det betyr at den må være et eget, skriftlig dokument, og at den må sendes databehandler.

Godkjennelsen skal inneholde en kompatibilitetstest

I veiledningen fremhever det franske datatilsynet at den behandlingsansvarlige må utføre en kompatibilitetstest før endelig godkjennelse kan gis. Vurderingstemaet i denne testen er hvorvidt databehandlers nye formål er kompatibelt med det opprinnelige formålet til behandlingsansvarlig. I realiteten betyr dette at behandlingsansvarlig må vurdere om prinsippet om formålsbegrensning i GDPR artikkel 5 nr. 1 bokstav b) er oppfylt, ikke for sin egen behandling av personopplysninger, men for den nye behandlingen som databehandler ønsker å gjøre. Formålsbegrensningsprinsippet handler om at personopplysninger bare skal kunne gjenbrukes til nye formål som er kompatible med det opprinnelige formålet. Dette er viktig ikke minst for de registrerte – det skal være forutsigbart hva personopplysningene til registrerte blir benyttet til. Det franske datatilsynet oppstiller flere momenter som behandlingsansvarlig kan legge vekt på i denne vurderingen og som vi kjenner igjen fra det norske datatilsynets veiledning om formålsbegrensningsprinsippet[4]:

Finnes det en naturlig kobling mellom det opprinnelige formålet og det nye formålet?

I hvilken sammenheng er personopplysninger for det opprinnelige formål samlet inn?

Hvilket forhold har behandlingsansvarlig til den registrerte? Er den registrerte en del av en særlig sårbar gruppe eller har et avhengighetsforhold til behandlingsansvarlig?

Er det nye formålet og behandling av personopplysninger fra databehandler side forutsigbart for den registrerte?

Er det snakk om særlige kategorier personopplysninger?

Innebærer den nye behandlingen av personopplysninger særskilt risiko for den registrerte?

Er det mulig å iverksette særlige beskyttelsestiltak eller nødvendige garantier for å ivareta den registrertes personvern, for eksempel ved bruk av pseudonymisering?

Typetilfeller og mulige anbefalinger til Microsoft sin standard databehandleravtale

En skyleverandør som behandler kundedata i form av telemetri eller diagnostiske data for det formål å forbedre skytjenesten, trekkes av det franske datatilsynet frem som et nytt formål som vil kunne være kompatibelt med opprinnelig formål. Viderebruk av kundedata for rene kommersielle formål trekkes imidlertid frem som et formål som sannsynlig ikke vil være i tråd med prinsippet om formålsbegrensning.

I eksempelet ovenfor fra Microsoft sin standard databehandleravtale, er flere av formålene knyttet til å forbedre tjenesten. Med utgangspunkt i det franske datatilsynets veileder, vil nok disse formålene være kompatible med opprinnelig formål. Videre har Microsoft også forpliktet seg til å ikke behandle personopplysninger for formålene «brukerprofilering», «annonsering eller lignende kommersielle formål», eller «markedsundersøkelser rettet mot å skape nye funksjoner, tjenester eller produkter». Dette er alle eksempler på formål som kan sies å være rene, kommersielle formål. Ut i fra veiledningen til tilsynet, vil disse formålene mest sannsynlig ikke ville være kompatible med opprinnelig formål.

En metode for et asymmetrisk maktforhold som ikke løser alle utfordringer

Veiledningen til det franske datatilsynet forutsetter en åpen dialog mellom behandlingsansvarlig og databehandler, noe som kan være vanskelig å gjennomføre i praksis. Personvernlovgivningen forutsetter en virkelighet hvor behandlingsansvarlig er den med mest makt som kan sette føringer for hvordan databehandler skal behandle personopplysninger.[5] Imidlertid lever vi i en virkelighet hvor mange behandlingsansvarlige er helt avhengige av store databehandlere, gjerne skyleverandører. De store databehandlerne bruker allerede i dag standardformuleringer i sine databehandleravtaler hvor de forbeholder seg retten til å viderebehandle personopplysninger fra behandlingsansvarlig til egne formål.

4 https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/formalsbegrensning/

5 GDPR artikkel 28 nr. 3 bokstav a) til h)

Når man vurderer ulike leverandører i en anskaffelsesprosess, bør standardvilkår som gir adgang til gjenbruk av opplysninger være et rødt flagg. Dette fordi databehandler i utgangspunktet kun kan behandle personopplysninger på uttrykkelig instruks fra behandlingsansvarlig. Standardvilkår som må godtas av behandlingsansvarlig vil ikke være i tråd med instruksmyndigheten. Men når databehandler er en stor skyleverandør, er det vanskelig – som regel umulig – for en behandlingsansvarlig å forhandle med databehandler for å unngå en standardavtale som også innebærer viderebehandling av personopplysninger.

Selv om den ikke på langt nær løser alle utfordringer, gir fremgangsmåten fra det franske datatilsynet likevel behandlingsansvarlig en metode for å ivareta prinsippet om formålsbegrensning. Det kan gi behandlingsansvarlig noe kontroll i det ellers asymmetriske maktforhold til større databehandlere.

En pragmatisk løsning?

Selv om en forespørsel om å behandle kundedata for egne formål burde komme fra databehandleren, vil det overfor større databehandlere være opp til behandlingsansvarlig å gi godkjennelse for viderebehandling av personopplysninger. De fleste behandlingsansvarlige vil måtte gjøre denne typen kompatibilitetsvurderinger før man aksepterer en standard databehandleravtale, for så å sende den til databehandler som en formell godkjennelse. Selv om mye står og faller på behandlingsansvarlig, må man ikke glemme konsekvensen for databehandler selv ved å behandle kundedata til egne formål: Denne type behandling gjør nemlig at databehandler blir behandlingsansvarlig, med alle de personvernforpliktelser som det innebærer.

Ida Thorsrud er jurist og arbeider som personvernkonsulent i Sopra Steria.

Hvilken betydning har det at databehandler har et morselskap i et ikke-godkjent tredjeland?

Av Eirin Helen Hauvik, Hanne Pernille Gulbrandsen og Marianne Lie Howard

I 2020 avsa EU-domstolen den prinsipielle og mye omtalte Schrems II-dommen (Sak C-311/18) om overføring av personopplysninger til land utenfor EU/EØS. Dommen har skapt en rekke praktiske utfordringer for både små og store virksomheter over hele verden. I realiteten innebærer dommen at personopplysninger vanskelig kan overføres lovlig til USA, og at behandlingsansvarlige må foreta konkrete vurderinger av hvorvidt destinasjonslandets lokale regelverk og praksis kan undergrave det beskyttelsesnivået som følger av GDPR.[1]

Det har i lys av dette også oppstått et spørsmål om det er tillatt å overlate behandling til et europeisk selskap som utfører all behandling av personopplysninger i EU/EØS når dette selskapet har en eier («morselskap») som er lokalisert i et ikke-godkjent tredjeland og dermed er underlagt lovgivning som kan medføre at også det europeiske selskapet kan bli pålagt å utlevere personopplysninger til tredjelandets myndigheter.

Særregler for overføring av personopplysninger ut av EU/EØS

All *overføring* av personopplysninger til et land utenfor EU/EØS, som GDPR omtaler som «tredjestater», forutsetter at vilkårene i GDPR kapittel V er oppfylt.[2] Innenfor EU/EØS er alle medlemslandene forpliktet til å følge GDPR, slik at personopplysninger fritt kan flyte innenfor EU/EØS uten krav til overføringsgrunnlag. Overføring av personopplysninger ut av EU/EØS, krever imidlertid et overføringsgrunnlag for å være lovlig og for å sikre at personvernet i GDPR ikke undergraves.

EU-kommisjonen har gjennom såkalte adekvansbeslutninger anerkjent at noen tredjeland har et tilstrekkelig nivå for vern av personopplysninger. Overføringer til et slikt forhåndsgodkjent land, er sammenlignbart med overføringer til

Eirin Helen Hauvik

Hanne Pernille Gulbrandsen

Marianne Lie Howard

1 Direktiv 2016/679 EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) [PVF, GDPR] gjennomført i personopplysningsloven (LOV-2018-06-15-38)

2 GDPR art. 44

land innenfor EU/EØS,[3] og det vil da ikke være krav om et særskilt overføringsgrunnlag, plikt til å foreta egne vurderinger om beskyttelsesnivået eller få godkjennelse fra Datatilsynet. Per i dag har 14 land fått en beslutning om tilstrekkelig beskyttelsesnivå.[4]

Europeiske selskaper som har morselskap i ikke-godkjente tredjeland

Etter Schrems II har det vært hyppig diskutert hvilken betydning det har at et europeisk selskap som utelukkende skal behandle personopplysninger i EU/EØS, har et morselskap som er lokalisert i et ikke-godkjent tredjeland og som er underlagt lovgivning som kan bety at det europeiske datterselskapet kan bli pålagt å utlevere personopplysninger. En slik utlevering fra et europeisk selskap kan være i strid med både GDPR og eventuell inngått databehandleravtale.

Hvilken betydning har dette i praksis? Må man avslutte alle slike databehandleroppdrag selv om kontrakt og databehandleravtale stadfester at det ikke skal skje en overføring av personopplysninger? Eller åpner personvernregelverket for en risikobasert tilnærming på dette området?

Grunnleggende forpliktelser hos den behandlingsansvarlige

Det er en forutsetning etter GDPR at en databehandler bare skal behandle personopplysningene på dokumenterte instrukser fra den behandlingsansvarlige.[5] Dette betyr i praksis at dersom man som behandlingsansvarlig ikke uttrykkelig, har gitt databehandleren tillatelse til å overføre personopplysninger til tredjeland, skal databehandleren ikke gjennomføre slik overføring.[6] Utfordringen oppstår imidlertid dersom databehandleren blir pålagt å utlevere personopplysninger i henhold til lovgivning i ikke-godkjente tredjeland, og blir stilt overfor dilemmaet med å velge hvorvidt en slik forespørsel skal etterkommes eller om databehandleren skal innrette seg etter GDPR, kontrakt og databehandleravtale.

GDPR legger til grunn at en databehandler som handler i strid med instruksjoner fra den behandlingsansvarlige, selv vil bli ansett som behandlingsansvarlig for en overføring i strid med instrukser som er gitt.[7] Slik sett kunne man tenkt at det vil være databehandlerens problem å sikre at utleveringen og overføringen ut av EU/EØS er lovlig. Så enkelt er det likevel ikke, da den behandlingsansvarlige har en grunnleggende forpliktelse til å sørge for at regelverket følges når personopplysninger behandles.[8] Etterlevelse skal kunne «påvises» og dokumenteres.[9] Den behandlingsansvarlige skal kun ta i bruk databehandlere som gir tilstrekkelige garantier for egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i GDPR.[10] Dette ansvaret innebærer blant annet at både databehandleren og den aktuelle behandlingen må risikovurderes for å sikre at personopplysningene blir tilstrekkelig beskyttet.[11] Dette må skje før kontrakt inngås og før behandlingen starter. Det må blant annet vurderes om det er risiko for at personopplysningene kan bli gjort tilgjengelige for uvedkommende.[12] Dette betyr i praksis at behandlingsansvarlig ikke kan se bort fra risiko ved at databehandlerens morselskap er underlagt lovgivning som kan medføre at databehandleren kan bli pålagt av mor å utlevere personopplysninger.[13]

Risikovurdering knyttet til morselskapsproblematikk

GDPR har en risikobasert tilnærming. Ved avgjørelsen av hvilken risiko som foreligger og hvilke tekniske og organisatoriske tiltak som er egnet til å ta ned risikoen, skal den behandlingsansvarlige ta utgangspunkt i behandlingens art, omfang, formål og sammenhengen den utføres i.[14] Ved vurderingen av hva som er riktig beskyttelses – og sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med ikke-autorisert utlevering av eller tilgang til de aktuelle personopplysningene[15]. Den behandlingsansvarliges vurdering av om en databehandlers garantier er tilstrekkelige, er en risikovurdering som vil avhenge av typen behandling som er betrodd databehandleren.[16]

Risikovurderinger er helhetsvurderinger hvor en rekke ulike elementer veies mot hverandre. Det er ved eierskapsproblematikk naturlig å starte med å undersøke hvorvidt morselskapet faktisk kan være bundet av inngripende lovgivning. Her kan man be om databehandlerens egne vurderinger, men disse bør ikke være avgjørende alene.[17] Dersom man kommer til at databehandleren kan bli pålagt å utlevere personopplysninger på bakgrunn av inngripende lovgivning i tredjelandet hvor morselskapet er etablert, må den behandlingsansvarlige også risikovurdere dette

3 GDPR art. 45
4 https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overforing-av-personopplysninger-ut-av-eos/omrader-med-tilstrekkelig-beskyttelsesniva/
5 GDPR art. 28 (3)
6 GDPR art. 28 (3)
7 GDPR art. 28 (10)
8 GDPR art. 5
9 GDPR art. 5
10 GDPR art. 28 (1)
11 GDPR art. 32
12 GDPR art. 32
13 Datatilsynet; Overføring av personopplysninger ut av EØS | kapittel 7 Opplysninger utelukkende behandlet i EØS
14 GDPR art. 24 og 32 (2)
15 GDPR art.32
16 Guidelines 07/2020 on the concepts of controller and processor in the GDPR, punkt 96.
17 Datatilsynet; Overføring av personopplysninger ut av EØS | kapittel 6 Tilleggskrav (Schrems II)

aspektet.[18] Relevante momenter vil blant annet være hvilke personopplysninger det er tale om, formålet med behandlingen og tjenesten, hvilken risiko en utlevering vil medføre for de registrerte, og hvilke tekniske, organisatoriske og kontraktuelle tiltak som vil iverksettes for å forhindre utlevering og redusere risiko.

Schrems II-dommen er kritisert for at den ikke åpner for en risikobasert tilnærming. Det er viktig å være oppmerksom på at når det gjelder eierskapsproblematikk, stiller dette seg annerledes. Det at regelverket åpner for en risikobasert tilnærming i denne sammenheng ble tydeliggjort i en avgjørelse fra den franske forvaltningsdomstolen Conseil d'Etat i mars 2021.[19] Saken gjaldt om personopplysninger som ble behandlet ved booking av Covid-19-vaksinasjoner var tilstrekkelig beskyttet på plattformen som ble driftet av AWS Sarl; et datterselskap av amerikanske Amazon Web Services (AWS). Klageren, fagforeninger i helsesektoren, hevdet at det ble behandlet sensitive personopplysninger og at det innebar et brudd på personvernrettighetene at personopplysninger ble behandlet i et system driftet av et datterselskap av det amerikanskbaserte AWS.

For det første påpekte Conseil d'Etat at det i dette tilfellet *ikke* skjedde en *overføring* av personopplysninger slik overføringsbegrepet skal forstås etter GDPR kapittel V. Dette fordi behandlingen skjedde i Europa av et europeisk selskap. De anså det imidlertid som en risiko at amerikanske myndigheter kunne få tilgang til personopplysninger på bakgrunn av det amerikanske eierskapet. Domstolen kom likevel frem til at personopplysningene ikke var sensitive under begrunnelse av dette kun gjaldt navn på personer og deres tidspunkt for vaksinering, og at beskyttelsesnivået var tilstrekkelig på bakgrunn av iverksatte tiltak. Av iverksatte tiltak ble det vist til at personopplysningene ville bli slettet etter tre måneder, det fantes sikkerhetsmekanismer (kryperting) som ville forhindre tredjeparter i å kunne lese data, og partene hadde avtalt en egen prosess som skulle følges dersom AWS Sarl skulle få innsynsbegjæringer fra utenlandske myndigheter. Her skulle alle forespørsler som ikke var i tråd med europeisk regelverk bestrides.

Selv om dommen ikke kan gis generell rekkevidde, underbygger den likevel forståelsen av at der databehandler har avgrenset behandlingen til EU/EØS, vil betydningen av eierskap og muligheter for utlevering til offentlige myndigheter på bakgrunn av dette, kunne avgjøres gjennom en risikovurdering av den konkrete databehandleren. Som del av disse vurderingene har det vært tatt til orde for at det bør undersøkes i hvilken grad databehandler og morselskapet tidligere har mottatt begjæring om utlevering av personopplysninger, hvilke personopplysninger som ble etterspurt og i hvilken grad personopplysningene ble utlevert. Videre bør det vurderes hva databehandler selv uttrykker om hvordan pålegg om utleveringer håndteres. Det må også vurderes om databehandler har iverksatt organisatoriske og tekniske tiltak for å hindre at myndigheter i ikke-godkjente tredjeland kan få tilgang.

Man bør imidlertid være oppmerksom på at det også er avsagt en avgjørelse som gir utrykk for at det at databehandler kan bli pålagt å utlevere personopplysninger, er å anse som en *overføring*. I desember 2021 kom den tyske forvaltningsdomstolen Wiesbaden Administrative Court til at Rhine-Main University of Applied Sciences måtte slutte å bruke et cookiesamtykkeverktøy fordi det overfører personopplysninger til et selskap som har eiere i USA. Opplysningene ble opplyst å være lagret i EU og avtalen skal ha vært inngått med det europeiske tilknyttede selskapet. Domstolen skal ifølge IAPP[20] aldri ha vurdert hvorvidt en overføring faktisk finner sted, men de formidler at domstolen går langt i å si at så lenge mottaker av personopplysningene formelt kan bli forespurt om utlevering av personopplysninger fra myndigheter utenfor EU, må det regnes som en overføring. Denne tilnærmingen er annerledes enn European Data Protection Board (EDPB) sin definisjon av hva en "overføring" er. Her viser ingen av eksemplene til EDPB knyttet til overføring, at personopplysningene fysisk fortsatt forblir i EU.[21]

Dersom eksisterende tiltak gjør behandlingsansvarlig trygg på at risikoen for at myndigheter i ikke-godkjente tredjeland får tilgang til personopplysningene er liten, sammenlignet med den nytten behandlingsansvarlig får av den aktuelle behandlingen, taler dette for at risikoen ved å bruke en databehandler med morselskap i et ikke-godkjent tredjeland kan aksepteres.

Det vil være særlig viktig at alle risikovurderinger knyttet til databehandleren og behandlingen dokumenteres. Slike vurderinger er ikke en engangsøvelse som er lett å gjennomføre. Her må det ofte benyttes flere ressurser med ulike kompetanser, og vurderingene som gjelder lokal lovgivning i ikke-godkjente tredjeland, kan være spesielt krevende.

Kontraktsvilkår som tillater overføring til ikke-godkjente tredjeland

Som nevnt skal databehandleren bare behandle personopplysningene basert på dokumenterte instrukser fra den behandlingsansvarlige, og slik kan det settes forbud mot overføring til ikke-godkjente tredjeland i partenes databehandleravtale. Imidlertid

18 GDPR art. 32
19 Conseil d'Etat (2021)
20 IAPP (2021)
21 EDPB (2021)

blir behandlingsansvarlig ofte møtt med standardvilkår som tar forbehold om at nettopp slik overføring kan skje, og hvor det oppleves å være lite forhandlingsrom.

For slike tilfeller vil det allerede ved kontraktsinngåelse være stadfestet at overføring er en reell mulighet som behandlingsansvarlig også har samtykket til på forhånd. Dette reiser både behovet for å fastslå hvem av partene som vil være behandlingsansvarlig for en slik overføring, og dersom databehandleren skal anses som behandlingsansvarlig for overføringen; hvilket behandlingsgrunnlag den behandlingsansvarlige kunden har for å tillate dette ettersom utlevering av personopplysninger også krever et gyldig behandlingsgrunnlag.[22] I praksis betyr dette at den behandlingsansvarlige kunden må identifisere det gyldige behandlingsgrunnlaget for at kontraktsinngåelse og benyttelse av databehandleren skal være i tråd med personvernregelverket.

Dersom det er særlige kategorier av personopplysninger som behandles, kan dette bli særlig utfordrende fordi behandlingen da også vil kreve at tilleggsvilkår for å behandle slike personopplysninger er oppfylte, og disse er betraktelig snevrere.[23]

Hva kan vi oppsummere med?

Det innebærer en risiko for en ulovlig utlevering å benytte en databehandler som utelukkende skal behandle personopplysninger i EU/EØS dersom morselskapet er etablert i et ikke-godkjent tredjeland og underlagt lovgivning som kan innebære pålegg om utlevering av personopplysninger. Det må i slike tilfeller foretas en dokumentert risikovurdering som hensyntar typen personopplysninger som behandles, risiko for personvernet, formålet med tjenesten, hvilke tekniske og organisatoriske tiltak som vil bli innført, hvordan forholdet skal kontraktreguleres mellom partene, og hvordan databehandleren håndterer henvendelser fra myndigheter. Særlig varsomhet bør utvises dersom man som behandlingsansvarlig i kontrakt samtykker til at slik utlevering kan skje, uten at roller, ansvar og behandlingsgrunnlag er vurdert.

Partner/advokatfullmektig Hanne Pernille Gulbrandsen, Senior Manager/advokatfullmektig Marianne Lie Howard og Senior Manager/advokat Eirin Hauvik i Deloitte Advokatfirma.

22 Datatilsynet; Overføring av personopplysninger ut av EØS | kapittel 7 Opplysninger utelukkende behandlet i EØS

23 GDPR art. 9

Kilder:

- Conseil-etat.fr/ (2021). URL: The urgent applications judge does not suspend the partnership between the Ministry of Health and Doctolib for the management of COVID-19 vaccination appointments (conseil-etat.fr) Hentet 2. mai 2022
- Direktiv 2016/679 EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) [PVF, GDPR]
- European Data Protection Board (EDPB) "Guidelines 05/21 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR" (2021) Hentet 14. mars 2022
- European Data Protection Board (EDPB) "Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 2.0 Adopted on 07 July 2021" Hentet 14. mars 2022.
- International Association of Privacy Professionals (IAPP) v/Daniel Felz og Peter Swire, "New EU data blockage as German court would ban many cookie management providers" (2021) New EU data blockage as German court would ban many cookie management providers (iapp.org) Hentet 14. mars 2022
- Sak C-311/18, CJEU, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, ECLI:EU:C:2020:559
- Det norske Datatilsynet URL: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overforing-av-personopplysninger-ut-av-eos/omrader-med-tilstrekkelig-beskyttelsesniva/ Hentet 20.05.2022
- Det norske Datatilsynet URL: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overforing-av-personopplysninger-ut-av-eos/personopplysninger-utelukkende-behandlet-i-eos/ Hentet 20.05.2022

Halvor Manshaus
Leder IP/Media-gruppen i Advokatfirmaet Schjødt AS, Oslo og fast spaltist i Lov&Data

Mats Hole
Fullmektig i Schjødt.

EU-domstolen balanserer opphavsrett og ytringsfrihet i sak om DSM artikkel 17

EUs Copyright Digital Single Market Directive (digitalmarkedsdirektivet, eller DSM-direktivet) trådte i kraft 6. juni 2019, med frist for implementering satt til 7. juni 2021. Ved utgangen av april 2022 hadde fortsatt kun 10 av 27 medlemsstater implementert direktivet i sin nasjonale rett. Flere land har måttet dele opp prosessen i flere trinn, delvis grunnet behovet for omfattende endringer i eksisterende nasjonal rett, delvis grunnet usikkerhet og debatt knyttet til direktivets innhold og rekkevidde.

Det er særlig direktivets artikkel 17 om delingsplattformers[1] ansvar for brukeropplastet innhold som har vært gjenstand for diskusjon. Artikkel 17 representerer en grunnleggende endring av ansvarsnormen for plattformers formidling av åndsverk og tilsvarende typer rettighetsbelagt materiale. I kjernen av debatten står balansen mellom opphavsrett og ytringsfrihet, ettersom en for streng regulering av brukernes formidling via ulike plattformer vil kunne gjøre uproporsjonale inngrep i ytringsfriheten. Det gjør ikke diskusjonen mindre interessant at begge typer rettigheter inngår i EUs charter om fundamentale rettigheter.

Saken ble satt på spissen ved at Polen 24. mai 2019 brakte en sak mot Europaparlamentet og Rådet vedrørende gyldigheten av artikkel 17 for EU-domstolen (CJEU). Polen anførte prinsipalt at domstolen måtte annullere deler av artikkel 17(4), spesifikt ordlyden «and made best efforts to prevent their future uploads in accordance with point (b)» i artikkel 17(4) bokstav b og c. Subsidiært, for det tilfelle at deler av ordlyden i bestemmelsen ikke kunne annulleres, ble det anført at retten måtte annullere hele artikkel 17.

Den 26. april 2022 kom avgjørelsen fra CJEU (C-401/19), der domstolen i storkammer fant at pliktene som pålegges plattformetilbyderne gjennom DSM-direktivets artikkel 17(4) ikke representerer et uproporsjonalt inngrep i brukernes ytringsfrihet. Dette var ikke et uventet resultat, og er i tråd med konklusjonen fra generaladvokatens uttalelse. Generaladvokaten fant i sin vurdering at direktivets ansvarsregler isolert sett innebærer en krenkelse av ytringsfriheten, men at denne ikke var i strid med vilkårene for slike inngrep etter EUs Charter om fundamentale rettigheter artikkel 52 første ledd. Likevel ble det fremholdt fra generaladvokaten at det nye regimet innebar en fare for «over blocking» som diskutert i avsnittene 141-143 i uttalelsen vedrørende artikkel 17:

«Nevertheless, the link that the EU legislature established, in those provisions, between the liability of sharing service providers and the effectiveness of such filtering entails a significant risk to freedom of expression, namely the risk of 'over-blocking' lawful content. Such a risk of an 'over-blocking' exists, generally, where public aut-

1 Direktivet definerer i artikkel 2 nr 6 hva en delingsplattform er og bruker begrepet «online content-sharing service provider» / «onlineindholdsdelingstjenester».

horities hold intermediary providers liable for illegal information provided by users of their services. In order to avoid any risk of liability, those intermediaries may tend to be overzealous and excessively block such information where there is the slightest doubt as to its lawfulness. In the present case, the risk is, more specifically, that, in order to avoid any risk of liability vis-à-vis rightholders, the sharing service providers systematically prevent the making available, on their services, of all content which reproduces works and other protected subject matter for which they have received the 'relevant and necessary information' or a 'sufficiently substantiated notice' from those rightholders, including content which does not infringe their rights.»

Slik indirekte struping eller innsnevring av ytringsfriheten omtales som «chilling effect» av den Europeiske Menneskerettsdomstolen (EMD). I norsk rettspraksis ser vi flere saker der betydningen av å unngå en slik nedkjølende effekt på muligheten til å ytre seg – eller motta ytringer – har blitt tillagt avgjørende vekt. Runesten-saken (Rt-2010-1381, omtalt i LoD-2011-105-15) er et eksempel på dette.

Domstolen fant altså likevel å opprettholde direktivet og artikkel 17 i sin eksisterende form. Som det fremgår ovenfor er det flere land som har avventet implementering av direktivet, og det er naturlig å legge til grunn at flere har avventet utfallet av denne konkrete saken. Avgjørelsen kan således ventes å få direkte betydning for den videre takten for implementering, samt innholdet av de endringer som gjøres på nasjonalt nivå. I det følgende skal vi se nærmere på artikkel 17 og enkelte av de forhold som har skapt så mye debatt rundt denne nye reguleringen.

Polen la i sin stevning til grunn at ordlyden i artikkel 17(4) innebar at plattformene som ble rammet av den nye ansvarsnormen måtte kontrollere og overvåke alt innhold som ble lastet opp av sine brukere. Polen anførte at et slikt krav i seg selv ville utgjøre et ulovlig inngrep i brukernes rett til ytringsfrihet og rett til informasjon, jf. EUs charter om grunnleggende rettigheter artikkel 11.

I lys av dagens tilgjengelige teknologi, ville en slik overvåkning i praksis bli ved bruk av automatiske filtreringsverktøy. Etter Polens syn ville slik forhåndskontroll utgjøre et inngrep i ytringsfriheten til brukerne av slike plattformer, ettersom slike filtreringsverktøy

(i) kan medføre en risiko for at lovlig innhold blir blokkert, og
(ii) vurderingen av om innholdet er lovlig eller ikke blir avgjort av algoritmer forut for selve publiseringen

Polen forklarte på denne bakgrunn at det var nødvendig med en rettslig avklaring. Som nasjonale myndigheter i EU måtte regjeringen påta seg ansvaret for et eventuelt inngrep i ytringsfriheten ved implementering av direktivet.

Den nylig avsagte avgjørelsen fra CJEU innleder med å ta stilling til hvorvidt den primære anførselen overhode kan være gjenstand for behandling. Her henviser domstolen til tidligere praksis fra CJEU, der delvis annullering kun er blitt ansett mulig der delene som skal annulleres ikke er uløselig knyttet til de resterende delene av regelen. Domstolen viser til at artikkel 17 som helhet etablerer et nytt ansvarsregime, og at annullering av kun deler av bokstav b og c i 17(4) ville medført et ansvarsregime som både var vesentlig annerledes, men også vesentlig mer i favør av plattformenes interesser på bekostning av interessene til rettighetsholderne. Ettersom en balansering av disse interessene er selve kjernen i artikkelen som helhet, kan ikke artikkelen delvis annulleres i tråd med den prinsipale anførselen. Direktivet som helhet ville derimot kunne stå seg uten artikkel 17. CJEU fant derfor at den subsidiære anførselen kunne behandles.

I sin behandling av hovedspørsmålet i saken, hvorvidt artikkel 17 i DSM-direktivet utgjør en ulovlig og uproporsjonal innskrenkning av ytringsfriheten, innleder domstolen med utgangspunktet som var gjeldende før DSM-direktivet, artikkel 3 i direktiv 2001/29 («InfoSoc») og artikkel 14 i direktiv 2000/31 («E-Commerce»).

InfoSoc-direktivet artikkel 3 regulerer retten til kommunisering og tilgjengeliggjøring av opphavsrettsbeskyttede verk til offentligheten. Det klare utgangspunkt var, og er fremdeles, at rettighetshaveren til et åndsverk også har eksklusiv rett til kommunisering og tilgjengeliggjøringen av verket til offentligheten, både fysisk og digitalt. E-Commerce-direktivet artikkel 14 gjelder særskilt for delingsplattformer, hvor man som plattform ikke kan holdes ansvarlig for ulovlig innhold på plattformen, såfremt man ikke har positiv kunnskap om dets eksistens eller etter omstendighetene burde hatt slik kunnskap. Med andre ord ble ikke disse plattformene rammet av bestemmelsen om kommunisering eller tilgjengeliggjøring av innhold, og var derfor heller ikke direkte ansvarlige for eventuelt ulovlig tilgjengeliggjort materiale.

Domstolen påpeker, med henvisning til avgjørelsen i *Youtube and Cyando AG (C-682/18)*, at enkelte plattformer kan se ut til å ha innrettet sin virksomhet og finansielle strategi etter denne gjeldende ansvarsnormen på en slik måte at disse nærmest oppfordrer brukerne til opplasting av beskyttet innhold.

Etter å ha fastlagt det rettslige utgangspunktet, går domstolen videre til å eksplisitt omtale artikkel 17 som en «*new specific liability mechanism*». Retten beskriver det nye ansvarsregimet i artikkel 17 i avsnitt 32 og 33:

«[…] Article 17(1) of Directive 2019/790 provides that an online content-sharing service provider performs an act of communication to the public or an act of making available to the public when it gives the public access to copyright-protected works or other protected subject matter uploaded by its users and that it must, the-

refore, obtain an authorisation from the rightholders for that purpose, for instance by concluding a licensing agreement.

At the same time, Article 17(3) of Directive 2019/790 excludes online content-sharing service providers from the exemption from liability, in relation to such acts, provided for in Article 14(1) of Directive 2000/31.»

Utgangspunktet er dermed motsatt fra det forrige ansvarsregimet, delingsplattformene (slik de nå er definert i DSM-direktivet) rammes av artikkel 3 i InfoSoc-direktivet, og kan ikke få beskyttelse av det som har blitt omtalt som «Safe Harbour»-regimet i artikkel 14 i E-commerce direktivet.

Et kjernepunkt i avgjørelsen er knyttet opp mot unntakene for ansvar i DSM artikkel 17 fjerde ledd:

«Article 17

Use of protected content by online content-sharing service providers

4. If no authorisation is granted, online content-sharing service providers shall be liable for unauthorised acts of communication to the public, including making available to the public, of copyright-protected works and other subject matter, unless the service providers demonstrate that they have:

(a) made best efforts to obtain an authorisation, and

(b) made, in accordance with high industry standards of professional diligence, best efforts to ensure the unavailability of specific works and other subject matter for which the rightholders have provided the service providers with the relevant and necessary information; and in any event

(c) acted expeditiously, upon receiving a sufficiently substantiated notice from the rightholders, to disable access to, or to remove from their websites, the notified works or other subject matter, and made best efforts to prevent their future uploads in accordance with point (b).»

Domstolen omtaler dette i avgjørelsens avsnitt 34 som «*a specific liability regime for where no authorisation is granted*». Delingsplattformene kan altså unngå ansvar for formidling av ulovlig innhold der vilkårene i bokstav a til c er innfridd. Deretter diskuteres de enkelte punktene i ansvarsregimet, som gir både plattformene, brukerne og ulike myndigheter retter og plikter i forbindelse med gjennomføringen av ordningen.

CJEU går deretter over til å vurdere hvorvidt det i det hele tatt foreligger en begrensning av ytringsfriheten til brukerne, enten direkte eller ved at resultatene av pliktene som pålegges plattformene uunngåelig kommer til å medføre begrensninger.

Polen anførte at utformingen av artikkel 17(4) nødvendigvis ville medføre en kontroll eller overvåkning av alt innhold som lastes opp, og at dette i seg selv ville utgjøre en begrensning i ytringsfriheten. Europaparlamentet og Rådet, støttet av partshjelperne Spania, Frankrike og Kommisjonen, avviste at en slik ordning som beskrevet i artikkel 17 ville begrense ytringsfriheten til brukerne, og hvis artikkel 17 skulle indirekte resultere i en slik begrensning ville ikke dette kunne lastes lovgiverne i EU.

CJEU redegjør deretter for tidligere rettspraksis knyttet til ytringsfriheten og retten til informasjon, og trekker her inn artikkel 10 om ytringsfrihet i den europeiske menneskerettskonvensjon og tilhørende praksis fra EMD. Domstolen knytter i denne sammenheng vurderingen opp mot de ulike pliktene som påhviler plattformene som et resultat av artikkel 17(4). Som også generaladvokaten hadde pekt på i sin vurdering fra 2021, viser domstolen til at det per dags dato ikke finnes noen annen løsning enn å anvende automatisert teknologi for automatisk gjenkjenning og filtrering. Mengden med data og innhold som lastet opp på slike plattformer er langt større enn kapasiteten til menneskelig behandling av hvert enkelt element.

Domstolen fant at en slik forhåndskontroll og filtrering rent faktisk er egnet til å begrense spredning av innhold. Ansvarssystemet etter artikkel 17 fjerde ledd må derfor anses som en begrensning av rettighetene som garantert for i EUs charter om grunnleggende rettigheter artikkel 11, ref avsnitt 55 i avgjørelsen:

«Such a prior review and prior filtering are liable to restrict an important means of disseminating online content and thus to constitute a limitation on the right guaranteed by Article 11 of the Charter.»

Det neste spørsmålet ble da hvorvidt en slik begrensning av ytringsfriheten er lovlig. Polen anførte at begrensningen ikke kunne sies å innfri EUs charter om grunnleggende rettigheter artikkel 52(1), som beskriver når og hvordan rettighetene lovlig kan begrenses. Av bestemmelsen fremgår det at begrensninger av rettighetene og frihetene må være hjemlet i lov, og må respektere *«the essence of those rights and freedoms»*. Begrensninger i frihetene og rettighetene som fremgår av EUs charter om grunnleggende rettigheter må også vurderes ut ifra et proporsjonalitetsprinsipp. Europaparlamentet og Rådet, støttet av Spania, Frankrike og Kommisjonen, bestred Polens anførsel, og mente at artikkel 17 inneholder tilstrekkelige sikkerhetsventiler og mekanismer til å ivareta de ulike hensynene som må veies opp mot hverandre.

I sin tolkning av legalitetsprinsippet i EUs charter om grunnleggende rettigheter artikkel 52(1), med henvisning til *Facebook Ireland and Schrems*, fant domstolen at lovregelen som begrenser den relevante rettigheten selv må angi omfanget av begrensningen. I proporsjonalitetsvurderingen skal det som normalt vurderes om begrensningen er *«appropriate and necessary»* for å ivareta formålet. Domstolen fremhver at der det er snakk om kolliderende rettigheter må det finnes en *«fair balance»* mellom de kryssende regelsett.

Domstolens lovtolkning på dette punktet legger viktige føringer for den videre vurderingen, spesielt med tanke på rettens forståelse av proporsjonalitetsprinsippet. I denne

saken er det nettopp snakk om spørsmål i kjernen av ytringsfriheten ved at det er snakk om forhåndssensur. CJEU viser også i avsnitt 68 i avgjørelsen til EMD og praksis knyttet til forhåndssensur, der det oppstilles skjerpede krav til et slikt regime:

«As regards, in particular, a limitation on the exercise of the right to freedom of expression and information such as that at issue in the present case, it follows from the case-law of the European Court of Human Rights that, although Article 10 ECHR does not prohibit prior restraints on a means of dissemination as such, such restraints nonetheless pose such a risk to compliance with that fundamental right that a particularly tight legal framework is required…»

Når det kommer til hvorvidt legalitetsprinsippet er oppfylt, finner retten at på tross av at artikkel 17 ikke inneholder en spesifikk definisjon av hvilke verktøy som skal brukes for å innfri kravene i 17(4) bokstav b og c, så er kravet til lovhjemmel innfridd. Grunnen til manglende spesifisering av virkemiddel er EUs ønske om å holde mekanismen teknologinøytral.

Angående proporsjonalitetsprinsippet, viser retten til at dette er en avveining mellom tre viktige hensyn: retten til ytringsfrihet, retten til å drive forretning og eiendomsretten til de immaterielle rettighetene, jf. henholdsvis § 11, 16 og 17(2) i EUs charter om grunnleggende rettigheter.

I den konkrete vurderingen av hvorvidt det foreligger en ulovlig begrensning av retten til ytringsfrihet, vektlegger domstolen ulike sikkerhetsventiler og mekanismer i artikkel 17 for å sikre rettighetene til forbrukerne. Særlig vektlegges 17(7) og 17(9) i avsnitt 80:

«It clearly follows, therefore, from Article 17(7) and (9) of Directive 2019/790 and from recitals 66 and 70 thereof that, in order to protect the right to freedom of expression and information of users of online content-sharing services, enshrined in Article 11 of the Charter, and the fair balance between the various rights and interests at stake, the EU legislature has laid down that the implementation of the obligations imposed on those service providers in point (b) and point (c), in fine, of Article 17(4) of that directive cannot, in particular, lead to the latter's taking measures which would affect the essence of that fundamental right of users who share content on their platforms which does not infringe copyright and related rights.»

Etter en vurdering av helheten finner domstolen at:

«It follows from the findings in paragraphs 72 to 97 above that, contrary to what the Republic of Poland maintains, the obligation on online content-sharing service providers to review, prior to its dissemination to the public, the content that users wish to upload to their platforms, resulting from the specific liability regime established in Article 17(4) of Directive 2019/790, and in particular from the conditions for exemption from liability laid down in point (b) and point (c), in fine, of Article 17(4) of that directive, has been accompanied by appropriate safeguards by the EU legislature in order to ensure, in accordance with Article 52(1) of the Charter, respect for the right to freedom of expression and information of the users of those services, guaranteed by Article 11 of the Charter, and a fair balance between that right, on the one hand, and the right to intellectual property, protected by Article 17(2) of the Charter, on the other.»

Retten fant således til at Polens anførsel ikke kunne føre frem. CJEU kommer likevel med flere bemerkninger til medlemslandene angående implementeringen av artikkel 17 i nasjonalt lovverk i avsnittene 86 og 99:

«[…] it must be borne in mind that the Court has already held that a filtering system which might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications, would be incompatible with the right to freedom of expression and information, guaranteed in Article 11 of the Charter, and would not respect the fair balance between that right and the right to intellectual property.»

«Member States must, when transposing Article 17 of Directive 2019/790 into their national law, take care to act on the basis of an interpretation of that provision which allows a fair balance to be struck between the various fundamental rights protected by the Charter. Further, when implementing the measures transposing that same provision, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with that provision but also make sure that they do not act on the basis of an interpretation of the provision which would be in conflict with those fundamental rights or with the other general principles of EU law, such as the principle of proportionality»

CJEUs avgjørelse i C-401/19 er en betydningsfull avgjørelse for både medlemslandene i EU, rettighetsholdere av opphavsrettsbeskyttede verk og plattformtilbyderne. Denne avgjørelsen vil bli referert til i tiden som kommer, både når det gjelder spørsmål om nasjonale implementeringer av den nye ansvarsnormen, men også i private tvister mellom plattformer og aktører i markedet.

Samtidig er avgjørelsen også viktig for *brukerne* av disse plattformene, både de som laster opp innhold og brukere som konsumerer slikt innhold. I større målestokk må det trekkes inn at disse plattformene har blitt en viktig del av hvordan vi som moderne mennesker kommuniserer, både globalt og lokalt. Informasjon som deles formidles videre, og går inn ikke bare i den aktuelle debatt, men blir liggende tilgjengelig som grunnlag for nye diskusjoner og meningsbrytninger også fremover i tid.

Det er i denne sammenheng at domstolen fremhever at implementeringen på nasjonalt nivå må hensynta balansen mellom verneregelene og ytringsfriheten. En implementering av artikkel 17 i nasjonalt lovverk som ikke har de nødvendige sikkerhetsventiler og kontroll-

mekanismer for å ivareta brukernes rettigheter vil kunne utgjøre uforholdsmessige inngrep i ytringsfriheten. Videre fremhever domstolen eksplisitt at artikkel 17 ikke medfører en *generell* plikt for plattformene til å overvåke og kontrollere alt innhold som lastes opp. Innholdet vil kun måtte kontrolleres opp mot *spesifikk* informasjon som blir tilgjengeliggjort av rettighetsholderne. Hvilken form en slik informasjonsutveksling mellom plattformene og rettighetsholderne vil ta i fremtiden er uklart, og det er liten veiledning i direktivet. Det som imidlertid er klart ut fra artikkel 17, og nå også eksplisitt vektlagt av CJEU, er i alle fall at overvåkningsplikten for plattformene er spesiell og konkret, ikke generell.

Det er likevel grunn til ettertanke om selve utformingen av artikkel 17 og det nye regimet som skal etableres. Et forsiktighetsprinsipp hos delingsplattformene vil raskt medføre en *de facto* chilling effect. Grensene her vil være uklare, og automatisk filtrering er alt annet enn feilsikkert. Vi har allerede erfaring med en rekke eksempler der bilder og innlegg på Facebook, Youtube og tilsvarende delingsplattformer blir slettet på fullstendig feil grunnlag. Diskusjon, kritikk og bruk av kilder i seg selv kan fort bli vesentlig vanskeligere enn vernet om ytringsfriheten skulle tilsi. Ved at opplastet materiale i praksis stanses før publikasjon vil den enkelte bruker stå relativt maktesløs, og det er grunn til å tro at klagebehandling på «overskuddssletting» vil være vanskelig og tidkrevende. Dette ligger blant annet i at flere av de store delingsplattformene opererer utenfor EU og i tillegg håndterer så store mengder av innlegg og opplastinger at dette i seg selv vil begrense effektiv saksbehandling.

Samtidig er det et klart behov for vern om rettighetshavernes interesser. Spørsmålet er mer om artikkel 17 har truffet riktig i balanseringen av de ulike interessene som spiller inn. I Norge har vi allerede i formålsparagrafen til den nye åndsverksloven fått inn en konkret henvisning til ytringsfriheten. Likevel er det klart fra forarbeidene til åndsverksloven at det er opp til rettsutøveren ved den konkrete anvendelsen av reglene å se hen til ytringsfriheten og trekke opp grensen i den konkrete saken. Disse vurderingene vil neppe bli enklere når man skal se hen til veiledningen i DSM artikkel 17 og grunnlovens forbud mot forhåndssensur i Grl § 100.

Kulturdepartementet sendte i 2020 ut invitasjon til å komme med innspill til gjennomføringen av DSM-direktivet i Norge. Departementet mottok ca. 50 innspill innen fristen i mars 2021. Etter departementets plan skal det sendes ut høringsnotat i løpet av 2022.

Foto: Shutterstock

Government cloud procurement
- Contracts, Data Protection, and the Quest for Compliance, Cambridge University Press, Desember 2021

Forfatter: *Kevin McGillivray*
Tittel: Government cloud procurement - Contracts, Data Protection, and the Quest for Compliance, Cambridge University Press,
Utgivelsesår: Desember 2021
ISBN: 9781108837675
Online ISBN:9781108942485

Bakgrunn

Skytjenester har mange fordeler som er attraktive for både private og offentlige brukere. Fordelene med skytjenester er blant annet at kostnadene ofte er lave, brukerne har mange valgmuligheter for programvarer og lagring, og skytjenestene gir lett tilgjengelig datakraft. Andre fordeler er at skytjenester gir tilgang til dynamisk eskalering og at betalingen kun er basert på faktisk bruk.

Selv om fordelene med skytjenestene er mange, fører teknologien til mange juridiske spørsmål, særlig vedrørende kontraktsrett og personvern. Lovgivningen er ofte uklar med hensyn til skytjenester og kan bli vanskelig å rettferdiggjøre med teknologien. I tillegg til bruk av skytjenester i det private næringsliv eller av private personer, har offent-

lig sektor begynt å bruke skytjenester i større grad.[1]
Offentlig sektor har ofte særskilte krav til informasjonssikkerhet samt lover om elektronisk arkiv, bokføringslover og offentlige anskaffelser. Offentlig sektor har også de samme kravene som vi finner i privat sektor vedrørende personvern. I tillegg må offentlig sektor ta særlig hensyn til befolkningens data over tid og nasjonal sikkerhet.

Government Cloud Procurement:

I *«Government Cloud Procurement»* utforsker Kevin McGillivray spørsmålet om offentlige myndigheter kan ta i bruk skytjenester og fortsatt oppfylle sine juridiske krav og andre forpliktelser overfor innbyggerne. Hovedspørsmålet i boken er om det er mulig for offentlig sektor å bruke skytjenester på en hensiktsmessig og lovlig måte. I boken stilles det også spørsmål om hva slags kontrakter og anskaffelsesplaner offentlig sektor bør ha for å ta i bruk skytjenester. Bokas omtaler også hvordan personvernregelverket påvirker bruken av skytjenester.

Boken fokuserer på samspillet mellom de tekniske egenskapene til skytjenstene og de komplekse juridiske kravene som gjelder for skyadopsjon og bruk. De juridiske spørsmålene som er evaluert, inkluderer personvernlovgivning (GDPR og det amerikanske regimet), jurisdiksjonsspørsmål, kontrakter og transnasjonale privatrettslige tilnærminger.

McGillivray adresserer også offentlig sektors unike posisjon når de outsourcer kjerneaspekter av informasjons- og kommunikasjonsteknologien til skytjenesteleverandører. Analysen i boken støttes av omfattende forskning som undersøker faktiske skykontrakter oppnådd gjennom Freedom of Information Act (FOIA) gjennom forespørsler til amerikansk myndigheter. Siden etterspørselen etter skytjenster er økende, fyller denne studien et tomrom i juridisk litteratur og gir veiledning til organisasjoner som vurderer skytjenster.

Anmeldelser og endorsements

«Cloud computing is an established standard component of the Internet environment. Yet, the regulation of cloud computing is still underdeveloped and plagued by uncertainty. Under such conditions, the value of McGillivray's contribution in Government Cloud Procurement cannot be overstated.»
– Dan Jerker B. Svantesson
- Faculty of Law, Bond University

«This book provides a welcome, well-researched, and well-written exposition of aspects of cloud computing which have hitherto received less attention than they deserve - namely the use of cloud computing by governments and the special legal challenges such usage presents.»
– Lee A. Bygrave - University of Oslo

Forfatter

Skrevet av Kevin McGillivray, PhD (Universitetet I Oslo, Senter for rettsinformatikk (SERI)). Kevin har publisert bredt innenfor juss og teknologi feltet. Han har også jobbet som forsker på flere EU-prosjekter, inkludert tjent som personvernombud på det Human Brain Project (HBP). Kevin er Skatteetatens nåværende personvernombud.

1 EDPB, «Launch of Coordinated Enforcement on Use of Cloud by Public Sector» (2022), <*https://edpb.europa.eu/news/news/2022/launch-coordinated-enforcement-use-cloud-public-sector_en*>. «According to EuroStat, the cloud uptake by enterprises doubled across the EU in the last 6 years.»

Personvern og kontroll i arbeidslivet

Marion Holthe Hirst og Signhild Nystad Blekastad.
Personvern og kontroll i arbeidslivet.
Oslo: Gyldendal, 2021. 448 s.
ISBN/EAN: 9788205538368

Boken gir en oversikt over de mest sentrale reglene og problemstillingene som gjelder personvern og de delene av arbeidsretten som gjelder kontroll i arbeidslivet.

Alle virksomheter behandler personopplysninger om sine ansatte for ulike formål og i ulike sammenhenger. Kjennskap til hvilke regler som gjelder for dette, er derfor noe mange har behov for.

Bokens tema er omfattende, noe som medfører at enkelte problemstillinger kun blir overfladisk behandlet. På andre områder går boken mer i dybden, det gjelder særlig temaer som er spesielt aktuelle, eller som ikke tidligere er grundig behandlet i faglitteraturen. Videre er boken utformet slik at den skal være mulig å forstå uten spesielle juridiske forkunnskaper.

Bokens tema er relevant for mange, både for arbeidstakere, arbeidsgivere, advokater, tillitsvalgte, personvernombud og andre som arbeider med juridiske problemstillinger i krysningspunktet personvern og arbeidsrett.

Åndsverkloven med kommentarer

Haakon Aakre, Stian Fagernæs, Thomas Rieber-Mohn.
Åndsverkloven med kommentarer.
Oslo: Gyldendal, 2021. 552 s.
ISBN/EAN: 9788205535114

Åndsverkloven er sentral både for rettighetshavere til og brukere av åndsverk og nærstående rettigheter.

Ny åndsverklov ble vedtatt i 2018. Loven bygger på hovedprinsippene i den tidligere loven fra 1961, men det er foretatt endringer i lovens språk og struktur i tillegg til en rekke materielle endringer. *Åndsverkloven med kommentarer* inneholder omfattende merknader til den nye lovens bestemmelser, og er ment å være et viktig verktøy for alle som trenger innsikt i dette rettsområdet.

Arrangementer 2022

Arrangementer i Danmark:

XXXVII Nordic Conference on Law and Information Technology arrangeres i København 31.10.2022–2.11.2022. Lenke til løpende oppdatert informasjon: *http://jura.ku.dk/ciir/nclit2022/*

Arrangementer i Sverige:

13 DECEMBER | HYBRID (DIGITALT ELLER I STOCKHOLM) IT-rätt 2022. Uppdatering, fördjupning och inblick inom IT-rätten: https://www.nj.se/nyhetsdag/it-ratt

Arrangementer i Norge:

Det XVIIIe nordiske opphavsrettssymposium, Kristiansand, 31. august – 2. september: https://www.opphavsrettsforeningen.no/symposium-2022

Norsk forening for JUS og EDB inviterer til Forum Rettsinformatikk 20. september i Gamle Festsal. Det blir blant annet en oppdatering av det som har hendt i året som har gått, samt en rapport fra Brussel om pågående utviklinger i EUs lovverk. Påmelding på *https://nfje.no/* Info kommer.

13-14. oktober blir det workshop i Sodi prosjektet. Tema Samfunnssikkerhet og digitale identiteter IfP prosjekt *https://www.jus.uio.no/ifp/forskning/prosjekter/sodi/*

VIROS prosjektet inviterer til en konferanse om «Vulnerability in the Robot Society» 27/28 oktober. *https://www.jus.uio.no/ifp/english/research/projects/nrccl/viros/events/* – Info kommer.

Personvernkonferansen 2022 blir arrangert 2. desember. Konferansen vil ta utgangspunkt Personvernkommisjonens innstilling som forventes overlevert i september. Nærmere informasjon om program og påmelding kommer i oktober på nettsidene for Senter for rettsinformatikk.

Illustrasjon: laws for atoms" by Will Lion is licensed under CC BY-NC-ND 2.0. To view a copy of this license, visit https://creativecommons.org/licenses/by-nc-nd/2.0/?ref=openverse.

Delphi

Lovisa Lennström

Sanktionsavgift mot Klarna, tillsyn mot Verisure och beviskrav för sanktionsavgifter

Sanktionsavgift mot Klarna

Den svenska Integritetsskyddsmyndigheten («IMY») meddelade den 29 mars 2022 beslut i ett tillsynsärende mot Klarna Bank AB («Klarna») efter en granskning av hur Klarna informerar om personuppgiftsbehandling på sin hemsida. Det mycket omtalade beslutet resulterade i en administrativ sanktionsavgift om 7,5 miljoner kronor.

I beslutet konstaterade IMY att Klarna inte informerat om ändamålen med sin personuppgiftsbehandling, vilken rättslig grund som använts till stöd för behandlingen eller till vilka kreditupplysningsföretag personuppgifterna lämnats ut. Klarna kritiserades också för att inte ha lämnat information om till vilka länder utanför EU/EES som personuppgifterna överfördes och om vilka skyddsåtgärder som tillämpades vid en sådan överföring. Klarna bedömdes även ha lämnat ofullständig information om hur länge personuppgifterna lagrades och de kriterier som användes för att fastställa lagringsperioderna. Slutligen konstaterade IMY att Klarna hade lämnat bristfällig information om de registrerades rättigheter, bland annat avseende rätten till radering av uppgifter.

Kraven på öppenhet och transparens är centrala för beslutet. I beslutet slår IMY fast att kravet på öppenhet innebär att en integritetspolicy ska innehålla information som bl.a. tydligt visar vilka personuppgifter som kan komma att delas med andra aktörer, vilka dessa aktörer är och vilka rättigheter som de registrerade har på ett sätt som gör det möjligt för den registrerade att förstå vad rättigheterna faktiskt innebär och när de kan göras gällande. Om personuppgifter överförs till ett tredje land utanför EU/EES ska det även anges till vilka länder personuppgifterna överförts, vilka skyddsåtgärder som vidtagits och hur de registrerade kan få tillgång till handlingar som visar vilka skyddsåtgärder som har vidtagits. Det är alltså inte tillräckligt att i en integritetspolicy generellt ange att personuppgifter kan komma att delas med mottagare i tredje land.

Vid bestämmandet av sanktionsavgiftens storlek tog IMY bl.a. hänsyn till att överträdelserna avsåg artiklar som är centrala för att den registrerade ska ha möjlighet att tillvarata sina rättigheter enligt GDPR, att överträdelsen berörde ett mycket stort antal registrerade och att överträdelsen hade pågått under en längre tid. Även faktumet att Klarna hade ändrat och förbättrat informationen om sin personuppgiftsbehandling under tillsynsperioden beaktades. Klarna har överklagat IMY:s beslut, så frågan om Klarnas personuppgiftsbehandling och den utdömda sanktionsavgiften är ännu inte slutligt avgjord.

Av intresse är även att IMY den 16 maj 2022 meddelade att de inleder en ytterligare tillsyn mot Klarna. Denna gång ska tillsynen avse Klarnas checkout-tjänst efter att klagomål inkommit till IMY avseende att tjänsten hämtar och fyller i personuppgifter efter att köparen endast fyllt i någon viss personuppgift.

Tillsynsärende mot Verisure Sverige AB

IMY meddelade den 22 april 2022 att de inleder en tillsyn av larmbolaget Verisure Sverige AB («Verisure») för att utreda de uppgifter som förekommit i media och klagomål som riktats från kunder om att anställda hos Verisure i samband med inkomna larm har delat filmmaterial och bilder mellan sig utan att det varit befogat. Det ska även ha förekommit att bilder sparats ner på anställdas egna hårddiskar.

IMYs tillsyn ska dels ta sikte på att utreda vad som har hänt, men också på vilka tekniska säkerhetsåtgärder Verisure har i form av behörighetsstyrning och loggar och

vilka instruktioner som ges till de anställda om hur bildmaterial får hanteras. I samband med att IMY offentliggjorde tillsynen uttalade IMY att det är viktigt för larmbolag som erbjuder hemlarm med kamerabevakning att tillhandahålla tydliga rutiner och regler för anställda om hur de får hantera bildmaterialet.

IMY:s beslut i ovan tillsynsärenden visar på vikten av att säkerställa att integritetspolicyer är korrekt utformade och kompletta samt vikten av att ha tydliga rutiner och regler för anställdas behandling av personuppgifter, särskilt i integritetskänsliga sammanhang.

Domar från Kammarrätten i Stockholm gällande sanktionsavgifter

Kammarrätten i Stockholm har den 16 maj 2022 meddelat dom i fem mål i vilka de upphäver förvaltningsrättens och IMY:s beslut att fem sjukhus och regioner ska betala sanktionsavgifter (mål nr. 4471-21, 4511-21, 4540-21, 4548-21 och 4611-21).

Kammarrätten anser att det ska ställas höga krav på IMY:s bevisning för att beslut om sanktionsavgift ska kunna fattas vid tillsynsärenden. Enligt kammarrätten har IMY inte bevisat att de aktuella sjukhusen och regionerna brustit i sina skyldigheter enligt GDPR när det gäller att säkerställa en lämplig säkerhetsnivå vid tilldelning av behörigheter i journalsystemen. Mot bakgrund av detta har det inte funnits skäl att påföra sanktionsavgifter och dessa upphävdes därmed

Kammarrättens avgöranden tydliggör att höga beviskrav ska uppställas för IMY:s beslut om påförande av administrativa sanktionsavgifter.

Lovisa Lennström, Associate, Advokatfirman Delphi.

Gorrissen Federspiel

Tue Goldschmieding

Ny vejledning om brug af cloud

Det danske Datatilsyn udgav den 9. marts 2022 en vejledning om brugen af cloudservices og tog initiativ til at nedsætte en ekspertarbejdsgruppe, der skal se på mulige tiltag, der kan sikre lovlig brug af cloudservices.

Vejledningen henvender sig primært til dataansvarlige og gennemgår de overvejelser, man som dataansvarlig skal foretage sig, hvis man ønsker at benytte en cloudservice. Dele af vejledningen er dog målrettet cloudleverandører, idet den beskriver, hvordan ydelser kan leveres i overensstemmelse med databeskyttelsesreglerne.

Vejledningen definerer «cloud» som en model til at tilvejebringe standardiserede it-ressourcer, typisk på større decentrale samlinger af servere, der tilgås via internettet. «Cloudservices» er en fællesbetegnelse, der dækker over mange forskellige services, og der kan således både være tale om specialiserede services skræddersyet til en enkelte organisation og standardiserede services. Cloudservices er kendetegnede ved, at kunden alene har kontrol over den type og mængde af ressourcer, f.eks. lagring, der ønskes leveret.

Vejledningen giver en køreplan, der kan tages udgangspunkt i ved vurderingen af brugen af cloud. Vejledningen giver således bl.a. retningslinjer for, hvilke risikovurderinger den dataansvarlige bør foretage, inden en behandlingsaktivitet overlades til en cloudleverandør; hvordan den dataansvarlige bør vurdere en cloudleverandør som databehandler; hvilke krav den dataansvarlige bør stille til leverandøren som databehandler; hvordan den dataansvarlige kan sikre, at behandlingen sker i tråd med den givne instruks, mv.

Herudover indeholder vejledningen afsnit, der omhandler overførsler til tredjelande generelt og til USA, herunder betydningen af EU-Domstolens dom i sag C-311/18, Schrems II, samt behandlinger inden for EU/EØS af selskaber, der kan blive mødt med anmodninger fra myndigheders tredjelande.

Læs nyheden her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/mar/ny-vejledning-og-ekspertgruppe-om-brug-af-cloud

Læs hele vejledningen på dansk her: https://www.datatilsynet.dk/Media/637824109172292652/Vejledning%20om%20cloud.pdf

Læs hele vejledningen på engelsk her: https://www.datatilsynet.dk/Media/637824108733754794/Guidance%20on%20the%20use%20of%20cloud.pdf

Kommissionen fremsætter forslag til Dataforordning om nye regler for, hvem der kan bruge og tilgå data genereret i alle økonomiske sektorer i EU

Den 23. februar 2022 fremsatte Kommissionen et forslag til Dataforordningen, der indeholder ny regulering af, hvem der kan få adgang til og benytte sig af de data, som de økonomiske sektorer i EU frembringer. Forslaget skal ses som led i Kommissionens datastrategi, der har til formål at fremskynde den digitale omstilling og til at nå de digitale målsætninger for 2030. Ambitionen er at hjælpe EU med at indtage en førende rolle inden for det datadrevne samfund.

De nye regler medfører blandt andet en beskyttelse af SMV'er (små og mellemstore virksomheder) mod urimelige kontraktsvilkår i datadelingskontrakter med parter, der indtager en stærkere forhandlingsposition end SMV'en. Desuden får offentlige organer mulighed for at benytte data, der besiddes af den private sektor, hvis det er nødvendigt f.eks. i tilfælde af offentlige nødsituationer. Endvidere kan de offentlige organer gennemføre et retligt mandat, såfremt dataet ikke på anden vis er tilgængeligt. Slutteligt kan det tilføjes, at de foreslåede regler vil muliggøre et effektivt skifte for kunder af forskellige clouddatabehandlingstjenester. Der fastsættes i denne forbindelse foranstaltninger, der skal forhindre ulovlig dataoverførsel.

Der lægges også op til at gennemgå dele af direktiv 96/9/EF af 11. marts 1996 om retlig beskyttelse af databaser («databasedirektivet»), ligesom forbrugere og virksomheder får muligheden for at få adgang til at benytte sig af data til eftersalgsservice og tillægstjenester som f.eks. prædiktiv vedligeholdelse. Erhvervslivets og industriens aktører vil ligeledes få adgang til flere data, hvorved de vil kunne se frem til et mere konkurrencedygtigt datamarked.

Læs pressemeddelelsen her: Dataforordningen: Foranstaltninger, der skal sikre en retfærdig og innovativ dataøkonomi (europa.eu)

Læs forslaget til Dataforordningen her: https://digital-strategy.ec.europa.eu/en/library/data-act-proposal-regulation-harmonised-rules-fair-access-and-use-data

Læs faktablad om Dataforordningen her: https://digital-strategy.ec.europa.eu/en/library/data-act-factsheet

Ny vejledning om brug af adfærdskodekser som overførselsgrundlag

Den 22. februar 2022 vedtog Det Europæiske Databeskyttelsesråd («EDPB») en vejledning om brugen af adfærdskodekser som overførselsgrundlag. Inden vedtagelsen havde vejledningen været i offentlig høring indtil den 1. oktober 2021. Høringssvarene var overvejende positive, og der blevet lavet enkelte ændringer i vejledningen på baggrund heraf.

Vejledningens formål er at specificere brugen af Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 («GDPR») artikel 40, stk. 3. Artikel 40, stk. 3 vedrører adfærdskodekser som egnede sikkerhedsforanstaltninger for overførsel af personoplysninger til tredjeland efter GDPR artikel 46, stk. 2, litra e. Formålet er også at give praktisk vejledning om indholdet af sådanne adfærdskodekser, deres vedtagelse og de involverede aktører. Ligeledes gives der anvisninger om kravene til adfærdskodekser og garantierne givet af adfærdskodekser som overførselsgrundlag.

Konkret angiver vejledningen de elementer, der skal adresseres i de «bindende tilsagn», som dataansvarlige eller databehandlere skal afgive efter GDPR artikel 40, stk. 3. Derudover indeholder vejledningen en tjekliste over de elementer, der skal være opfyldt i et adfærdskodeks, der er bestemt til overførsel. Tjeklisten indeholder de eksisterende overførselsværktøjer efter GDPR artikel 46, og tager hensyn til EU-Domstolens dom i sag C-311/18, ***Schrems II***, for at sikre ensartethed i beskyttelsesniveauet.

Vejledningen giver klarhed over de forskellige aktørers roller i at fastætte adfærdskodekser til brug for overførsler og for deres vedtagelse.

Læs Datatilsynets pressemeddelelse her: https://www.datatilsynet.dk/internationalt/internationalt-nyt/2022/feb/edpb-vedtager-vejledning-om-brug-af-adfaerdskodekser-som-overfoerselsgrundlag

Læs EDPB's pressemeddelelse her: https://edpb.europa.eu/news/news/2022/edpb-adopts-reply-libe-2nd-additional-protocol-cybercrime-convention-guidelines_en

Læs vejledningen her: https://edpb.europa.eu/system/files/2022-03/edpb_guidelines_codes_conduct_transfers_after_public_consultation_en_1.pdf

Datatilsynet i Norge fravælger Facebook efter en databeskyttelsesretlig risikovurdering

Den 22. september 2021 offentliggjorde det norske Datatilsyn, at det har besluttet at fravælge brugen af Facebook, og derfor ikke opretter og kommunikerer gennem en virksomhedsside på Facebook.

Baggrunden for beslutningen er en databeskyttelsesretlig risikovurdering og konsekvensanalyse, som Datatilsynet har foretaget af risiciene og konsekvenserne for de registreredes rettigheder ved at have en virksomhedsside på Facebook. Tilsynets rolle i udarbejdelsen af vurderingerne var udelukkende som dataansvarlig og organisation, og ikke til tilsynsmyndighed.

Ved beslutningen lagde tilsynet vægt på, at behandlingen af personoplysninger på en eventuel virksomhedsside på Facebook ville medføre en høj risiko for de registreredes rettigheder og friheder. Tilsynet uddy-

bede dette ved bl.a. at fremhæve, at den registreredes reelle medbestemmelse over en række behandlinger er begrænset, og at Facebooks behandlinger kan være uforudsigelige for de registrerede.

Tilsynet lagde endvidere vægt på, at de ikke ville kunne opfylde betingelserne i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 («GDPR») artikel 26 om fælles dataansvar, da aftalen mellem Facebook og Datatilsynet er mangelfuld. Det blev bl.a. fremhævet, at tilsynet ikke kan indgå sine egne aftaler med Facebook, ligesom at tilsynet ikke kan svare på, hvilke oplysninger der gemmes om brugere, der «synes godt om» et opslag på virksomhedssiden eller blot besøger siden. Tilsynet var tillige af den opfattelse, at Facebook ikke giver tilstrækkelige garantier for, at de har indarbejdet databeskyttelse gennem design og standardindstillinger i henhold til GDPR artikel 25.

Læs nyheden her: https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2021/datatilsynet-velger-a-ikke-bruke-facebook/

Læs risikovurderingen her: https://www.datatilsynet.no/contentassets/8561465062b04a6b904c-8c3573a24687/risikovurdering_skal-datatilsynet-ha-side-pa-facebook_.pdf

Belgisk afgørelse om it-service der håndterer samtykker til annoncering (TCF-rammeværket)

Den 2. februar 2022 traf det belgiske Datatilsyn en afgørelse i en klagesag om en it-service kaldet TCF-rammeværket (Transparency and Consent Framework).

TFC-rammeværket håndterer indsamling og formidling af samtykker til annoncering på hjemmesider og i apps, bl.a. registrering af cookiesamtykker og præferencer. Rammeværket er meget udbredt og bruges bl.a. til såkaldt Real-Time Bidding, hvor teknologivirksomheder, som repræsenterer en masse annoncører, øjeblikkeligt («in real time») kan byde på annoncepladser ud fra, hvilke personer der besøger hjemmesiden/app'en i netop dét øjeblik.

TCF-rammeværket er baseret på betingelser og et teknisk set up, som er udviklet af IAB Europe (en brancheorganisation for medier og annoncører), og formålet med rammeværket er at sikre, at de organisationer, som bruger «the OpenRTB protocol» (en af de mest udbredte protokoller til Real-Time Bidding), overholder GDPR.

Det belgiske Datatilsyn vurderede imidlertid, at TCF-rammeværket ikke levede op til en række regler i GDPR, bl.a. bestemmelser om de grundlæggende principper for behandling af personoplysninger, hjemmelsgrundlag, oplysningspligt og behandlingssikkerhed. Hielke Hijmans fra Datatilsynet beskrev problemet således, at selvom brugerne bliver bedt om at give samtykke, er det de færreste af dem, der ved, at deres profil bliver solgt flere gange dagligt med henblik på at vise dem personaliseret reklame.

Det belgiske datatilsyn pålagde derfor IAB Europe som dataansvarlig en bøde på 250.000 euro og gav en frist på to måneder til at præsentere en handlingsplan for, hvordan aktiviteterne skal bringes i overensstemmelse med GDPR.

Det afgørende for, at IAB Europe blev anset for dataansvarlig (sammen med de medier og annoncører, der bruger TCF-rammeværket) var, at IAB Europe som udvikler og udbyder kunne pålægge de deltagende organisationer at følge en række retningslinjer og betingelser vedrørende TCF-rammeværket.

Ifølge det danske Datatilsyn bør de hjemmesideudbydere, annoncører og formidlere af reklamer og annoncepladser, der benytter TCF-rammeværket skifte til en løsning, der overholder GDPR.

Læs nyheden fra det danske datatilsyn her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/feb/belgisk-afgoerelse-kan-have-betydning-for-danske-hjemmesider

Læs pressemeddelelsen fra det belgiske datatilsyn her: https://www.dataprotectionauthority.be/citizen/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr

Læs hele afgørelsen fra det belgiske datatilsyn her: https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf

Afgørelse om ulovlig brug af Google Analytics fra det østrigske datatilsyn giver anledning til udarbejdelse af vejledning hos det danske Datatilsyn

Det danske Datatilsyn udsendte den 19. januar 2022 en nyhed om, at Datatilsynet planlægger at udgive en vejledning om brugen af Google Analytics og lignende værktøjer.

Nyheden blev udgivet i anledning af en afgørelse fra det østrigske datatilsyn Datenschutzbehörde («DSB») af 22. december 2021 i en sag angående en østrigsk hjemmesides ulovlige brug af Google Analytics (sags-nr. 2021-0.586.257 (D155.027)). Sagen hos DSB udsprang af 101 klager, som organisationen None of Your Business («NOYB») har sendt ud til europæiske datatilsynsmyndigheder i kølvandet på EU-Domstolens dom i sag C-311/18, Schrems II.

DSB fandt i sagen, at en overførsel af personoplysninger til Google LLC i USA i forbindelse med brugen af Google Analytics-værktøjet i lyset af EU-Domstolens praksis i Schrems II-sagen, ikke var i overensstemmelse med Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 («GDPR») artikel 44 om overførsler af personoplysninger til tredjelande.

DSB fandt, at virksomheden grundet ineffektive supplerende foranstaltninger i tillæg til de anvendte standardkontraktsbestemmelser ikke havde formået at sikre et beskyttelsesniveau for de overførte personoplysninger, der i det væsentligste svarede til beskyttelsesniveauet i EU. DSB lagde vægt på, at virksomheden ikke havde implementeret suppleren-

de foranstaltninger, der adresserede mulighederne for overvågning af og adgang til de overførte personoplysninger fra USA's retshåndhævende myndigheder.

Det danske Datatilsyn udtrykte i deres nyhed forståelse for den usikkerhed, mange private virksomheder og offentlige myndigheder oplever i forhold til deres brug af Google Analytics og lignende værktøjer. Datatilsynet oplyste derfor, at de på baggrund af afgørelsen fra DSB og de fremtidige afgørelser, der forventes at komme som følge af NOYB's klager, forventer at udarbejde en opsummerende vejledende tekst om brug af Google Analytics og lignende værktøjer inden for rammerne af databeskyttelsesreglerne, herunder reglerne om overførsel af personoplysninger til tredjelande.

Læs nyheden her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/jan/afgoerelse-om-brug-af-google-analytics-fra-det-oestrigske-datatilsyn

Læs afgørelsen fra det østrigske datatilsyn her: https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_EN_bk.pdf

Datatilsynet udtaler kritik af automatisk udfyldning af oplysninger ved køb på hjemmeside

Det danske Datatilsyn traf den 13. december 2021 afgørelse i en sag med journalnummer 202o-31-3611 vedrørende Rito ApS' («Rito») behandling af personoplysninger i forbindelse med automatisk udfyldning af personoplysninger om kunder ved køb på Ritos webshop.

Datatilsynet udtalte kritik af behandlingen af personoplysninger. Kritikken baserede sig på, at Rito anvendte en funktion på deres hjemmeside, hvorved der automatisk blev udfyldt en række felter med personoplysninger, hvis der blev indtastet en e-mailadresse, som allerede var kendt i systemet, og hvortil disse personoplysninger tidligere havde været anvendt. Funktionen forudsatte ikke, at kunden i forvejen var logget ind, og andre uvedkommende personer ville derfor potentielt kunne tilgå personoplysninger om disse ved at indtaste tidligere kunders e-mailadresser.

Datatilsynet fandt, at Rito ved brugen af denne funktionalitet ikke levede op til kravene om et passende sikkerhedsniveau i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 («GDPR») artikel 32.

Datatilsynet meddelte Rito et påbud om at ophøre med at anvende automatisk udfyldning af personoplysninger om kunder ved køb på virksomhedens hjemmeside. I samme forbindelse vurderede Datatilsynet dog, at autoudfyldning godt kan ske inden for reglerne, hvis den registrerede på forhånd har verificeret sig tilstrækkeligt på anden måde.

Læs pressemeddelelsen her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/mar/-datatilsynet-udtaler-kritik-af-automatisk-udfyldning-af-oplysninger-ved-koeb-paa-hjemmeside

Læs afgørelsen her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/dec/datatilsynet-udtaler-kritik-af-automatisk-udfyldning-af-oplysninger-ved-koeb-paa-hjemmeside

Datatilsynet udtaler alvorlig kritik af Den Blå Avis' samtykkeløsning

Det danske Datatilsyn traf den 26. januar 2022 afgørelse i egendriftssagen 2020-431-0085. Datatilsynet havde indledt sagen af egen drift for at se, om tilsynets nye vejledninger om behandling af personoplysninger om hjemmesidebesøgende fra 2020 blev overholdt.

Datatilsynet udtalte alvorlig kritik af, at Den Blå Avis' («DBA») tidligere og nuværende samtykkeløsning til behandling af personoplysninger ikke var i overensstemmelse med reglerne i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 («GDPR») artikel 4, nr. 11 om krav til samtykke. Derudover fandt datatilsynet, at den nuværende samtykkeløsning var i strid med artikel 5, stk. 1 om grundlæggende principper om lovlighed, rimelighed og gennemsigtighed.

Endeligt vurderede datatilsynet, at DBA's behandling af personoplysninger ikke forfulgte et lovligt formål efter GDPR artikel 6, stk. 1, litra f.

Ifølge GDPR skal et samtykke være givet på baggrund af en frivillig, specifik, informeret og utvetydig viljeserklæring. Datatilsynet vurderede, at DBA's tidligere samtykkeløsning ikke overholdt kravet om frivillighed, idet det ikke var muligt at til- og fravælge specifikke formål med behandlingen af personoplysningerne. Samtykkeløsningen levede heller ikke op til kravet om at være specifikt, idet behandlingen blev brugt til flere upræcist angivne formål.

Datatilsynet vurderede, at hjemmesidebesøgende heller ikke blev informeret tilstrækkeligt om, hvad de samtykkede til, og lagde særlig vægt på, at det ikke fremgik tydeligt, hvilke tredjepartsselskaber personoplysningerne blev videredelt med. Endvidere afgav de hjemmesidebesøgende ikke en utvetydig viljeserklæring. DBA's tidligere samtykkeløsning anså et klik på et link eller et billede som accept af behandling af personoplysninger. Datatilsynet vurderede, at der derved ikke var tale om en utvetydig viljeserklæring.

Vedrørende vurderingen af DBA's nuværende samtykkeløsning, så fandt datatilsynet, at DBA's behandling ikke fulgte et legitimt formål og ikke kunne ske på baggrund af interesseafvejningsreglen i GDPR artikel 6, stk. 1, litra f. Datatilsynet lagde særligt vægt på, at det forretningsmæssige sigte og formål med behandlingsaktiviteterne ikke var veldefineret og afgrænset tilstrækkeligt. Derudover lagde datatilsynet vægt på, at det ikke fremgik af den nuværende samtykkeløsning, at oplysningerne blev videregivet til tredjepartsselskaber med henblik på disses markedsføring.

Datatilsynet udtalte på baggrund af det ovenstående alvorlig kritik af DBA.

Læs pressemeddelelsen her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/feb/datatilsynet-udtaler-alvorlig-kritik-af-den-blaa-avis%e2%80%99-samtykkeloesning

Læs hele afgørelsen her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/jan/datatilsynet-udtaler-alvorlig-kritik-af-den-blaa-avis%E2%80%99-samtykkeloesning

Alvorlig kritik, påbud og advarsel til Region Hovedstaden efter to sikkerhedsbrud

Det danske datatilsyn traf den 18. februar 2022 afgørelse i en sag med journalnummer 2020-442-8862 vedrørende to klager indgivet af Sundhedsdatastyrelsen over Region Hovedstadens behandling af personoplysninger.

Regionen havde som dataansvarlig for Sundhedsplatformen («SP») forårsaget to sikkerhedsbrud, da kodeændringer i SP medførte utilsigtede ændringer i det Fælles Medicin Kort («FMK»), hvor Sundhedsdatastyrelsen er dataansvarlig. De to sikkerhedsbrud opstod, idet integrationsmekanismen mellem FMK og SP muliggør, at ændringer i SP's funktionalitet eller datagrundlag kan påvirke integriteten af visningen af oplysninger i FMK.

Det første sikkerhedsbrud opstod i forbindelse med en kodeændring i SP, som medførte en utilsigtet dobbeltordination i FMK, således at der skete tab af integritet af personoplysninger i 4.223 medicinordinationer vedrørende 2.310 registrerede. Det andet sikkerhedsbrud opstod på baggrund af en kodefejl ved opgradering i SP, der resulterede i en uoverensstemmelse i produktbeskrivelserne for 164 lægemidler, hvilket blev vist i FMK. Der skete således et tab af integritet af personoplysninger i 1.311 lægemiddelordinationer fordelt på 1.149 patienter.

Datatilsynet udtalte alvorlig kritik af Regionens behandling af personoplysninger, da den ikke var sket i overensstemmelse med Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 («GDPR») artikel 32, stk. 1 om behandlingssikkerhed. Tilsynet meddelte endvidere et påbud i henhold til GDPR artikel 58, stk. 2, litra d, om at udarbejde og indføre en proces, der sikrer, at ingen ændringer i SP's funktionalitet eller datagrundlag gennemføres, før det er sikret, at der ikke er urigtige informationer i integrerede systemer. Derudover udstedte tilsynet en advarsel i henhold til GDPR artikel 58, stk. 2, litra a om, at idriftsættelse af systemændringer i SP uden test af dataintegritet, sandsynligvis vil være i strid med GDPR artikel 5, stk. 1, litra a og d og artikel 32, stk. 1.

Datatilsynet lagde vægt på, at Region Hovedstaden ikke havde truffet passende organisatoriske og tekniske foranstaltninger for at sikre et sikkerhedsniveau, der passede til de risici, der opstår i forbindelse med behandlingsaktiviteter via integrerede it-systemer med flere selvstændige dataansvarlige, jf. GDPR artikel 32, stk. 1.

Datatilsynet noterede sig, at Region Hovedstaden havde foretaget en sundhedsfaglig underretning af de berørte registrerede i overensstemmelse med GDPR artikel 34, stk. 1.

Læs pressemeddelelsen her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/feb/alvorlig-kritik-paabud-og-advarsel-til-region-hovedstaden-efter-to-sikkerhedsbrud-

Læs afgørelsen her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/feb/alvorlig-kritik-paabud-og-advarsel-til-region-hovedstaden-efter-to-sikkerhedsbrud-

Datatilsynet udtaler alvorlig kritik af, at underdatabehandler afviste af udlevere oplysninger til den dataansvarlige

Det danske Datatilsyn traf den 7. februar 2022 afgørelse i sagen 2022-431-0167 vedrørende en dataansvarliges klage over en underdatabehandler, der ikke ville tilbagelevere den dataansvarliges kundeoplysninger.

Datatilsynet udtalte alvorlig kritik af, at underdatabehandlerens behandling af personoplysninger var sket i strid med reglerne i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 («GDPR») artikel 6, stk. 1, artikel 9, stk. 2 og artikel 28, stk. 10.

Derudover meddelte Datatilsynet underdatabehandleren påbud om at udlevere den dataansvarliges kundeoplysninger, jf. GDPR artikel 58, stk. 2, litra d, samt et forbud mod behandling af den dataansvarliges kundeoplysninger, jf. GDPR artikel 58, stk. 2, litra f.

Der var indgået en databehandleraftale mellem databehandler A og underdatabehandler B. Det fremgik af aftalen, at det var databehandler A, der var den dataansvarlige over for underdatabehandleren, og dermed ikke den oprindelige dataansvarlige. Det var underdatabehandler B's opfattelse, at de ikke var underlagt nogen instruktionsbeføjelse til den oprindelige dataansvarlig. Underdatabehandleren B afviste således at have handlet i strid med GDPR-reglerne, idet denne mente, at det kun var databehandler A, der kunne instruere underdatabehandler B i at udlevere kundeoplysningerne.

Datatilsynet lagde særligt vægt på de faktiske forhold i sagen og lagde til grund, at den oprindelige dataansvarlige ligeledes var dataansvarlig over for underdatabehandler B i medfør af GDPR artikel 4, nr. 7, som definerer den dataansvarlige som den, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger.

Datatilsynet udtalte, at det faktum, at databehandler A og databehandler B har indgået en databehandleraftale, ikke resulterer i, at databehandler A bliver dataansvarlig,

idet oplysningerne behandles på vegne af den oprindelige dataansvarlige.

Læs pressemeddelelsen her: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/mar/alvorlig-kritik-underdatabehandler-afviste-at-udlevere-oplysninger-til-den-dataansvarlige

Læs hele afgørelsen her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/feb/alvorlig-kritik-underdatabehandler-afviste-at-udlevere-oplysninger-til-den-dataansvarlige

Tue Goldschmieding er partner i Gorrissen Federspiel og en av de danske redaktørene for Lov&Data.



Wiersholm

Guro Mangen, Fride Støve Hedin og Carl Emil Bull-Berg

Datatilsynet oppsummerer personvernåret 2021

I mars publiserte Datatilsynet sin årsrapport for 2021. Rapporten oppsummerer fjorårets tall og tendenser for tilsynets virksomhet og gir et frempek på hvilke personvernutfordringer tilsynet vil fokusere på i tiden fremover.

Hovedmål og prioriteringer

Tilsynets prioriterte hovedområder for 2021 var kontroll og saksbehandling, internasjonalt samarbeid og drift av regulatorisk «sandkasse». Faglig lå fokuset på personvern relatert til skole, barn og unge, samt koronarelaterte problemstillinger. Datatilsynet påpeker at det de siste årene har blitt iverksatt tiltak som ikke ville vært akseptable i en normal situasjon, herunder kontrolltiltak i arbeidslivet. Datatilsynet mener det er viktig at vi kommer tilbake til en «før korona-tilstand». I praksis innebærer det at tiltak som ikke er risikovurdert enten må risikovurderes, eller avsluttes. Ifølge tilsynet må også kontrolltiltak i arbeidslivet reduseres.

Håndtering av klagebehandling og avviksmeldinger

I løpet av 2021 registrerte Datatilsynet 3 474 nye saker, en økning på seks prosent fra 2020. Av disse utgjorde i underkant av 600 klagesaker fra enkeltindivider. Klagesakene gjaldt blant annet følgende temaer:

- Rundt 25 prosent gjaldt virksomheters behandling av personopplysninger om sine kunder
- Rundt 12-13 prosent gjaldt behandling av helseopplysninger
- Rundt 12-13 prosent gjaldt behandling av personopplysninger i arbeidslivet

For øvrig mottok Datatilsynet et betydelig antall klager om behandling av personopplysninger ved bruk av digitale tjenester (som for eksempel nettjenester, sosiale medier og apper), innhenting av kredittvurderinger, bruk av kameraovervåkning og barns personvern.

Det har videre vært en moderat økning i antall mottatte avviksmeldinger, hvor flere store saker var knyttet til cyberangrep. Datatilsynet realitetsbehandler ca. 20 prosent av avviksmeldingene de får inn. Vedtakene viser at Datatilsynet har fokusert på håndheving av særlig alvorlige avvik, som for eksempel overtredelsesgebyret mot Østre Toten kommune. Til tross for at Datatilsynet behandler få saker om brudd på personopplysningssikkerheten, legger de til grunn at de vedtakene som treffes har stor signaleffekt og viser til at mange kommuner skjerpet sine sikkerhetsrutiner i kjølvannet av Østre Toten-saken.

Overtredelsesgebyrer

I 2021 utstedte Datatilsynet 26 overtredelsesgebyrer, en dobling fra året før. Overtredelsesgebyrenes størrelse har økt betydelig, med to-

talt ca. 80 millioner kroner i overtredelsesgebyrer fordelt på 26 saker i 2021, mot ca. 6 millioner kroner fordelt på 13 saker i 2020. Ett av gebyrene var på 65 millioner kroner, og representerer det høyeste gebyret som hittil er gitt i Norge for brudd på personvernet. Vedtaket er enda ikke rettskraftig.

Enkelte av klagesakene som ble behandlet i Personvernnemnda førte til reduksjon overtredelsesgebyrene. Nemnda uttrykte i disse sakene blant annet at lang saksbehandlingstid fører til lavere overtredelsesgebyr.

Tilsynsaktivitet

Datatilsynet har en risikobasert tilnærming til sin tilsynsrolle. Virksomhetene de velger å kontrollere faller normalt innenfor en av følgende kategorier: (i) virksomheter hvor tilsynet antar at der er en særskilt risiko, og (ii) representative virksomheter hvor tilsynet ønsker å avdekke status innenfor en sektor eller et tematisk område. I tillegg gjennomfører Datatilsynet hendelsesbaserte tilsyn og har også som mål å gjennomføre såkalte profilerte tilsyn.

Tilsynsaktiviteten gikk ned både i 2020 og 2021, særlig som følge av koronapandemien og restriksjonene denne medførte. I løpet av disse årene har Datatilsynet utformet en ny tilsynsmetodikk tilpasset nytt lovverk og tilsynsobjektene, samt opprettet en tilsynskoordinator. Dette kan tilsi at Datatilsynet vil øke sin tilsynsaktivitet i årene som kommer. Samtidig fremgår det av rapporten at selv om Datatilsynet ønsker å gjennomføre flere stedlige tilsyn og andre kontrolltiltak av eget tiltak fremover, kan dette bli utfordrende som følge av økningen i antallet klagesaker som må prioriteres.

Internasjonalt samarbeid

Det internasjonale arbeidet har i 2021 vært prioritert fra Datatilsynets side. Gjennom deltakelse i Personvernrådet og dets undergrupper får Datatilsynet mulighet til å påvirke rettsutviklingen. Datatilsynet er for eksempel hovedrapportør for Personvernrådets retningslinjer om verktøy for avdekking av barneovergrepsmateriale.

Framtidsutsikter og fokusområder

Datatilsynet antar at deres avgjørelser i større grad vil bli utfordret rettslig fremover, både i Personvernnemda og i domstolene. Som følge av den stadige utviklingen på teknologiområdet, anser Datatilsynet det også sannsynlig at sakene vil øke i kompleksitet.

Datatilsynet uttrykker misnøye over manglende håndhevelse av regelverket overfor internasjonale teknologigiganter, noe de også anser som en fremtidsutfordring. Videre peker de på at en harmonisert tolkning og praktisering av personvernforordningen er en kontinuerlig utfordring.

I tillegg trekker tilsynet frem behovet for arbeid med personvern innenfor kommunesektoren. Mange kommuner mangler tilstrekkelig kompetanse, og det foreligger derfor et behov for blant annet veiledning og samordning av kunnskap.

Datatilsynet uttrykker også bekymring over det store antallet henvendelser om personvern i arbeidslivet. De mener dagens regelverk er godt, men at det svikter i etterlevelsen. Det er verdt å merke seg at Datatilsynet ofte reagerer med overtredelsesgebyr eller andre korrigerende tiltak i saker hvor en arbeidsgiver bryter personvernregelverket, som for eksempel i saker om kameraovervåkning på arbeidsplassen. Datatilsynet skriver i rapporten at de ser alvorlig på disse sakene, blant annet som følge av det ujevne styrkeforholdet mellom arbeidsgiver og arbeidstaker.

Avslutningsvis fremholder tilsynet manglende digitalsikkerhet som en fremtidsbekymring. I 2021 ble det gjennomført en rekke større dataangrep mot offentlige og private norske virksomheter. Datatilsynet påpeker at mange virksomheter ikke tar sikkerhet tilstrekkelig på alvor før en uønsket hendelse inntreffer, og at mange angrep kan forhindres gjennom relativt enkle tekniske tiltak.

Guro Mangen, Fride Støve Hedin og Carl Emil Bull-Berg er associates i Advokatfirmaet Wiersholm.


simonsen vogtwiig

Hedda Baumann Heier og Emile Schjønsby-Nolet

Varemerkesak om utmåling av vederlag og erstatning sluppet inn til behandling i Høyesterett

Anke av lagmannsrettens avgjørelse i sak LB-2021-20075 mellom Kysgjerdet AS på den ene siden og Norgesgjerde AS og Vindex AS på den andre siden, er delvis sluppet inn til behandling for Høyesterett. Lagmannsretten kom i sin behandling av saken til at Kystgjerdet sin bruk av kjennetegnene «Vindex» og «Norgesgjerde» i betalte annonser på internett utgjorde varemerkeinngrep. Høyesteretts skal ta stilling til rettanvendelsen og bevisbedømmelsen ved utmåling av vederlag og erstatning ved varemerkeinngrep. Dato for behandling er ikke satt.

Les Høyesteretts ankeutvalgs beslutning med saksnummer HR-2022-765-U i lovdatas database.

Lagmannsretten avgjør forføyningssak om bruk av Harry Potter-musikk

Borgarting lagmannsrett avsa den 4. mars 2022 kjennelse i sak med saksnr. LB-2022-26097 mellom Warner Bros. Entertainment Inc. («Warner») og Star Entertainment GmbH («Star»). Faktum var i korte trekk at Star hadde planlagt å fremføre konserter med bl.a. musikk fra Harry Potter-filmene. Warner er eier av rettighetene til musikken og motsatte seg konsertene. Ettersom partene ikke kom til enighet begjærte Warner midlertidig forføyning for å stanse gjennomføringen av konsertene.

For å få medhold i en midlertidig forføyning kreves det at den som går til sak sannsynliggjør at den har både et hovedkrav og en sikringsgrunn, jf. tvisteloven § 34-2 første ledd. Lagmannsretten måtte dessuten ta stilling til om en midlertidig forføyning ville påføre Star en ulempe som stod i åpenbart misforhold til Warners interesse i at forføyning blir besluttet, jf. tvisteloven § 34-1 andre ledd.

Partene var i saken enige om at Tono, en kollektiv forvaltningsorganisasjon for visse musikkrettigheter, hadde anledning til å gi tillatelse til bruk av den omtvistede komposisjonen. Tonos adgang til å gi slik tillatelse var imidlertid begrenset til verket i sin opprinnelige form, og omfattet ikke rett til å bearbeide verket. Tvistepunktet i saken var derfor om Star sin fremføring utgjorde en bearbeidelse av musikkverket.

Lagmannsrettens delte seg når det gjaldt den konkrete vurderingen. Flertallet begynte med å påpeke at det avgjørende for om det foreligger en bearbeidelse er om bearbeidelsen selv har verkshøyde. Under henvisning til HR-2017-2165-A avsnitt 72, ble det slått fast at bearbeidelser må avgrenses nedad mot gjengivelser og endringer som er resultat av teknisk og håndverksmessig arbeid.

Ved sin vurdering av Stars bruk av musikken lente flertallet seg særlig på en sakkyndig vurdering, som bla. trakk frem at verkene *var* endret ved at bestemte partier var utelatt eller slått sammen. Selve arrangementene var også endret, i tillegg til at nye instrumenter var introdusert. Flertallet trekker også frem at den sakkyndige var av den oppfatning at endringene var av et slikt omfang at han som komponist ville forvente å bli bedt om samtykke.

På bakgrunn av ovenstående fant flertallet det «ikke tvilsomt» at endringene var å regne som en bearbeidelse. Warner hadde dermed sannsynliggjort hovedkravet. Flertallet fant videre også at det forelå sikringsgrunn fordi Star hadde til hensikt å gjennomføre konsertene før hovedkravet kan komme til pådømmelse. Flertallet fant også at en midlertidig forføyning ikke sto i åpenbart misforhold til Warners interesse i at forføyning ble besluttet.

Mindretallet kom under en viss tvil til at det ikke var sannsynliggjort at Stars forestillinger måtte anses som en bearbeidelse av de musikkverk Warner har rettighetene til. Mindretallet la vekt på at Star hadde varslet visse endringer i de kommende fremføringene. Mindretallet kom også til at det ikke forelå noen varemerkekrenkelse eller opptreden i strid med god forretningsskikk.

Les lagmannsrettens avgjørelse med saksnummer LB-2022-26097 i Lovdatas database.

Lagmannsretten avgjør forføyningssak om bruksrett til IT-løsning

Borgarting lagmannsrett avsa 14. februar 2022 kjennelse i en sak mellom Lividi AS og Staten v/Forsvarsdepartementet. Lividi har vært leverandør av programmeringstjenester til Forsvaret og har i denne forbindelse utviklet det såkalte Hermod-systemet som er en taktisk kommunikasjonsløsning for mobile nettverk. Utviklingen av Hermod-systemet startet i 2013 og har i sin helhet blitt finansiert av Forsvaret.

Tvisten mellom partene oppsto da Forvaret i 2020 inngikk en intensjonsavtale med Kongsberg Grup-

pen, der formålet var å utrede mulighetene for visse former for samarbeid. Lagmannsretten legger til grunn at det er uenighet mellom partene om hva denne intensjonsavtalen egentlig innebar. Lividi gjorde uansett da gjeldende at det ville være i strid med selskapets eiendoms- og opphavsrettigheter til elementer i programvaren, dersom Forsvaret ga Kongsberg Gruppen eller andre tredjeparter tilgang til kildekoden i Hermod-systemet. Lividi tok deretter ut en begjæring om midlertidig forføyning for å sikre at slik tilgang ikke ble gitt.

Det forelå i utgangspunktet flere ulike avtaler mellom partene. For lagmannsretten hadde Lividi frafalt anførslene sine knyttet til de tidlige avtalene og saken var derfor begrenset til tolkningen av en avtale mellom partene inngått i 2020. Etter denne avtalen skulle Lividi beholde eierskapet til opphavs- og eiendomsretten til programvaren som ble utviklet under avtalen, mens Forsvaret fikk en bruksrett. Bruksretten var formulert slik:

«*Kunden får en tidsubegrenset, vederlagsfri og ikke-eksklusiv rett til å utnytte de enkelte deler av programvaren som utvikles eller tilpasses spesielt for Kunden (utvidet disposisjonsrett). Utvidet disposisjonsrett omfatter rett til å bruke, kopiere, modifisere og videreutvikle tilpasningene, enten selv eller ved hjelp av tredjepart. Kunden har slik utvidet disposisjonsrett innenfor totalforsvaret.*» […]

Det sentrale spørsmålet i saken var hvordan denne bestemmelsen skulle fortolkes. Lagmannsretten delte seg her i et flertall og et mindretall.

Flertallet fant at det var sannsynliggjort at Forvaret og Kongsberg Gruppen hadde inngått et samarbeid som innebar konkrete planer om at Kongsberg Gruppen, og ikke Lividi, skulle få adgang til å kommersialisere Hermod-systemet. Etter flertallets syn kunne den utvidede disposisjonsretten ikke tolkes slik at den gav Forsvaret anledning til å gi Kongsberg Gruppen tilgang til programvare eller kildekode utviklet av Lividi under 2020-avtalen, i en situasjon der det foreligger konkrete planer om samarbeid med Kongsberg Gruppen vedrørende industrialisering og kommersialisering. Flertallet la ved sin tolkning av avtalen særlig vekt på at det var en synlig forutsetning fra Lividis side ved avtaleinngåelsen at Lividi skulle settes i posisjon til å industrialisere og kommersialisere programvaren.

Flertallet mente videre også at overlevering av programvare/kildekode til Kongsberg Gruppen ville innebære en nærliggende risiko for at Lividi påføres vesentlig skade eller ulempe. Kravet om sikringsgrunn var dermed også oppfylt. Resultatet i kjennelsen ble derfor at Lividi ble gitt medhold.

Mindretallet var til dels uenig med flertallet i avtaletolkningen, men fant uansett at det ikke var sannsynliggjort at Forsvaret hadde konkrete planer om teknologioverføring til Kongsberg Gruppen med påfølgende industrialisering og generell kommersialisering av Hermod-programvaren, slik flertallet la til grunn.

Les avgjørelsen med saksnummer LB-2021-83141 i Lovdatas database.

Bidragene er skrevet av senioradvokat Hedda Baumann Heier og advokatfullmektig Emile Schønsby-Nolet ved Simonsen Vogt Wiigs avdeling for Teknologi og Medier i Oslo.

Gorrissen Federspiel

Tue Goldschmieding

DesignNævnet og Responsumudvalget er officielt åbnet

Den 24. februar 2022 åbnede Foreningen for Retsbeskyttelse af Arkitektur, Design og Kunsthåndværk de to nye private sagsbehandlingsinstanser Responsumudvalget og DesignNævnet.

Responsumudvalget er et uafhængigt responsumudvalg, der kan afgive responsa om den retlige beskyttelse af arkitektur, design og kunsthåndværk. Responsumudvalget afgiver ikke retlig bindende responsa.

Nævnet for Retsbeskyttelse af Arkitektur, Design og Kunsthåndværk («DesignNævnet») er et uafhængigt klagenævn, der kan træffe afgørelse i konkrete tvister om retsbeskyttelse og krænkelse af arkitektur, design og kunsthåndværk efter høring af tvistens parter.

DesignNævnet vil ved deres behandling indhente bemærkninger fra begge parter. Sagens parter kan inden sagens afgørelse aftale mediati-

on, hvor DesignNævnets sekretariat udpeger en mediator, med henblik på at opnå en forligsmæssig løsning af sagen. Såfremt modparten ikke har ønsket at deltage i sagens behandling afsiges DesignNævnets afgørelse alene baseret på klagerens oplysninger.

Afgørelser fra DesignNævnet er ikke retligt bindende, og er derfor mere tilsigtet at afværge en retssag, tjene som grundlag for forlig eller anvendes som materiale til fremlæggelse i en senere retssag. DesignNævnet kan dog fungere som voldgift, hvor parterne ønsker dette og indgår en voldgiftsaftale herom, mod et vederlag fastsat af DesignNævnets forperson, og dermed afsige afgørelser, der er retlig bindende efter reglerne i lov nr. 533 af 24. juni 2005 («den danske voldgiftslov»).

Læs nyheden her: https://www.danskindustri.dk/di-business/arkiv/nyheder/2022/3/nu-kan-du-fa-behandlet-sager-om-ophavsret-i-designnavnet/

Læs om DesignNævnet på dets hjemmeside her: https://www.designnævnet.dk/

Forberedelsesfasen (PAP) for den fælles patentdomstol (UPC) er begyndt

Den 18. januar 2022 indgav Østrig som den trettende medlemsstat sin ratifikation af protokollen om midlertidig ikrafttrædelse af den fælles patentdomstol. Det medførte, at patentdomstolens midlertidige ikrafttrædelsesfase, også kaldet «PAP» (provisional application phase) trådte i kraft den 19. januar 2022. Dermed er de sidste praktiske forberedelser til patentdomstolen begyndt. På patentdomstolens hjemmeside beskrives ikrafttrædelsen af PAP som *«the birth of the Unified Patent Court as an international organisation»*.

Den forberedende komité forventer, at PAP vil vare i cirka 8 måneder, og det, der skal ske i løbet af perioden, er, at patentdomstolen skal gøres klar til sit virke. Der skal bl.a. rekrutteres dommere, færdiggøres IT-systemer og laves budgetter. De første konstituerende møder i den administrative komité og budgetkomitéen blev afholdt den 23. februar og 2. marts 2022.

Når medlemsstaterne er sikre på, at patentdomstolen er funktionel, vil Tyskland ratificere selve UPC-aftalen. UPC-aftalen vil træde i kraft den første dag i den fjerde måned derefter, og når det sker, vil patentdomstolen begynde sit arbejde og være tilgængelig for brugerne af det europæiske patentsystem. Som det ser ud nu, er der udsigt til, at patentdomstolen vil begynde sit virke i slutningen af 2022 eller begyndelsen af 2023. Samtidig vil det europæiske enhedspatent blive indført.

Læs nyheden her: https://www.unified-patent-court.org/news/austria-closes-loop-protocol-provisional-application-upc-agreement-has-entered-force

Læs flere nyheder fra patentdomstolen her: https://www.unified-patent-court.org/news

Ny AI-løsning til at søge efter billeder af varemærker og designs i EUIPOs database

Den 29. november 2021 tilgængeliggjorde EUIPO et nyt billedsøgningsværktøj via eSearch. Baggrunden herfor er, at der gennem årene har været en stor udfordring i forbindelse med at søge efter billeder af varemærker og design. EUIPO har i lyset heraf udgivet sit nye AI-baseret billedsøgningsværktøj.

EUIPO planlægger at implementere billedsøgningsværktøjet i sine to værktøjer TMview og DesignView. Formålet hermed er at give brugerne mulighed for at søge efter billeder i verdens største varemærke- og designdatabaser. EUIPO vil ligeledes tilbyde tjenesten til andre IP-kontorer i European Union Intellectual Property Network (EUIPN). Disse kontorer vil være i stand til at bruge billedsøgningsfunktionen med deres egne systemer. Dette vil bl.a. føre til øget effektivitet og en reduktion af omkostningerne for deltagende IP-kontorer.

Læs nyheden her: https://euipo.europa.eu/ohimportal/en/news?p_p_id=csnews_WAR_csnewsportlet&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&journalId=9130327&journalRelatedId=manual/

Foretag billedsøgning her: https://euipo.europa.eu/eSearch/

Nye guidelines for behandling af varemærkeansøgninger i Kina

China's National Intellectual Property Administration («CNIPA») offentliggjorde nye retningsliner for behandling af varemærkeansøgninger den 22. november 2021, som trådte i kraft 1. januar 2022.

De nye retningsliner beskriver den kinesiske varemærkelovs artikel 4, der bl.a. foreskriver, at varemærkeansøgninger i ond tro, der ikke er beregnet til brug, skal afvises. Retningslinerne opstiller ti situationer, der som udgangspunkt kan kategoriseres som ond tro, medmindre parterne kan føre bevis for det modsatte. Det drejer sig blandt andet om, at der indleveres et enormt stort antal varemærkeansøgninger, der åbenlyst overstiger, hvad der er nødvendigt i forhold til normale forretningsaktiviteter og mangler reel brugshensigt, eller at der indleveres et stort antal ansøgninger om varemærkeregistrering af kopier eller efterligninger af andre rettighedshaveres velrenommerede varemærker.

Det følger endvidere af retningslinerne, at når der er tale om et varemærke med både beskrivende og særprægede elementer, kan der kun opnås registrering, hvis ansøgeren accepterer en ansvarfraskrivelse for de beskrivende elementer. Listen over ord, der mangler særpræg, er endvidere blevet udvidet og omfatter nu bl.a. dagligdagsord og -udtryk, internet buzzwords, populære emojis og almindeligt anvendte tegn og symboler.

Endelig fremgår det af retningslinjerne, at «untrusted entities» iht. det kinesiske social credit system

ikke kan få deres varemærker registreret i Kina.

Læs nyheden her: https://www.natlawreview.com/article/china-s-new-guidelines-trademark-examination-and-trial-elaborate-malicious-trademark

Uregistreret EF-designbeskyttelse for enkelte dele af et produkt

Den 28. oktober 2021 afsagde EU-Domstolen dom i sag C-123/20 mellem Ferrari SpA og Mansory Design & Holding GmbH. Sagen var anlagt af den tyske Forbundsdomstol som et præjudicielt spørgsmål angående en fortolkning af reglerne i forordning (EF) nr. 6/2002 af 12. december 2001 om EF-design («designforordningen») om beskyttelse af et ikke-registreret EF-design. Ferrari påstod, at Mansory Design havde krænket et eller flere af deres ikke-registrerede EF-design.

Ferrari havde i november 2014 offentliggjort to billeder af deres nye model, Ferrari FXX K, på deres hjemmeside. Siden 2016 havde Mansory Design fremstillet og markedsført udstyrsdele, hvis formål var at nærme udseendet af en Ferrari 488 GTB til en Ferrari FXX K. I marts 2016 præsenterede Mansory Design en modificeret udgave af Ferrari 488 GTB, hvis udseende var tilpasset, så det afspejlede en Ferrari FXX K endnu mere. Dette indebar også det samme «V» på motorhjelmen og samme synlige karosseri. Ferrari anså dette for en krænkelse af deres ikke-registrerede EF-designrettigheder, som de mente at være indehaver af siden offentliggørelsen på deres hjemmeside i november 2014.

Det præjudicielle spørgsmål for EU-Domstolen var, om der som følge af et helhedsbillede af et produkt efter designforordningens artikel 11, stk. 1 og 2 kunne opnås ikke-registrerede EF-designrettigheder til de enkelte dele eller komponenter af produktet. Yderligere blev der spurgt, i bekræftende fald, i hvilket omfang en del af et produkts udseende efter designforordningens artikel 3, litra a, eller en komponent af et sammensat produkt i designforordningens artikel 3, litra c og artikel 4, stk. 2, skulle være selvstændigt i forhold til produktet i dets helhed, før udseendet havde individuel karakter som følge af designforordningen artikel 6, stk. 1.

EU-Domstolen fortolkede designforordningens artikel 11, stk. 2 således, at offentliggørelsen af billeder af et produkt, som det i dommen behandlede, godt kunne indebære en offentliggørelse af designet af en del af dette produkt efter artikel 3, litra a, eller en komponent af et produkt som et sammensat produkt efter artikel 3, litra c og artikel 4, stk. 2. Dette forudsætter, at udseendet af den enkelte del eller komponent kan identificeres klart ved offentliggørelsen. Domstolen fortolkede artikel 6, stk. 1 således, at for at det kan vurderes, om udseendet opfylder kravet om individuel karakter, er det nødvendigt, at den pågældende del eller komponent udgør et synligt udsnit af produktet eller det sammensatte produktet. Dette kan være som skarpt afgrænset af særlige linjer, konturer, farver eller en særlig form eller tekstur.

EU-Domstolen konkluderede, at såfremt de ovenstående betingelser er opfyldt, så kan offentliggørelsen af billeder af et produkt udgøre en offentliggørelse af designet af en del af produktet.

Læs hele dommen her: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:62020CJ0123&from=DA

Krænkelse af ophavsret til Den Lille Havfrue ikke omfattet af undtagelse om parodier og karikaturer

Østre Landsret afsagde den 9. februar 2022 dom i sagen BS-47536/2020 mellem arvingerne til skaberen af Den Lille Havfrue, og chefredaktøren for Berlingske Tidende.

Sagen omhandlede, hvorvidt der forelå en ophavsretlig krænkelse af værket «Den Lille Havfrue» eller om der var tale om (a) et selvstændigt værk, (b) en lovlig karikatur eller (c) lovlige ytringer beskyttet af EMRK art. 10 om ytringsfrihed.

(a)

Landsretten udtalte, at lov nr. 1144 af 23. oktober 2014 om ophavsret («den danske ophavsretslov») § 4, stk. 2, som er bestemmelsen der i tidligere praksis har dannet grundlag for at opnå særkilt ophavsretlig beskyttelse, skal fortolkes således, at der udelukkende kan opnås selvstændig ophavsretlig beskyttelse til et værk, hvis sammenligningen til det oprindelige værk er begrænset til stilelementer, ideer eller lignende. Går henvisningen derimod udover blot at indeholde ideer og stilelementer, er der tale om en bearbejdning efter ophavsretslovens § 4, stk. 1, som kræver tilladelse.

Efter en samlet vurdering fandt retten, at der, uanset forskellen på havfruens hoved, var tale om ligheder mellem de to værker i en sådan grad, at der var tale om en bearbejdning. Der forelå ikke nogen tilladelse fra ophavsmanden til denne bearbejdning.

(b)

Berlingske gjorde gældende, at der i lovmotiverne til den danske ophavsretslov fra 1961 gælder en undtagelse til den danske ophavsretslovs § 3, stk. 2 vedrørende parodier og traverstier.

Landsretten udtalte, at denne undtagelse anses for at have et meget snævert anvendelsesområde. Tegningen af Den Lille Havfrue var derfor ikke en lovlig parodi. Retten lagde særligt vægt på, at tegningen ikke benyttedes som en karikatur af Den Lille Havfrue, men at statuen derimod blev brugt som et værktøj til at karikere «Ondskaben i Danmark».

(c)

Landsretten udtalte, at tegningerne utvivlsomt behandlede emner af væsentlig samfundsmæssig interesse,

men at formålet ikke nyder direkte beskyttelse af ophavsretslovens undtagelsesbestemmelser i § 23- 24a. Derudover fandt retten, at brugen af det ophavsretligt beskyttede værk «Den Lille Havfrue» ikke på nogen måde var nødvendigt, da man også kunne have illustreret artiklens emne og formål ved brugen af andre illustrationer, hvorfor det ikke er i strid med EMRK at fastslå en ophavsretlig krænkelse af værket «Den Lille Havfrue».

Sammenfattende udtalte landsretten, at der forelå en krænkelse af den danske ophavsretslovs § 2 om ophavsmandens eneret til et givent værk og § 3, stk. 2 om respektretten. Derudover fandt landsretten, at der forelå en overtrædelse af lov nr. 426 af 3. marts 2017 («den danske markedsføringslov») § 3 om god markedsføringsskik. Østre Landsret stadfæstede herefter byrettens afgørelse og forhøjede vederlag og godtgørelse til 300.000 kr.

Læs resumé af dommen her: https://domstol.dk/oestrelandsret/aktuelt/2022/2/kraenkelse-af-ophavsret-til-den-lille-havfrue/

Læs hele dommen her: https://domstol.dk/media/o3fbar3p/dom-bs-47536-2020_.pdf

Dom fra Østre Landsret bekræfter, at «forbudsretlig passivitet» kan hindre midlertidige forbud og påbud

Østre Landsret afsagde den 22. december 2021 kendelse i sagen BS-16491/2021-OLR mellem Illumina Cambridge Limited («Illumina») og BGI Europe A/S («BGI»).

Kæresagen vedrørte udelukkende spørgsmålet om, hvorvidt betingelserne i lov nr. 1835 af 15. september 2021 («den danske retsplejelov») § 413, nr. 3 var opfyldt. Ifølge den danske retsplejelov § 413, nr. 3 kan forbud eller påbud meddeles, hvis den anmodende part godtgør eller sandsynliggør, at partens mulighed for at opnå sin ret vil forspildes, hvis parten henvises til at afvente tvistens retlige afgørelse.

Illumina anlagde i maj 2019 en hovedsag mod BGI med anmodning om forbud og påbud baseret på Illuminas patentrettigheder for sekventeringskits. Året efter blev sagen udsat, da retten afventede afgørelse fra det Europæiske Patentkontor vedrørende en verserende indsigelsessag om stridspatentet, DK/EP 3 002 289 T3. Herefter indgav Illumina begæring om midlertidigt forbud og påbud mod BGI's salg og markedsføring af sekventeringskits. Sø- og Handelsretten afslog denne begæring.

Retten lagde særligt vægt på, at anmodningen om det midlertidige forbud og hovedsagen i overvejende grad vedrørte samme sagsgenstand, idet der var tale om de samme patentretlige krænkelser. Derudover fandt retten, at der var forløbet væsentligt længere tid mellem hovedsagens anlæg og forbudsbegæringen, end det med rimelighed var nødvendigt for iværksættelse af retlige skridt. Retten mente således, at betingelserne for at nedlægge forbud efter den danske retsplejelov § 413, nr. 3 ikke var opfyldt, idet Illumina ikke havde sandsynliggjort, at deres ret ville forspildes ved at afvente hovedsagens afgørelse.

Under kæresagen gjorde Illuminas gældende, at årsagen til, at der gik 15 måneder, indtil man anmodede om forbudsbegæring, skyldtes, at man ikke tidligere havde haft fornødne beviser til at sandsynliggøre en krænkelse af patentrettighederne.

I hovedsagens stævning havde Illuminas gjort gældende, at de havde konstateret, at der forelå en krænkelse af patentrettighederne. På den baggrund mente Østre Landsret, at Illumina på dette tidspunkt allerede måtte have været i besiddelse af de fornødne beviser til at sandsynliggøre krænkelsen af stridspatentet.

Derudover anførte landsretten, at det var uden betydning, at Illumina nogle måneder før anmodningen om forbudsbegæring havde varslet dette over for BGI, idet det alene var tidspunktet for indgivelsen af begæringen om forbud der suspenderede passivitetsperioden. Landsretten stadfæstede herefter Sø- og Handelsrettens kendelse.

Læs resumé af kendelsen her: https://domstol.dk/oestrelandsret/aktuelt/2022/1/kendelse-om-saakaldt-forbudsretlig-passivitet/

Læs hele kendelsen her: https://domstol.dk/media/qntd52fa/bs-16391-2021.pdf

Fremstilling af måleapparater i strid med lov om forretningshemmeligheder

Østre Landsret afsagde den 21. januar 2022 dom i sagen BS-34317/2020-OLR mellem Valmet Automation Inc. og Emco Controls A/S.

Sagen omhandlede, hvorvidt Emco havde krænket Valmets ophavsrettigheder ved fremstilling og salg af måleapparater til ledningsevnemåling. Derudover omhandlede sagen, hvorvidt Valmets måleapparater med softwareindeholdende opskrifter var omfattet af legaldefinitionen på «forretningshemmeligheder» efter § 2, nr. 1 i lov nr. 309 af 25. april 2018 («den danske lov om forretningshemmeligheder»), og i så fald hvorvidt Emco havde gjort uretmæssigt brug af disse oplysninger.

Sagen blev afgjort i første instans den 21. august 2020 ved Sø- og Handelsretten, hvor der blev nedlagt forbud for Emco mod at producere og sælge måleapparaterne.

Landsretten afviste ligesom Sø- og Handelsretten påstanden om, at Emco havde krænket Valmets ophavsrettigheder, idet det ikke fandtes godtgjort, at softwaren i Valmets produkter var ophavsretligt beskyttet. Med udgangspunkt i EU-Domstolens afgørelser i sagerne C-393/09 og C-406/10 udtalte landsretten, at det udelukkende er et EDB- programs udtryksform, der er ophavsretligt beskyttet, hvorimod

ideer og principper ikke nyder samme beskyttelse.

Landretten lagde ved den samlede ophavsretlige vurdering særlig vægt på, at det på baggrund af skønsmandens oplysninger ikke var bevist, at apparaternes software udgjorde en egen intellektuel frembringelse.

Landsretten tiltrådte Sø- og Handelsrettens afgørelse om, at Valmets algoritmer og software er omfattet af lov om forretningshemmeligheders § 2, nr. 1. Landsretten udvidede bedømmelsen således, at softwaren af typen 1511-1705 ligeledes er omfattet af lov om forretningshemmeligheder, idet skønsmanden havde konkluderet, at det *«overvejende ikke er sandsynligt, at Emco 1711 er udviklet uafhængigt af Valmet TCU'en»*.

Landsretten stadfæstede således Sø- og Handelsrettens afgørelse om, at Emco ulovligt havde erhvervet en erhvervshemmelighed uden forretningshemmelighedshaverens samtykke, samt at der var handlet i strid med god markedsføringsskik. Landsretten stadfæstede ligeledes forbuddet mod fremstillingen og markedsføringen af måleapparaterne af de ovenfor nævnte typer.

Emco skulle betale 4.000.000 kr. i erstatning til Valmet jf. lov om forretningshemmeligheder § 15 og markedsføringslovens § 24, stk. 2 og 3.

Læs resumé af dommen her: https://domstol.dk/oestrelandsret/aktuelt/2022/1/uretmaessig-brug-af-anden-virksomheds-forretningshemmeligheder/

Læs hele dommen her: https://domstol.dk/media/kwxlg1rw/dom-34317.pdf

Dom fra SH om misbrug af forretningshemmeligheder 4. januar 2022

Sø- og Handelsretten afsagde den 4. januar 2022 dom i sagen BS-40573/2021-SHR mellem OK a.m.b.a og OK Varmeservice A/S (benævnes samlet «OK») som sagsøgere og Søberg Energiservice A/S («Søberg») som sagsøgte. OK a.m.b.a. er et energiselskab, og OK Varmeservice A/S, der er ejet af OK a.m.b.a., udfører service og reparation af gas og oliefur/kedler, varmepumper/jordvarme mv. Søberg udfører dels arbejde som serviceparter for energiselskaber og fungerer dels som energiselskab.

Sagen omhandlede, hvorvidt Søberg havde misbrugt OK's forretningshemmeligheder efter ophøret af en samarbejdsaftale og overtrådt lov nr. 426 af 3. marts 2017 («den danske markedsføringslov»), samt om der på baggrund heraf var grundlag for at nedlægge et midlertidigt forbud.

Retten oplyste, at det måtte lægges til grund, at Søberg som følge af parternes tidligere samarbejde var i besiddelse af afgørende oplysninger om tekniske anlæg og deres serviceringsaftaler. Retten fandt det godtgjort, at oplysningerne udgjorde forretningshemmeligheder, samt at Søberg uberettiget havde anvendt forretningshemmelighederne over for en række kunder. Søberg havde derfor overtrådt lov nr. 309 af 25. april 2018 («den danske lov om forretningshemmeligheder») § 4, stk. 2, nr. 3, hvorefter brug af en forretningshemmelighed er ulovligt, hvis forretningshemmeligheden bruges af en person, der har misligholdt en fortrolighedsaftale eller enhver anden lignende pligt.

Retten fandt det dog ikke sandsynliggjort, at Søberg generelt og systematisk eller i væsentligt omfang havde handlet i strid med den danske lov om forretningshemmeligheder. Betingelserne for at nedlægge forbud som begæret efter lov nr. 1835 af 15. september 2021 («den danske retsplejelov») § 413, nr. 2 og 3, og § 414, stk. 1., var derfor ikke opfyldt.

Læs resumé af dommen her: https://domstol.fe1.tangora.com/Domsoversigt.16692/BS-40573-2021-SHR.2336.aspx

Læs hele dommen her: https://domstol.fe1.tangora.com/media/-300011/files/BS-40573-2021-SHR_Kendelse.pdf

Der var ikke stiftet brugsbaserede varemærkeret til varemærket «Gyro», som desuden ikke var registeret i ond tro

Sø- og Handelsretten afsagde den 17. februar 2022 dom i sagen BS-40415/2020-SHR samt BS-26608/2021-SHR mellem Unilamp Norden AS, All-Light A/S og SG Armaturen AS. Sagen udsprang af spørgsmålet om, hvem der havde retten til varemærket «Gyro», og hvorvidt Unilamp Norden AS og All-Light A/S kunne forbydes at bruge varemærket i Danmark.

Tvisten i førstnævnte sag angik, hvorvidt SG Armaturen AS var forpligtet til at overdrage varemærkeregistreringen af varemærket «Gyro» til Unilamp AS vederlagsfrit, subsidiært at varemærkeregistreringen skulle ophæves i sin helhed. Modsat anførte SG Armaturen AS, at de øvrige parter forbydes at anvende varemærket erhvervsmæssigt i Danmark.

Retten fandt, at der ikke var stiftet brugsbaserede varemærkerettigheder for nogen af parterne forud for den ene parts registrering af varemærket, idet bl.a. anvendelsen af «Gyro» i det fremlagte markedsføringsmateriale ikke havde godtgjort, at den relevante kundekreds havde haft tilstrækkelig mulighed for at gøre sig bekendt med anvendelsen heraf som varemærke eller som forretningskendetegn for SG Armaturen eller de resterende parter i øvrigt.

Endelig fandt Retten, at SG Armaturens registrering af varemærket ikke var foretaget i ond tro efter det selvstændige EU-retlige ond tro-begreb på trods af deres kendskab til Unilamps «Gyro» varemærker i Norge og Sverige. Dette skyldtes, at Retten ikke fandt det godgjort, at SG Armaturens hensigt bag registreringen alene var at skade Unilamps interesser. Endelig nedlagde Retten forbud mod Unilamp og All-Rights brug af varemærket «Gyro» i Danmark.

Læs resumé af dommen her: https://domstol.fe1.tangora.com/Domsover-

sigt.16692/BS-40415-2020-SHR-og-BS-26608-2021-SHR.2346.aspx

Læs hele dommen her: https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-40415-2020-SHR_og_BS-26608-2021-SHR.pdf

En smykkevirksomheds rettigheder til varemærkerne «Mads Heindorf Jewellery» og «Heindorf» hindrede Sanne Heindorf i at benytte «Heindorf Diamonds» som mærke og som del af sit virksomhedsnavn

Den 4. marts 2022 afsagde Sø- og Handelsretten dom i sag BS-13486/2021-SHR mellem Mads Heindorf Jewellery («sagsøger») og Heindorf Diamonds («sagsøgte»).

Sagen angik, om sagsøgte ved at benytte sig af virksomhedsnavnet «Heindorf Diamonds» havde krænket de rettigheder, som sagsøger havde til varemærkerne «Mads Heindorf Jewellery» og «Heindorf». Det var sagsøgtes opfattelse, at selskaberne arbejdede inden for to forskellige segmenter af samme branche (hhv. sagsøgers håndlavede og unikke smykker og sagsøgtes masseproducerede og formstøbte smykker). Slutteligt påpegede sagsøgte, at hun burde have ret til at bruge sit eget navn.

Retten konkluderede, at der eksisterede en forvekslingsrisiko mellem selskaberne. I sin vurdering fremhævede retten bl.a., at selskaberne bevægede sig inden for samme branche, ligesom at begge selskaber var karakteriseret ved mærkeelementet «Heindorf». Retten fandt derved heller ikke, at lov nr. 88 af 29. januar 2019 om varemærkeloven («den danske varemærkelov») § 10, stk. 1 om retten til brug af eget navn fandt anvendelse, idet en sådan anvendelse ville stride mod god markedsføringsskik efter VML § 10, stk. 2.

Retten tog således sagsøgers påstand til følge og meddelte sagsøgte et forbud mod anvendelse af virksomhedsnavnet «Heindorf Diamonds». Sagsøgte skulle betale 25.000 kr. i erstatning.

Læs resumé af dommen her: https://domstol.fe1.tangora.com/Domsoversigt.16692/BS-13486-2021-SHR.2353.aspx

Læs dommen her: https://domstol.fe1.tangora.com/media/-300011/files/BS-13486-2021-SHR_-_Dom.pdf?rev1

Facebook ændrer annoncesystem, eftersom salg af målrettet markedsføring af lån til spilinteresserede er i strid med god skik

Den danske Forbrugerombudsmand oplyste i en pressemeddelelse af 14. december 2021, at Facebook over for Forbrugerombudsmanden har tilkendegivet at ville ændre sit annoncesystem, så annoncører ikke længere kan målrette deres låneannoncer til spilinteresserede forbrugere.

Det sociale medies annoncesystem havde førhen været tilrettelagt på en sådan måde, at kreditgivere, kreditformidlere m.v., der lånte penge til forbrugere, mod betaling kunne målrette deres annoncer til forbrugere, som førhen havde vist interesse for «online gambling» og lignende. Forbrugerombudsmanden vurderede, at Facebooks annoncesystems mulighed for såkaldt «targeted advertising» mod spilinteresserede var i strid med god markedsføringsskik.

Facebook valgte på Forbrugerombudsmandens opfordring derfor at fjerne denne mulighed for at målrette markedsføringen af lån til forbrugere, som havde vist interesse for spil. Afslutningsvist knyttede Forbrugerombudsmand Christina Toftegaard Nielsen en kommentar til denne form for markedsføring, som ifølge hende «er i strid med almene samfundshensyn».

Læs hele pressemeddelelsen her: https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2021/facebook-overtraadte-god-skik-ved-at-saelge-maalrettet-markedsfoering-af-laan-til-spilinteresserede/

Flere leadvirksomheder udtrak ikke det lovede antal vindere i konkurrencer på nettet

Den 16. december 2021 offentliggjorde den danske Forbrugerombudsmand en pressemeddelelse om, at Forbrugerombudsmanden har undersøgt seks leadvirksomheders brug af konkurrencer på internettet i 2019. Formålet med konkurrencerne, der udlovede mange forskellige præmier, var at indhente de deltagende forbrugeres samtykke til at blive kontaktet med markedsføring fra en lang række forskellige virksomheder. Undersøgelsen viste, at fire af leadvirksomhederne havde trukket færre vindere end lovet, og at to af virksomhederne endda slet ikke kunne dokumentere at have udtrukket nogen vindere af konkurrencerne.

Forbrugerombudsmanden fandt, at det er i strid med vildledningsforbuddet i lov nr. 426 af 3. marts 2017 («den danske markedsføringslov»), ikke at udtrække ligeså mange vindere af en konkurrence, som man har lovet. Det er også vildledende at markedsføre én konkurrence i forskellige udgaver, der hver især fremstår som selvstændige konkurrencer, hvis der kun udtrækkes én samlet vinder. Forbrugernes samtykke til at modtage markedsføring er ugyldige i sådanne tilfælde af vildledning, og det vil være strafbart at kontakte forbrugerne på baggrund af disse samtykker.

Læs hele pressemeddelelsen her: https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2021/flere-leadvirksomheder-vildledte-om-praemier-i-netkonkurrencer/

Nyt studie af kunstig intelligens rolle i håndhævelsen af IP-rettigheder i dag

Den 2. marts 2022 udgav The European Observatory on Infringements of Intellectual Property et nyt studie om kunstig intelligens' indvirkning på krænkelse og håndhævelse af ophavsret og design. Formålet

med studiet var at analysere AI-teknologiers indvirkning på den nutidige håndhævelse af IP-rettigheder.

Studiet ser nærmere på 20 scenarier, som er designet til at demonstrere det eksisterende eller potentielle misbrug af kunstig intelligens, når det omhandler krænkelser af ophavsret, beslægtede rettigheder og designs, samt brugen af AI til håndhævelsen af selvsamme rettigheder.

Studiet fandt, at brugen af AI i forbindelse med krænkelser og håndhævelsen af IP-rettigheder medfører såvel muligheder som begrænsninger. AI-teknologi bidrager med en række muligheder for at forbedre effektiviteten i opdagelsen af IP-retlige krænkelser, da man ved brugen af kunstig intelligens eksempelvis kan forudse krænkelser. Ligeledes har andre teknologier, som forbedres ved hjælp af AI, såsom blockchain, 3D-print, generativt design, cloud-tjenester mv, et stort potentiale.

Omvendt viste studiet også, at den kunstige intelligens' forskellige muligheder også kan benyttes til ulovlige formål, idet nogle forbrydelser ved brug af AI vil kunne blive udført i meget større skala, hvilket inkluderer området for krænkelse og håndhævelse af IP-rettigheder.

Endeligt blev det anført i studiet, at det er værd at have i tankerne, at der altid vil være et menneske bag enhver AI-algoritme, og at AI med fordel vil kunne blive brugt af retshåndhævende myndigheder som en del af en række mere innovative værktøjer i forbindelse med analyser og forudsigelser. En sådan brug skal ifølge studiet dog være underlagt stærke sikkerhedsforanstaltninger og menneskeligt tilsyn.

Læs nyheden her: https://euipo.europa.eu/ohimportal/da/news/-/action/view/9230001

Læs hele rapporten om studiet her: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2022_Impact_AI_on_the_Infringement_and_Enforcement_CR_Designs/2022_Impact_AI_on_the_Infringement_and_Enforcement_CR_Designs_FullR_en.pdf

Tue Goldschmieding er partner i Gorrissen Federspiel og en av de danske redaktørene for Lov&Data.


Bird & Bird

Gunnar Hjalt, Joel Tholin,
Nathalie Lindes Sjölander, Leonard Garg

Invändning mot registrering av varumärket «FALLOUMI» från innehavaren av EU-kollektivmärket «HALLOUMI», PMÖÄ 5507-20

Patent- och marknadsöverdomstolen (PMÖD) har i ett avgörande, efter invändning av *Foundation for the Protection of the Traditional Cheese of Cyprus named Halloumi* (innehavare av EU-kollektivmärket «HALLOUMI»), bedömt att det registrerade varumärket «HALLOUMI» för produkttypen ost inte utgör hinder mot att, i samma varumärkesklass (nr 29), registrera varumärket «FALLOUMI» för produkttypen falafel. I målet framhöll PMÖD inledningsvis att omsättningskretsen för bedömningen var konsumenter i allmänhet som kunde anses vara normalt informerade och skäligen upplysta. Vidare ansåg PMÖD, i likhet med PMD, att det inte var visat att «HALLOUMI» hade sådant anseende i den mening som avses i artikel 9.2 c i EU:s varumärkesförordning och att «HALLOUMI» därför inte kunde anses åtnjuta ett utökat skydd (s k förstärkt kännetecknenskraft). Vad gällde förväxlingsbarhet instämde PMÖD vidare med PMD om att det i sig fanns en hög grad av märkeslikhet mellan «HALLOUMI» och «FALLOUMI». Däremot, i fråga om varuslagslikheten, framhöll PMÖD att ost respektive falafel, vilka båda var livsmedel som kunde konsumeras direkt, inte kunde anses vara att betrakta som substitut till köttprodukter och därmed till viss del vara konkurrerande varuslag. Istället var dessa varuslag sådana som enligt PMÖD snarare kunde anses komplettera varandra. Vidare slog PMÖD fast att «HALLOUMI» numera kunde anses ha låg särskiljningsförmåga, däribland då «HALLOUMI» på senare tid även kommit att användas som en generell benämning på en viss typ av ost, exempelvis som ingrediens i recept. Sammantaget så menade PMÖD att «FALLOUMI» inte var förväxlingsbart med «HALLOUMI», och att sådant hinder mot registrering inte förelåg.

Se avgörandet i dess helhet här: https://www.domstol.se/globalassets/filer/domstol/patentochmarknadsoverdomstolen/avgoranden/2021/pmoa-5507-20.pdf

Riksåklagaren överklagar dom om upphovsrättsbrott till HD, AMR 1534-22

Riksåklagaren har överklagat en dom av Patent- och marknadsöverdomstolen (PMÖD), där PMÖD ogillade stora delar av åtalet, till Högsta domstolen (HD). Saken rör upphovsrätt till tv-sändningar och olovligt innehav av avkodningsutrustning. Riksåklagaren menar att det är av vikt för rättstillämpningen att HD klargör hur begreppet *tv-utsändning* i 12 § internationella upphovsrättsförordningen ska tolkas när rättighetshavaren har säte i ett land utanför EU/EES som inte tillträtt Romkonventionen samt hur begreppet innehav ska tolkas i lagen om förbud beträffande viss avkodningsutrustning. I målet hade två personer åtalats för de ska ha stått bakom ett omfattande illegalt IPTV-nätverk där TV-sändingar återutsänts till ett stort antal abonnenter runt om i världen. Riksåklagaren yrkar på att de bägge åtalade ska dömas för brott mot upphovsrättslagen och avkodningslagen samt att påföljden ska bestämmas till fängelse.

Se överklagandet i dess helhet här: https://www.aklagare.se/globalassets/dokument/verksamheten-i-hogsta-domstolen/overklaganden/amr-1534_22.pdf

Konsumentombudsmannens föreläggande till spelbolag stred mot yttrandefrihetsgrundlagen, PMÖÄ 340-21

Patent- och marknadsöverdomstolen (PMÖD) upphävde nyligen i ett avgörande Konsumentombudsmannens (KO) beslut i vilket KO inom ramen för ett pågående tillsynsärende, med stöd av en bestämmelse i marknadsföringslagen, förelagt *Svenska Spel* att inkomma med uppgifter om ett samarbetsavtal ingånget med *TV4* avseende vissa inslag relaterade till lotteri i tv-bolagets morgonprogram. Både *Svenska Spel* och *TV4* hade överklagat KO:s beslut och anförde att uppmaningen stred mot efterforskningsförbudet i yttrandefrihetsgrundlagen (YGL). PMÖD konstaterade att YGL som utgångspunkt skyddar yttranden i vilket ämne som helst, d.v.s. även reklam eller annan marknadsföring. Skyddet gäller därav även för framställningar som är av utpräglad kommersiell natur. PMÖD konstaterade vidare att myndigheter inte utan stöd i YGL får ingripa mot någon som omfattas av grundlagsskyddet, ett uttryck för den s.k. exklusivitetsprincipen. PMÖD framhöll att efterforskningsförbudet innefattar ett förbud för en myndighet att efterforska vilka som är upphovsmän eller lämnat uppgifter till en framställning i ett program, även om syftet inte är att ingripa mot dessa. Det är vidare själva sökandet som är förbjudet, oberoende av om det faktiskt finns någon som har lämnat sådana uppgifter som förbudet är ämnat att skydda. Domstolen konstaterade vidare att efterforskningsförbudet ska ges en bred tillämpning. Sammantaget fann PMÖD att KO:s föreläggande innefattade ett sökande av uppgifter om identiteten på sådana som bidragit till programmets tillkomst och om hur uppgiftslämnandet har gått till. Slutsatsen blev därför att uppmaningen stred mot efterforskningsförbudet i YGL och att KO:s beslut om föreläggande skulle upphävas.

Se avgörandet i dess helhet här: https://www.domstol.se/globalassets/filer/domstol/patentochmarknadsoverdomstolen/avgoranden/2022/pmoa-340-21.pdf

Den s.k. giltighetspresumtionen m.m. i mål om informationsföreläggande, PMÖ 11599-21

Patent- och marknadsöverdomstolen (PMÖD) har i ett beslut, efter yrkande av patenthavaren *ASSA ABLOY* i anslutning till ett intrångsmål avseende patent, funnit att det saknades förutsättningar att meddela ett informationsföreläggande. PMÖD konstaterade att det för ett informationsföreläggande ska kunna meddelas krävs att en patenthavare visar sannolika skäl för att någon gjort patentintrång. Frågan som domstolen hade att bedöma var därmed om det förelåg sannolika skäl för att det påstådda intrånget föll under det aktuella patentets (slutbleck till låsanordning) skyddsomfång och att patentintrång därmed förelåg. Då den påstådda intrångsgöraren hade invänt att patentet i fråga var ogiltigt hade domstolen inledningsvis även att bedöma om det framstod som sannolikt att patentet var ogiltigt. I den senare frågan konstaterade PMÖD att det den s.k. giltighetspresumtionen var tillämplig, innebärandes att ett meddelat patent presumeras vara giltigt om inte annat visas, exempelvis genom nya omständigheter som inte hade beaktats under ansökningsförfarandet. PMÖD fastslog i denna fråga att sådana presumtionsbrytande omständigheter inte hade kunnat visas och att patentet därför i och för sig var giltigt. Avseende frågan om det framstod som sannolikt att den påstådda intrångsgörarens slutbleck föll under patentets skyddsomfång konstaterade domstolen att slutblecket i fråga inte hade sådana tekniska särdrag att det innefattades av det som avsågs i patentkraven och på så sätt inte föll under patentets skyddsomfång.

Se avgörandet i dess helhet här: https://www.domstol.se/globalassets/filer/domstol/patentochmarknadsoverdomstolen/avgoranden/2022/pmo-11599-21.pdf

Gunnar Hjalt, Senior Counsel, Joel Tholin, Associate, Nathalie Lindes Sjölander, Trainee, Leonard Garg, Trainee, Bird & Bird Advokat.


Tim Krarup Nielsen
og Claus F. Sørensen

Ny version af den danske standardaftale for IT-drift (D17)

D17 for begyndere

D17 har siden introduktionen i 2017 været en anerkendt branchestandardkontrakt for IT-drift i små og mellemstore virksomheder i Danmark. D17 er i det væsentligste et balanceret «agreed document» skabt i samarbejde mellem kundesiden (Dansk IT), leverandørsiden (IT-Branchen), neutrale praktiske kompetencer (Danske IT-advokater) og neutrale akademiske kompetencer (professor, dr. jur. Henrik Udsen).

Der er løbende frigivet opdateringer til D17. Den seneste opdatering - version 4 – er netop frigivet.

Kontrakten er tilgængelig på D17.dk.

Baggrund for version 4

En af ambitionerne bag D17 er at sikre en tidssvarende driftskontrakt. Markedet for IT-drift udvikles løbende – og dermed må D17 følge med udviklingen og de ændrede behov hos branchen.

En af de mest markante ændringer af betydning for kontraktparadigmet for IT-drift knytter sig til branchens bevægelse mod øget brug af Public Cloud.

Et andet væsentligt tema er behovet for en balanceret sikring af driften ved uenigheder.

Ligeledes er IT-sikkerhed et stadigt mere aktuelt emne.

Ansvarsbegrænsning ift. GDPR er også reguleret i den opdaterede version.

Version 4 af D17 er i det hele taget den hidtil mest gennemgribende opdatering af kontrakten, og indeholder et bud på håndteringen af blandt andet disse emner.

Første danske standardkontrakt til håndtering af Public Cloud

Ingen danske standardkontrakter har tidligere indeholdt regulering af Public Cloud. Heller ikke D17. Det ændres med version 4.

D17 er nu opdateret til at kunne bruges i en Public Cloud leverance.

Behovet for håndtering af Public Cloud i driftskontrakten har været efterspurgt af branchen. Det bliver mere og mere almindeligt for virksomheder at benytte sig af cloudydelser.

Problemet med Public Cloud er typisk, at der ikke er tale om en leverance, som leverandøren har rådigheden over – og som kun kan indkøbes af leverandøren på standardiserede og ensidige aftalevilkår. Det svarer i mange tilfælde til leverance af standardsoftware.

Den nye version af D17 balancerer dette markedsvilkår op mod leverandørens ansvar som IT-driftsleverandør, der i udgangspunktet forventes at tage et samlet leveranceansvar.

Leverandøren skal som udgangspunkt være kundens kontaktpunkt over for Public Cloud leverandører. Derudover skal leverandøren sikre kunden nem adgang til at gøre sig bekendt med vilkårene for adgangen til Public Cloud ydelserne og loyalt rådgive kunden om konsekvenserne af brugen af Public Cloud ydelserne, sikkerhed og opfyldelsen af servicemål.

Leverandørens leveranceansvar præciseres også. For det første pålægges Leverandøren ansvaret for at have sikret sig, at valgte Public Cloud ydelser er egnet til understøttelse af de aftalte services. For det andet pålægges Leverandøren ansvaret for at sikre integrationen af Public Cloud ydelser i kundens aftalte services. Leverandøren er i den forbindelse ansvarlig for, at Public Cloud ydelserne ikke hindrer, at afprøvninger i transitions- og transformationsfasen forløber efter de aftalte tidsplaner.

Et væsentligt reguleringstema ifm. reguleringen af Public Cloud har i den forbindelse været leverandørens ansvar for fejl eller mangler fra Public Cloud leverandøren. Løsningen er, at leverandørens ansvar skal baseres på et Back-to-back-princip ift. Public Cloud leverandøren, således at leverandøren ikke påtager sig mere ansvar, end Public Cloud leverandøren gør efter sine

standardvilkår. Dette forudsætter dog, at fejlen kan henføres til en Public Cloud ydelse, og at leverandøren har indrapporteret fejlen eller manglen til Public Cloud leverandøren. Ved kritiske fejl er leverandøren endvidere forpligtet til at udøve rimelige og sædvanlige bestræbelser på at søge afhjælpning af fejlens konsekvenser for kunden.

Endeligt regulerer D17 hvilke ændringer og konsekvenser i Public Cloud ydelserne, der skal betales af leverandøren, og hvilke der skal behandles som en betalbar ændring.

Øget fokus på sikring af fortsat drift ifm. uenigheder

En kendt problemstilling er, at kunden og leverandøren bliver uenige om f.eks. kategoriseringen af en fejl, mangel eller om afhjælpning af disse er særskilt betalbare, ligesom der kan opstå uenighed om, hvorvidt en rekvireret ydelse er inkluderet i aftalte services eller ej.

I disse situationer hænder det, at leverandøren nægter at udbedre fejlen eller manglen, eller udfører den rekvirerede ydelse, indtil der er taget hånd om disse spørgsmål og betaling er aftalt. Det kan medføre økonomiske tab og driftsproblemer for kunden – særligt ved drift af kritiske IT-systemer.

Dette er løbende søgt løst gennem forskellige varianter, samlet kendt under betegnelser som «Fix and deliver first, settle later». Løsningerne har dog haft tendens til enten at favorisere den ene eller den anden part ved praktisk brug.

I den nye version af D17, forsøges dette balanceret yderligere.

«Fix first, settle later» medfører, at leverandøren skal iværksætte afhjælpning uanset om leverandøren er uenig i kundens indsigelser.

«Deliver first, settle later» medfører, at leverandøren fortsat skal levere alle services, der vurderes som nødvendige for opretholdelse af kundens drift, uanset uenighed om hvorvidt servicen er særskilt betalbar eller ej. Derudover er leverandøren ikke berettiget til at udøve tilbageholdsret i, standse eller udskyde leveringen af services i tilfælde af, at kunden gør en indsigelse gældende.

Begge forhold er reguleret i D17. Reguleringen er med til at sikre kunden hurtigere afhjælpning ifm. driftsproblemer og sikrer at driften fortsætter uændret uanset uenigheder.

For at sikre balancen, kan leverandøren anmode kunden om at indhente en udtalelse fra en juridisk eller teknisk ekspert, hvis uenigheder om afhjælpningspligt eller betalingskrav ikke afklares inden et nærmere aftalt antal dage. En sådan udtalelse vil derefter være bindende, medmindre spørgsmålet efterfølgende kræves afgjort ved voldgift.

Viser det sig efterfølgende, at der ikke var tale om en mangel, eller at servicen var en særskilt betalbar service, skal kunden fuldt ud kompensere leverandøren for dennes dokumenterede tidsforbrug anvendt til afhjælpningen eller leveringen af services. Hvis det derudover ved sagkyndig vurdering godtgøres, at kunden var eller burde være klar over, at kravene var uberettigede, skal der tages hensyn til dette ved omkostningsfordelingen og leverandøren vil være berettiget til et aftalt tillæg på sine timepriser for det udførte arbejde.

Der er således søgt en yderligere balancering mellem sikringen af driften overfor konsekvensen af kundens standpunktsrisiko.

Yderligere regulering af leverandørens forpligtelser og garantier

Som noget nyt i version 4 er der indsat regulering af leverandørens forpligtelser i forbindelse med sikkerhedshændelser.

Det følger herefter, at leverandøren skal reagere på sikkerhedshændelser, når leverandøren bliver bekendt med disse. Derudover skal leverandøren af egen drift tage initiativ til at sikre en hensigtsmæssig håndtering af sikkerhedshændelserne i overensstemmelse med god IT-skik, herunder foretagelse af en årsagsanalyse, rådgive kunden om eventuelle sikkerhedsbrister samt afhjælpe og implementere workarounds. Leverandørens assistance med håndteringen af sikkerhedshændelser er herefter kun særskilt betalbar, hvis leverandøren kan godtgøre, at sikkerhedshændelsen ikke kan henføres til forhold, som leverandøren har ansvaret for.

Derved skærpes fokus på sikkerhed. Omvendt forpligtes leverandøren ikke ud over sit ansvarsområde. Dermed skabes basis for, at parterne i højere grad håndterer sikkerhedsproblematikken som en egentlig service – og dermed begge parter har opmærksomhed på at levere; hvilke sikkerhedsydelser er ønskelige for kunden, hvad skal de koste og hvad er kravene til disse? Anvendt korrekt, bliver sikkerhed dermed en forebyggende foranstaltning mere end et efterfølgende ansvarsspørgsmål.

I D17's tidligere versioner var der lagt op til, at parterne selv skulle udarbejde en liste over leverandørens afgivne garantier over for kunden. Version 4 indeholder en liste over visse standardgarantier, som leverandøren afgiver. Leverandøren garanterer herefter, at leverandørens services ikke krænker tredjemands immaterielle rettigheder, at kundens brug af leverandørens services i overensstemmelse med driftskontrakten, ikke vil udgøre en krænkelse af tredjemands immaterielle rettigheder, at leverandøren besidder og opretholder de licenser og tilladelser, der er påkrævet for at kunne levere de aftalte services, samt at kundens data kan udleveres og anvendes i et almindeligt tilgængeligt dataformat i tilfælde af et eventuelt ophør af samarbejdet.

Det er en særskilt diskussion, hvor effektive garantier reelt er i den nordiske retstradition.

Leverandøren må dog forventes i højere grad at blive objektivt ansvarlig for kundens tab som følge af garantisvigt, medmindre det skyldes forhold, som leverandøren ikke har ansvaret for. Dette er nu eksplicit angivet i D17. I driftskontrakten præciseres det desuden, at kontraktens ansvarsbegrænsningsbestemmelse også gælder for tab, der opstår som følge af garantisvigt.

Ansvarsbegrænsning og GDPR

Et udtalt kritikpunkt til K04 (et af Digitaliseringsstyrelsen udarbejdet kontaktparadigme for statslige indkøb af IT-driftsydelser) har været kontraktens manglende stillingtagen til Leverandørens ansvar for udgifter til erstatning og godtgørelse til registrerede ved ulovlig behandling af personoplysninger. Kontrakten giver ganske vist to alternativer, men den ene indebærer, at den beløbsmæssige ansvarsbegrænsning helt bortfalder i visse tilfælde, og det kan allerede konstateres, at i de tilfælde, hvor kontrakten anvendes, vælger hovedparten af kunderne denne løsning.

D17 har aktivt taget stilling til dette, og indeholder nu en bestemmelse som medfører, at de i øvrigt indeholdte beløbsbegrænsningen forhøjes til 150% af det beløb, Leverandøren har modtaget i de foregående 12 måneder for tab opstået som følge af ulovlig behandling af personoplysninger, herunder udgifter til erstatning og godtgørelse til registrerede.

Øvrige ændringer

Den nye version indeholder fortsat en regulering af kundens ret til at tilbageholde en rimelig og forholdsmæssig andel af betalinger for leverancer, hvis kunden har en rimelig grund til at bestride fakturabeløbet. I tidligere versioner af D17, var kunden herefter forpligtet til at deponere det omstridte beløb i sit pengeinstitut og kun udbetale beløbet til leverandøren efter nærmere betingelser var opfyldt eller efter fælles aftale. I version 4 er reguleringen af tilbageholdelse effektiviseret og kravet om deponering fjernet da dette redskab under alle omstændigheder ikke bliver anvendt.

I D17s tidligere versioner var der lagt op til at parterne skulle udfylde to særskilte bilag om tredjepartskontrakter; et bilag om hvilke tredjepartskontrakter, leverandøren skulle overtage administrationen af, og et bilag om hvilke kontrakter, der skulle overdrages til leverandøren. I version 4 er reguleringen af tredjepartskontrakter ændret og forsimplet. I stedet for at lægge op til, at der skal udfyldes to bilag, skal der nu kun udfyldes et bilag. Som i den tidligere version, skal der fortsat angives en liste over de tredjepartskontrakter, som leverandørens skal overtage administrationen af, men som noget nyt skal parterne ikke længere anføre, hvilke tredjepartskontrakter, leverandøren skal overtage. Parterne skal derimod angive hvilke kontrakter, kunden skal opretholde som forudsætning for leverandørens levering af aftalte services.

Af øvrige ændringer af betydning kan nævnes, at kundens bestilling af overdragelsesplan fra leverandøren fremover vil karakteriseres som en service, der bestilles og betales af kunden efter medgået tid. Derudover er de tidligere versioners regulering af overdragelse af medarbejdere udgået.

Endelig skal nævnes, at force majeure klausulen nu eksplicit tager stilling til, at der ikke kan kræves bod eller erstatning i tilfælde, hvor klausulen kan påberåbes, men til gengæld præciseres også, at forholdsmæssigt afslag ikke er afskåret som sanktion.

Tim Krarup Nielsen, partner & certificeret IT-advokat, DAHL Advokatpartnerselskab

Claus F Sørensen, partner & certificeret IT-advokat, DAHL Advokatpartnerselskab

Karnov Lovkommentarer, sømløst integrert i Lovdata Pro.

Skrevet av landets fremste jurister og kvalitetssikret av våre 25 fagredaktører.

KOMMENTARENE

Kommentarene er utstyrt med interne og eksterne henvisninger og med tilrettelegging for rask navigering i loven og til andre rettskilder – herunder internasjonale, og spesielt EU/EØS-relevante, kilder.

Du får også tilgang til den danske EU-Karnoven som inneholder kommentarer til TEU, TEUF i tillegg til noter til utvalgte direktiver og forordninger. Du finner også domsanalyser og utvalgte EU-dommer i EU-Karnoven.

MER INFORMASJON

Har du spørsmål eller ønsker å vite mer, vennligst ta kontakt med oss.

www.karnovgroup.no

KARNOV GROUP

BESTILL I DAG

Er du Lovdatakunde kan du bestille direkte gjennom Lovdata Pro.

https://pro.lovdata.no

LOVDATA PRO

KLIMANØYTRAL DISTRIBUSJON
Levert av Posten

NORGE P. P.
posten

Returadresse:
Lovdata
Pb. 6688 St. Olavs plass
NO-0129 Oslo
Norge

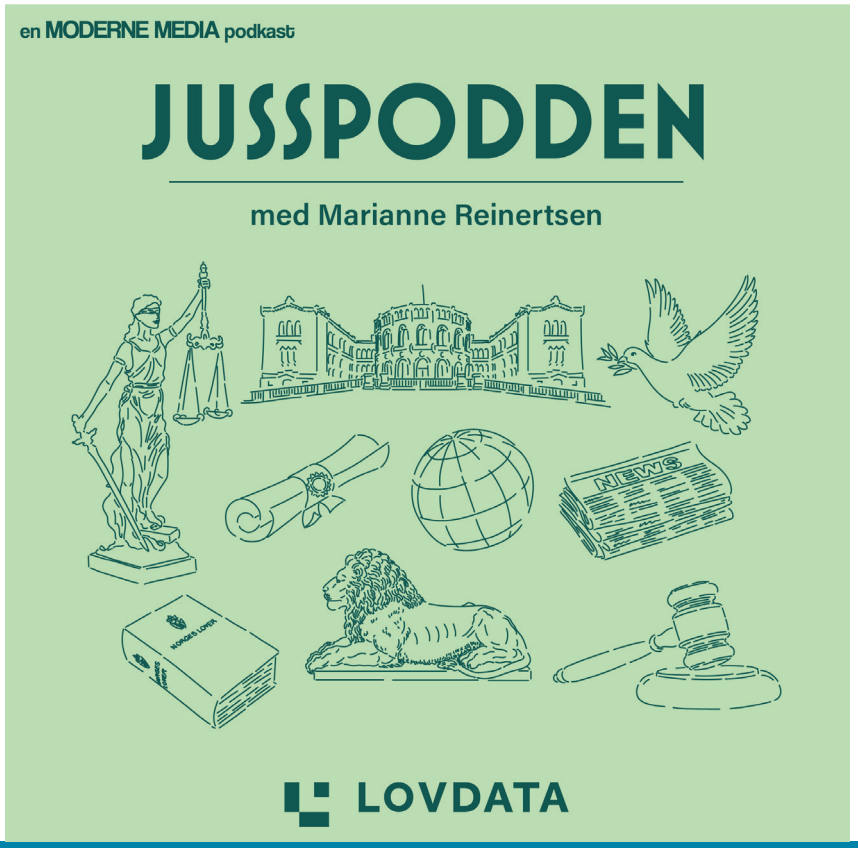
Nytt fra

LOVDATA

Lovdata har inngått samarbeid med Jusspodden om jussformidling!

Jusspodden er en ukentlig podkast om jus og samfunn. Podkasten tar utgangspunkt i dagsaktuelle hendelser og setter en journalistspinn på jussen.

Jusspodden kan høres på via alle podkastplattformer, som Spotify og Apple Podcasts.



Produksjon: 07 Media AS