Lov & Data

Nr. 143
September 2020
Nr. 3/2020

Innhold

Lov&Data

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

Lovdata
Postboks 2016 Vika
NO-0125 Oslo, Norge
Tlf.: +47 23 11 83 00
Faks: +47 23 11 83 01
E-post: lovogdata@lovdata.no
Nettside: www.lovdata.no

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

Abonnementspriser for 2020
Norge: nkr 370,- pr. år
Utland: nkr 450,- pr. år
Studenter, Norge: nkr 175,- pr år
Studenter, utland: nkr 235,- 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/*

Leder

AI och juridik – "same same but different"

Artificiell intelligens (AI) är i ropet. Igen, bör tilläggas. Den som följt rättsinformatiken från starten har varit med om flera tidigare perioder, bl.a. på 1960-talet och 1980-talet.

Under dessa perioder var logisk, programmerad AI i fokus. Diskussionen rörde bl.a. de rättsliga konsekvenserna av att beslutsfattande automatiserades. Hur kunde transparens och rättssäkerhet säkras i en automatiserad förvaltning? Gick det att göra lagstiftningen mer automatiseringsvänlig?

Dagens stora intresse kring AI är framför allt kopplat till olika former av maskininlärning. Algoritmerna som bedömer och fattar beslut är i dessa sammanhang inte – som i tidigare generationers AI – en produkt av direkt mänskligt skapande, utan de utvecklas mer eller mindre automatiskt genom att systemet analyserar stora mängder data. I rättsliga sammanhang kan det t.ex. handla om avtal eller domar.

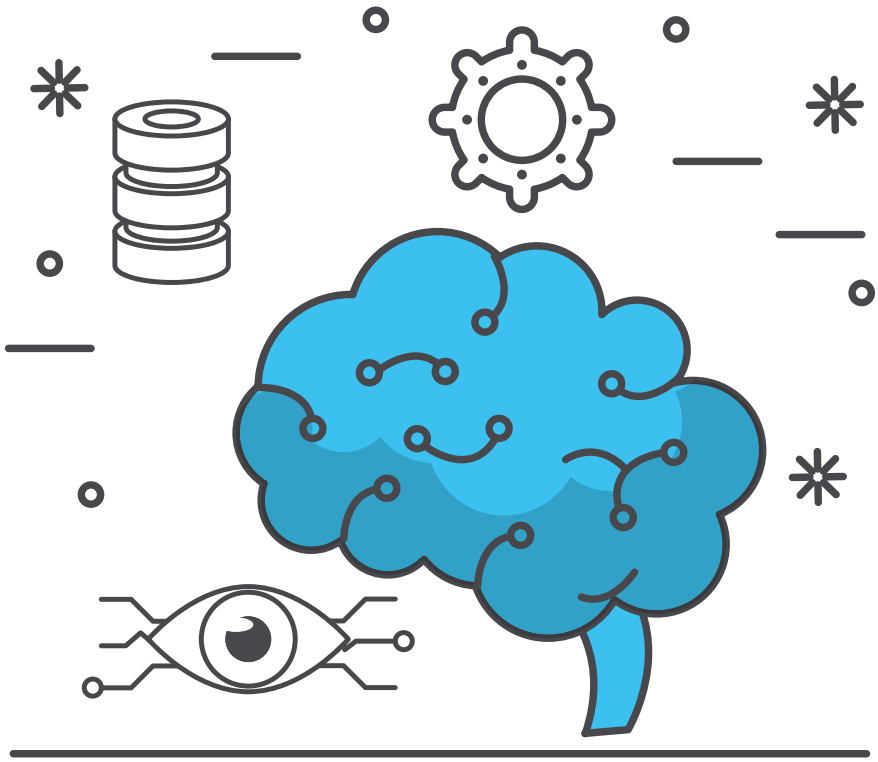
AI-tillämpningar som bygger på maskininlärning är ofta utformade för att förutsäga beteende och hitta samband. De skiljer sig på den punkten från logisk AI som – precis som rättsreglerna – har en tydlig "om-så"-funktion.

AI-system som bygger på maskininlärning, t.ex. analys av tidigare domar, bör användas med stor för-

siktighet för direkt rättstillämpning. Även om förutsebarhet och enhetlighet är viktiga komponenter i ett rättssäkert beslutsfattande finns det principiella invändningar mot system som imiterar beteenden istället för att självständigt tillämpa en rättsregel.

Denna typ av system kan dock spela en viktig roll när det handlar om att skapa beslutsunderlag. Medvetenhet krävs dock om att ofullständiga eller felaktiga datamängder kan leda till felaktiga bedömningar eller förutsägelser. Det finns flera exempel på sådana incidenter, även på det rättsliga området.

Juridiskt arbete innehåller samtidigt en mängd arbetsuppgifter som



ARTIFICIAL INTELLIGENCE

inte handlar om direkt rättstillämpning, t.ex. informationssökning, granskning och utformning av dokument, juridiska riskbedömningar och avtalsutformning. Här är potentialen för system som bygger på maskininlärning betydande. Även om de flesta jurister idag arbetar med digitala verktyg är få arbetsuppgifter ännu automatiserade.

Det är framför allt inom detta område vi idag ser en kraftig utveckling, inte minst driven av mindre legaltech-företag. På sikt kan denna utveckling komma att få stor påverkan, inte minst på den stora marknaden för juridisk rådgivning.

Parallellt kommer vi säkerligen att se en utveckling också av tillämpningar som bygger på logisk AI och här kan det arbete som har gjorts inom den rättsinformatiska forskningen komma till praktisk användning.

Det är som bekant alltid svårt att sia om framtiden, men ett rimligt antagande är att framtidens jurister främst kommer att ha sådana arbetsuppgifter som inte kan utföras effektivare eller bättre av ett AI-system. I praktiken kommer det att innebära stora förändringar för många jurister. Parallellt med att vissa arbetsuppgifter tas över av AI-system kommer emellertid vissa nya att skapas, t.ex. som en följd av höjda ambitionsnivåer. En central uppgift för morgondagens jurister, inte minst bolags- och myndighetsjurister, kommer att vara att bidra till utvecklingen och kontrollen av nya AI-system.

Sammantaget ställer denna utveckling krav på förändringar av juristutbildningen och på att jurister under sitt arbetsliv är flexibla och villiga att ta sig an nya arbetsuppgifter.

Daniel Westman

EU-domstolens Schrems II-avgjørelse: Privacy Shield kjent ugyldig og skjerpede krav til overføring av personopplysninger

Av Thomas Olsen, Malin Tønseth og Haakon D. Føyen

Thomas Olsen

Malin Tønseth

Haakon D. Føyen

Innledning

Den 16. juli 2020 avsa EU-domstolen en prinsipiell avgjørelse om overføring av personopplysninger til USA i avgjørelsen mellom Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, her omtalt som Schrems II-avgjørelsen.[1] Domstolen underkjenner Privacy Shield som overføringsgrunnlag USA med umiddelbar virkning. EUs standardavtaler for overføring opprettholdes, men EU-domstolen presiserer at dataeksportør og dataimportør er pliktige til å vurdere om beskyttelsesnivået i mottakerlandet er tilstrekkelig. Vurderingsplikten gjelder også for overføringer som baserer seg på bindende virksomhetsregler (BCR) som overføringsgrunnlag.

Bakgrunn for saken – Schrems vs. Facebook

At Privacy Shield nå er underkjent av EU-domstolen vekker nok en følelse av «déjà vu» for mange. Et bakteppe for Schrems II er nemlig EU-domstolens prinsippielle Safe Harbor-avgjørelse i 2015 (Schrems I).[2] Saken omhandlet den østerrikske jusstudenten Maximilian Schrems sin klage om at Safe Harboravtalen fra år 2000 mellom EU og USA ikke ga tilstrekkelig vern mot amerikansk masseovervåkning. I klagen anførte Schrems at hans rett til personvern ikke ble ivaretatt når Facebook Ireland Ltd overførte personopplysninger til USA under Safe Harbour-ordningen. I lys av blant annet avsløringene fra Edward Snowden om USAs overvåkningsprogram underkjente EU-domstolen Safe Harbor fordi den ikke ga tilstrekkelig vern i henhold til EUs grunnleggende prinsipper. Avgjørelsen rystet det transatlantiske forholdet mellom EU og USA og hadde store konsekvenser for et stort antall virksomheter som baserte sine overføringer på ordningen. En ny ordning var ønskelig, og ikke

1 Sak C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, 16 juli 2020, (Schrems II).

2 Sak C-362/14 Schrems v. Data Protection Commissioner, 6. oktober 2015, ECLI:EU:C:2015:650 (Schrems I).

lenge etter Schrems I kom EU og Obama-adminstrasjonen til enighet om en ny overføringsavtale kalt EU-U.S. Privacy Shield og EU-kommisjonen fattet vedtak om Privacy Shield som gyldig overføringsgrunnlag til USA.[3]

Da Safe Harbour ble underkjent, tok Facebook i bruk EUs standardavtaler og Privacy Shield for overføringen til USA. Maximilian Schrems omformulerte da sin klage til at EUs standardavtaler og Privacy Shield er i strid med EUs charter om grunnleggende rettigheter[4] som følge av utilstrekkelig vernenivå. Schrems klage endte til slutt i i Irish High Court[5] som altså har bedt EU-domstolen å vurdere om Facebooks overføring til USA på grunnlag av de to overføringsgrunnlagene er lovlig gitt amerikanske myndigheters overvåkningsprogrammer.

EU-domstolens vurderinger og konklusjoner

Innledende betraktninger om vernenivå og tilsynsmyndighetenes rolle

Domstolen innleder med generelle bemerkninger om at EU-retten og GDPR gjelder selv om personopplysninger som blir overført blir aksessert av tredjelands myndigheter av hensyn til allmenn sikkerhet, forsvar eller nasjonal sikkerhet. Det vern som kreves ved overføring basert på standardavtaler må ifølge domstolen i det vesentlige være tilsvarende («essentially equivalent») det som følger av GDPR, sett i lys av EUs Charter. Vernenivået mht. innsyn fra tredjelands myndigheter må vurderes både ut fra de kontraktsvilkår som gjelder mellom data eksportør og data importør og relevante aspekter av tredjelandets rettssystem, særlig de ikke-uttømmende momentene som er listet i GDPR artikkel 45 (2).[6]

Når det gjelder tilsynsmyndighetenes rolle, slår domstolen fast at, i de tilfellene hvor det ikke foreligger beslutning om tilstrekkelig vernenivå fra EU-kommisjonen etter artikkel 45, er tilsynsmyndighetene forpliktet til å suspendere en overføring hvis de vurderer at (i) kontraktsvilkårene ikke kan etterleves, (ii) det vern som kreves etter EU-retten ikke kan sikres på annet vis og (iii) dataimportøren selv ikke har stoppet overføringen.[7]

Vurdering av gyldigheten av EUs standardavtaler

Innledningsvis minner domstolen om at standardavtalene er vedtatt av EU-kommisjonen på grunnlag av GDPR artikkel 46 (2) (c) og er ment å gi kontraktsrettslige garantier som anvendes likt i alle tredjeland, og dermed uavhengig av disse landenes vernenivå. Dette kan tilsi at det kan være behov for å supplere standardavtalene med ytterligere tiltak. Domstolen minner her om GDPRs fortale 109 som oppfordrer behandlingsansvarlige (dataeksportører) til å ha på plass tilleggstiltak som supplerer standardavtalene.

I følge domstolen skal ikke den omstendighet at standardavtalene er kontraktsbestemmelser som ikke binder tredjelands myndigheter alene påvirke gyldigheten av standardavtalene. Gyldigheten avhenger derimot av om standardavtalene inneholder effektive mekanismer *som i praksis* gjør det mulig å sikre vernet som kreves etter EU-retten, og at overføringer suspenderes eller forbys hvis bestemmelsene overtres eller det er umulig å overholde dem.

Domstolen gjennomgår bestemmelsene i standardavtalen og viser at avtalen, særlig Clause 4 og 5 lest i lys av EUs Charter, inneholder slike mekanismer:[8]

> Gyldigheten avhenger derimot av om standardavtalene inneholder effektive mekanismer som i praksis gjør det mulig å sikre vernet som kreves etter EU-retten, og at overføringer suspenderes eller forbys hvis bestemmelsene overtres eller det er umulig å overholde dem.

For det første vises det til at dataeksportør og dataimportør er forpliktet til å *verifisere, før en overføring*, om det vil være mulig i praksis å etterleve bestemmelsene i det relevante tredjelandet. I denne forbindelse bemerker domstolen at fotnoten til Clause 5 slår fast at bindende krav i tredjelandets lovgivning som ikke går lenger enn det som er nødvendig i et demokratisk samfunn for ivareta, blant annet nasjonal sikkerhet, forsvar og allmenn sikkerhet, *ikke* er i strid med bestemmelsene i standardavtalen.

Videre vises det til at dataimportøren skal varsle dataeksportøren om enhver manglende evne til å overholde standardavtalene.

Dersom dataeksportøren mottar slikt varsel, er dataeksportøren ifølge standardavtalen forpliktet til å stanse overføringen eller si opp kontrakten.

Hvis dataeksportøren fortsetter å overføre data til tross for varselet, skal datatilsynsmyndigheten varsles.

3 Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield.

4 Charter of Fundamental Rights of the European Union, 26. oktober 2012, OJ C 326.

5 The High Court Commercial, The Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, 3. oktober 2017, 2016 No. 4809 P

6 Se dommen avsnitt 105.

7 Se dommen avsnitt 121.

8 Se dommen avsnitt 138-149.

Avslutningsvis minner domstolen om at tilsynsmyndighetene er forpliktet til å suspendere eller forby en overføring hvis de vurderer at (i) kontraktsvilkårene ikke kan etterleves, (ii) det vern som kreves etter EU-retten ikke kan sikres på annet vis og (iii) dataimportøren selv ikke har stoppet overføringen.

Vurdering av Privacy Shield

Domstolen innleder sin vurdering av Privacy Shield med å bemerke at ordningen legger til grunn et prinsipp, slik tilfellet var også med Safe Harbour, om at amerikansk lovgivning går foran Privacy Shield prinsippene. Det vises til at de amerikanske virksomhetene underlagt ordningen kan gjøre unntak fra etterlevelsen i den grad det er nødvendig for å etterleve forpliktelser i henhold amerikansk lovgivning som skal ivareta USAs nasjonale sikkerhet, allmenne interesser og rettshåndhevelse.

Domstolen vurderer deretter, med utgangspunkt i EU-kommisjonens vurderinger knyttet til Privacy Shield og informasjon fra den irske domstolen, hvorvidt amerikansk lovgivning sikrer tilfredsstillende vern som påkrevet av GDPR artikkel 45, lest i lys av de grunnleggende rettighetene i Charteret artiklene 7 (privatliv), 8 (personopplysningsvern) og 47 (domstolsprøving).

Domstolen vurderer konkret lovgivningen som ligger til grunn for amerikanske overvåkningsprogrammer som PRISM og UPSTREAM. Dette er for det første Foreign Intelligence Surveillance Act (FISA) Section 702, også kjent som 50 USC § 1881a, som gir hjemmel til å kreve utlevering av informasjon fra «electronic communications providers» i vid forstand. Videre gjelder det Executive Order 12 333 (E.O. 12 333) som gir hjemmel for overvåkning av datatrafikk.

I følge domstolen gir ikke denne lovgivningen rettsikkerhetsgarantier tilsvarende det som er påkrevet etter EU-retten, særlig fordi overvåkningsprogrammene som bygger på den aktuelle lovgivningen ikke er begrenset til hva som er strengt nødvendig.

Etter domstolens vurdering gir heller ikke Ombudsmanns-ordningen rettssikkerhetsgarantier som er i det vesentlige tilsvarende det som kreves etter EU-retten når det gjelder Ombudsmannens uavhengighet og kompetanse til å fatte beslutninger som er bindende for amerikanske myndigheter.

> Personvernrådet slår innledningsvis fast at dataeksportør må sørge for at beskyttelsesnivået for vern av personopplysninger som vil oppnås i praksis, faktisk er tilsvarende som i EØS, alle forhold tatt i betraktning. Dette gjelder både ved bruk av EU standardavtalene og BCR.

På denne bakgrunn kjente domstolen EU-kommisjonens beslutning vedrørende Privacy Shield som ugyldig med umiddelbar virkning.

Veiledninger fra Personvernrådet og Datatilsynet

Veiledning fra Personvernrådet

I kjølvannet av dommen har Personvernrådet (EDPB) kommet med en detaljert uttalelse om hvordan dommen skal forstås og om konsekvensene i praksis[9]. Personvernrådet slår relativt kortfattet fast at Privacy Shield ikke lenger er gyldig overføringsgrunnlag, og at dommen ikke åpner for en overgangsperiode.

Dernest vies mye plass til forklare implikasjonene av dommen og vilkårene for fortsatt bruk av EU standardavtalene. Også konsekvensene for andre overføringsgrunnlag, herunder BCR, trekkes frem.

Personvernrådet slår innledningsvis fast at dataeksportør må sørge for at beskyttelsesnivået for vern av personopplysninger som vil oppnås i praksis, faktisk er tilsvarende som i EØS, alle forhold tatt i betraktning. Dette gjelder både ved bruk av EU standardavtalene og BCR. Man skal derfor undersøke nøye om det finnes omstendigheter som gjør at beskyttelsesnivået som standardavtalene eller BCR er ment å sikre, ikke vil realiseres i praksis, herunder foreta en vurdering av lokal lovgivning i mottakerlandet og andre forhold som kan ha betydning.

Når det gjelder den nærmere vurderingen som må foretas vedrørende lokal lovgivning og øvrige forhold i mottakerlandet så peker Personvernrådet særlig på at det kan være relevant å se hen til den (ikke uttømmende) listen av vurderingsmomenter som fremgår av GDPR artikkel 45 (2). Listen angir relevante faktorer som EU Kommisjonen er forpliktet å vurdere når de skal ta stilling til om enkelte tredjeland skal anses som forhåndsgodkjente for overføringer. Det er verd å merke seg at listen i artikkel 45 (2) omfatter relativt krevende vurderingsmomenter. Det kan her nevnes at EU Kommisjonen gjerne bruker 1–2 år på å vurdere forholdene i enkelte land opp mot disse momentene for deretter å ta stilling til om det gis et tilstrekkelig vernenivå i mottakerlandet.

Listen over vurderingsmomenter angir blant annet at det vil være relevant å vurdere:

- prinsippet om rettstaten, respekt for menneskerettigheter og grunnleggende friheter, relevant lovgivning mv.
- om det finns en eller flere uavhengige og velfungerende tilsyns-

9 Se FAQ fra EDPB av 23. juli 2020: *https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf*

myndigheter i tredjestaten med ansvar for å sikre håndhevelse
- internasjonale forpliktelser som mottakerlandet har påtatt seg, herunder rettslig bindende konvensjoner mv.

Personvernrådet peker dernest på at dersom man kommer frem til at det foreligger forhold som gjør at beskyttelsesnivået i mottakerlandet ikke vil være tilsvarende som i EØS, må det iverksettes *ytterligere tiltak* som veier opp for dette og som sikrer et tilsvarende beskyttelsesnivå i praksis. Dersom det ikke finnes slike ytterligere tiltak, eller man ikke er i stand til å iverksette slik tiltak, kan man ikke overføre personopplysningene. Personvernrådet kommer ikke med konkret veiledning på hvilke ytterligere tiltak som kan være aktuelle og tilstrekkelige, men uttaler at man vil foreta en nærmer analyser av dette spørsmålet og komme tilbake med utdypende veiledning.

Særlig når det gjelder overføringer til USA peker Personvernrådet på at de to amerikanske lovene som domstolen har vurdert finner anvendelse på enhver overføring som skjer ved bruk av elektroniske hjelpemidler uavhengig av hvilket overføringsverktøy som anvendes. Dersom lovene finner anvendelse og det ikke er mulig å iverksette ytterligere tiltak som demmer opp for risikoen knyttet til personvernet, må opplysningene ifølge Personvernrådet lagres annet sted enn i USA. Dersom dataeksportøren likevel velger å fortsette dataoverføringene til USA må det kompetente datatilsynet (tilsynet i landet til dataeksportørens) notifiseres. Datatilsynet må i slikt tilfelle ta stilling til om overføringene skal suspenderes eller om de kan fortsettes, eventuelt under særlige vilkår.

Veiledning fra Datatilsynet

Også Datatilsynet har gitt foreløpig veiledning om dommen og dens praktiske konsekvenser.[10] Tilsvarende som Personvernrådet, slår Datatilsynet fast at dataeksportør må sørge for et tilstrekkelig beskyttelsesnivået i praksis. Tilsynet peker på at det er viktig å undersøke om *dataimportøren*, dataimportørens *infrastruktur* eller eventuelle *underleverandører* er underlagt lover, regler eller systemer som er i strid med importørens forpliktelser etter overføringsgrunnlaget eller som på annet vis senker beskyttelsesnivået.

Med hensyn til hva som utgjør «ytterlige tiltak» viser Datatilsynet til at Personvernrådet jobber med å utrede dette. Datatilsynets foreløpige veiledning er følgende:

> «Hva de ytterligere tiltakene kan gå ut på, må avgjøres i hver enkelt sak, i lys av de konkrete omstendighetene. Det kan potensielt være snakk om juridiske, tekniske eller organisatoriske tiltak. Per nå er det imidlertid stor usikkerhet om hva slags ytterligere tiltak som kan være tilstrekkelige dersom tredjelandet har lover som går foran forpliktelsene etter overføringsgrunnlagene eller på annet vis senker beskyttelsesnivået. Det vil si at det på nåværende tidspunkt er svært utfordrende å overføre personopplysninger til slike tredjeland, og i praksis vil det nok for de fleste ikke være mulig å gjennomføre.» (vår understreking)

Datatilsynet er med andre ord svært strenge i sin veiledning knyttet til dommen og går langt i å konkludere i at overføringer til en rekke tredjeland per i dag ikke vil være mulig på lovlig grunnlag. Tilsynet understreker også at det ikke gjelder noen overgangsperiode før de skjerpede kravene etter dommen gjelder.

Ifølge tilsynet er det de samme vurderingene som det er redegjort for over som må gjøres mht. overføring til USA. Tilsynet trekker her frem de to amerikanske overvåkningslovene som særlig ble vurdert av EU-domstolen:
- Foreign Intelligence Surveillance Act (FISA) Section 702, også kjent som 50 USC § 1881a
- Executive Order 12 333 (E.O. 12 333)

I følge tilsynet er amerikanske «electronic communications providers» (tilbydere av elektroniske kommunikasjonstjenester) underlagt FISA 702. Dette er definert vidt, og omfatter f.eks. «remote computing services». Loven gjelder både innenfor og utenfor amerikansk territorium og selv om informasjonen er lagret i EØS-området.

Executive Order 12 333 (E.O. 12 333) gjelder overvåkning av privat kommunikasjon. Etter vår vurdering vil denne lovgivningen først og fremst være aktuell der det faktisk overføres personopplysninger til en underleverandør i USA. E.O. 12 333 regulerer amerikanske etterretningsmyndigheters adgang til å avlytte selve kommunikasjonen.

Selv om man bruker SCC, vil disse to lovene – ifølge Datatilsynet – innebære at beskyttelsesnivået i USA ikke er tilsvarende som i EØS. Dersom dataimportøren, dataimportørens infrastruktur eller eventuelle underleverandører er underlagt disse *eller tilsvarende lover* – noe Datatilsynet mener som regel vil være tilfellet – må det eventuelt iverksettes «ytterlige tiltak» som beskrevet ovenfor. I følge Datatilsynet kan dette imidlertid være «svært utfordrende eller umulig å få til i praksis, og i så fall kan ikke overføring av personopplysninger til USA finne sted».

Når det gjelder dataimportøren sitt ansvar, peker Datatilsynet i sin veiledning på at dataimportøren for det første vil kunne hjelpe dataeks-

10 Se Datatilsynets spørsmål og svar om nye regler for overføring av personopplysninger til land utenfor EØS: *https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/sos-om-nye-regler-for-overforing/*

portøren med å forstå lovene og forholdende i tredjelandet. For det andre har dataimportøren en plikt til å si fra til dataeksportøren dersom den ikke kan følge sine forpliktelser etter SCC, f.eks. dersom det innføres nye lover i tredjelandet eller tolkningen av eksisterende lover endres. I slike tilfeller må dataeksportøren enten iverksette ytterligere tiltak, eller slutte å overføre personopplysninger og be om at dataimportøren tilbakefører eller sletter dataene som allerede er overført.

Hvilke konsekvenser har dommen?

Privacy Shield kan ikke lenger benyttes som overføringsgrunnlag

Som redegjort for over har EU-domstolen slått fast at Privacy-Shield-avtalen mellom EU og USA er ugyldig som overføringsgrunnlag. Samtidig er det slått fast fra EU-domstolens side at EUs standardavtaler inneholder tilstrekkelige sikkerhetsmekanismer forutsatt at disse brukes riktig. Dommen har umiddelbar virkning, dvs. det åpnes ikke for noen mellomperiode.

> Vi merker oss at enkelte leverandører fastholder at de fortsetter å etterleve personvernprinsippene i Privacy Shield. Dette er fortsatt et relevant rammeverk, men etter avsigelsen av dommen gir den ikke gyldig overføringsgrunnlag til USA.

Dette innebærer at alle virksomheter som frem til nå har basert overføring av personopplysninger til USA på Privacy Shield ordningen, umiddelbart må finne et annet rettslig grunnlag for overføringen. I praksis gjelder dette en stor andel norske og europeiske virksomheter der leverandører, underleverandører eller egne konsernselskaper i USA mottar eller har tilgang til personopplysninger. Vi merker oss at enkelte leverandører fastholder at de fortsetter å etterleve personvernprinsippene i Privacy Shield. Dette er fortsatt et relevant rammeverk, men etter avsigelsen av dommen gir den ikke gyldig overføringsgrunnlag til USA.

Konsekvenser for bruk av EU standardavtaler og BCR

Dommen innebærer videre at EUs standardavtaler for overføring fremdeles er gyldige. Bruk av standardavtalene er imidlertid ikke i seg selv tilstrekkelig for å gjøre overføring av opplysninger til tredjeland lovlig. I følge domstolen skal dataeksportøren, med bistand fra dataimportøren, gjøre en vurdering av om garantiene som stilles i standardavtalen kan oppfylles i praksis. Særlig skal det vurderes om lokal lovgivning som pålegger mottaker å utlevere opplysninger til offentlige myndigheter gir tilstrekkelige rettsikkerhetsgarantier. Det er altså ikke tilstrekkelig å vurdere de ovennevnte lovene som EU-domstolen tok direkte stilling til. Også annen tilsvarende lokal lovgivning må vurderes konkret og terskelen som er satt av EU-domstolen gjelder da også ved slik vurdering av annen lovgivning.

I tillegg må det som nevnt over gjøres en særlig vurdering av det rettslige regimet i samtlige land hvor data skal overføres til, og resultatet fra vurderingen må dokumenteres. Dette gjelder altså hva enten overføringen skjer til tjenesteleverandør eller til dennes underleverandører i tredjeland. Dommen har derfor vidtrekkende konsekvenser for adgangen til fremover å støtte seg på EU standardavtaler for overføring til tredjeland.

Dommen har, som også påpekt av Personvernrådet og Datatilsynet, i tillegg direkte konsekvenser for lovligheten av overføringer på grunnlag av BCR. Fremover gjelder med andre ord samme terskel der overføring av opplysninger skjer til konserninterne selskap i tredjeland på bakgrunn av BCR. En virksomhet som er etablert i EØS, og som ønsker å basere seg på BCR for å dele personopplysninger med andre selskap innenfor samme konsern etablert utenfor EØS, må derfor gjøre en tilsvarende vurdering av lokal lovgivning i slike land.

Ved vurderingen av lokal lovgivning i tredjeland må dataeksportøren og dataimportøren se hen til hvilke garantier som er gitt i overføringsgrunnlagt og det må gjøres en konkret vurdering av om garantiene kan etterleves i praksis. Som nevnt har EU standardavtalene en rekke vilkår som direkte regulerer hvordan partene skal håndtere utlevering av opplysninger til myndigheter i tredjeland og som stiller krav om at det ikke kan skje omfattende, uforholdsmessige og tilfeldige utleveringer. Tilsvarende krav og garantier er også å finne i forbindelse med BCR som overføringsgrunnlag og det er altså slike garantier som dataeksportøren konkret må ta stilling til om det er mulig å etterleve i praksis. I tillegg til å vurdere lokal lovgivning må det ses hen til eventuelle særlige omstendigheter ved dataoverføringene og det må gjøres en generell vurdering av det rettslige regimet i mottakerlandet.

Dersom dataeksportøren konkluderer med at lokal lovgivning i mottakerlandet er til hinder for etterlevelse av garantiene i overføringsgrunnlaget må det tas stilling til om det kan iverksettes tiltak som likevel sikrer et tilstrekkelig vernenivå. Som nevnt over er det ikke klargjort av domstolen hvilke tiltak som kan være relevante og dette er derfor fortsatt noe uklart.

Konsekvenser for bruk av unntakene i artikkel 49

Det skal nevnes at EU-domstolen ikke får konsekvenser for overføringer til tredjeland basert på de særlige

unntakene i GDPR artikkel 49. Dette innebærer at det fortsatt er mulig å basere overføringer for eksempel på samtykke fra den registrerte. Overføringer til tredjeland basert på samtykke vil imidlertid sjeldent være anvendelig i forbindelse med omfattende og systematiske overføringer. Et samtykke må for det første være frivillig og den registrerte kan til enhver tid trekke tilbake sitt samtykke, som vil innebære at overføringen må opphøre og eventuelle overførte opplysninger tilbakeføres. Dette kan være vanskelig å etterleve i en lang rekke tilfeller, for eksempel når overføring skjer ved bruk av skytjenester og basert på standardvilkår. Videre må et samtykke være uttrykkelig og informert, hvilket innebærer at dataeksportøren blant annet må informere den registrerte om at lovgivningen i mottakerlandet gir et utilstrekkelig vernenivå for opplysningene. De øvrige unntakene etter artikkel 49 har et desto mer begrenset nedslagsfelt enn samtykke-unntaket. Eksempelvis kan unntaket om overføring når det er nødvendig for å «oppfylle en avtale» bare brukes i enkeltstående tilfeller (ad-hoc) og altså heller ikke ved gjentatte eller systematiske overføringer.

Hva bør virksomheter gjøre nå?

Ugyldiggjøringen av Privacy Shield med umiddelbart virkning og skjerpede krav for bruk av EUs standardavtaler og BCR har dramatiske konsekvenser for de aller fleste virksomheter. Hvor eksponert den enkelte virksomhet er vil avhenge av graden av internasjonal samhandling og bruken av internasjonale leverandører og underleverandører.

I lys av foreliggende strenge veiledning fra Datatilsynet oppfatter vi at det forventes at virksomhetene så raskt som praktisk mulig skaffer seg oversikt over egen situasjon og setter i gang med nødvendige tiltak.

Basert på dommen og foreliggende veiledninger fra Personvernrådet og datatilsynsmyndighetene anbefaler vi følgende konkrete tiltak:

For det *første* bør virksomhetene følge med på veiledning fra Personvernrådet og de lokale tilsynsmyndighetene, særlig med hensyn til vurdering av vernenivå i tredjeland og hva slags juridiske, tekniske og organisatoriske tilleggstiltak som vil være relevante for å verne mot tredjelands myndigheters tilgang til personopplysninger.

For det *andre* bør virksomhetene kartlegge alle overføringer som skjer ut av EØS på grunnlag av Privacy Shield og EU standardavtaler (særlig overføringer til USA). For større virksomheter vil det være naturlig å etablere rutiner for «transfer due diligence», som bør gjelde for nye overføringer, men også for å følge opp foreliggende avtaler og samarbeid som innebærer overføring av personopplysninger.

For alle overføringer som tidligere var basert på *Privacy Shield*, bør virksomheten vurdere om overføringen kan fortsette på annet grunnlag, f. eks. EU standardavtaler eller BCR, eller om det er hensiktsmessig at databehandlingen flyttes innenfor EØS

For alle overføringer som baseres på *EUs standardavtaler* og *BCR*, er det viktig å merke seg at det forutsettes en vurdering av beskyttelsesnivået i mottakerlandet i henhold til domstolen og tilsynsmyndighetenes anvisninger.

For overføringer til USA, bør det særlig sjekkes om mottaker er underlagt FISA Section 702 eller E.O. 12 333. Forespør gjerne en redegjørelse fra dataimportør, som for databehandlere blant annet bør omfatte oversikt over underleverandører, overføringer og tilhørende overføringsgrunnlag.

Dersom vurderingene viser at beskyttelsesnivået knyttet til overføringer til tredjeland ikke er tilstrekkelig, til tross for evt. relevante tilleggstiltak som f.eks. kryptering, må overføringen suspenderes og data importøren må instrueres til å tilbakelevere og/eller slette opplysningene.

Dersom dataimportøren er kjent med forhold som tilsier at opplysningene ikke kan gis et tilfredsstillende vern, skal dataeksportør varsles. Dataeksportør skal da stoppe overføringen, evt. varsle Datatilsynet om at man ikke anser det nødvendig å stoppe overføringen.

I tillegg til ytterligere veiledning fra tilsynsmyndighetene, er det også ventet initiativer fra EU-kommisjonen. Gjeldende standardavtaler for overføring til databehandler og behandlingsansvarlig er tuftet på gammelt regelverk. Arbeidet med å oppdatere standardavtalene har vært satt i bero i påvente av avgjørelsen. Så snart de oppdaterte standardavtalene er tilgjengelige bør disse tas i bruk og erstatte tidligere versjoner.

EU-kommisjonen og U.S. Department of Commerce har for øvrig i en nylig pressemelding uttalt at det er initiert samtaler for å «vurdere potensialet for et forbedret Privacy Shield rammeverk».[11] I pressemeldingen nevnes blant annet felles utfordringer med å gjenopprette den globale økonomien etter covid-19-pandemien. Forhåpentligvis lykkes EU og USA på sikt å forenes om forholdet mellom personvern og overvåkning. I påvente av en eventuell ny og forbedret Privacy Shield, må virksomhetene inntil videre skaffe seg oversikt og navigere på best mulig måte ut fra de overføringsgrunnlagene og tiltakene som er tilgjengelig.

Thomas Olsen (PhD) er assosiert partner og leder for Simonsen Vogts Wiigs personvernteam.

Malin Tønseth er assosiert partner i Simonsen Vogt Wiig, med spesialkompetanse innen personvern- og informasjonssikkerhet og leder av Compliance & Risk-teamet..

Haakon D. Føyen er advokatfullmektig i Simonsen Vogt Wiig, og er tilknyttet firmaets avdeling for teknologi og media.

11 Se felles pressemelding 10. august 2020: *https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=684836*.

Halvor Manshaus

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

Beskatning av GAFA-aktører: Dom I apple-saken

De såkalte «GAFA»-selskapene, Google, Apple, Facebook og Amazon tilbyr ulike digitale tjenester gjennom egne plattformer og tekniske løsninger. I motsetning til tradisjonelle distribusjonssystemer kan GAFA distribuere proprietære tjenester gjennom nettverk på tvers av landegrenser. Dette gir store skaleringsfordeler gjennom bruk av sentraliserte distribusjonsnoder som betjener større geografiske områder. Opprettelsen av en slik sentral enhet kan få stor betydning for den lokale økonomien i vertslandet, blant annet i form av arbeidsplasser og et langsiktig kompetanseløft som vil kunne være viktig for konkurranseevnen på lengre sikt. I tillegg vil det tilkomme en jevn inntektsstrøm i form av skatteinntekter fra virksomheten, som i seg selv kan utgjøre betydelige beløp. Vi har mange eksempler på at ulike land legger til rette for denne typen internasjonale aktører ved bruk av ulike insentivordninger. Et velkjent eksempel er Irland, som gjennom lav virksomhetsbeskatning har vært et attraktivt vertsland for IT-gigantene.

Skatteplanlegging har derfor vært et viktig moment ved den fysiske lokaliseringen for digitale tjenesteleverandører. For vertslandet gjelder det å ha gunstige skatteordninger som kan friste til nye etableringer, mens aktørene vil søke frem til optimale skattebetingelser for sin virksomhet.

Slik skatteplanlegging kan fremstå som relativt aggressiv, spesielt for andre land som mottar tjenester og ser stor økonomisk aktivitet som i liten grad blir beskattet lokalt. Dette er et tema som får stadig større oppmerksomhet, og som er gjenstand for internasjonal koordinering og nye reguleringer med sikte på å jevne ut skattegrunnlag og skatteinntekter. OECD har i flere år hatt dette som et prioritert fokusområde (*www.oecd.org/tax/beps*), og viser blant annet til at *"Domestic tax base erosion and profit shifting (BEPS) due to multinational enterprises exploiting gaps and mismatches between different countries' tax systems affects all countries…. Business operates internationally, so governments must act together to tackle BEPS and restore trust in domestic and international tax systems. BEPS practices cost countries 100-240 billion USD in lost revenue annually, which is the equivalent to 4-10% of the global corporate income tax revenue."*

BEPS-prosjektet under OECD/G20 innebærer at 135 land har blitt enige om en 15-punkts plan som skal motarbeide skatteomgåelse, utvikle et mer enhetlig internasjonalt regelverk innen skatterett og legge til rette for større transparens. Norge har deltatt i dette arbeidet, og tilbakemeldingene har gjennomgående vært positive etter diverse møter og seminarer de siste årene. Dette synes å ha skiftet like før sommeren 2020, noe som skinner klart gjennom i forbindelse med et intervju med avtroppende skattedirektør Hans Christian Holte. Holte har deltatt i flere G20-møter om BEPS, og har tidligere vært positiv til utviklingen. En av sine siste arbeidsdager som skattedirektør tvitret han imidlertid 29. juli 2020:

> *«Med denne saken takker jeg nok for meg i offentligheten som leder av @Skattenmin, @NAVnorge venter meg på mandag. Synd at jeg ikke kan avslutte med mer optimisme, men slik er altså ståa. Ikke enige om skatt for teknologigiganter: – Ser tøffere ut nå»*

Saken han viste til var et intervju med Holte i Aftenposten 29. juli 2020[1] der det ble påpekt at arbeidet med et felles regelverk er satt langt tilbake. Holte peker på koronapandemien, som har medført at skattemyndighetene i de enkelte land

1 (https://www.nrk.no/norge/ikke-enige-om-skatt-for-teknologigiganter_-_-ser-toffere-ut-na-1.15103231)

har vært overveldet med andre oppgaver. Videre viser han til at USA i juni 2020 meldte at de ville trekke seg fra videre dialog om digitalskatt. Ettersom samtlige GAFA-aktører og en rekke andre tunge digitale virksomheter hører hjemme nettopp i USA, får dette store praktiske konsekvenser for harmoniseringsarbeidet.

Uttalelsene fra Holte veier tungt. I tillegg til å være Norsk skattedirektør gjennom arbeidet på dette området, har Holte også vært toppsjef for skattenettverket i OECD FTA – Form on Tax Administration. FTA ble opprettet i 2002, og har med seg samtlige G20-land. FTA har hatt en helt sentral rolle i OECDs BEPS-innsats omtalt ovenfor, som nå ser ut til å ha fått en kraftig nedbremsing.

Ved inngangen til sommeren 2020 var det altså ikke lenger så stor optimisme knyttet til BEPS-arbeidet.

15. juli 2020 nedkom EU-domstolen (EU-General Court, syvende kammer) med en avgjørelse i en langvarig diskusjon mellom EU-kommisjonen og Apple (Apple Sales International og Apple Operations Europe). Saken går tilbake til et skattevedtak i Irland fra 1991 i favør av Apple, som senere ble opprettholdt i et nytt vedtak i Irland i 2007. Vedtakene godkjente Apples modell for inntektsberegning, som dermed sto seg fra 1991 og helt frem til Apple innførte en ny virksomhetsstruktur i 2014. Kommisjonen besluttet i 2016 at de to skattevedtakene fra Irland i realiteten utgjorde 13 milliarder Euro i urettmessig statsstøtte fra Irland til Apple. Det omtvistede beløpet utgjorde med andre ord om lag 140 milliarder kroner. Denne saken er altså et godt eksempel på hvorfor temaet digital skatteplanlegging har så stor internasjonal oppmerksomhet, ved at det gir slike enorme økonomiske utslag.

Innenfor EU står medlemslandene i utgangspunktet fritt til å utforme egne skatteregimer, i den forstand at skattereglene ikke er gjenstand for et EU-rettslig harmoniseringskrav. Samtidig setter EU-traktaten rammer for det enkelte lands skatteregime ved at skattereglene ikke kan diskriminere basert på nasjonalitet, eller være i strid med restriksjonsforbudene, eller reglene om statsstøtte. EU har med andre ord i utgangspunktet akseptert en viss skattekonkurranse mellom landene. Problemet innenfor EU-systemet oppstår når enorme skatteinntekter fra GAFA og tilsvarende aktører forsvinner ut av EU som en konsekvens av «skattekonkurranse» mellom medlemslandene. Irland har drevet med slik skattekonkurranse ved at det er gitt gunstige skattebetingelser for å tiltrekke internasjonale aktører til etablering i nettopp Irland. Ved at aktørene betaler mindre skatt i Irland enn om de hadde vært lokalisert i andre EU-land, kan det hevdes at det oppstår en lekkasje av skatteinntekt ut av EU.

Ettersom det ikke eksisterer noe EU-rettslig harmoniseringskrav, kunne ikke EU-kommisjonen i denne saken benytte reglene om de fire friheter som grunnlag for å angripe skattevedtakene. I stedet ble spørsmålet i saken om Irland hadde brutt reglene om statsstøtte, altså om gunstige skattebetingelser utgjorde ulovlig statsstøtte overfor Apple. Dermed dreide saken for EU-domstolen seg om en prøving av om Apple ble forskjellsbehandlet innenfor det eksisterende skattesystem i Irland på tidspunktet for de to vedtakene. En urettmessig forskjellsbehandling kan etter reglene om statsstøtte være resultatet av to forhold. Enten er det reglene selv som forskjellsbehandler, eller så praktiseres ett ellers nøytralt regelverk slik at det oppstår forskjellsbehandling. Dersom virksomheten grunnet forskjellsbehandling oppnår en mindre skatteregning enn sammenlignbare

foretak i en sammenlignbar situasjon, utgjør dette en fordel som innebærer statsstøtte.

Både Irland (sak T-778/16) og Apple (sak T-892/16) krevde at avgjørelsen fra kommisjonen måtte settes til side og annulleres. I den ferske avgjørelsen skriver domstolen at kommisjonen ikke har klart å godtgjøre at Irland har gitt Apple en økonomisk fordel i juridisk forstand. Det kunne da heller ikke foreligge noen form for urettmessig statsstøtte som anført av kommisjonen. Dommen kan ankes til øverste nivå i EU-domstolen, som da vil ha begrenset kompetanse til kun å vurdere lovanvendelsen.

Flere land og organisasjoner hadde ønske om å delta i saken som partshjelpere. Polen og Luxemburg ble i særskilt avgjørelse, T-778/16, tillatt å tre inn som partshjelpere, Polen for EU-kommisjonen, og Luxemburg for Irland. I en ytterligere særskilt avgjørelse, T-892/16, kom Irland inn som partshjelper for Apple. Dette fordi de to hovedsakene hadde Apple og Irland som selvstendige parter i individuelle saker, mens Irland altså ønsket å intervenere i Apples sak og yte støtte også her. I samme prosessuelle avgjørelse slapp EFTAs overvåkningsorgan inn som partshjelper for EU-kommisjonen. USA og IBEC (en organisasjon for nasjonale og internasjonale virksomheter som driver i Irland) slapp derimot ikke til som partshjelpere, hovedsakelig grunnet manglende rettslig interesse. Pågangen med partshjelpere understreker den sterke interessemotsetningen og spenningen som var knyttet opp mot utfallet av dette sakskomplekset.

Domstolen konkluderer i avgjørelsen først med at kontroll knyttet til statsstøtte i dette sakskomplekset ligger innenfor EU-kommisjonens kompetanse, og går deretter til å diskutere de materielle problemstillingene i saken (avsnitt 124).

Et nøkkelpunkt i den videre drøftelsen var hvorvidt EU-kommisjonen hadde identifisert riktig referansesystem som grunnlag for den komparative analysen av skatteordningen. Dette er et sentralt tema i saker om statsstøtte, som gir seg direkte utslag i den etterfølgende vurdering av om det er gitt urettmessig statsstøtte. Apple og Irland anførte at EU-kommisjonen uriktig hadde sammenlignet Apple med ordinære nasjonale irske virksomheter, mens Apple var en utenlandsk virksomhet undergitt særskilte regler. Domstolen la derimot til grunn at referansegrunnlaget ga et riktig grunnlag for analysen, og viste til at ulikheter på enkelte områder ikke var avgjørende, så lenge det overordnede formålet med regelverket var tilsvarende. I dette tilfellet var formålet å sikre at alle virksomheter, både nasjonale og internasjonale, betalte like mye i skatt på sine respektive inntekter (avsnitt 161):

> *"When seen from that perspective, resident and non-resident companies carrying on a trade in Ireland through a branch are in a comparable situation in the light of the objective pursued by that regime, namely the taxation of chargeable profits. The fact that the latter's chargeable profits are specifically defined in section 25(2)(a) of the TCA 97 does not establish that section as the reference framework; rather, that provision is the legislative means used for the purpose of applying corporation tax to that category of company. As is apparent from the case-law cited in paragraphs 148 and 149 above, the fact that, pursuant to those legislative means, one category of company is treated differently as compared with other companies does not mean that those two categories of company are not in a comparable situation in the light of the objective pursued by that regime."*

Domstolen måtte også ta stilling til en anførsel fra Irland om at armlengdeprinsippet ikke er en del av irsk skatterett, og derfor ikke kunne anvendes ved vurderingen opp mot EU-regelverket om statsstøtte. EU-rettens prinsipp om armlengde innebærer at det skal vurderes om skattereglene gir et inntektsbilde som gjenspeiler det en vil forvente å gjenfinne ellers i markedet. Det skal altså vurderes om allokering av inntekter etter vedtakene hadde blitt det samme om de to involverte Apple-selskapene hadde vært fullstendig uavhengige av hverandre, med andre ord om de ble vurdert med armlengdes avstand. EU-domstolen fulgte her tilsvarende resonnement som i en tidligere sak fra 2019 som involverte Starbucks (T-760-15 og T-636/16), og sier i avsnitt 207 at for at armlengdeprinsippet skal få anvendelse:

> *"…it must be clear from national tax law that the profits derived from the activities of the branches of non-resident undertakings should be taxed as if they resulted from the economic activities of stand-alone undertakings operating under market conditions."*

I sin vurdering viser domstolen blant annet til at Irland bekreftet at det internrettslige regelverket forutsatte at verdigrunnlaget ble fastsatt ut ifra en vurdering av antatt markedsverdi, og at inntekt til et konsernledd skal beskattes ut ifra denne markedsverdien. Etter en bredere drøftelse konkluderer domstolen med at EU-kommisjonen må kunne anvende prinsippet om armlengdes avstand ved sin vurdering opp mot reglene om statsstøtte.

Saken reiste flere problemstillinger, men når det først var slått fast at EU-kommisjonen hadde kompetanse til å behandle saken, og at utgangspunktet for vurderingen måtte være prinsippet om armlengdes avstand, ble det springende punkt hvorvidt Apples to virksomhetsledd var blitt vurdert riktig opp mot dette prinsippet. Sentralt i denne vurderingen var (litt forenklet) hvorvidt konserninterne lisensavtaler til de to Apple-virksomhetene i sin helhet skulle allokeres til de irske leddene i virksomheten, ettersom dette var

den fysiske delen som også hadde ansatte som kunne betjene lisensene. Alternativt skulle inntekten kun allokeres til den irske delen av virksomheten – så langt som lisensene faktisk var kontrollert fra Irland. Apple viste til at strategiske avgjørelser knyttet til utvikling, design, markedsføring osv knyttet opp mot lisensene ble styrt fra Apples hovedkvarter i Cupertino, California. Virksomheten i Irland utøvet ikke denne reelle kontrollen med lisensene, og det ville derfor være feil å allokere skatteinntektene i den retning. Domstolen sa seg enig i denne vurderingen, og oppsummerer i avsnitt 310:

> *"It is apparent from the foregoing considerations that, in the present instance, the Commission has not succeeded in showing that, in the light, first, of the activities and functions actually performed by the Irish branches of ASI and AOE and, second, of the strategic decisions taken and implemented outside of those branches, the Apple Group's IP licences should have been allocated to those Irish branches when determining the annual chargeable profits of ASI and AOE in Ireland."*

EU-kommisjonen hadde med andre ord ikke påvist at de opprinnelige skattevedtakene som godkjente allokering av lisensavtaler og de underliggende immaterielle verdiene til virksomhetsledd utenfor Irland, ga Apple en urettmessig skattefordel. Med andre hadde EU-kommisjonen ikke grunnlag for å hevde at allokering av IP-rettigheter og lisensavtaler med Apple til den amerikanske virksomheten i Cupertino var et annet resultat enn det man ville sett under et tenkt åpent marked i tråd med armlengdeprinsippet. Dermed legges det til grunn en høy terskel for EU-kommisjonen i lignende saker, der det uansett feil i den nasjonale vurderingen må gjøres en selvstendig analyse som kan bevise at det er gitt en økonomisk fordel til skattesubjektet. På den annen side fikk EU-kommisjonen gjennomslag for at prinsippet om armlengdes avstand skal legges til grunn der det nasjonale systemet forutsetter at inntektsgrunnlaget skal kartlegges som om det ble handlet på det åpne marked. I tillegg fikk EU-kommisjonen også medhold i grunnlag for denne analysen, med domstolens uttalelser om referansesystem og vurderingsmetode.

Det er verdt å merke seg at Irland altså var på samme side som Apple i denne saken, som innebar at Irland heller ville stå ved de opprinnelige vedtakene enn å høste skattekravet som EU-kommisjonen mente lå der. Apple på sin side uttalte i en pressemelding at *"[t]his case was not about how much tax we pay, but where we are required to pay it."* Det er greit fra Apples perspektiv, og de fleste virksomheter vil ha et sterkt behov for forutberegnelighet når det er snakk om slike enorme pengesummer. Men innen EU vil nok denne saken innebære at diskusjonen om skattekonkurranse og skattelekkasjer vil stå sentralt på EUs dagsorden, uavhengig av OECD-initiativet beskrevet ovenfor. Den lave nasjonale virksomhetsbeskatningen for internasjonale aktører som etablerer seg i Irland, vil da stå sentralt. Selv om Applesaken i snever forstand var en sak om statsstøtte, understreker den virkningene av ulike beskatningsregler overfor internasjonale aktører. Vi kan altså konstatere at den siste utviklingen innenfor OECD og EU ikke synes å ha gjort veien frem mot et harmonisert skattesystem på dette området kortere. Den uttalte planen fra Finansdepartementet er at et utkast fra G20-landene skal foreligge i oktober[2], med en internasjonal løsning på plass ved utgangen av 2020. Det kan holde hardt.[3]

2 Finansminister Jan Tore Sanner, innlegg i Adresseavisen 08.08.2020

3 Artikkelforfatter jobber i Advokatfirmaet Schjødt AS, som har bistått Apple, blant annet i HR-2020-1142-A

Gorrissen Federspiel

Tue Goldschmieding

1. Datatilsynet udtaler alvorlig kritik efter offentliggørelse af personoplysninger på kommunes hjemmeside

Det danske Datatilsyn ('Datatilsynet') afsagde den 15. april 2020 afgørelse med journalnummer 2019-442-4873, i en sag vedrørende en dansk kommunes behandling af personoplysninger. Kommunen anmeldte den 1. november 2019 et brud på persondatasikkerheden til Datatilsynet. Kommunen blev den 18. oktober 2019, klokken 10.00, opmærksom på, at 15 høringssvar med personoplysninger var offentligt tilgængelige på kommunens hjemmeside. Kommunen har præciseret, at der i 11 af høringssvarene fremgik oplysninger om familier med børn på specialskole, og at der i 4 af høringssvarene fremgik oplysninger om personer med navne- og adressebeskyttelse.

Høringssvarene var tilgængelige på kommunens hjemmeside i perioden fra den 17. oktober 2019, klokken 09.52, hvor det første høringssvar blev uploadet på kommunens hjemmeside, til den 18. oktober 2019, klokken 21.00, hvor alle oplysningerne blev fjernet fra kommunens hjemmeside. På denne baggrund fandt Datatilsynet for det første, at kommunen ikke havde gennemført passende tekniske og organisatoriske foranstaltninger for at sikre et passende sikkerhedsniveau, jf. Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') artikel 32, stk. 1. For det andet fandt Datatilsynet, at kommunen ikke havde anmeldt det skete brud på persondatasikkerheden til Datatilsynet inden for den fastsatte frist, jf. databeskyttelsesforordningens artikel 33, stk. 1, og for det tredje, at kommunen ikke havde underrettet de berørte personer om bruddet på persondatasikkerheden, uden unødig forsinkelse, jf. databeskyttelsesforordningens artikel 34, stk. 1-2.

Ved afgørelsen lagde datatilsynet vægt på, at de oplysninger, der blev offentliggjort på hjemmesiden, var af beskyttelsesværdig karakter, idet der fremgik oplysninger om børns trivsel, diagnose og tilknytning til specialskole, samt oplysninger om navne og adressebeskyttelse. Datatilsynet konstaterede yderligere, at brud på persondatasikkerheden skal anmeldes inden for 72 timer, og at en overskridelse af denne frist kun kan begrundes i, at det ikke var muligt for den dataansvarlige at foretage anmeldelsen inden fristens udløb.

Læs hele afgørelsen her:
https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/apr/brud-paa-persondatasikkerheden-hos-randers-kommune/

2. Offentliggjorte klubblade med personoplysninger var ikke i strid med reglerne

Det danske datatilsyn ('Datatilsynet') afsagde den 8. juni 2020 afgørelse i sag med journalnummer 2019-31-2363 vedrørende offentliggørelse af Jyllinge Sejlklubs ('Sejlklubben') gamle klubblade.

Sagen blev indledt på baggrund af, at et klubmedlem klagede til Datatilsynet over, at vedkommendes navn, adresse, alder og billede fremgik af Sejlklubbens klubblade fra 1981 og 1982, idet Sejlklubben havde afvist at slette klagers oplysninger.

Vedrørende offentliggørelsen på internettet fandt Datatilsynet, at denne behandling af klagers personoplysninger var sket i overensstemmelse med interesseafvejningsreglen i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') artikel 6, stk. 1, litra f. Ved vurderingen lagde Datatilsynet blandt andet vægt på, at Sejlklubben havde en legitim interesse i at beskytte og informere om sin historie i en naturlig kontekst. Herudover lagde Datatilsynet vægt på, at klubbladene havde været tilgængelige i knap 40 år, og at der samtidig ikke var tale om følsomme oplysninger. Det forhold at klager har hemmelig adresse kunne ikke begrunde et andet resultat, idet adressen fra klubbladene ikke er identisk med klagers nuværende adresse.

I forhold til klagers anmodning om sletning af klagers oplysninger, fandt Datatilsynet, at Sejlklubben var berettiget til ikke at imødekomme anmodningen i overensstemmelse med databeskyttelsesforordningens artikel 17. Ved vurderingen lagde Datatilsynet vægt på, at det fortsat var nødvendigt for Sejlklubben at behandle klagers oplysninger, samt at behandlingen skete på lovligt grundlag.

Læs hele afgørelsen her:
https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/jun/offentliggoerelse-af-gamle-klubblade/

3. Manglende sletning af videooptagelser og billeder af tidligere medarbejder udløste alvorlig kritik fra Datatilsynet

Det danske datatilsyn ('Datatilsynet') afsagde den 18. maj 2020 afgørelse med journalnummer 2019-31-2316, i en sag vedrørende manglende sletning af videooptagelser og billeder af en tidligere medarbejder på internettet, efter vedkommende havde trukket sit samtykke tilbage. En tidligere medarbejder hos Dansk Miljørådgivning A/S ('DMR A/S') klagede over, at videooptagelser og billeder af vedkommende til brug for markedsføringsmateriale på DMR A/S' hjemmeside, Facebookside og YouTube, ikke blev slettet efter, at han havde henvendt sig til DMR A/S herom. Medarbejderen havde fulgt op på sine henvendelser om sletning, hvortil DMR A/S havde svaret samme dag, at de var i gang med at behandle hans anmodning. Syv dage efter opfølgningen, oplyste DMR A/S at de havde klippet billeder og videooptagelser af medarbejderen ud af noget af deres markedsføringsmateriale, men ikke ud af det hele, da de henviste til, at klageren havde givet skiftlig samtykke til, at billeder og videoer af ham måtte offentliggøres.

Datatilsynet fandt dog, at den tidligere medarbejders henvendelser skulle anses som om, at han havde trukket sit samtykke til behandling af personoplysninger tilbage, og dermed at DMR A/S ikke havde behandlet anmodning om sletningen i overensstemmelse med Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningens') artikel 17, stk. 1, litra b. Datatilsynet begrundede deres afgørelse med, at DMR A/S ikke uden unødig forsinkelse slettede oplysningerne om den tidligere medarbejder, da de ikke umiddelbart efter at samtykket var trukket tilbage foretog sletningen af billederne og videooptagelserne, som han fremgik i.

Der blev lagt vægt på, at den tidligere medarbejder havde oplyst overfor DMR A/S, at han ønskede de videooptagelser, som han fremgik i, slettet, og at DMR A/S havde tilkendegivet, at de ville foretage denne sletning fra det offentligt tilgængelige materiale, men at dette først skete med en betydelig forsinkelse. Datatilsynet har derfor udtalt alvorlig kritik af DMR A/S over deres behandling af personoplysningerne.

Læs hele afgørelsen her:
https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/maj/klage-over-manglende-sletning/

4. Datatilsynet fandt efter endt tilsyn ved Carlsberg Denmark A/S, at behandling af personoplysninger om ansøgere var sket i overensstemmelse med reglerne

Det danske Datatilsyn ('Datatilsynet') offentliggjorde den 25. maj 2020, at de havde afsluttet skriftligt tilsyn med Carlsberg Danmark A/S ('Carlsberg') med journalnummer 2019-41-0039. Tilsynet var sket med fokus på, hvordan Carlsberg opbevarede og slettede personoplysninger om ansøgere, der ikke blev ansat, og hvis oplysninger var indsamlet i forbindelse med rekrutteringsprocessen.

I forhold til Carlsbergs opbevaring af personoplysninger skete dette til to formål. For det første, som sikring af dokumentation i tilfælde af at der måtte komme klager over rekrutteringsforløbet. Dette var i overensstemmelse med Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') artikel 6, stk. 1, litra f om legitim interesse. For det andet, blev oplysningerne opbevaret med det formål at informere om fremtidige jobmuligheder i Carlsberg. Denne opbevaring skete på baggrund af samtykke, som blev indhentet via rekrutteringssystemet SuccesFactors. Herudover havde Carlsberg fremsendt et anonymiseret eksempel på en samtykkeerklæring, og opbevaringen var derfor lovlig i overensstemmelse med databeskyttelsesforordningens artikel 6, stk. 1, litra a.

Med hensyn til sletning af personoplysninger, var det i overensstemmelse med databeskyttelsesforordningen, at Carlsberg slettede oplysninger om ansøgere efter en periode på 6 måneder efter endt rekrutteringsforløb, jf. databeskyttelsesforordningens artikel 5, stk. 1, litra e, om opbevaringsbegrænsning, og artikel 5, stk. 2 om ansvarlighed.

På baggrund af ovenstående fandt Datatilsynet ikke anledning til at udtale kritik af Carlsbergs behandling af personoplysninger om ansøgere.

Læs hele afgørelsen her:
https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/maj/tilsyn-med-carlsberg-danmark-as-behandling-af-oplysninger-om-ansoegere/

5. EDPB opdaterer Artikel 29-gruppens vejledning om betingelserne for et gyldigt samtykke

Det Europæiske Databeskyttelsesråd ('EDPB') offentliggjorde den 4. maj 2020 en opdateret version af Artikel 29-gruppens vejledning om betingelserne for et gyldigt samtykke i henhold til Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen'). I de opdaterede retningslinjer præciserer EDPB en række forhold omkring betingelserne for at opnå et gyldigt samtykke, herunder gyldigheden af et samtykke fra den registrerede, når denne bliver mødt af såkaldte »cookie walls«, samt hvorvidt scrolling og swiping på en hjemmeside kan anses som gyldigt samtykke.

Begge punkter relaterer sig således til brugen af hjemmesider eller lignende. Mødet med cookie walls sker, hvor en bruger bliver nægtet adgang til en hjemmeside, hvis brugeren ikke giver samtykke til alle cookies på hjemmesiden. Et sådant

samtykke er, ifølge EDPD, ikke afgivet frivilligt, idet brugeren ikke bliver præsenteret for et reelt valg. Et sådant samtykke vil ifølge retningslinjerne ikke være gyldigt.

Det andet punkt præciserer, at scrolling og swiping på ingen måde kan udgøre en klar bekræftelse i, at den pågældendes personoplysninger gøres til genstand for behandling, hvorfor en sådan handling ikke kan anses som en utvetydig viljestilkendegivelse.

Læs hele vejledningen her: *https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202 005_consent_en.pdf*

6. Virksomhed indstilles til bøde for krænkelse af databeskyttelsesforordningen

Det danske datatilsyn ('Datatilsynet') vurderede den 15. maj 2020, at virksomheden JobTeam A/S havde handlet i strid med god databehandlingsskik.

Virksomheden havde, efter at have modtaget en indsigtsanmodning fra en registreret, slettet de pågældende oplysninger, førend virksomheden havde svaret den registrerede. Dette afskar den registrerede fra at kunne få prøvet sin indsigtsanmodning ved Datatilsynet eller domstolene, og var derfor i strid med Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen'). Behandlingen af personoplysningerne havde ikke været lovlig, rimelig eller været foregået på en gennemsigtig måde.

Den registrerede klagede herefter til Datatilsynet. På denne baggrund har Datatilsynet politianmeldt JobTeam A/S og indstillet virksomheden til en bøde på 50.000 danske kroner. Det er herefter op til politiet at undersøge, om der er grundlag for at rejse en sigtelse i sagen. Spørgsmålet om en eventuel bøde vil i så fald blive endeligt afgjort ved domstolene.

Læs hele udtalelsen her: *https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/maj/jobteam-indstillet-til-boede/*

7. Datatilsynet udtaler alvorlig kritik af kommune for mangelfulde kontrolforanstaltninger

Det danske datatilsyn ('Datatilsynet') traf den 22. april 2020 afgørelse i j.nr. 2019-442-4365, vedrørende Kolding Kommunes behandling af personoplysninger. Datatilsynet udtalte i sagen alvorlig kritik af Kolding Kommunes behandling af personoplysninger, idet kommunens behandling var sket uden passende tekniske og organisatoriske foranstaltninger som foreskrevet i artikel 32, stk. 1 i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen').

Den 30. september 2019 anmeldte Kolding Kommune et brud på persondatasikkerheden til Datatilsynet. Sikkerhedsbruddet vedrørte kommunens elektroniske sags-og dokumenthåndteringssystem, Acadre, ('ESDH'), som kommunen siden 2012 havde anvendt til behandling af dokumenter indeholdende personoplysninger. Dokumenterne angik ca. 400.000 sager.

Sikkerhedsbruddet blev opdaget ved en intern kontrol den 17. september 2019 og havde stået på i cirka syv et halvt år. Bruddet indebar, at kommunens ca. 2400 ansatte i perioden havde haft en utilsigtet adgang til dokumenter, der under normale forhold alene kunne tilgås via ESDH-dokumentserveren. Derudover, var deres adgang til dokumenterne ikke blevet logget.

Datatilsynet anførte i deres afgørelse, at det måtte anses for særlig relevant, at der er etableret procedurer for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerheden.

Datatilsynet lagde ved denne vurdering vægt på, at kommuner behandler store mængder personoplysninger om mange registrerede, herunder også oplysninger omfattet af databeskyttelsesforordningens artikel 9, om behandling af særlige kategorier af personoplysninger, og at risikoen for de registrerede ved tab af f.eks. fortrolighed generelt måtte antages at være høj.

Hvad angik kontrol havde Kolding Kommune oplyst over for Datatilsynet, at det ikke havde været muligt at konstatere fejlen under daglig brug, og at der ikke forud for scanningen den 17. september 2019 var foretaget intern scanning af netværket for åbne fildrev. Kolding Kommune havde dog fået udført revisioner i årene 2016, 2017 og 2018. De pågældende revisioner angik primært kommunes generelle it-kontroller og it-systemer af betydning for regnskabsområdet, hvorfor hverken kommunens EDHS-system eller it-infrastruktur som helhed havde været direkte omfattet.

Vedrørende revision eller periodisk kontrol, udtalte Datatilsynet, at revision efter omstændighederne også skal omfatte kontrol af en organisations centrale it-infrastruktur, der understøtter adgangen til primære administrative systemer, som f.eks. ESDH-systemer, og at mangel på sådan periodisk kontrol efter Datatilsynets opfattelse indebærer en unødig høj risiko for, at utilstrækkelige eller mangelfulde sikkerhedsforanstaltninger ikke identificeres rettidigt.

Datatilsynet fandt, at Kolding Kommune hverken havde gennemført eller haft procedurer for regelmæssig afprøvning, vurdering og evaluering af de etablerede foranstaltninger i relation til kommunens it-infrastruktur med henblik på at etablere et passende sikkerhedsniveau som foreskrevet i databeskyttelsesforordningens artikel 32, stk. 1, og at der derfor var grundlag for at udtale alvorlig kritik af Kolding

Kommunes behandling af personoplysninger.

Afslutningsvist anførte Datatilsynet, at de havde noteret sig Kolding Kommunes oplysning om at kommunen fremover bl.a. ville foretage scanninger efter åbne drev på netværket som del af GDPR-årshjulet og kommunens arbejde med implementering af ISO27 000 og ISO27 701.

Læs hele afgørelsen her:

https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/apr/kolding-kommune-havde-ikke-truffet-passende-tekniske-og-organisatoriske-foranstaltninger/

8. Datatilsynet udtaler alvorlig kritik og meddeler påbud for virksomheds mangelfulde risikovurdering

Det danske datatilsyn ('Datatilsynet') traf den 5. marts 2020 afgørelse i j.nr. 2019-441-3399, 2019-441-4055 og 2019-441-4160 under j.nr. 2019-441-3399, vedrørende brud på persondatasikkerheden i BroBizz A/S ('BroBizz'). Datatilsynet udtalte i sagen alvorlig kritik af, at BroBizz' behandling af personoplysninger ikke fandtes at være sket i overensstemmelse med artikel 32, stk. 1 og stk. 2 i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen'), og fandt endvidere grundlag for at medelle BroBizz påbud om foretagelse af en risikovurdering.

Sagen udsprang af tre anmeldelser af brud på persondatasikkerheden fra BroBizz j.nr. 2019-441-3399, 2019-441-4055 og 2019-441-4160 af henholdsvis 20. september, 29. november og 12. december 2019.

Anmeldelsen af 20. september 2019 vedrørte BroBizz' kundeservices videregivelse af personoplysninger, herunder oplysninger om lokation, vedrørende en kunde og dennes to passagerer til en uvedkommende person, som var kundens ekskæreste, efter personen til BroBizz alene havde oplyst kundens telefonnummer. Anmeldelserne af 29. november og 12. december 2019 vedrørte to hændelser, hvor BroBizz' kundeservice, i forbindelse med kundehenvendelser, havde overført adgangen til en kundes konti til en anden uvedkommende kunde, grundet henholdsvis en manuel fejl fra en medarbejder i kundeservice og at identitetsverifikationen alene skete på baggrund af et kundenummer.

Datatilsynet lagde i sagen til grund, at BroBizz ved de tre hændelser havde videregivet personoplysninger til uvedkommende personer grundet manglende identitetsverifikation og foretog en vurdering af BroBizz' behandlings overensstemmelse med databeskyttelsesforordningens artikel 32, stk. 1, om passende tekniske og organisatoriske foranstaltninger.

Ved vurderingen tillagde Datatilsynet det vægt, at den samme type hændelse var forekommet hos BroBizz tre gange på to en halv måned, samt at der bl.a. var blevet videregivet oplysninger om lokation, hvilket Datatilsynet fandt indebar en forholdsvis høj risiko for de registreredes rettigheder. Datatilsynet tillagde det endvidere vægt, at BroBizz' uddannelse og træning af medarbejderne i databeskyttelse fandtes at være utilstrækkelig. Datatilsynet hæftede sig bl.a. ved, at kundeservicemedarbejdernes løbende uddannelse foregik på ad hoc basis.

Datatilsynet fandt på baggrund af ovenstående, at BroBizz, ved deres behandling af personoplysninger, ikke havde truffet passende tekniske og organisatoriske foranstaltninger i overensstemmelse med databeskyttelsesforordningens artikel 32, stk. 1.

Datatilsynet vurderede endvidere under sagen en af BroBizz fremsendt risikovurdering for general verificering af kunder. Datatilsynet anførte indledningsvist om databeskyttelsesforordningens artikel 32, stk. 2, vedrørende vurderingen af passende sikkerhedsniveau, at risikovurderingen burde tage udgangspunkt i risici for de registrerede og ikke risici for den dataansvarlige.

Datatilsynet fandt i forlængelse heraf, at risikovurderingen fra BroBizz alene omhandlede hændelsen i sig selv og ikke de risici en videregivelse til uvedkommende kunne udgøre for de registreredes rettigheder, og at BroBizz' vurdering af hvilket sikkerhedsniveau, der var passende, dermed ikke var foretaget i overensstemmelse med databeskyttelsesforordningens artikel 32, stk. 2.

Ved vurderingen hæftede Datatilsynet sig bl.a. ved BroBizz' mangel på dokumentation for deres vurdering af sandsynligheden for »behandling af kundehenvendelser uden verificering« som værende »meget lille«. Datatilsynet fandt endvidere, at angivelsen af »medarbejder følger instruks/proces« som forbyggende handling var utilstrækkelig, og at angivelsen af »kundeinfo oplyses til forkert kunde/ej kunde« som konsekvensen for kunden var mangelfuld med henvisning til et mangel på eksempler som fx risici for identitetstyveri eller chikane og stalking i lyset af den konkrete hændelse, hvor den registreredes lokation var blevet videregivet til dennes ekskæreste.

Datatilsynet fandt på baggrund af uoverensstemmelserne med artikel 32, stk. 1 og stk. 2, i databeskyttelsesforordningen, grundlag for at udtale alvorlig kritik af BroBizz' behandling af personoplysninger. Datatilsynet fandt endvidere grundlag for at meddele BroBizz påbud om at foretage en ny risikovurdering for verificering af kunder i overensstemmelse med databeskyttelsesforordningens artikel 32, stk. 2, inden for en frist af 4 uger.

Datatilsynet anførte i forlængelse af deres påbud, at risikovurderingen skulle indeholde en kortlægning over risici for de registreredes rettigheder samt en afvejning af risiciene i forhold til forholdsreglerne truffet for at beskytte de registreredes ret-

tighederne og henviste endvidere til Datatilsynets og Rådet for Digital Sikkerheds Vejledende tekst om risikovurdering, af juni 2019, for yderligere vejledning.

Læs hele afgørelsen her:

https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/mar/risikovurdering-ved-videregivelse-af-personoplysninger/

Læs Datatilsynets og Rådet for Digital Sikkerheds Vejledende tekst om risikovurdering her:

https://www.datatilsynet.dk/media/7697/vejledende-tekst-om-risikovurdering.pdf

9. Test af monitoreringsprogrammet'Den Digitale Prøvevagt' affødte alvorlig kritik fra Datatilsynet

Det danske datatilsyn ('Datatilsynet') afsagde den 6. marts 2020 afgørelse med journalnummer 2019-432-0020. Sagen vedrørte Styrelsen for IT og Lærings ('STIL') test af monitoreringsprogrammet, Den Digitale Prøvevagt, der blev gennemført den 7. marts 2019. Datatilsynet udtalte alvorlig kritik af STIL, idet STIL ikke havde gennemført foranstaltninger, der var passende for det efterfølgende identificerede risikoniveau, jf. Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') artikel 32.

I forbindelse med generalprøven den 7. marts 2019, installerede ca. 8.000 elever frivilligt programmet, Den Digitale Prøvevagt, hvorved der blev behandlet personoplysninger om disse elever. Programmet har til formål at sikre, at prøver og eksamener ved gymnasiale institutioner er objektive og fair.

STIL havde ikke inden generalprøven lavet en risikovurdering som foreskrevet i databeskyttelsesforordningens artikel 32. I en efterfølgende risikovurdering fandt STIL, at den implementerede sikkerhed var utilstrækkelig. Datatilsynet fandt af denne grund, at STIL ved generalprøven ikke havde gennemført foranstaltninger, der var passede for det efterfølgende identificerede risikoniveau, og STIL havde derfor ikke levet op til databeskyttelsesforordningens artikel 32, hvorfor Datatilsynet udtalte alvorlig kritik.

Herudover, gav afgørelsen Datatilsynet anledning til at indskærpe, at en risikovurdering, med formål om at identificere det passende sikkerhedsniveau, skal foretages inden behandlingen af personoplysninger påbegyndes.

Idet udviklingen af programmet er sat i bero, og STIL har besluttet at foretage en ny særskilt risikovurdering inden ibrugtagning, fandt Datatilsynet ikke grundlag for at tage stilling til behandling af personoplysninger ved brug af programmet fremadrettet.

Læs hele afgørelsen her:

https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/mar/den-digitale-proevevagt/

10. Advokatnævnet havde ikke iagttaget oplysningspligt over for indklaget advokat

Det danske datatilsyn ('Datatilsynet') traf den 22. maj 2020 afgørelse i en sag vedrørende oplysningspligten i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') artikel 14, stk. 3, litra a, jf. stk. 1 og stk. 2. I afgørelsen udtalte Datatilsynet kritik af, at det danske advokatnævn ('Advokatnævnet') først orienterede en advokat mere end 5 måneder efter indsamlingen af vedkommendes personoplysninger.

Sagen udsprang af en klage til Datatilsynet fra en advokat vedrørende Advokatnævnets behandling af advokatens personoplysninger. Advokatnævnet modtog en klage over advokaten den 14. juni 2018, hvorefter Advokatnævnet behandlede advokatens personoplysninger. Advokaten blev orienteret herom den 28. november 2018. Datatilsynet fandt, at det forhold at Advokatnævnet havde udskudt orienteringen af hensyn til at få sagen oplyst tilstrækkeligt, bl.a. under hensyn til advokatens mulighed for kommentere på sagen, ikke kunne undtage Advokatnævnet fra sin oplysningspligt i medfør af databeskyttelsesforordningens artikel 14, stk. 5, litra a-d om undtagelserne til oplysningsforpligtelsen.

Advokatnævnet havde således ikke orienteret advokaten inden for en rimelig frist, hvorfor Advokatnævnet ikke havde opfyldt sin oplysningspligt over for den indklagede advokat.

Læs hele afgørelsen her:

https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/maj/manglende-opfyldelse-af-oplysningspligt

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

Delphi

Erik Ålander

Datainspektionen om bostadsrättsföreningars möjlighet att tillämpa kamerabevakning

Den svenska Datainspektionen har under de senaste två åren mottagit en stor mängd frågor och klagomål avseende bostadsrättsföreningars kamerabevakning. Datainspektionen har under våren 2020 granskat en förenings kamerabevakning och fattade den 16 juni 2020 ett beslut som bör ses som vägledande för hur svenska bostadsrättsföreningar bör förhålla sig till kamerabevakning framöver (DI-2018-14 593).

Bostadsrättsföreningen ifråga har under en period om ca två år övervakat entré, trapphus samt en el-central i anslutning till fastighetens källarförråd. Sammantaget har fyra kameror upptagit bild och ljud dygnet runt. Bostadsrättsföreningen har uppgett att ändamålet för kamerabevakningen var att komma tillrätta med återkommande skadegörelse i fastigheten.

Datainspektionens bedömning

Datainspektionen konstaterar att ändamålet för kamerabevakningen är att anses som ett berättigat ändamål samt att bostadsrättsföreningen efterlever principen om ändamålsbegräsning. Datainspektionens utredning är därefter centrerad kring principen om uppgiftsminimering samt avvägningen som bostadsrättsföreningen har att göra inom ramen för en intresseavvägning som tillämplig rättslig grund.

Datainspektionen konstaterar att kamerabevakning av entré och trapphus i flerbostadshus möjliggör en kartläggning av de boendes vanor, besök och umgängeskrets samt avser deras hemmiljö. Datainspektionen påpekar att detta innebär att det krävs synnerligen starka skäl för att kamerabevakningen ska vara tillåten. Datainspektionen framhåller att skadegörelse och annan brottslighet kan utgöra sådana skäl. Dock poängterar Datainspektionen att bevakningen måste vara nödvändig för att uppfylla ändamålet vid inspelningstillfället. Behovet av kamerabevakning ska därför omprövas var sjätte månad. I det aktuella fallet hade inga incidenter inträffat i fastigheten sedan kamerorna sattes upp. Datainspektionen fastslår därför att de registrerades intresse av att inte bli bevakade väger tyngre än föreningens bevakningsintresse och att föreningen därför inte har rättslig grund för behandlingen av de personuppgifter som samlas in genom bildupptagning av trapphus och entré. Bevakningen av el-centralen bedömdes dock som nödvändig för att uppfylla ändamålet. Datainspektionen konstaterar att el-centralens placering i ett låst källarutrymme där de boende endast rör sig i begränsad omfattningen talar för att integritetsintresset väger relativt lätt i anslutning till el-centralen. Bostadsrättsföreningen förelades dock att rikta om kameran då upptagningsområdet även omfattade delar av källarförråden. Datainspektionen framhåller att även behovet av bevakning av el-centralen ska omprövas var sjätte månad.

Vidare konstaterar Datainspektionen att ljudupptagning ska anses som särskilt integritetskänsligt. Datainspektionen anser dessutom att ljudupptagning inte är nödvändig för att uppnå ändamålet med kamerabevakningen. Mot bakgrund av ovan anser Datainspektionen sammantaget att föreningens ljudinspelning saknar rättslig grund och strider mot principen om uppgiftsminimering. Datainspektionen framhåller även att den information som föreningen tillhandahåller förvisso upplyser om att kamerabevakning bedrivs genom en skylt i fastigheten, men att informationen på skylten inte är tillräcklig för att uppnå kraven enligt artikel 13 i dataskyddsförordningen.

Mot bakgrund av ovan förelades bostadsrättsföreningen att upphöra med kamerabevakningen i trapphus och entré, justera bevakningen av el-centralen samt betala en administrativ sanktionsavgift om SEK 20 000.

Sammanfattningsvis kan det konstateras att det krävs starka skäl för att en bostadsrättsförenings kamerabevakning ska vara förenlig med dataskyddsförordningen. Vidare ska bostadsrättsföreningen ompröva behovet av bevakning var sjätte månad samt tillse att boende och besökare tillhandahålls med adekvat information avseende kamerabevakningen och föreningens behandling av de registrerades personuppgifter.

Erik Ålander arbetar främst med kommersiella avtal, samt fintech och integritetsfrågor i Advokatfirman Delphis Stockholmskontor i byråns Corporate Commercial-grupp.


Rune Opdahl og Pernille Gjerde Lia

Privacy Shield underkjent

Den 16. juli 2020 avsa EU-domstolen avgjørelsen omtalt som Schrems II (C-311/18). I denne dommen ugyldiggjør EU-domstolen EU-US Privacy Shield, en ordning ment å sikre trygg overføring av personopplysninger fra EØS til USA. EU-domstolen anerkjenner at standard personvernbestemmelser (SCC) fremdeles kan være et gyldig overføringsgrunnlag til tredjestater, men går likevel langt i å slå bena under også denne ordningen.

Privacy Shield

Under Privacy Shield-ordningen kunne personopplysninger overføres til mottakere i USA som var sertifisert i henhold til rammeverket. Ved Schrems II ugyldiggjør EU-domstolen denne ordningen med umiddelbar virkning.

Begrunnelsen for at EU-domstolen anser Privacy Shield å være ugyldig, er at ordningens regulering viker for USAs nasjonale sikkerhet, offentlige interesser og rettshåndhevelse, og at det kan ikke konstateres et tilstrekkelig beskyttelsesnivå i henhold til europeiske personvernregler, særlig kravet til proporsjonalitetsbetraktninger, de registrertes håndhevingsmuligheter og rett til domstolsbeskyttelse.

Forgjengeren til Privacy Shield, Safe Harbour-ordningen, ble ugyldiggjort av EU-domstolen ved den opprinnelige Schrems-avgjørelsen. Begge de to Schrems-avgjørelsene knytter seg i stor grad til USAs sikkerhetslover og manglende mulighet til å overprøve disse, som oppleves problematisk i henhold til europeisk personvernlovgivning.

Standard personvernbestemmelser

I Schrems II anser EU-domstolen EUs dataoverføringsavtaler, ofte omtalt som «Model Clauses» eller «Standard Contractual Clauses» (SCC) som gyldig, men fremhever at gyldighet avhenger av at det sikres et tilstrekkelig beskyttelsesnivå som må være tilnærmet likt det som gis under GDPR. Faktorer som reduserer beskyttelsesnivået i en tredjestat er særlig nasjonale regler som gir myndighetene tilgang til data, og manglende muligheter for å håndheve registrertes rettigheter etter GDPR.

En eksportør må dermed vurdere om det rettslige regimet i mottakerlandet gir tilstrekkelig beskyttelse av personopplysninger. Dette skaper åpenbare utfordringer for en eksportør, som enten må tilegne seg inngående kjennskap til nasjonal rett i et mottakerland, eller stole på en importør for disse vurderingene. I tillegg er nasjonal sikkerhetslovgivning særlig relevant for en slik vurdering, en lovgivning som ikke alltid er lett tilgjengelig.

Hvis mottakerlandet ikke har et tilstrekkelig beskyttelsesnivå, påpekes det at det må tas stilling til de øvrige omstendighetene ved overføringen og eventuelle supplerende tiltak, uten at dette forklares nærmere. Hvis omstendighetene og tiltakene ikke gjør at opplysningene beskyttes på et nivå som er tilnærmet likt beskyttelsesnivået under GDPR, kan ikke overføringen finne sted.

Konsekvenser

Schrems II-avgjørelsen har umiddelbar betydning for all eksport av personopplysninger til USA. Overføring basert på Privacy Shield-ordningen må enten stanses eller baseres på et nytt overføringsgrunnlag. I tillegg har EU-domstolen eksplisitt pekt på amerikanske overvåkningslover som uforenlig med beskyttelsesnivået som kreves under GDPR. Dette betyr at overføringer til USA med andre overføringsgrunnlag, slik som SCC, må vurderes i lys av om det sikrer et tilstrekkelig beskyttelsesnivå.

Avgjørelsen har også generell betydning for all eksport av personopplysninger til andre tredjestater som baserer seg på SCC. EU-domstolen fremhever at SCC ikke i seg selv sikrer et tilstrekkelig beskyttelsesnivå, og at eksportøren derfor må foreta en konkret vurdering ved slike overføringer. Det må antas at Schrems II særlig vil innebære at overføring til land som blant annet Russland og Kina vil kreve supplerende tiltak for å sikre et tilstrekke-

lig beskyttelsesnivå. Her kan det også tenkes at selve vurderingen vil by på utfordringer, ettersom den nasjonale sikkerhetslovgivningen i disse landene trolig er mindre tilgjengelig for den gjengse eksportør enn tilfellet er for USA. Amerikansk sikkerhetslovgivning har blitt grundig belyst i EU-systemet gjennom flere saker for EU-domstolen.

Schrems II innebærer dermed at EU-retten igjen går utover sine bredder. Den vil kunne føre til at visse tredjestater vil løfte sitt personvern nærmere et europeisk beskyttelsesnivå for å tilrettelegge for fortsatt flyt av personopplysninger. Den vil også kunne føre til mindre økonomisk samarbeid mellom EØS og andre land, som det transatlantiske økonomiske samarbeidet, hvis aktører i EØS blir tilbakeholdne med å overføre data utenfor EØS.

Inntil videre vil det tryggeste alternativet for aktører i EØS være å finne leverandører innen EØS der dette er mulig. Imidlertid vil et slikt alternativ for mange være vanskelig å gjennomføre, enten av tekniske/praktiske eller økonomiske årsaker. Da må man, som nevnt, vurdere om omstendighetene og eventuelle tiltak likevel gjør at opplysninger som overføres til et tredjeland underlegges en beskyttelse som er tilnærmet lik den som gis under GDPR.

Relevante omstendigheter vil muligens kunne være opplysningenes karakter. Eksempelvis kan man tenke seg at overføring av trivielle data, eller data som for øvrig er offentlig tilgjengelig, kan finne sted. En annen relevant omstendighet vil potensielt kunne være at overføring kun skjer flyktig ved support o.l. som utføres av personell i et tredjeland, men at opplysningene ikke lagres der.

Supplerende tiltak kan tenkes å være kontraktuelle forpliktelser mellom eksportøren og importøren, slik som forpliktelser til rapportering ved myndighetsforespørsler. En eksportør og importør kan imidlertid ikke binde nasjonale myndigheter, og i den grad supplerende tiltak er ment å avbøte potensielle aktiviteter fra nasjonale myndigheter, vil det isteden være mer nærliggende å iverksette tiltak i form av tekniske virkemidler. Dette kan for eksempel kunne være kryptering, hvor krypteringsnøkler befinner seg i Europa, eller pseudonymisering av personopplysninger, hvor identifikatorene befinner seg i Europa.

Det forventes at europeiske personvernmyndigheter vil gi ytterligere veiledning om relevante omstendigheter og supplerende tiltak som kan tilsi at overføringen er lovlig. Inntil videre er hver behandlingsansvarlig overlatt til å foreta sine egne vurderinger, noe som er utilfredsstillende.

Rune Opdahl er partner i Wiersholms team for teknologi, person og immaterielle rettigheter.

Pernille Gjerde Lia jobber særlig med saker relatert til personvern, teknologi og immaterielle rettigheter som advokatfullmektig i Wiersholm.

Gorrissen Federspiel

Tue Goldschmieding

1. Keramiker tilkendt vederlag og erstatning efter supermarkedskædes krænkende brug

Den danske Østre Landsret ('Landsretten') afsagde den 11. juni 2020 dom i sagen BS-48 928/2019-OLR mellem Salling Group A/S ('Salling Group') og Anne Black ApS ('Anne Black').

Sagen angik, hvorvidt 3 af Anne Blacks produkter var beskyttet efter henholdsvis lovbekendtgørelse nr. 1144 af 23. oktober 2014 ('den danske ophavsretslov') og/eller lov nr. 426 af 3. maj 2017 ('den danske markedsføringslov'), og hvorvidt Salling Group ved i 2016 at have markedsført og solgt en hængepotte, en vase, og en lågkrukke, krænkede Anna Blacks beskyttelse. Efter den danske ophavsretslov § 1, stk. 1, og EU-domstolens dom i sag C-683/17, Cofemel, skal et værk være resultatet af ophavsmandens »egen intellektuelle frembringelse« og være »resultatet af et frit valg foretaget af designeren«, førend det er ophavsretligt beskyttet. Efter den danske markedsføringslov § 3, skal erhvervsdrivende udvise god markedsføringsskik blandt andet under hensyntagen til andre erhvervsdrivende, hvilket indebærer et forbud mod krænkende markedsføringsforanstaltninger.

Landsretten fandt, at hængepottens design var udtryk for Anne Blacks egen intellektuelle frembringelse, og at denne derfor var beskyttet efter både den danske ophavsretslovs § 1, stk. 1 og den danske markedsføringslovs § 3. Vasen og lågkrukken levede derimod ikke op til kravene for beskyttelse efter ophavsretslovens § 1, stk. 1, hvorfor disse kun nød beskyttelse efter markedsføringslovens § 3. Der forelå derfor både krænkelser af ophavsretslovens § 1, stk. 1 og markedsføringslovens § 3.

Den danske Sø- og Handelsret havde ved tidligere dom i samme sag tilkendt 1.500.000 danske kroner til Anna Black i vederlag og erstatning. På baggrund af usikkerhed angående størrelsen af det tab, som Anne Black havde lidt, fandt Landsretten, at vederlaget og erstatningen samlet ikke kunne fastsættes til et højere beløb end 300.000 danske kroner.

Læs hele udtalelsen her:
https://domstol.dk/media/kbui514w/dom-sambehandling.pdf

2. Højesteret fandt at gummistøvle ikke nød beskyttelse efter ophavsretsloven eller markedsføringsloven

Den danske højesteret ('Højesteret') afsagde den 10. juni 2020 dom i sagen BS-7741/2019-HJR mellem IJH A/S ('IJH') og Morsø Sko Import A/S ('Morsø'). Sagen angik spørgsmålet, om hvorvidt en af IJH udarbejdet gummistøvle kunne anses for en sådan selvstændig og kreativ frembringelse, at den nød beskyttelse efter lovbekendtgørelse nr. 1144 af 23. oktober 2014 ('den danske ophavsretslov') eller lov nr. 426 af 3. maj 2017 ('den danske markedsføringslov').

Stifter og ejer af IJH, Ilse Jacobsen, havde skabt gummistøvlen »RUB 1«, som efter eget udsagn skulle være trendy, således at den kunne bruges til andet end blot at holde fødderne tørre i regnvejr. RUB 1 gummistøvlen var sammensat af 27 dele, som ved manuelt håndarbejde var sat sammen i en vanskelig og fordyrende fremstillingsproces. Morsø havde solgt lignende gummistøvler til Dansk Supermarked, der efterfølgende blev sat til salg i blandt andet Bilka til en pris på 199 kr. Højesteret skulle på den baggrund tage stilling til, om RUB 1 kunne betegnes som et værk efter den danske ophavsretslovs § 1, subsidiært om der var tale om en krænkelse efter den danske markedsføringslovs § 3 om god markedsføringsskik.

For så vidt angår den ophavsretlige bedømmelse, henviste Højesteret til EU-Domstolens synspunkter i sagen C-683/17 (Cofemel), hvorefter det ikke er tilstrækkeligt til at blive kvalificeret som et værk, at produktet frembringer en særegen og karakteristisk effekt set ud fra en æstetisk synsvinkel, heller ikke selvom produktet er frugten af innovative fremstillingskoncepter og -processer i branchen. Med afsæt i samme betragtninger, fandt Højesteret, at RUB 1 ikke kunne betegnes som et værk. For så vidt angår gummistøvlens beskyttelse efter den danske markedsføringslov, tiltrådte Højesteret Sø- og Handelsretten og Landsrettens vurderinger og fandt, at de to gummistøvler var forskellige både med hensyn til deres kvalitet, produktidentitet og designmæssige udtryk, hvorfor der ikke var tale om en krænkelse efter den danske markedsføringslov.

Læs hele udtalelsen her:
http://domstol.fe1.tangora.com/media/-300 016/files/7741-19-dom.pdf?rev1

3. Forbrugerombudsmanden indskærpede kravet om, at rigtigheden af faktiske påstande skal kunne dokumenteres

Den danske forbrugerombudsmand ('Forbrugerombudsmanden') indskærpede den 27. april 2020 over for to erhvervsdrivende, at rigtigheden af markedsføring med sundhedsegenskaber skal kunne dokumenteres af den erhvervsdrivende.

Forbrugerombudsmanden vurderede, at to erhvervsdrivendes markedsføring på henholdsvis Instagram og Facebook med sundhedsmæssige udsagn som »hot yoga strengthen your immune system by over 60%, that is a fact«, og udsagn om, at deres produkt »vitaliserer lunge-og luftvejssystem. Et naturligt valg til at hjælpe dig i disse tider med Corona virus«, var i strid med lov nr. 426 af den 3. maj 2017 ('den danske markedsføringslov') § 5, sammenholdt med § 8, om forbud mod vildledende handlinger, og væsentlig forvridning af den økonomiske adfærd.

De erhvervsdrivende kunne ikke dokumentere rigtigheden af deres sundhedsmæssige udsagn i opslagene på henholdsvis Instagram og Facebook, hvilket er et krav efter den danske markedsføringslov § 13 om oplysningsforpligtelsen.

Forbrugerombudsmanden indskærpede derfor over for de erhvervsdrivende, at når de anvender faktiske oplysninger i deres markedsføring, skal de kunne dokumentere rigtigheden heraf, jf. den danske markedsføringslovs § 13, da der ellers vil være tale om vildledende markedsføring efter den danske markedsføringslovs § 5, stk. 1, sammenholdt med § 8.

Læs hele udtalelsen her:
https://www.forbrugerombudsmanden.dk/find-sager/markedsfoeringsloven/sager-efter-markedsfoeringsloven/vildledning/indskaerpelser-for-vildledende-markedsfoering-ved-brug-af-udokumenterede-udsagn-om-sundhedsegenskaber/

4. Fibernet-udbyder politianmeldt for spam udsendt over e-boks

Den danske forbrugerombudsmand ('Forbrugerombudsmanden') udtalte i en pressemeddelelse fra 6. maj 2020, at en virksomhed er politianmeldt for at overtræde spamforbuddet i lov nr. 426 af 3. maj 2017 ('den danske markedsføringslov') § 10, stk. 1.

Virksomheden, som udbyder fibernet, havde i samarbejde med en række kommuner udsendt uanmodede henvendelser til en række borgere over e-boks omkring tilslutning til et forestående fibernet-projekt. Forbrugerombudsmanden vurderede, at kommunerne havde udsendt brevene på foranledning af virksomheden, som både var kommet med tekstforslag og adresselister for modtagerne af brevene.

Spamforbuddet i den danske markedsføringslovs § 10, stk. 1 forbyder erhvervsdrivende at rette elektroniske henvendelser i markedsføringsmæssigt øjemed, når modtageren ikke forinden har samtykket til henvendelsen.

Virksomheden har accepteret at betale en bøde på 964.600 danske kroner. Bøden er udmålt efter antallet af spammails ud fra standardtaksten for overtrædelser af spamforbuddet.

Læs hele udtalelsen her:
https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2020/forbrugerombudsmanden-har-politianmeldt-fibia-for-spam/

5. Butikskæde skal betale millionbøde for vildledende prismarkedsføring

Den danske Forbrugerombudsmand ('Forbrugerombudsmanden') udtalte den 23. april 2020, at butikskæden Bilka i flere tilfælde havde vildledt forbrugerne ved markedsføring af besparelser, der ikke var reelle. Bilka har accepteret at betale en bøde på 3 millioner danske kroner.

Den konkrete sag omhandlede forbuddet mod vildledende handlinger i lov nr. 426 af 3. maj 2017 ('den danske markedsføringslov') § 5. Bilkas markedsføring af grill, cykler og støvsugere var sket til urealistiske normalpriser, da de i næsten et år vedvarende var blevet markedsført med besparelser på over 50 procent.

Forbrugerombudsmanden vurderede blandt andet, at prisen for en grill ikke var reel, da den kunne købes inklusiv udstyr for over 10.000 kr. mindre. Idet ingen forbruger i sådan en situation ville købe grillen til normalprisen, kunne denne pris ikke danne grundlag for prissammenligningen. Herved var der sket vildledende prismarkedsføring.

Læs hele udtalelsen her:
https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2020/bilka-accepterer-boede-paa-tre-millioner-kroner/

6. Der var ikke søgsmålskompetence til at føre sag om ulovlig filmdeling, da sagsøger hverken var producent eller distributør af film

Den danske Østre Landsret ('Landsretten') afsagde den 8. april dom i sagen Ø.L.D. 8. april 2020 i anke 10. afd. BS-39 423/2019-OLR mellem privatpersonen B og et engelsk indregistreret selskab ('A Ltd'). Sagen angik download og deling af en ophavsretligt beskyttet film via en fildelingstjeneste. I sagen skulle Landsretten tage stilling til om A, der hverken var producent eller distributør af filmen, havde søgsmålskompetence til at føre sagen i eget navn.

A Ltd havde under sagen i byretten nedlagt påstand om, at B skulle betale 7.500 kr. for at have foretaget download og fildeling af filmen i strid med lovbekendtgørelse

nr. 1144 af 23. oktober 2014 ('den danske ophavsretslov'). B blev i byretten dømt til at betale de 7.500 kr. og ankede med Procesbevillingsnævnets tilladelse dommen til Landsretten. B gjorde under sagen i Landsretten gældende, at A Ltd ikke havde dokumenteret at være berettiget til at påtale krænkelser af filmen og således ikke var berettiget til at anlægge sagen. Hertil gjorde A Ltd gældende, at selskabet ved aftale havde erhvervet påtaleret for krænkelsen og dermed havde søgsmålskompetence i sagen.

Landsretten fandt, at A Ltd ikke havde bevist, at det ved aftalen havde opnået søgsmålskompetence til at føre sagen i eget navn. Landsretten henviste til, at aftalen alene antog A Ltd. til at håndtere retssager til håndhævelse af ophavsrettigheder, og altså ikke overdrog nogen rettigheder, herunder en påtaleret, til denne. På denne baggrund ophævede Landsretten byrettens dom og afviste sagen fra domstolene.

Læs hele dommen (U.2020.2014 Ø) her (med login):

https://pro.karnovgroup.dk/document/7 000 850 517/1#AFGR_2020-0410-1

7. Formen på en type chips kunne ikke udgøre et tredimensionelt varemærke

Den 27. april 2020 afsagde den danske Sø- og Handelsret ('Sø- og Handelsretten') dom i sagen BS-17 352/2018-SHR mellem Orkla Confectionery & Snacks Danmark A/S ('Orkla') og Ankenævnet for Patenter og Varemærker ('Ankenævnet'). Sagen drejede sig om, hvorvidt Ankenævnets afgørelse om ophævelse af Orklas midlertidige registrering af et tredimensionalt varemærke i form af et billede af en firkantet chips med riller i overfladen af typen KiMs Snack Chips, var berettiget.

Spørgsmålet var, om varemærkeregistreringen var i strid med begrænsningen i den dagældende Lovbekendtgørelse nr. 223 af 26. februar 2017 ('den danske varemærkelovs') § 2, stk. 2. Bestemmelsen vedrører, at der ikke kan opnås varemærke til tegn, der udelukkende består af en udformning, som følger af varens egen karakter eller en udformning af varen, som er nødvendig for at opnå et teknisk resultat.

Sø- og Handelsretten lagde vægt på, at det væsentlige kendetegn ved udformningen var den rillede overflade. Den bølgede og firkantede form var således ikke-væsentlig, da den ikke adskiller produktet fra andre lignende på markedet. Endvidere fandt Sø- og Handelsretten, at den rillede overfalde udgjorde en teknisk funktion, der gjorde chipsene mere smagsfulde. Hvis Orkla fik registreret et tredimensionalt varemærke til denne udformning, ville det derfor forhindre konkurrenter i at anvende den samme tekniske løsning.

Sø- og Handelsretten fandt tillige at udformningen fulgte af varens egen karakter, der er knyttet til varens generiske funktion. Af disse grunde, fandt den dagældende danske varemærkelovs § 2, stk. 2 anvendelse, og Ankenævnets afgørelse om ophævelse blev derfor opretholdt.

Læs hele dommen her:

http://domstol.fe1.tangora.com/media/-300 011/files/Dom-BS-17 352-2018.pdf

8. Forbud nedlagt mod anvendelsen af »Cloud City« som selskabsnavn, varemærke og forretningskendetegn

Den danske Sø- og Handelsret ('Sø- og Handelsretten') afsagde den 16. april 2020 kendelse i sagen BS-48 699/2019-SHR mellem sagsøgerne Ejendomsfonden Artcenter Spritten (Ejendomsfonden) og Studio Tomás Saraceno GmbH (STS) og sagsøgte Cloud City Spritten A/S (Cloud City Spritten) og A, der er stifter af og direktør i Cloud City Spritten.

Sagen omhandlede nedlæggelse af et midlertidigt forbud mod A og Cloud City Sprittens brug af Cloud City Spritten som selskabsnavn, varemærke og forretningskendetegn samt brug af et selskabsnavn, varemærke eller forretningskendetegn, hvori Cloud City indgår.

Kunstneren Tomás Saraceno er kendt for sine kunstværker i Cloud City universet. STS indgik i 2014 aftale med A om opførsel af et Cloud City kunstværk i en ny bydel i Aalborg på den gamle spritfabrik, som A var ved at udvikle i et byudviklingsprojekt. I den forbindelse, fik A lov til at bruge selskabsnavnet Cloud City Aalborg til at rejse kapital til opførslen af kunstværket. I 2018 blev det aftalt mellem parterne, at Ejendomsfonden skulle opføre kunstværket i Aalborg i stedet for A.

I den forbindelse, ville Ejendomsfonden og STS have, at A skulle ophøre med at bruge navnet Cloud City og Cloud City Aalborg kommercielt. De udarbejdede et udkast til en erklæring, der anerkendte dette, som blev sendt til A med henblik på underskrivelse. A underskrev erklæringen og sendte den retur, men havde imidlertid fjernet Cloud City således, at han kun forpligtede sig til ikke at anvende Cloud City Aalborg. Efterfølgende ændrede han Cloud City Aalborgs selskabsnavn til Cloud City Spritten.

Sø- og Handelsretten fandt, at Ejendomsfonden og STS ikke, ved underskrift af erklæringen A sendte retur, havde givet tilladelse til brug af navnet Cloud City, da A ikke havde gjort opmærksom på, at han havde fjernet dette. Endvidere fandt Sø- og Handelsretten, at Cloud City ikke er blevet en betegnelse for det geografiske område, men alene bliver brugt, når der refereres til kunstværket.

Sø- og Handelsretten kom af disse grunde frem til, at A krænkende Ejendomsfonden og STS's rettigheder. Betingelserne i lovbekendtgørelse nr. 938 af den 9. oktober 2019 ('den danske retsplejelovs')

§ 413 var endvidere opfyldt, og Sø- og Handelsretten nedlagde derfor forbud mod Cloud City Sprittens brug af Cloud City Spritten som selskabsnavn samt brug af et selskabsnavn, varemærke eller forretningskendetegn, hvori Cloud City indgår.

Læs hele dommen her:
http://domstol.fe1.tangora.com/media/-300 011/files/Kendelse-48 699-2019.pdf

9. Varemærketten til »Quickfire« var fortabt ved passivitet

Den danske Sø- og Handelsret ('Sø- og Handelsretten') afsagde den 15. april 2020 dom i sagen BS-50 854/2018-SHR mellem Quick Fire ApS ('Quick Fire') og Burner International A/S ('Burner'). Sagen angik spørgsmålet om Burners brug af varemærket »QUICKFIRE« udgjorde en krænkelse af Quick Fires rettigheder efter lovbekendtgørelse nr. 88 af 29. januar 2019 ('den danske varemærkelov') og lov nr. 426 af 3. maj 2017 ('den danske markedsføringslov'), og i givet fald det erstatningsretlige opgør som følge heraf.

Quick Fire havde siden 2004 produceret og solgt optændingsposer til brug for optænding af blandt andet grill og brændeovne. Af poserne fremgik mærket QUICKFIRE, som dog ikke var registreret som varemærke. Sø- og Handelsretten skulle derfor tage stilling til, om Quick Fire havde opnået varemærkeret ved ibrugtagning efter den danske varemærkelovs § 3, stk. 1.

Sø- og Handelsretten fandt, blandt andet under henvisning til Sø- og Handelsrettens dom af 21. februar 2018 i sag V-78-16, hvor Quick Fire blev frifundet for påstande om at deres logo og etiket krænkede Burners rettigheder efter den danske varemærkelov og markedsføringslov, at mærket QUICKFIRE havde den fornødne adskillelsesevne og særpræg til at kunne opnå beskyttelse efter den danske varemærkelov. Retten fandt, at Quick Fire ved ibrugtagen havde stiftet en varemærkeret for QUICKFIRE i medfør af den danske varemærkelovs § 3, stk. 1. Sø- og Handelsretten fandt dog ikke, at Quick Fire havde godtgjort, at denne ret efter 2015 vedvarende havde været i brug på det danske marked. Varemærkerettigheden var som følge heraf bortfaldet jf. den danske varemærkelovs § 10 c, stk. 3, og Burner blev på den baggrund frifundet.

Læs hele dommen her:
http://domstol.fe1.tangora.com/media/-300 011/files/Dom-BS-50 854-2018.pdf

10. Keramik var ophavsretligt beskyttet

Den danske Sø- og Handelsret ('Sø- og Handelsretten') afsagde den 25. marts 2020 deldom i sagen BS-1370/2016-SHR mellem K H Würtz v/ Kasper Heie Würtz ('Würtz') og F & H A/S ('F&H') samt Christian Bitz. Spørgsmålet var, om Würtz' keramikstel var ophavsretligt beskyttet, herunder om den specielle glasur han havde udviklet til dette var selvstændigt ophavsretligt beskyttet, og i så fald om de sagsøgte havde foretaget en krænkelse af disse rettigheder ved salg og markedsføring af Bitz-keramikstellet.

Kasper Würtz havde siden 2010 håndrejet og håndglaseret et stel af høj kvalitet i stentøjsler. Stellet var i mørke farver med spættet glasur, og stellet blev solgt til butikken Skjalm P og restaurant Noma.

F&H begyndte i 2014 at samarbejde om udvikling af et stel med den kendte danske ernæringsekspert Christian Bitz, som også lagde navn til stellet, der blev markedsført og solgt i adskillige boligforretninger i Danmark. Christian Bitz havde forinden besøgt keramikeren Würtz på sit værksted og efterfølgende holdt møder med F&H om stellet. I forbindelse med produktion af stellet i Kina, sendte F&H adskillige e-mails til potentielle producenter med billeder og links til Würtz' hjemmeside.

Sø- og Handelsretten lagde vægt på, at denne korrespondance viste, at Würtz-stellet havde et udtryk som Bitz-stellet søgte at efterligne. Endvidere fandt Sø- og Handelsretten, at Würtz-stellet var udtryk for en selvstændigt skabende indsats og derfor var beskyttet af lovbekendtgørelse nr. 1144 af 23. oktober 2014 ('den danske ophavsretslovs') § 1, stk. 1 om beskyttelse af kunstneriske værker. For så vidt angik glasurudtrykket, fandt Sø- og Handelsretten imidlertid ikke, at der var ført bevis for hverken værkshøjde eller grundlag for beskyttelse løsrevet fra de konkret omhandlede værker i deres helhed.

Ud fra en helheldsvurdering konkluderede Sø- og Handelsretten, at der var en sådan oplevelse af identitet mellem stellene, at dette faldt inden for beskyttelsessfæren i den danske ophavsretslovs § 2 om ophavsmandens eneret. Samlet set forelå der derfor en krænkelse, både af den danske ophavsretslov § 2 og lov nr. 426 af 3/5/2017 ('den danske markedsføringslov') § 3, stk. 1 om illoyal markedsfortrængning. Da dommen er en deldom, mangler Sø- og Handelsretten at tage stilling til spørgsmålet om krav på vederlag og erstatning.

Læs hele dommen her:
http://domstol.fe1.tangora.com/media/-300 011/files/Dom_BS-1370-2016.pdf

11. The Old Irish Pub's naboplacering til The Old English Pub var ikke retsstridig

Den danske Sø- og Handelsret ('Sø- og Handelsretten') afsagde den 20. marts 2020 dom i sagen BS-20 954/2019-SHR mellem Engelsk Pub Vesterbrogade 2 B ApS ('Engelsk Pub') og Old Irish Pub Denmark A/S ('Old Irish Pub'). Sagen angik, hvorvidt Old Irish Pubs etablering af »The Old Irish Pub« på adressen Vesterbrogade 2 D krænkede naboens, »The

Old English Pub«s, rettigheder efter Lov nr. 426 af 3. maj 2017 ('den danske markedsføringslov').

Engelsk Pub åbnede »The Old English Pub« i maj 1992 og har siden drevet restaurationsvirksomhed på Vesterbrogade 2 B i København V. Irish Pub åbnede »The Old Irish Pub« på naboadressen den 1. juni 2018. Herudover driver selskabet 31 pubber fordelt over Danmark, Norge og Finland.

Engelsk Pub gjorde gældende, at der var en forvekslingsrisiko grundet lighed mellem »The Old English Pub« og »The Old Irish Pub«, hvorfor etableringen var illoyal udnyttelse af Engelsk Pubs forretningskendetegn i strid med god markedsføringskik i den danske markedsføringslov § 3, stk. 1. Herudover gjorde Engelsk Pub gældende, at Old Irish pub snyltede på deres goodwill og renommé.

Old Irish Pub bestred Engelsk Pubs anbringender og gjorde gældende, at Engelsk Pubs pubnavn og forretningskendetegn manglede særpræg. Herudover, at der var markante forskelle mellem to parter, blandt andet med hensyn til facader, indretning, anvendelse af lokaler og typen af afholdte arrangementer.

Sø- og Handelsretten lagde i deres begrundelse først vægt på, at parternes pubber er beliggende i et attraktivt og efterspurgt område for bar- og pubdrift. Sø- og Handelsretten fandt endvidere, at de to pubber har fællestræk, men forretningsmæssigt er de forskellige med forskelligartede tilbud til pubbernes respektive kundegrupper, samt at »The Old English Pub« ikke nyder en varemærkeretlig beskyttelse. Sø- og Handelsretten fandt det derfor ikke godtgjort, at etableringen af »The Old Irish Pub« var tilsigtet en illoyal udnyttelse af »The English Pub«s goodwill eller markedsposition. Samlet havde Old Irish Pub derfor ikke handlet i strid med den danske markedsføringslov.

Læs hele dommen her:

http://domstol.fe1.tangora.com/media/-300 011/files/Dom_BS-20 954-2019-SHR.pdf

12. To regnjakker opfyldte ikke kravene til ophavsretlig beskyttelse, men var beskyttet mod efterligninger efter markedsføringsloven

Den danske Sø- og Handelsret ('Sø- og Handelsretten') afsagde den 15. maj 2020 dom i sagen BS-9667/2017-SHR mellem Rains ApS ('Rains') og Fashion Retail S.A. samt Zara Danmark A/S (herefter samlet'Zara'). Sagen angik spørgsmålet om, hvorvidt Zaras markedsføring og salg af to forskellige regnjakker krænkede Rains rettigheder efter lovbekendtgørelse nr. 1144 af 23. oktober 2014 ('den danske ophavsretslov') eller lov nr. 426 af 3. maj 2017 ('den danske markedsføringslov') til to regnjakker med navnene Long Jacket og Parka Coat.

I relation til den mulige krænkelse af Long Jacket udtalte Sø- og Handelsretten, at jakken generelt udgjorde et enkelt og stilrent produkt. Jakken var sammensat af en række designelementer, som på frembringelsestidspunktet var kendte i forvejen og alle havde grundlag i allerede eksisterende former. Jakken opfyldte derfor samlet ikke kravene til ophavsretlig beskyttelse. Derimod, nød jakken beskyttelse efter den danske markedsføringslov, da der efter Sø- og Handelsrettens vurdering var tale om et produkt med et kvalitetsmæssigt, selvstændigt og minimalistisk udtryk med en tilstrækkelig grad af udtryksmæssigt særpræg og kommerciel adskillelsesevne. Da Zaras jakke, uanset enkelte detailforskelle, havde samme fremtoningsmæssige udtryk, fandt Sø- og Handelsretten, at der var tale om et brud på den danske markedsføringslovs § 3.

For så vidt angik Parka Coat, som ifølge designerens forklaring var en videreudvikling af Long Jacket, gjorde Sø- og Handelsretten sig samme bemærkninger som i sin vurdering af Long Jacket, og statuerede, at den ikke nød beskyttelse efter den danske ophavsretslov. Derimod nød jakken beskyttelse mod efterligninger efter den danske markedsføringslov, eftersom det anvendte PU-materiale (bestående af 50 % polyurethane og 50 % polyester) resulterede i et produkt med et karakteristisk, cool og sporty udtryk, der herved havde kommerciel adskillelsesevne. Da Zaras jakke var fremstillet af samme materiale og havde samme overordnede designmæssige udtryk, var der derfor handlet i strid med den danske markedsføringslovs § 3.

Læs hele dommen her:

http://domstol.fe1.tangora.com/media/-300 011/files/BS-9667-2017-SHR_Deldom.pdf

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


simonsen vogtwiig
Hedda Baumann Heier og
Cecilia Orheim

Høyesterett opprettholder resultatet fra lagmannsretten i iPhone-saken

Høyesterett avsa den 2. juni 2020 dom i saken mellom Apple Inc. og en reparatør av smarttelefoner som hadde fått tilbakeholdt et parti importerte mobiltelefonskjermer på grunnlag av mistanke om varemerkekrenkelse. Bakgrunnen for tolletatens tilbakeholdelse var at innsiden av alle skjermene var påført Apples karakteristiske eplelogo tildekket med tusj. Tvisten gjaldt hvorvidt importen av mobiltelefonskjermene med det tildekkede varemerket utgjorde en varemerkekrenkelse, jf. varemerkeloven § 4. Mobiltelefonreparatøren ble frikjent i tingretten, mens Apple vant frem i ankeomgangen (tingretts- og lagmannsrettsdommene er tidligere omtalt i Lov&Data nr. 134 Juni/2018 og nr. 139 September/2019).

Høyesterett starter med å konstatere at innførsel av et originalt produkt med ulovlig påført varemerke i utgangspunktet er ulovlig varemerkebruk og i kjernen av varemerkevernet, se avgjørelsens avsnitt 27. Spørsmålet i den foreliggende saken var om det faktum at varemerket er tildekket med tusj (som kan fjernes) gjør at det likevel ikke er en varemerkekrenkelse.

Under henvisning til HR-2018-110-A *Ensilox,* konstaterer Høyesterett at det kreves at den aktuelle bruken er *eigna til å skade* merkehaverens vernede interesser knyttet til varemerkets funksjoner, blant annet opprinnelses- og kvalitetsgarantien, for at det skal kunne utgjøre varemerkebruk etter varemerkeloven § 4 første ledd bokstav a. Dette må vurderes i relasjon til den relevante omsetningskretsen som i denne saken ble funnet å være reparatører og profesjonelle omsetningsledd.

Når det gjelder hva som nærmere kreves for at det er fare for skade, viser Høyesterett særlig til EU-domstolens avgjørelse i C-129/17 *Mitsubishi* der saksforholdet i korte trekk var at et selskap hadde kjøpt originale Mitsubishi gaffeltrucker utenfor EØS-området og importert dem til EØS for deretter å fjerne Mitsubishis varemerke og i stedet påføre sitt eget. Selv om varemerket var helt fjernet kom EU-domstolen til at det forelå en varemerkekrenkelse.

Høyesterett konstaterer kort at det ikke kan være et svakere vern i de tilfellene der overstrykingen av varemerket ikke er permanent, enn i de tilfellene der det originale varemerket var permanent fjernet, se avgjørelsens avsnitt 36. Og videre viser Høyesterett til at en heller ikke kan se helt bort i fra risikoen for at de som får skjermene i hende vil ta bort tildekkinga ettersom det ved videre omsetning vil kunne øke verdien på produktet, se avsnitt 37. Ut fra slik premissene er formulert, kan det stilles spørsmål ved hvor godt disse betraktningene er forankret i den aktuelle omsetningskretsen.

Til sist avfeier også Høyesterett relevansen av reparatørens argumenter knyttet til bærekraft. At konkurranse på reservedelsmarkedet er viktig i et bærekraftperspektiv var etter Høyesteretts syn et argument som falt på siden av saken ettersom saken ikke gjaldt skjermene som sådan men bruken av varemerket på skjermene, se avgjørelsens avsnitt 39.

Les hele dommen med saksnummer HR-2020-1142-A i Lovdatas database.

Hedda Baumann Heier er senioradvokat i Advokatfirmaet Simonsen Vogt Wiig AS, Oslo.

Cecilia Orheim er assosiert partner i Advokatfirmaet Simonsen Vogt Wiig AS, Oslo.


Bird & Bird

Karin Söderberg och Rebecca Fassihi

Internetoperatörer, piratsajter och dynamiska förbudsförelägganden

Frågan om huruvida en internetoperatör kan åläggas att blockera sina användares tillgång till piratsajter såsom exempelvis The Pirate Bay har länge diskuterats i Sverige. I den så kallade Blockeringsdomen från 2017 (PMÖD 2017:1) besvarades frågan jakande. I domen ålades Bredbandsbolaget att, genom blockering av domännamn, hindra sina användares tillgång till vissa sajter som bryter mot upphovsrätten på internet. I en nyligen meddelad dom bekräftade Patent- och marknadsöverdomstolen rättsläget samt utvidgade hur ett blockeringsföreläggande kan utformas i och med till att det även omfattade ett så kallat dynamiskt föreläggande (dom av den 29 juni 2020 i mål PMT 13 399-19).

Ett antal filmbolag väckte talan mot Telia och yrkade att domstolen skulle förbjuda Telia att medverka till upphovsrättsintrång på så sätt att Telia skulle åläggas att hindra sina abonnenter tillgång till olika piratsajter, bland annat The Pirate Bay. Detta skulle ske genom att Telia skulle blockera vissa specifika domännamn och webbadresser samt även domännamn och webbadresser vars enda eller övervägande ändamål är att möjliggöra eller underlätta tillgången till de aktuella piratsajterna och som filmbolagen underrättar Telia om. Det innebär att förbudet i så fall även skulle omfatta domännamn och webbadresser som skapas i framtiden, men som uppfyller nämnda kriterier.

Domstolen började med att behandla frågan om medverkansansvar och huruvida det är möjligt att i enlighet med 53 b § första stycket upphovsrättslagen, vid vite förbjuda en internetleverantör att medverka till upphovsrättsintrång. Enligt domstolen ska nämnda bestämmelse tolkas konformt med EU-rätten, det vill säga i enlighet med artikel 8.3 i Infosoc-direktivet och EU-domstolens tolkning av artikeln. Därmed konstaterade domstolen att eftersom Telias abonnenter, via den internetuppkoppling som Telia tillhandahåller dem, har kunnat få tillgång till piratsajterna har Telia medverkat till upphovsrättsintrång.

Därefter genomfördes en proportionalitetsbedömning mellan filmbolagens intresse av att intrång i deras rättigheter kan beivras och Telias näringsfrihet samt internetanvändarnas informationsfrihet. Domstolen fann att filmbolagens intresse vägde tyngst, bland annat eftersom syftet med The Pirate Bay och de andra piratsajterna är att olovligen tillgängliggöra upphovsrättsligt skyddat material.

Gällande utformningen av förbudsföreläggandet fastslogs inledningsvis att det inte föreligger någon oklarhet eller teknisk svårighet att hindra tillgången till piratsajterna genom blockeringsåtgärder avseende specificerade domännamn och webbadresser. De av filmbolagen angivna domännamnen och webbadresserna skulle således omfattas av förbudet.

En av de intressantare aspekterna i domen avser dock utvidgningen av utformningen av förbudsföreläggandet. Piratsajter byter ofta domännamn och webbadresser för att kringgå effekten av ett blockeringsföreläggande. För att ett blockeringsföreläggande effektivt ska kunna tillvarata filmbolagens intresse av att intrång inte begås, bör föreläggandet inte enbart ta sikte på vissa preciserade domännamn och webbadresser utan även ta sikte på piratsajterna som sådana. För att hindra att ett förbudsföreläggande skulle bli verkningslöst konstaterade domstolen således att ett förbudsföreläggande även bör omfatta nya domännamn och webbadresser som skapas i framtiden och som har till huvudsakligt syfte att ge tillgång till någon av de i målet aktuella piratsajterna. Enligt domstolen kan det dock inte krävas att Telia ensamt ska behöva bevaka nya domännamn

och webbadresser på internat för att se till att föreläggandet följs. Däremot bör Telia agera om filmbolagen anmält till Telia vilka domännamn och webbadresser som ska blockeras. Förbudet gäller i tre år och Patent- och marknadsöverdomstolens dom går inte att överklaga.

Karin Söderberg är Senior Associate och advokat och arbetar i Bird & Birds IP grupp sedan 2013. Hon har under sina verksamma år arbeta brett med olika immaterialrättsliga frågor, bland annat inom varumärkesrätt, upphovsrätt och marknadsrätt.

Rebecca Fassihi är biträdande jurist och arbetar i Bird & Birds IP-grupp. Hon arbetar med alla typer av frågor inom främst immaterialrätt och marknadsrätt.


SELMER
Vemund Sande og
Martin Tandstad Ege

Force Majeure – om rekkevidden av «umulighetsvilkåret» i SSA

Under SSA er det et vilkår for force majeure at det må være «umulig» å oppfylle i henhold til avtalen – er det egentlig en heldig regulering? Covid-19-pandemien og de medfølgende restriksjonene offentlige myndigheter har innført av smittevernhensyn har gjort det vanskelig for en rekke parter å levere avtalt ytelse under inngåtte avtaler. IT-avtaler i ulike former og farger er intet unntak. Dette har aktualisert force majeure-klausuler som fritaksgrunn for oppfyllelse av kontraktuelle forpliktelser.

For at force majeure-unntaket i Statens standardavtaler (SSA) skal komme til anvendelse må det for det første foreligge en «*ekstraordinær situasjon … som etter norsk rett må regnes som force majeure*» og for det andre må force majeure-situasjonen «*gjør[e] det umulig å oppfylle plikter etter denne avtalen*». Det første vilkåret synes å forutsette at force majeure er et rettslig begrep. Dette kan i seg selv problematiseres ettersom force majeure som rettslig begrep er erstattet av kontrollansvar i kontraktslovgivningen. Praktisk sett synes det likefullt å være gjengs oppfatning at covid-19-pandemien utgjør en force majeure-situasjon, og vi har derfor valgt ikke å problematisere dette videre.

Når det gjelder «umulighetsvilkåret» skiller SSA seg fra mange andre avtaler. Til sammenligning krever IKT-Norges standard kun at situasjonen «*vesentlig vanskeliggjør gjennomføring av avtalen*» og PS2000 Flex at parten «*ikke kan innfri sine forpliktelser etter Kontrakten*». Generelt synes det å være en høyere terskel for suspensjon av en parts forpliktelser etter SSA enn det som må anses som bransjenormen.

En naturlig forståelse av ordlyden «umulig» tilsier at vilkåret ikke vil være oppfylt så lenge det finnes et handlingsalternativ og ordlyden setter ingen begrensninger for størrelsen på partens ressursbruk dersom forpliktelsene teoretisk sett kan oppfylles. Tar man ordlyden på ordet, skulle det altså tilsi en tilstand hvor SSAenes force majeure-klausuler er av, i mange tilfeller, en illusorisk karakter. Avtaler inngått mellom næringsdrivende skal i utgangspunktet tolkes objektivt og terskelen er høy for å fravike en klar ordlyd, jf. Rt-2002-1155. På denne bakgrunn kan det være vanskelig å innfortolke vide begrensninger i «umulighetsvilkåret» selv om reelle hensyn tilsier det. Basert på de foregående forhandlinger kan man tenke seg at det vil være mulig å identifisere faktorer som taler for at «umulighetsvilkåret» må forstås mildere enn hva som følger av ordlyden. Praktisk sett er det imidlertid vår oppfatning at force majeure-klausulen i SSA i stor utstrekning forblir uendret, og derfor må ha det innhold den strenge ordlyden legger opp til.

Praktisk sett vil en slik forståelse, avhengig av de faktiske omstendigheter, medføre at en part vil kunne komme lengre gjennom de alminnelige regler om avtalerevisjon (for eksempel gjennom avtalelovens paragraf 36) enn force majeure-klausulen i SSA. Dette er etter artikkelforfatternes syn en lite gunstig løsning.

Tar man utgangspunkt i kontrollansvaret slik det er regulert i kontraktslovgivningen, synes det klart at terskelen det legges opp til i SSA er vesentlig høyere enn hva som finnes av relevant lovgivning som har søkt å adressere sammenlignbare situasjoner. Overføringsverdien av dette er isolert sett begrenset, men det gir uttrykk for et underliggende prinsipp – det er ikke naturlig at en part alene er skadelidende for forhold som klart nok ligger utenfor partens kontroll. Det er standpunkt som har gode grunner for seg. Det kanskje viktigste argumentet til støtte for en slik regulering er at det praktisk sett ikke vil være mulig å kvantifisere denne risikoen på en

fornuftig måte. Å prise det ukjente er en krevende øvelse.

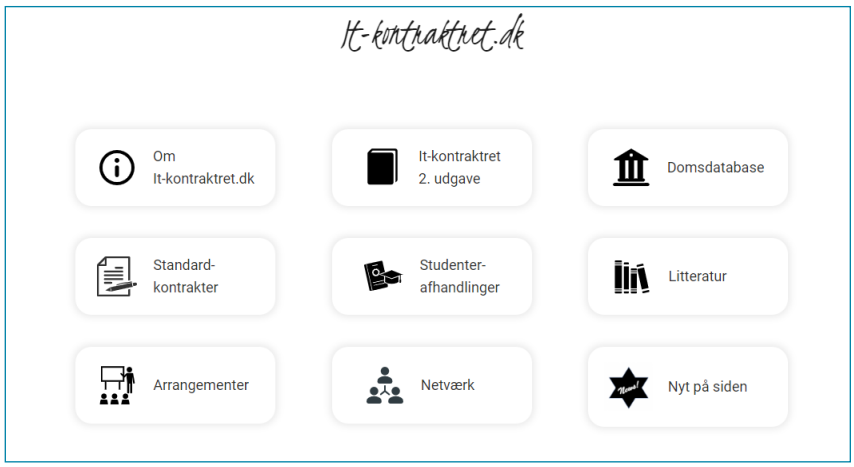
Det er artikkelforfatterens synspunkt at reguleringen i SSA ikke dekker de situasjoner en force majeure-klausul typisk sett er ment å ivareta. Det kan selvfølgelig innvendes at en del IT-leveranser er av en slik karakter at det nettopp er meningen at ytelsen skal leveres 24/7/365, uansett. Det er vi ikke uenige i. Det er imidlertid ikke det samme som at en leverandør skal dekke hele regningen når ekstraordinære forhold som ligger utenfor partens kontroll oppstår. Det bør gå en grense for hvilke ekstra kostnader en leverandør kan pålegges alene. Reguleringen som er valgt i IKT-Norges standard synes å harmonisere bedre med vår oppfatning av hva force majeure bør være. Også denne avtalen legger opp til en høy terskel, men den er likevel langt fra like streng som ordlyden som benyttes i SSA.

Vemund Sande er advokatfullmektig i avdelingen for HITEK i Advokatfirmaet Selmer, Oslo.

Martin Tandstad Ege er senioradvokat i avdelingen for HITEK i Advokatfirmaet Selmer, Oslo.

Ny it-kontraktretlig domsdatabase og vidensportal

Professor Henrik Udsen har samlet en række danske og norske it-kontraktretlige domme i en ny domsdatabase, der løbende vil blive suppleret med yderligere domme. Databasen er frit tilgængelig fra *www.it-kontraktret.dk*, hvor der også ligger andet it-kontraktretligt materiale og information, bl.a. standardkontrakter, studenterafhandlinger, litteraturoversigt mv.



Returadresse:
Lovdata
Postboks 2016 Vika
NO-0125 Oslo
Norge

Nytt fra

LOVDATA

Få Lovdata Pro ut året uten noen kostnad i pris!

For Lov&Datas lesere tilbyr vi nye kunder Lovdata Pro for resten av 2020 uten noen kostnad. Det eneste du trenger å gjøre er å registrere din interesse på *https://lovdata.no/tjenester/pro/tilgang* og benytte rabattkode «L&D».

Abonnementet vil løpe videre om du ikke aktivt sier opp tjenesten innen 1. desember 2020.

Produksjon: 07