

LOV & Data

Nr. 142
Juni 2020

Nr. 2/2020

Innhold

Leder 2

Artikler

Mari Klungsøyr Kristiansen og
Stian Hultin Oddbjørnsen:
Adgangen til å foreta endringer
i IT-kontrakter underlagt
anskaffelsesregelverket 4

Ove André Vanebo:
Personopplysningslovens unntak fra
informasjonsplikt og innsynsrett for
opplysninger i tekst som er utarbeidet
for intern saksforberedelse 10

JusNytt 16

Bokomtale 19

Nytt om personvern 20

Nytt om immaterialrett 32

Nytt om IT-kontrakter 42

Nytt fra Lovdata 44



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

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

Ansvarlig redaktør er Jarle Roar Sæbø, juridisk direktør i HPE, Oslo og leder for Domeneklagenemnda.

Medredaktører er Ida Marie Vangen og Trine Shil Kristiansen, Lovdata.

Redaktører for Danmark er dr.juris Henrik Udsen ved Center for informations- og innovationsret, Københavns universitet og Tue Goldschmieding, partner i firmaet Gorrissen Federspiel, København.

Redaktør for Sverige er Daniel Westman, uavhengig rådgiver og forsker.

Fast spaltist er Halvor Manshaus, partner i advokatfirmaet Schjødt.

Trykk: ISSN 0800-7853

Elektronisk: ISSN 1503-8289

Utkommer med 4 nummer pr. år.

Abonnementspriser for 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/>



Leader

Bör de sociala medierna regleras för att skydda demokratin?

I Twitters och Facebooks barndom var det många som uppfattade dessa tjänster och andra sociala medier som en välsignelse för demokratin. Både i demokratier och i totalitära stater skapade tjänsterna nya möjligheter för var och en med en internetanslutning att enkelt sprida information och åsikter.

Sedan ett par år är tongångarna i den allmänna debatten betydligt mer dystra. ”De amerikanska nätjättarna”, som de nu oftast kallas, anklagas för att inte göra tillräckligt för att hindra sina användare från att sprida falsk information, terroristpropaganda, nätkränkningar m.m. Det har gått så långt att vissa nu istället uppfattar de sociala medierna som ett hot mot demokratin.

Så här i efterhand är det uppenbart att den tidiga bilden av de sociala medierna var allt för rosaskimrande, bl.a. underskattades dessa aktörers maktställning. Men på samma sätt är det tydligt att den allmänna debatten idag ensidigt rör de sociala mediernas negativa sidor. Traditionella medieaktörer driver inte sällan på denna debatt, samtidigt som de konkurrerar med de

sociala medierna på annonsmarknaden eller förhandlar med dessa om upphovsrättigheter.

Eventuella ingripanden från det allmännas sida bör dock baseras på tydliga faktaunderlag och utgå från användarnas/medborgarnas intresse. Allmän moralpanik eller uppblåsning av marginella företeelser måste för det första sällas bort från debatten. Att reglera de sociala mediernas verksamhet är förstas inte fel i sig, men det får inte göras på ett sätt som innebär att användarnas yttrandefrihet eller rättssäkerhet begränsas på ett oproportionerligt sätt.

Om man blickar ut i världen kan man nu se vissa oroväckande tendenser. Flera länder har infört eller diskuterar att inför förbud mot ”falsk information” i sociala medier eller vaga skyldigheter för tillhandahållare av sociala medier att skydda användarna mot ”skadligt” innehåll. Dessa former av lagstiftning är svåra att förena med internationella yttrandefrihetsnormer.

Både i USA och inom EU diskuteras det att mjuka upp de särskilda regler som innebär att t.ex. sociala



medier inte kan hållas ansvariga för användarnas brottsliga eller skadeståndsgrundande inlägg (för EU:s del finns dessa regler i det s.k. e-handelsdirektivet). Vissa justeringar kan säkert vara nödvändiga, men den principiella utgångspunkten bör även fortsättningsvis vara att det är användarna som ansvarar för sina yttranden och att staterna därför måste tillsätta resurser för att upprätthålla lag och ordning även på nätet. I Sverige sker det nu också i betydligt större utsträckning än tidigare.

Ett utökat straff- eller skadeståndsansvar för mellanhänder leder till att dessa privata aktörer måste strama åt användarvillkor och införa hårdare moderering och därmed indirekt till begränsningar av användarnas yttrandefrihet. Det sammanhänger bl.a. med att mellanhänderna har svårt att göra kvalificerade rättsliga bedömningar och därför ofta väljer att hålla viss marginal till det otillåtna. Trots att modereringen sker med ofullkomliga automatiserade system ges användarna dessutom sämre processuellt skydd än när det är det allmänna som ingriper

mot misstänkt missbruk av yttrandefriheten.

Varje steg mot att de sociala medieföretagen ges ett ökat ansvar för användarnas yttranden som ändå anses nödvändigt – framför allt för att skydda andra grundläggande rättigheter, såsom rätten till privatliv – måste därför kombineras med regler som garanterar att resultatet i praktiken blir en korrekt balans mellan olika rättigheter och att användarna ges processuella möjligheter att få felaktiga borttagningar av sina yttranden prövade.

Facebooks nya initiativ med en oberoende nämnd som ges rätt att med bindande verkan överpröva företagets egna modereringsbeslut är utan tvekan ett steg i rätt riktning, men systemets otillräcklighet i det här diskuterade hänseendet framgår genom att nämndens beslut inte gäller framför nationell lag, som alltså kan framtvunga ett borttagande från dessa företag. Garantier för användarnas yttrandefrihet och rättssäkerhet måste alltså finnas i nationella rättsordningar för att få fullt genomslag.

Det råder ingen tvekan om att de sociala medierna idag har blivit en viktig maktfaktor som måste bli föremål för myndighetstillsyn och kanske också särskild reglering i vissa hänseenden. Inte minst företagens användning av personuppgifter för profilering och s.k. microtargeting bör ge anledning till vaksamhet. Att ge dessa aktörer ett utökat ansvar för användarnas yttranden bör däremot inte ses som patentlösningen för att ”rensa upp på nätet”.

* Lästips: Westman, Daniel, *Sociala medier – yttrandefrihet och ansvar*, i Ord och rätt: Festskrift till Hans-Gunnar Axberger (tillgänglig på <http://su.diva-portal.org/smash/record.jsf?pid=diva2%3A1388868&dsid=7164>)

Daniel Westman

Adgangen til å foreta endringer i IT-kontrakter underlagt anskaffelsesregelverket

– Særlig om endringsklausuler og forbudet mot vesentlige endringer

Av Mari Klungsøyr Kristiansen og Stian Hultin Oddbjørnsen

1 Innledning

Regelverket for offentlige anskaffelser gjelder i hovedsak prosessen frem til kontraktsinngåelse. Den etterfølgende kontraktsfasen reguleres i utgangspunktet av kontraktsretten.

Et viktig unntak fra dette utgangspunktet er reguleringene av hvilke endringer som er tillatt å gjøre i kontrakter som er underlagt anskaffelsesregelverket. Overordnet må en endring ha hjemmel i regelverket for å være tillatt. En endring som foretas uten hjemmel, vil potensielt anses som en ulovlig direkte anskaffelse, som er sanksjonsbelagt med overtredelsesgebyr på inntil 15 % av (den nye) kontraktens verdi, jf. anskaffelsesloven¹ § 12. Den nye kontrakten kan også potensielt bli kjent «uten virkning» og derved opphøre ved dom, jf. anskaffelsesloven § 13.

Bakgrunnen for disse begrensningene i adgangen til å foreta endringer er at anskaffelsesregelverkets formål og hensikt lett ville bli omgått dersom oppdragsgiver fritt kunne ha endret kontrakten etter inngåelsen. Dersom kontraktsgjensstand endres i for stor grad etter inngåelsen, vil markedet ikke ha fått anledning til å konkurrere om den leveransen som i realiteten



Mari Klungsøyr Kristiansen

foretas. Samtidig vil for vidtrekkende begrensninger stille oppdragsgiver (og leverandør) i en vanskelig posisjon i kontrakter der det er reelt behov for endringer i ettertid. I slike situasjoner vil det være svært lite effektivt enten å fastholde en kontraktsgjensstand som ikke lenger er relevant eller å tvinges ut i en ny konkurranse. I slike situasjoner befinner endringene seg i skjæringspunktet mellom de anskaffelsesrettslige prinsippene om konkurranse, forutberegnelighet og etterprøvnbarhet i anskaffelsesloven § 4 og formålet om effektiv bruk av samfunnets ressurser i anskaffelsesloven § 1.



Stian Hultin Oddbjørnsen

IT-kontrakter er blant anskaffelsene der det ikke sjelden vil oppstå et behov for endringer i forhold til de kunngjorte anskaffelsesdokumentene underveis i kontraktsforløpet. Selv om partene er enige om endringene som ønskes, må man i slike situasjoner i tillegg ta stilling til hvilket endringsrom den offentlige oppdragsgiveren har etter anskaffelsesregelverket.

Dette endringsrommet reguleres av anskaffelsesforskriften² § 28-1 første ledd. Bestemmelsen angir flere mer eller mindre vilkårsbestemte

1 Lov 17. juni 2016 nr. 73 om offentlige anskaffelser.

2 Forskrift 12. august 2016 nr. 974 om offentlige anskaffelser.

muligheter for endring i bokstavene b-e. Vilkårene er knyttet til ulike konkrete situasjoner som foranlediger endringsbehovet (tilleggsleveranser, uforutsette omstendigheter o.l.) og/eller maksimalbegrensning på endringens verdi, gjerne knyttet til terskelverdi eller prosentmessige begrensninger i forhold til opprinnelig verdi på kontrakten.

De nevnte alternativene er ofte interessante å se hen til, men i denne artikkelen skal vi rette fokus mot alternativene i bokstav a og e, om henholdsvis endringer med grunnlag i endringsklausuler og ikke-vesentlige endringer.

Alternativene er formulert slik:

«(1) Oppdragsgiveren kan foreta følgende endringer i en kontrakt uten å gjennomføre en ny konkurranse etter forskriften:

a) endringer som foretas etter en endringsklausul som nevnt i § 19-1 annet ledd;

[...]

f) endringer, uavhengig av verdi, som ikke er vesentlige, jf. § 28-2.»

Det er vår opplevelse at man i praksis ofte vil stå igjen med å vurdere disse bestemmelsene, særskilt for større endringer. Som vi vil komme tilbake til, glir de to alternativene noe over i hverandre. Vi vil likevel behandle dem hver for seg, og begynner med reguleringen av bruken av endringsklausuler, i punkt 2. Rammene for ikke-vesentlige endringer behandles i punkt 3.

2 Om viktigheten av - og kravene til - endringsklausuler i kontrakter underlagt anskaffelsesregelverket

I sak C-549/14 *Finn Frogne* uttalte EU-domstolen at en oppdragsgiver som forutsetter at utviklingen i en kontrakt fremstår som usikker, forventes å «definere kontraktens genstand med omhu». ³ Med grunnlag i denne uttalelsen uttalte Klagenemnda for

offentlige anskaffelser («Kofa») i sak 2018/7 *Steigen kommune* at det ikke var tilstrekkelig for en oppdragsgiver å henvise til den teknologiske utviklingen som grunnlag for en overgang til sky-løsning i en kontrakt der tilbyderne hadde konkurrert på en on premise-løsning (mer om saken nedenfor). Dette illustrerer viktigheten av gode endringsklausuler i IT-kontrakter.

“ IT-kontrakter er blant anskaffelsene der det ikke sjelden vil oppstå et behov for endringer i forhold til de kunngjorte anskaffelsesdokumentene underveis i kontraktsforløpet.

For at en endringsklausul skal kunne benyttes som hjemmel for endring av kontakten etter anskaffelsesforskriften § 28-1 første ledd bokstav a, må den oppfylle følgende krav etter forskriftens § 19-1 andre ledd andre og tredje punktum:

«Endringsklausulene skal angis i anskaffelsesdokumentene, og det skal fremgå klart hvilke endringer oppdragsgiveren kan foreta, i hvilket omfang og på hvilke vilkår. Endringsklausulene kan ikke åpne for at anskaffelsens overordnede karakter blir endret.»

Endringsklausulen må altså angi *arten* og *omfanget* av de aktuelle endringene, og på *hvilke vilkår* disse kan skje. I tillegg angis som absolutt begrensning at endringene ikke kan endre anskaffelsens *overordnede karakter*.

Den viktige vurderingen blir dermed hva som skal til for at en endringsklausul anses tilstrekkelig «klar». Ordlyden synes i seg selv å stille høye krav. Samtidig modifierer anskaffelsesdirektivets fortale

klarhetskravet til at klausulen kun behøver å være «tilstrekkelig» («sufficiently») klar.⁴

Utfordringen i IT-kontrakter er imidlertid at selv om oppdragsgiver gjerne forutsetter at det vil oppstå et behov for endringer underveis i kontraktsperioden, er det vanskelig å forutse *hva behovet vil gå ut på*. Ingen vet hvordan morgendagens teknologi vil se ut.

Uttalelsene i *Finn Frogne* og *Steigen kommune* gjør det likevel klart at oppdragsgiver forventes å formulere en slik endringsklausul, tross uvishheten. Et spørsmål som oppstår i forlengelsen av dette er hvorvidt endringsklausulene i statens – og IKT Norges standardavtaler – som svært ofte tas i bruk i ulike IT-anskaffelser, i tilstrekkelig grad ivaretar klarhetskravet, slik at det ikke er *nødvendig* for oppdragsgiver å formulere egne endringsklausuler i bilagene.

Når det gjelder klausuler om muligheten for *kvantitative* endringer, har mange av SSA-ene angitt en grense på $\pm 15\%$ av opprinnelig netto kontraktspris.⁵ *Omfangsmessig* vil denne typen bestemmelse i seg selv oppfylle forskriftens klarhetskrav.

Tilsvarende kan imidlertid ikke sies om standardavtalenes regulering av handlingsrommet for *kvalitative* endringer. I IKT Norges standardavtaler finner man *ingen* angivelse av hvilke endringer partene kan gjøre i leveransens art. Dette skyldes antageligvis at IKT Norges avtaler i liten grad er tilpasset kontraktsforhold som er underlagt anskaffelsesregelverket. Men heller ikke i SSA-ene er rommet for kvalitative endringer særlig spesifisert. Det nærmeste finner man i SSA-T, SSA-S og SSA-D, hvor oppdragsgiver kan pålegge endringer som «*ligger innenfor hva partene med rimelig*

⁴ Fortalen premiss 111.

⁵ SSA-T punkt 3.1, SSA-S punkt 3.1 og SSA-D punkt 3.1 (kun 15 % økning).

³ C-549/14 premiss 36.

grunn kan ha forventet da avtalen ble inngått.⁶

Det kan nok argumenteres for at en formulering som i de nevnte SSA-ene i noen tilfeller kan være klar nok for enkelte endringer, dersom den kan tolkes i sammenheng med en aktuell kontrakts øvrige formuleringer. Men det fordrer trolig at andre formuleringer i anskaffelsesdokumentene i tilstrekkelig grad angir i hvilken retning den aktuelle leveransen vil utvikle seg.

“ Vår vurdering er derfor at det i de fleste tilfeller vil være behov for å innta særskilte klausuler i bilagene som nærmere regulerer endringsrommet, for å skape større fleksibilitet i kontraktsforholdet.

Hva gjelder på *hvilke vilkår* disse endringene skal skje, sier imidlertid standardene lite. Det vil nok ofte være naturlig å ta utgangspunkt i avtalte timepriser, men for andre og «nye» utgifter gir klart nok ikke standardavtalene noen fast regulering som vil oppfylle forskriftens klarhetskrav.

Vår vurdering er derfor at det i de fleste tilfeller vil være behov for å innta særskilte klausuler i bilagene som nærmere regulerer endringsrommet, for å skape større fleksibilitet i kontraktsforholdet. Dette er i seg selv ikke oppsiktsvekkende, ettersom det er vanskelig for standardavtaler å hensynte dette tilstrekkelig presist. Likevel opplever vi i praksis at det ofte ikke er arbeidet med endringsklausuler i kontraktene.

De endringer man på tidspunkt for konkurranseutsetting ser som aktuelle, bør man naturligvis be-

skrive og få priser på i konkurransefasen. Dette vil resultere i klare opsjoner som er prissatt, og som dermed fritt kan utløses i kontraktsfasen.

Beskrivelse og reguleringen av de *kvalitative* sider ved endringsbehov (arten av endringer) utover klare opsjoner, vil som nevnt, ofte være utfordrende hva gjelder påfølgende teknologiske utvikling.

For endringer man ikke kan overskue på tidspunktet for konkurranseutsetting, mener vi at det ofte bør være tilstrekkelig å angi noe i retning av at kontrakten kan endres *i tråd med den naturlige videreutviklingen innenfor det gitte teknologiområdet*.

Selv om det kan innvendes at en henvisning til den naturlige videreutviklingen innenfor det gitte teknologiområdet ikke er særskilt «klar[t]», er det ofte vanskelig å skrive noe mer presist om arten av endringene på en klarere måte. Og reglene bør ikke stille umulige krav til oppdragsgiver. Ved en slik formulering signaliserer man i alle fall tydelig til markedet at man ser for seg en videreutvikling i løpet av kontraktsforholdet.

I noen tilfeller er imidlertid rammen av de aktuelle endringene som kan bli foretatt, klarere for oppdragsgiver. Men også i tilfeller der rammen av de aktuelle endringene som kan bli foretatt fremstår noe klarere for oppdragsgiver (men ikke så klare at det kan formuleres klare opsjoner), bør man være forsiktig med å formulere seg for snevert. Dersom teknologien utvikler seg i en annen retning enn leveransemetoder eller funksjonalitet e.l. angitt i endringsklausulene, vil endringsklausulenes snevre ramme ikke bare hindre at en endring i tråd med den teknologiske utviklingen kan foretas med hjemmel i disse, men de vil potensielt også brukes som selvstendig argument i retning av at endringen er *vesentlig* etter anskaffelsesforskriften §§ 28-1 første ledd bokstav f jf. 28-2, jf. nedenfor.

“ Det er derfor lurt å innhente priser i anskaffelsen på tjenester som er priset etter volumforbruk både langt over og under det umiddelbare behovet for virksomheten.

Angivelse av det *kvantitative* endringsrommet vil gjerne være enklere. Angis for eksempel en fast nedre og øvre prosentgrense, vil kravet om at det må være «*klart [...] i hvilket omfang*» oppdragsgiver kan foreta endringer være oppfylt.⁷ Ved kontrakter der prisene styres av volum (for eksempel data eller antall brukere) er det viktig at prismatrisen har angitt et stort nok spenn til å ivareta både større utvidelser og nedskjæringer. Da vil det ikke utgjøre et anskaffelsesrettslig problem om man endrer volumet innenfor de allerede angitte rammene i prismatrisen. Mange skytjenester har slike vederlagsmodeller. Problemet oppstår da først hvor man sprenger rammene for angitt volum. Dette er ikke helt upraktisk i situasjoner der oppdragsgiver eksempelvis øker antall ansatte betraktelig gjennom en organisatorisk sammenslåing. Det er derfor lurt å innhente priser i anskaffelsen på tjenester som er priset etter volumforbruk både langt over og under det umiddelbare behovet for virksomheten.

7 Et særskilt spørsmål er om det er noen grenser for hvor bredt dette kvantitative endringsrommet kan angis. Det er mulig den absolutte begrensningen i anskaffelsesforskriften § 19-1 andre ledd tredje setning om at anskaffelsens overordnede karakter ikke kan endres, utgjør en skranke for svært store prosentintervaller. Vår vurdering er likevel at det skal mye til for at dette vil være tilfellet. Se også Trygstad (red.), *Offentlige kontrakter: Aktuelle tema*, Oslo 2020 (ved Per Ole Svor) s. 213.

6 Samme sted.

Endringsklausulenes regulering av på hvilke *vilkår* endringen kan foretas, vil ofte, på lik linje med arten av endringen, kunne utgjøre en utfordring – særlig dersom endringen kan innebære uforutsigbare priselementer.⁸ Generelt mener vi likevel det vil være tilstrekkelig å regulere rammene for hvordan prising av det ukjente skal foregå. Etter vårt syn er en god tilnærming å angi at kontraktens priser skal brukes så langt de er anvendelige også for endringer, med tillegg av dokumenterte og nødvendige eventuelle øvrige kostnader forbundet med endringen. Har man da i konkurransefasen innhentet (1) *timepriser som kan benyttes for merarbeid knyttet til endringene* samt (2) *et fortjenestetillegg på øvrige ytelser*, har man etter vårt syn gode rammer for å fastsette vilkårene uten særskilt behov for forhandling hva gjelder vilkårene for de merkantile forhold knyttet til endringen. Der det er relevant kan det også hentes inn priser på en tjenestekatalog av ulike lisenser eller tjenester.

Det innrømmes at det er vanskelig å unngå at noen elementer ved endringene må være gjenstand for noe forhandling mellom partene. Men dersom man lar disse generelle vilkårene for prising (timepriser og fortjenestepåslag, ev. tjenestekatalog) utgjøre konkurranseelement allerede i tilbudsfasen, bør det være lite behov for å forhandle mye på vilkår knyttet til prising av endringen. I så fall mener vi at anskaffel-

sesregelverkets formål og prinsipper vil være tilstrekkelig hensyntatt og at endringsklausulen er tilstrekkelig klar.

Konsekvensene av ikke å tilstrekkelig regulere rommet for endringer i en IT-kontrakt der dette kunne vært forutsett ble tydelig i den nevnte saken 2018/7 *Steigen kommune*. Her hadde kommunen i anskaffelsesdokumentene angitt at de muligens så for seg «*en blanding av eget datasenter og skytjenester*», og at leverandøren etter hvert ville «*ta ansvar for at nye skybaserte løsninger på en behøvelig måte integreres med de tradisjonelle tjenester*». Samtidig var det eneste tilbudene kunne levere pris på i konkurransen en «on premise»-løsning. Da Steigen kommune i ettertid gjorde avrop på IKT-tjenester som skulle leveres som skyløsninger, konstaterte Kofa at det forelå en ulovlig direkte anskaffelse. At det var angitt i anskaffelsesdokumentene at kommunen så for seg at man kunne gå over til en skyløsning, var ikke tilstrekkelig, når leverandørene ikke hadde konkurrert på dette.

Oppsummert mener vi dermed at endringsklausuler som angir at endringer kan skje innenfor et visst omfang, på visse prisvilkår og innenfor den naturlige teknologiske utviklingen i tilstrekkelig grad vil ivareta klarhetskravet i anskaffelsesforskriften § 19-1 andre ledd andre punktum. Det er viktig å få med seg at særlig arten av endringene etter vår vurdering ikke bør angis for snevert.

Samtidig påpeker vi at man bør ha et bevisst forhold til den absolute begrensningen i § 19-1 andre ledd *tredje punktum*, om at endringsklausulen ikke kan åpne for at anskaffelsens «*overordnede karakter*» blir endret. Ordlyden gir oppdragsgiver et bredt spillerom. Det foreligger foreløpig ingen praksis som belyser innholdet i vilkåret, men vi antar at vurderingen vil inneholde momenter som vil overlappe med vesentlig endring-vurderingen etter forskrif-

ten § 28-2. Dette innebærer at et viktig vurderingstema vil være hvorvidt andre leverandører ville ha deltatt i eller kunne ha vunnet konkurransen dersom endringene hadde blitt satt inn som en del av den opprinnelige konkurransen.⁹

3 Der endringsklausulen ikke strekker til: vesentlighetslæren

Dersom endringsklausulene ikke er tilstrekkelig klare, der disse ikke dekker den ønskede endringen eller dersom det ikke er formulert noen endringsklausul i det hele tatt, vil spørsmålet gjerne bli om endringen kan foretas med grunnlag i «generalhjemmelen» i anskaffelsesforskriften § 28-2¹⁰ om ikke-vesentlige endringer.

Her fremgår:

«*En endring er ikke tillatt etter § 28-1 første ledd bokstav f dersom den fører til at innholdet i kontrakten blir vesentlig forskjellig fra den opprinnelige kontrakten. En endring er alltid vesentlig dersom den:*

- a) *gjelder nye betingelser som, dersom de hadde vært en del av den opprinnelige konkurransen, ville ha ført til at andre leverandører potensielt kunne ha deltatt, eller at oppdragsgiveren kunne tildelt kontrakten til en annen leverandør,*
- b) *endrer kontraktens økonomiske balanse til fordel for leverandøren,*
- c) *utvider kontraktens omfang betydelig eller*
- d) *gjelder skifte av leverandøren i andre tilfeller enn dem som er nevnt i § 28-1 første ledd bokstav e.»*

Bestemmelsen er utformet på en kasuistisk måte, men Kofa synes tidvis å bruke alternativene mer som momenter i en helhetsvurde-

8 I artikkelen fokuserer vi på *virkningsvilkår*. Kravet i anskaffelsesforskriften § 19-1 andre ledd andre punktum kan imidlertid også leses som et krav om at endringsklausulen også må angi *situasjonsvilkårene* i hvilke tilfeller endringsklausulen faktisk kan anvendes. Dersom begge deler angis, vil man klart oppfylle forskriftens krav. I Trygstad (red.), *Offentlige kontrakter: Aktuelle tema* (ved Per Ole Svor) på s. 211 konkluderes med at det er tilstrekkelig å fastsette *enten* *situasjonsvilkår* eller *virkningsvilkår*. Vi er enige i denne konklusjonen.

9 Se igjen Trygstad, *Offentlige kontrakter: Aktuelle tema* (ved Per Ole Svor) s. 212.

10 Jf. anskaffelsesdirektivet artikkel 72 nr. 4. Bestemmelsen er i stor grad en kodifisering av EU-domstolens uttalelser i sak C-454/06 *Pressetext*.

ring.¹¹ Andre momenter av betydning er (1) *hva slags type kontrakt det er snakk om, herunder om den har karakter av å være en utviklingskontrakt*¹², (2) *hensiktsmessigheten av å foreta en særskilt anskaffelse knyttet til den aktuelle endringen*¹³ og (3) *hvor forutberegnelig det er for tilbyderne at det vil forekomme endringer*.¹⁴ Når det gjelder moment (3), vil dette ha en klar kobling til endringsklausulene i kontrakten, og andre formuleringer i anskaffelsesdokumentene som angir mulige utviklinger.

Alle disse momentene kan likevel sies å ha en særlig relevans i IT-anskaffelser, og særskilt hvis det er snakk om en langvarig anskaffelse. Dette vil typisk gjelde langvarige drift- og vedlikeholdskontrakter. Dersom oppdragsgiver har synliggjort i anskaffelsesdokumentene at det kan forekomme endringer, at disse innebærer en naturlig videreutvikling av tjenestene og det fremstår noenlunde klart under hvilke vilkår de skal prises, er vår vurdering at det skal en del til for at slike endringer skal anses å utgjøre en vesentlig endring. Dette selv om formuleringene ikke oppfyller klarhetskravet til endringsklausuler som beskrevet over.

Det er imidlertid både kvalitative og kvantitative grenser også her. Hva gjelder kvalitative endringer, ble, som nevnt ovenfor, en endring fra en premisse til skyleveranser ansett som en vesentlig endring i Ko-

fas sak 2018/7. Sak 2016/196 fikk samme konklusjon. Her hadde Norges statsbaner AS anskaffet tog. Senere bestilte de vedlikeholdsarbeid på togenes boggier under samme kontrakt. Her uttalte Klagenemnda:

*«Det kan i et slikt tilfelle ikke være avgjørende at endringen bare utgjør i underkant av 0,7 prosent av den opprinnelige estimerte anskaffelsesverdien. Det avgjørende må være at endringsordren reelt sett utgjør en ny anskaffelse av noe kvalitativt annet – vedlikeholdstjenester. Det er da ikke avgjørende at innklagede har sett det slik at endringen har en kommersiell og funksjonell sammenheng med den opprinnelige avtalen.»*¹⁵

Også *kvantitativt* synes det vanskelig å gi noen klare føringer på hva som er tillatt. I KOFAs sak 2017/145 ble en forlengelse som innebar en prisøkning på 20 % ikke tillatt, og det samme gjaldt en prisreduksjon på 50 % i den nevnte *Finn Frogne*-saken fra EU-domstolen. I KOFAs sak 2010/179 ble imidlertid en reduksjon på 50 % tillatt etter en konkret vurdering.

Den største tillatte endringen finner man likevel trolig i sak 2010/212. Avtalen omhandlet vedlikehold av laboratorieinstrumenter og kjøp av forbruksmaterieil til disse. Her hadde innklagede foretatt en endring i avtalen ved at selve instrumentparken hadde blitt utvidet i form av at leverandøren hadde installert tre nye maskiner hos oppdragsgiver som et *kostnadsfritt lån* fra leverandør. Konsekvensen av dette ble økt bruk av forbruksmaterieil, med tilhørende økte årlige utgifter med 19-20 % og økte årlige serviceutgifter med ca. 56 %. Endringen ble godtatt. I vurderingen fokuserte nemnda på at det var snakk om en hensiktsmessig endring som ivaretok oppdragsgivers behov. Nemnda viste også til at alternativet – å gå ut med ny anskaffelse – ikke ville ha

¹⁵ Premiss 36.

sikret ivaretagelse av formålet om mest mulig effektiv ressursbruk. Vi bemerker at nemnda her selv ikke fokuserte på den kvantitative endringen, og at de ikke selv beregnet ut denne.¹⁶

I Kofa-sak 2017/165 hadde Skattedirektoratet (senere videreført til DFØ) i år 2000 kunngjort en anskaffelse om systemløsning på lønns- og personalområdet for skattefogdkontorene og deres kunder. I anskaffelsesdokumentene var det angitt at formålet var å anskaffe en *«ny og fremtidsrettet løsning»*, og at det skulle gjennomføres et pilotprosjekt der erfaringene fra dette kunne innebære at direktoratet ville ta *«initiativ til et hovedprosjekt for videre innføring av systemløsningen hos de virksomheter som ønsket å delta»*. Det hadde i årenes løp skjedd en utvidet bruk av lisenser, i tillegg til at selve programvaren var blitt videreutviklet. Nemnda kom til at det *ikke* forelå en vesentlig endring ut ifra det som ble uttrykt i anskaffelsesdokumentene.

Et særskilt spørsmål, som en stund var uavklart, er i hvilken grad *forlengelser* som ikke kan hjemles i opsjoner alltid vil utgjøre en vesentlig endring. Rettskildene knyttet til den tidligere forskriften tilsa isolert sett at enhver forlengelse utover kontraktens rammer ville være en ulovlig direkte anskaffelse, så lenge disse oversteg *de minimis*-regelen i om endringer på maks 10 % økning eller var over terskelverdiene, slik at det ikke egentlig skulle foretas noen vesentlig endringsvurdering.¹⁷

I Kofas avgjørelse 22. april 2020 i sak 2018/479 ble imidlertid denne praksisen endret. I saken hadde Utlendingsdirektoratet forlenget avtaler om drift av et asylmottak. Driftsavtalen varte totalt i syv år, og ble

¹⁶ Jf. Dragsten, *Offentlige anskaffelser* s. 743.

¹⁷ Se blant annet Ot.prp. nr. 62 (2005–2006) s. 26, Kofas saker 2011/220, 2011/209, 2011/8, 2010/165, 2010/71 og 2009/97.

¹¹ Se blant annet Kofas sak 2010/212 og sak 2018/479. Saken fra 2010 er riktignok avsagt før forskriften trådte i kraft, men forskriftens ordlyd er, som nevnt i fotnote 10, i stor grad en kodifisering av allerede gjeldende rett.

¹² Se blant annet EU-domstolens sak C-337/98 *Matra*.

¹³ Jf. anskaffelsesloven § 1 og Thue m.fl., *Lov og forskrift om offentlige anskaffelser med kommentarer*, 2018 s. 1039.

¹⁴ Jf. Kofas sak 2017/162 premiss 49–50, anskaffelsesloven § 4 og Dragsten, *Offentlige anskaffelser*, 2013 s. 743.

forlenget i ytterligere fem måneder. Verdien av forlengelsen oversteg terskelverdien, og prisøkningen på 7,4 millioner kroner innebar en økning på 6,3 % av den opprinnelige kontraktsverdien.

Om den tidligere strenge praksisen knyttet til forlengelser uttalte Klagenemnda kort at den «gjaldt rettstilstanden under den tidligere forskriften, og var basert på uttalelser i tidligere forarbeider og daværende litteratur».¹⁸ Deretter foretok Kofa en grundig vurdering av om det forelå en vesentlig endring. Nemnda fant at prisøkningen på 6,3 % ikke utvidet kontraktens omfang betydelig, at denne beløpsmessig innebar en begrenset overskridelse av terskelverdien på tidspunktet for forlengelsen, og at forholdene ikke var slik at forlengelsen – dersom den hadde vært en del av den opprinnelige konkurransen – ville ha ført til at andre leverandører potensielt kunne ha deltatt eller blitt tildelt kontrakten.¹⁹

Avgjørelsen innebærer ikke at det nå er «fritt frem» for forlengelser. Det tryggeste er fremdeles å sørge for at man har tilstrekkelig med op-



Det viktigste oppdragsgiver gjør for å oppnå fleksible og dynamiske kontrakter er derfor etter vårt syn å arbeide grundig med endringsklausuler og gode beskrivelser av kontraktens anvendelsesområde.

sjoner og at man sørger for å planlegge ny anskaffelse i god tid før utløpet av disse. Her minner vi om at eksempelvis SSA-D (punkt 4.5) og SSA-V (punkt 4.4) allerede inneholder «redningsplanker» i form av opsjoner i standardteksten på forlengelse av avtalene i ytterligere seks måneder etter tidspunktet for avtalens opphør. Avgjørelsen innebærer imidlertid at det – i tråd med reglene i anskaffelsesforskriften – faktisk skal foretas en vurdering av om endringen er vesentlig. Oppdragsgiverne står dermed ikke den samme vanskelige situasjonen i tilfeller der det eneste hensiktsmessige alternativet er å forlenge kontrakten i en periode. Vi synes Kofas retningsskift

på akkurat dette punktet er svært fornuftig.

4 Avslutning

Vår gjennomgang viser at vurderingen av en endring opp mot vesentlighetsterskelen er sammensatt og utpreget skjønnsmessig. Dette skaper ofte stor usikkerhet og risiko der man har et reelt behov for endring underveis i kontraktsforløpet. Noe av risikoen kan tas ned ved en såkalt intensjonskunngjøring av endringen, men det rekker bare til et visst nivå og kan uansett medføre langvarige og ressurskrevende prosesser for Kofa eller domstolen uavhengig av det endelige utfallet av saken. Det viktigste oppdragsgiver gjør for å oppnå fleksible og dynamiske kontrakter er derfor etter vårt syn å arbeide grundig med endringsklausuler og gode beskrivelser av kontraktens anvendelsesområde.

Mari Klungøy Kristiansen er advokatfullmektig i Kluge Advokatfirma AS.

Stian Hultin Oddbjørnsen er partner i Kluge Advokatfirma AS.

18 Premiss 37.

19 Premiss 42.

Personopplysningslovens unntak fra informasjonsplikt og innsynsrett for opplysninger i tekst som er utarbeidet for intern saksforberedelse

Av Ove André Vanebo

1 Innledning

Personopplysningsloven (heretter «pol.») av 2018 gjennomfører EUs personvernforordning¹ (heretter «forordningen») i norsk rett, se § 1. Forordningen pålegger den behandlingsansvarlige å gi informasjon om sin opplysningsbehandling til personen som en personopplysning kan knyttes til («den registrerte»),² i samsvar med artiklene 13 og 14. Den registrerte har også rett til innsyn vedrørende opplysningsbehandlingen, se forordningen artikkel 15.

Loven inneholder imidlertid flere unntak fra artiklene 13, 14 og 15. Et prinsipielt viktig unntak gjelder opplysninger som «*utelukkende finnes i tekst som er utarbeidet for intern saksforberedelse, og som heller ikke er utlevert til andre, så langt det er nødvendig å nekte innsyn for å sikre forsvarlige interne avgjørelsesprosesser*», jf. pol. § 16 første ledd bokstav e. Unntaket gjelder uavhengig av om opplysningene er lagret elektronisk eller manuelt.³

Det er den behandlingsansvarlige som gis adgang til å gjøre unntak fra rettighetene etter forordningen art. 13, 14 og 15. Unntaket kan *ikke* an-



Ove A. Vanebo

ses som en *plikt* til å unnta opplysningene, og den behandlingsansvarlige må kunne velge å gi ut de aktuelle opplysningene i interne dokumenter selv om vilkårene for unntak er til stede.⁴ Andre lover kan imidlertid pålegge den behandlingsansvarlige likevel å unnta opplysningene fra innsyn, f.eks. forbudet mot å bryte taushetsplikt etter straffeloven §§ 209 første ledd og 211.

Når unntaket gir adgang til å la være å informere og gi innsyn, bør behandlingsansvarlige kunne påvise at unntaksbestemmelsen kommer til

anvendelse for dem.⁵ Det kan utledes av forordningen art. 23 nr. 2 bokstav h at behandlingsansvarlig bør informere de registrerte om begrensningen av informasjonspliktene, med mindre dette vil skade formålet med unntaksreguleringen.

Under redegjør jeg for innholdet i pol. § 16 første ledd bokstav e. Etersom forvaltningsrettens unntak for organinterne dokumenter i stor grad vil regulere unntaksadgangen i offentlig sektor, vil jeg fokusere på betydningen for behandlingsansvarlige i privat sektor. Hvorvidt reguleringen faktisk omfatter intern saksforberedelse i privat sektor er et eget spørsmål. Min oppfatning er at den gjør det, noe jeg redegjør for i punkt 3.

Den personopplysningsrettslige innsynsretten gjelder for øvrig ved siden av retten til innsyn etter forvaltningsloven og offentleglova. Unntakene fra innsynsrett etter forvaltningsloven og offentleglova utgjør ikke unntak fra innsynsretten etter personvernforordningen.⁶ Pol. § 16 første ledd bokstav e unntar imidlertid kun *opplysninger*, mens offentleglovas unntaksreguleringer i

1 Forordning (EU) 2016/679.

2 Se forordningen artikkel 4 (1); sml. også definisjonen i personopplysningsloven av 2000 § 2 nr. 6.

3 Uttrykket «tekst» trekker i denne retning, og NOU 1997: 19 s. 84 la dette til grunn for den lignende reguleringen i personopplysningsloven av 2000 § 23.

4 Michal Wiik Johansen, Knut-Brede Kaspersen og Åste Marie Bergseng Skullerud, *Personopplysningsloven; Kommentartutgave*, (2001) s. 175–176. Kilden gjelder personopplysningsloven av 2000, men må også gjelde for dagens lov.

5 Artikkel 29-gruppa, *Guidelines on transparency under Regulation 2016/679* (WP260 rev.01), (2018) s. 30.

6 Prop. 56 LS (2017–2018) s. 63.

flere tilfeller kan omfatte *både* opplysninger og hele dokumenter.⁷

“ Når unntaket gir adgang til å la være å informere og gi innsyn, bør behandlingsansvarlige kunne påvise at unntaksbestemmelsen kommer til anvendelse for dem

2 Kort om Reguleringsbakgrunn og innhold

Unntaket for opplysninger i interne dokumenter var tidligere inntatt i personopplysningsloven av 2000 § 23 første ledd bokstav e, som unntok opplysninger som «*utelukkende finnes i tekst som er utarbeidet for den interne saksforberedelse og som heller ikke er utlevert til andre*». Bestemmelsen har vært delvis praktisk begrunnet, og delvis bygget på hensynet til den interne saksforberedelse.⁸

Departementet foreslo opprinnelige å la være å videreføre bestemmelsen i den nye personopplysningsloven av 2018, begrunnet i forordningen artikkel 23, som legger rammer for unntak fra registrertes rettigheter. Begrensningene må overholde det vesentlige innholdet i de grunnleggende rettighetene og frihetene og være nødvendige og forholdsmessige tiltak i et demokratisk samfunn av hensyn til et av målene i art. 23 nr. 1 bokstav a til j. Unntaksregelen ville i mange tilfeller kunne favne videre enn det som

kan anses som nødvendig og proporsjonalt.⁹

Flere høringsinstanser mente imidlertid at unntaket var svært praktisk, og departementet ønsket å etterkomme ønsker om å beholde det.¹⁰ Unntaket for opplysninger i interne dokumenter ble derfor videreført med tilleggsvilkår som skal sikre at det bare gjøres unntak i den utstrekning hensynet til den interne saksforberedelse gjør seg gjeldende og unntak er nødvendig av hensyn til denne. Departementet uttrykte at et slikt vilkår medførte at unntaket kunne videreføres med grunnlag i

“ Unntaket for opplysninger i interne dokumenter ble derfor videreført med tilleggsvilkår som skal sikre at det bare gjøres unntak i den utstrekning hensynet til den interne saksforberedelse gjør seg gjeldende og unntak er nødvendig av hensyn til denne

artikkel 23 nr. 1 bokstav e og i.¹¹ Bestemmelsen regulerer omfanget av begrensningen, kategoriene av

behandling og garantiene for å unngå misbruk.¹²

Kilder som belyser den forrige reguleringen i pol. av 2000 er relevante i analysen, fordi den nye bestemmelsen i utgangspunktet er en videreføring av den tidligere rettstilstanden.¹³ Unntaket i pol. av 2000 § 23 første ledd bokstav e var utformet med inspirasjon av offentlighetsloven § 5 første ledd (nå offl. § 14 første ledd) og fvl. § 18 annet ledd første punktum. Disse forvaltningsrettslige reguleringene kan derfor kaste lys over forståelsen av pol. § 23 første ledd bokstav e.¹⁴ Vilkåret om nødvendighet i forbindelse med beslutningsprosesser svarer til vilkåret i offl. § 15 første ledd, og departementet mener innholdet i offentliglovas bestemmelse også kan gi veiledning for tolkningen av pol. § 16 første ledd litra e.¹⁵

3 Gjelder reguleringen både offentlig og privat sektor?

I lovkommentaren til personopplysningsloven fra Bergsens Skullerud m.fl. (2019) går forfatterne langt i å mene at unntaket for interne dokumenter kun gjelder for offentlig sektor. Forfatterne argumenterer med at det i «*forarbeidene ser [...] ut til å være forutsatt at dette unntaket kun skal gjelde for offentlige organer*».¹⁶ Videre viser de til at unntaket må holde seg innenfor rammene av forordningen artikkel 23, noe som tilsier at et unntak kan aksepteres når det er «*snakke om tungtveiende samfunnsmessige interesser*».¹⁷ Forordningens formuleringer indikerer at det neppe «*er rom for nasjonale unntak fra*

7 Personvernemndas avgjørelse PVN-2016-15 *Tromsø kommune II. Begjæring om omgjøring*. Se også Dag Wiese Schartum, *Personvern og offentlig innsyn; Utredning for Offentlighetslovutvalget*, (2002) s. 36–37, som går inn på reguleringen i personopplysningsloven av 2000 § 23, men som også må sies å gjelde for dagens bestemmelse.

8 Ot.prp. nr. 92 (1998–99) side 122–123.

9 Jf. artikkel 23 nr. 1, se Justis- og beredskapsdepartementet, *Ny personopplysningslov – gjennomføring av personvernforordningen i norsk rett*, datert 6. juli 2017. s. 50.

10 Prop. 56 LS (2017–2018) s. 61 og 63.

11 Prop. 56 LS (2017–2018) s. 63. Artikkel 23 nr. 1 bokstavene e og i gir grunnlag for å fravike registrertes rettigheter for henholdsvis andre viktige mål av generell allmenn interesse for Unionen eller en medlemsstat, og vern av den registrertes interesser eller andres rettigheter og friheter.

12 Forordningen artikkel 23 nr. 2 bokstavene a, c, d og h.

13 Prop. 56 LS (2017–2018) s. 217.

14 Wiik Johansen m.fl. (2001) s. 180, og Wiese Schartum (2002) s. 37.

15 Prop. 56 LS (2017–2018) s. 217.

16 Åste Marie Bergsens Skullerud, Cecilie Rønnevik, Jørgen Skorstad og Marius Engh Pellerud, *Personopplysningsloven og personvernforordningen (GDPR); Kommentartutgave*, (2019) s. 89.

17 I.c.

innsynsretten i personopplysninger i interne dokumenter i privat sektor.¹⁸

Etter mitt skjønn holder ingen av disse begrunnelsene for å tolke unntaket så snevert at det kun gjelder for offentlig sektor. For det første påpeker Bergsens Skullerud m. fl. at:¹⁹

«Departementet henviser [i forarbeidene] til offentleglova § 14 første ledd, som gjelder dokumenter som et forvaltningsorgan har utarbeidet for «si eiga interne saksførebuing», se Prop. 56 LS (2017–2018) kapittel 38, særmerknadene til personopplysningsloven § 16 (forarbeidene viser her feilaktig til offentleglova § 15, som gjelder dokumenter som er innhentet fra underordnede organer).»

Argumentet synes å være at dette underbygger at unntaket kun gjelder for organer som er underlagt offentleglova. Resonnementet er i alle tilfelle noe uklart. At departementet har latt seg inspirere av offentleglovas unntak impliserer neppe at unntaket ikke kan anvendes på privat virksomhet, som også vil ha saksforberedelser. I motsetning til offentleglova henviser ikke ordlyden i personopplysningslovens regulering til at den gjelder offentlige organer, og er dermed nøytral hva gjelder offentlig eller privat sektor. Jeg er også uenig i at departementets henvisning til § 15 må være feilaktig. Det fremstår som logisk at departementet har sett hen til ordlyden i offentleglova § 15, som gjelder unntak når «det er nødvendig for å sikre forsvarlige interne angjerdsprosessar».

En oppfatning om at det nye unntaket kun gjelder for offentlig sektor, synes også å være vanskelig å forene med forarbeidenes uttalelser om at unntaket er ment å være en videreføring av den tilsvarende reguleringen i personopplysningsloven av 2000 – med kun et tilleggsvilkår om nødvendighet av hensyn

til saksbehandling.²⁰ Sistnevnte regulering i loven av 2000 gjaldt også privat sektor.²¹

For det annet er jeg uenig i at rammene for unntak i medhold av artikkel 23 kun vil omfatte «tungtveiende samfunnsmessige interesser» i mer snever forstand. Etter artikkel 23 nr. 1 bokstav i vil unntaket også kunne forankres i «vern av den registrertes interesser eller andres rettigheter og friheter». Alternativet i bokstav i må trolig favne vidt, og det er antatt at det vil innbefatte en rekke individorienterte rettigheter og interesser. Eksempler på dette er bl.a. rett til eieendom, opphavsrettigheter, bedriftshemmeligheter, taushetsplikt, mulighet for rettssaksforberedelser, og å hindre at opplysningsutlevering utsetter andre for fare.²²

Tilsvarende betraktninger er lagt til grunn for den danske databeskyttelsesloven,²³ som inneholder unntak for informasjonsplikt og innsynrett i henhold til forordningen. Etter lovens § 22 første ledd gjelder ikke rettighetene «hvis den registrertes interesse i opplysningerne findes at burde vige for afgørende hensyn til private interesser, herunder hensynet til den pågældende selv». Hensynene antas å kunne ligge innenfor rammene av forordningen artikkel 23 nr. 1 bokstav i.²⁴ Reguleringen i § 22 første ledd kan gi grunnlag for unntak bl.a. begrunnet i avgjørende hensyn til andre involverte personer (f.eks. barn av den registrerte), beskyttelse av vitner, hvis formålet med innsamlingen forspilles dersom den registrerte får informasjon mv.²⁵

20 Prop. 56 LS (2017-2018) s. 63 og 217.

21 Ot.prp.nr. 92 (1998–1999) s. 121 og Wiik Johansen m.fl. (2001) s. 181.

22 Sören Öman, *Dataskyddsförordningen (GDPR) m.m.; En kommentar*, (2019) s. 376.

23 Lov nr. 502 av 23. mai 2018.

24 Justisministeriet, *Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning; Betænkning nr. 1565*, (2017) s. 398.

25 Lovforslag nr. L 68, fremsatt for Folketinget den 25. oktober 2017, s. 191.



Det er neppe noe krav om at teksten faktisk brukes til saksforberedelse, noe som innebærer at det avgjørende vil være at formålet var slik bruk. Noen ganger blir dokumenter utarbeidet av flere grunner, og det må være tilstrekkelig at formålet i hovedsak var intern saksforberedelse.

Som eksempler nevnes følgende i forarbeidene:

«Efter en konkret vurdering vil det være muligt at nægte indsigt i oplysninger, hvis dette vil medføre, at virksomhedens forretningsgrundlag, forretningspraksis eller know-how derved vil lide væsentlig skade. Det vil endvidere efter en konkret vurdering være muligt at nægte indsigt i interne vurderinger af, hvorvidt virksomheden på basis af foreliggende oplysninger vil indgå et kontraktforhold, andre et bestående kontraktforhold, stille særlige vilkår for fortsættelse, eventuelt helt opsigte et kontraktforhold og lignende tilfælde. På samme måde vil det efter omstændighederne være muligt at nægte indsigt i f.eks. et notat, der vurderer, hvorvidt der er udsigt til, at en bestemt retssag mod en kunde kan vindes, eller et internt notat i en sag, der påpeger mulige tegn på, at en kunde har forsøgt at udøve forsikringsvig over for et forsikringselskab eller forsøgt at unddrage sig forpligtelsen i medfør af f.eks. en lånekontrakt.»²⁶

Også artikkel 23 bokstav e vil ha et nokså vidt anvendelsesområde, som i ytterste konsekvens kan utfordre

18 I.c.

19 I.c.

26 I.c.

forordningens harmoniseringsmålsetting.²⁷

Reguleringen i § 16 første ledd bokstav e omfatter derfor etter min oppfatning både offentlig og privat sektor. Dette synes også å ha støtte i lovkommentaren fra Eva Jarbekk m.fl. (2019), som forutsetter at «*unntaket vil ha stor praktisk betydning i privat sektors*».²⁸

4 Intern saksforberedelse

At teksten må være «*utarbeidet for intern saksforberedelse*», betyr etter alt å dømme at *formålet* med utarbeidelsen av dokumentet må være at det skal anvendes av behandlingsansvarlig som en del av forberedelsen av en sak.²⁹ Vilkåret vil sjelden få selvstendig betydning for om bestemmelsen kan anvendes.³⁰

Det er neppe noe krav om at teksten *faktisk* brukes til saksforberedelse, noe som innebærer at det avgjørende vil være at *formålet* var slik bruk.³¹ Noen ganger blir dokumenter utarbeidet av flere grunner, og det må være tilstrekkelig at formålet i hovedsak var intern saksforberedelse.³² Antagelig er det heller ikke noe krav om at dokumentet må gjelde én bestemt sak, slik at også et

dokument som er laget for flere saker kan unntas fra innsyn.³³

Teksten behøver heller ikke alltid gjelde *spesifikke* synspunkter knyttet til en bestemt sak; også mer generelle utredninger og synspunkter *kan* etter forholdene anses å være utarbeidet for interne saksforberedelse.³⁴ Terskelen for unntak for slike opplysninger synes imidlertid å være nokså høy.³⁵

Bestemmelsen kan komme til anvendelse på tallrike situasjoner som må anses som saksforberedelse. Utkast til brev og andre dokumenter, samt konsepter, som utarbeides og bearbeides i forbindelse med saker, kan typisk falle inn under unntaket.³⁶ Unntaket har blitt brukt ofte i forbindelse med utarbeidelse av arbeidsmiljøundersøkelser.³⁷ Normalt må man også kunne unnta arbeidsgivers vurderinger av den ansattes arbeidsinnsats og fremtidige planer for den ansatte.³⁸ Et praktisk tilfelle er når en saksbehandlers tolkning av saksforhold utformes og legges frem for ledelsen som grunnlag for virksomhetens beslutning i en sak.³⁹ Et annet eksempel er at en virksomhet samler inn personopplysninger fra for-

skjellige kilder for å planlegge en ny nettbasert tjeneste.⁴⁰

5 Utleveringskriteriet

Loven gir liten veiledning om hva som menes med at opplysningene ikke må være «*utlevert til andre*». I lovproposisjonen som lå til grunn for personopplysningsloven av 2000 heter det at: «*Unntaket gjelder bare dersom opplysningene ikke er utlevert til andre, dvs andre forvaltningsorganer eller andre rettssubjekter enn den behandlingsansvarlige*».⁴¹

Det betyr at korrespondanse i forbindelse med at et selskap kjøper tjenester av et annet, i utgangspunktet vil innebære en utlevering til andre av de personopplysninger som er inntatt i korrespondansen. Det samme må som hovedregel gjelde dersom et datterselskap sender til morselskap dokumenter til en sak, etter som unntaket ikke gjelder for opplysninger i konserninterne dokumenter.⁴² Det kan likevel tenkes at overføringene ikke innebærer at opplysninger er «*utlevert til andre*» i lovens forstand, avhengig av avsenderens og mottakerens roller, se under.

Etter min oppfatning er det naturlig å se hen til når et organinternt dokument mister sin interne karakter etter offentliglova § 14, jf. overføringsverdien nevnt i punkt 2 over. Den opprinnelige bestemmelsen i personopplysningsloven av 2000 § 23 første ledd bokstav e var ment å omfatte det som tilsvarer offentlighetslovens forståelse av organinterne dokumenter.⁴³ I kravet til at dokumentet er organinternt ligger det at: «*Adgangen til å unnta dokumentet går tapt dersom det blir utlevert, enten i original eller i kopi, for eksempel til en part i saken*».⁴⁴

40 Dag Wiese Schartum og Lee A. Bygrave, *Personvern i informasjonssamfunnet*, 3. utgave (2016) s. 210.

41 Ot.prp.nr. 92 (1998–1999) s. 123.

42 Prop. 56 LS 2017–2018 s. 64.

43 Ot.prp.nr. 92 (1998–1999) s. 121–122.

44 Note 180 av Jan Fridthjof Bernt til offentliglova i Gyldendal Rettsdata (2014).

27 Paul Voigt og Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide Book*, (2017) s. 185. Voigt og von dem Bussche henviser i note 238

videre til Jan-Michael Grages kommentar til artikkel 23, avsnitt 26, I: Kai-Uwe Plath (red.), *BDSG/DS-GVO. Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG*, (2016).

28 Eva Jarbekk (red.), *Personopplysningsloven og personvernforordningen (GDPR) med kommentarer*, (2019) s. 69.

29 Ot.prp. nr. 102 (2004–2005) s. 133 og Johan Greger Aulstad, *Innsynsrett*, (2018) s. 273.

30 Antatt om den lignende reguleringen i offl. § 15, se note 200 av Jan Fridthjof Bernt til offentliglova i Gyldendal Rettsdata (2014).

31 Justis- og politidepartementet, *Rettleiar til offentliglova*, G-2009-419 (2010) pkt. 7.3.2.4.

32 Ot.prp. nr. 102 (2004–2005) s. 133.

33 Justis- og politidepartementet (2010) pkt. 7.3.2.4.

34 Aulstad (2018) s. 274.

35 Kristian Brandt, Jon Sverdrup Eftestad, Hanne Harlem og Camilla Selman, *Offentliglova; Lovkommentar*, (2018) s. 251.

36 Ot.prp.nr. 92 (1998–1999) s. 24–25 og 122.

37 Kari Gimmingsrud, «*En ny tidsalder for personvern i Europa*», I: *Arbeidsrett* vol. 14 nr. 2 (2017), s. 234.

38 Dette var tilfellet etter den gamle personregisterforskriftens unntak for interne saksdokumenter, som var forankret i forskriften § 1-5, jf. personregisterloven § 7 fjerde ledd, se Dag Wiese Schartum note 27 til personregisterloven i Gyldendal Rettsdata (udatert).

39 Kommunal- og moderniseringsdepartementet, *Informasjonsplikt og innsynsrett etter personopplysningsloven*, (2015) s. 23.

Dokumentet vil ut fra dette ikke anses som utlevert til andre bare fordi det blir vist frem for utenforstående, så lenge det ikke utleveres kopi eller utskrift av teksten.⁴⁵

Oversending til klage-, kontroll- eller tilsynsorganer vil trolig heller ikke medføre at teksten mister sin interne karakter, jf. forståelsen av offl. § 14 første ledd.⁴⁶

En annen problemstilling er om opplysningene vil være «utlevert til andre» dersom en annen enn den behandlingsansvarlige står for utarbeidelse av teksten i saksforberedelsen. Vi kan typisk tenke oss at en bedrift får en advokat til å utrede et spørsmål i forbindelse med en sak, som så sender en rapport til bedriften. Jeg mener også slike situasjoner med innhenting av råd, utredninger m.v., *ikke* vil medføre at opplysninger er «utlevert til andre». En vid forståelse av kriteriet gjør unntaket svært begrenset, og ville videre medføre en uthuling av unntakets formål. Lovens ordlyd gir ingen anvisning om at teksten må være utarbeidet av den behandlingsansvarlige selv – i motsetning til fvl. § 18 a, som krever at det må være tale om «dokument som *et forvaltningsorgan har utarbeidd* for sin egen interne saksforberedelse» [min kursivering]. Det tilsvarende unntaket i pol. av 2000 § 23 første ledd bokstav e ga et vidt spillerom for så vidt gjaldt personkrets som kunne stå for utarbeidelse av tekst, og juridisk teori påpekte følgende:⁴⁷

«Unntaket i personopplysningsloven har ingen begrensninger med hensyn til hvem som har utarbeidet dokumentet som ønskes unntatt. Det er utelukkende formålet for utarbeidelsen av dokumentet som er avgjørende for om det kan unntas etter personopplys-

ningsloven. [...] Private behandlingsansvarlige vil kunne unnta opplysninger i dokumenter som er utarbeidet av andre utenforstående enn særlig rådgivere eller sakkyndige.»

Wiese Schartum nevner imidlertid at utleveringskriteriet innebærer at: «Personopplysninger og beskrivelser av hvorledes personopplysninger blir behandlet som sakkyndig sender et forvaltningsorgan, kan ... ikke unntas fra innsyn etter personopplysningsloven (med mindre det gjelder taushetsplikten) fordi det er «utlevert til andre.»⁴⁸ I noen tilfeller vil dette utvilsomt være riktig, men det fremkommer ikke hvilke sakkyndige han sikter til eller hvilke situasjoner eksempelet omfatter. Det er derfor naturlig å oppfatte at Wiese Schartum mener dette må gjelde generelt for sakkyndiges oversendinger. Det er ikke nærmere problematisert hva som ligger i utleveringskriteriet, og jeg finner ikke Wiese Schartums resonneringer overbevisende, jf. mine vurderinger over.

Også ulike eksterne representanter for virksomheten bør kunne utveksle opplysninger fritt med den aktuelle virksomheten, uten at dette anses som «utlevering». Datatilsynet har avvist å tolke unntaket så begrenset at «bruk av advokat i personalkonflikter i seg selv [vil] medføre at dokumenter som utelukkende er til intern saksforberedelse ikke vil være omfattet av dette unntaket fra innsynsretten».⁴⁹ I Datatilsynet praksis er det derfor lagt til grunn at virksomhetens korrespondanse med advokater som representerer virksomhetene, ikke er utlevering – bl.a. begrunnet i konsekvenshensyn, se bl.a. PVN-2012-13.

I juridisk teori er det antatt at det etter offentleglova ikke er skjedd en utsending ved at et dokument oversendes til private firmaer som utfører granskningsoppdrag. Dokumentet mister heller ikke sin organinterne karakter dersom intervjuobjektet under gransknin-

gen har fått lese gjennom referatet. At et intervjuobjekt som er ansatt i virksomheten får en kopi av referatet vil etter offentleglova ikke være nok til at dokumentet er utlevert utenfor organet.⁵⁰ Det er gode grunner for å mene at dette også må gjelde for personopplysningslovens unntak her. En annen sak er om eksterne intervjuobjekter får tilsendt referater for signering/godkjenning e.l., noe som vil utelukke at unntaket i § 16 kan anvendes.⁵¹

Det kan problematiseres om opplysningene er «utlevert til andre» ved utveksling mellom felles behandlingsansvarlige – dvs. når to eller flere behandlingsansvarlige i fellesskap fastsetter formålene med og midlene for behandlingen, jf. forordningen artikkel 26 nr. 1. Problemstillingen er ikke berørt av departementet. Tradisjonelt sett har delt behandlingsansvar medført at selskaper kan utveksle opplysninger seg imellom uten hindre som begrenser utlevering til tredjeparter.⁵² Etter forordningens definisjoner synes heller ikke andre felles behandlingsansvarlige å være «tredjepart» overfor en behandlingsansvarlig, se forordningen artikkel 4 (10).⁵³ Selv om løsningen her er uklar, me-

50 Brandt m.fl. (2018) s. 229–230.

51 Ibid. s. 231.

52 Thomas Olsen, *Personvernøkende identitetsforvaltning* (CompLex 2015-02), (2015) s. 299.

53 Selv om felles behandlingsansvarlige ikke vil være tredjepersoner overfor hverandre, kan de likevel være «mottakere», jf. forordningen 4 (9), se Artikkelen 29-gruppa, *Guidelines on transparency under Regulation 2016/679* (WP260 rev.01) s. 37: «The term “recipient” is defined in Article 4.9 as “a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, *whether a third party or not*” [emphasis added]. As such, a recipient does not have to be a third party. Therefore, other data controllers, joint controllers and processors to whom data is transferred or disclosed are covered by the term “recipient” and information on such recipients should be provided in addition to information on third party recipients.»

45 Note 180 av Jan Fridthjof Bernt til offentleglova i Gyldendal Rettsdata (2014).

46 Note 180 av Jan Fridthjof Bernt til offentleglova i Gyldendal Rettsdata (2014).

47 Wiik Johansen (2001) s. 180–181.

48 Wiese Schartum (2002) s. 37.

49 PVN-2012-13.

ner jeg dette taler for at utlevering mellom felles behandlingsansvarlige ikke innebærer utlevering til andre.

6 Kravet til nødvendighet

Nødvendighetskriteriet innebærer at bestemmelsen kan anvendes bare i tilfeller hvor det er et reelt og saklig behov for å gjøre unntak.⁵⁴ Begrepet «nødvendig» må trolig – i likhet med offentliglovas tilsvarende regulering – forstås som synonymt med «påkrevd», dvs. at nødvendighetskriteriet tolkes strengt.⁵⁵ Dette er etter alt å dømme strengere enn slik uttrykket «nødvendig» tradisjonelt forstås i persondataretten, hvor det er en mer relativ standard avhengig av behandlingen⁵⁶ – og som regel et spørsmål om den aktuelle behandlingen vil innebære en effektivisering eller påtakelig reduksjon i kostnader.⁵⁷ Nødvendighetskriteriet skal antagelig kun vektlegge hensynet til

den aktuelle behandlingsansvarliges egen saksforberedelse.⁵⁸

Sivilombudsmannen har i flere uttalelser lagt til grunn at kjerneområdet for unntaket i offentliglova for dokumenter av hensyn til interne beslutningsprosesser, er behovet for fri og fortrolig meningsutveksling i saksforberedelsen, se eksempelvis SOM-2010-2832 og SOM-2016-1004. De samme hensyn ligger også til grunn for unntaket på det persondatarettslige området, jf. Personvernemndas avgjørelse PVN-2016-15. Ut fra dette synes forsvarlighetskriteriet særlig å bygge på behovet for å få en opplyst og grundig drøftet avgjørelsesprosess.

Unntaket skal ikke bare ivareta hensynet til å sikre forsvarlige avgjørelsesprosesser i den konkrete saken, men også f.eks. mer langsiktige prosesser og saksforberedelse generelt. Av den grunn er det også relevant å hensynta at innsyn kan få skadevirkninger også i senere prosesser, ved at innsyn f.eks. kan få involverte til å bli mer tilbakeholdne med å drøfte forhold.⁵⁹ Vurderingen

av om det er nødvendig å unnta opplysningene fra innsyn, må imidlertid alltid bli konkret. Det er naturlig å se hen til bl.a. dokumenttype, situasjonen/sammenhengen dokumentet er opprettet og avgitt i forbindelse med, opplysningstyper og avsenderens rolle.⁶⁰

Typiske eksempler på når nødvendighetsvilkåret kan tenkes oppfylt, er når det skal utformes utkast til endelig avgjørelse i saker. Det samme gjelder når det gis råd og vurderinger om hvordan en virksomhet bør forholde seg i en sak. Det vil derimot trolig være i mer spesielle tilfeller man kan unnta råd og vurderinger i rene administrative og faglige spørsmål, særlig om de ikke knytter seg til hvordan virksomheten bør forholde seg i en bestemt sak. Det samme gjelder tekst som bare inneholder generelle premisser for beslutningsgrunnlaget – som generelle utredninger av faktiske forhold eller gjeldende rettstilstand.⁶¹

Ove A. Vanebo er senioradvokat i Kluge Advokatfirma.

54 Brandt m.fl. (2018) s. 249 og Aulstad (2018) s. 274.

55 Jan Fridthjof Bernt og Harald Hove, *Offentliglova med kommentarer*, (2009) s. 145 og Aulstad (2018) s. 274.

56 Ot.prp. nr. 92 (1998–99) side 103.

57 EU-domstolens dom *Huber mot Tyskland*, C-524/06, jf. også SOU 2017:39 s. 105–106.

58 Aulstad (2018) s. 275 og Bernt og Hove (2009) s. 145 for den lignende reguleringen i offl. § 15 første ledd.

59 Prop. 56 LS (2017–2018) s. 217 og Ot.prp. nr. 102 (2004–2005) s. 134.

60 Brandt m.fl. (2018) s. 250.

61 Ot.prp. nr. 102 (2004–2005) s. 134 og Brandt m.fl. (2018) s. 250–251.





Halvor Manshaus

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

USPTO: AI kan ikke være «oppfinner»

Ved at det stadig frembringes nye og mer avanserte former for kunstig intelligens, eller AI (Artificial Intelligence), gir det seg selv at bruksområdene for AI utvides tilsvarende. Fra å være rene forskningsprosjekter innen begrensede aspekter av AI, har dette blitt et bredt område drevet frem av sterke kommersielle interesser. Det investeres i dag milliarder av kroner på utvikling innen denne fronten, samtidig som store teknologikonserner kjøper opp oppstartsvirksomheter innen AI for tilsvarende beløp.

Det finnes flere ulike måter å definere hva en AI er. En vanlig tilnærming er å definere AI som informasjonsteknologi som justerer sin egen aktivitet (Store Norske Leksikon), eller at AI er en teknikk benyttet for å gi teknologiske innretninger en intelligent respons. En mer funksjonell tilnærming vil kunne beskrive AI som databaserte systemer i stand til å utføre oppgaver eller tankerekker som normalt krever intelligens og erfaring på nivå med et voksent menneske. I informatikken snakker man gjerne om svake og sterke former for AI, der førstnevnte omfatter semi-intelligente datasystemer som utfører konkrete oppgaver uten at det foreligger tilsvarende konkrete programrutiner som beskriver handlingen. Dagligdagse eksempler på en slik snever AI er Alexa, Siri og Google Assistant. Spesialiserte systemer som overvåker og flagger mate-

rialtretthet på flydeler eller som tolker meteorologiske data ligger også innenfor denne kategorien.

Sterke former for AI er kategorien som beveger seg i retning av menneskets evne til å absorbere og behandle informasjon, for deretter å resonnerer, konkludere og handle. Dette er den formen for AI som fanger opp det vi tenker på som en menneskelignende eller generell intelligens – der AI'en også kan omtales som superintelligent grunnet de fordelene et datasystem har ved lagring og behandling av store mengder informasjon. Det er slik sterk eller generell kunstig intelligens (GKI) som på sikt har et potensial til virkelig å forandre vår verden.

Et skritt mot GKI ser vi i spesialiserte dataenheter som har vekket oppsikt ved å vinne over de beste menneskene i verden innenfor flere forskjellige spill som krever ulike nivåer av innsikt, forståelse og erfaring. Dette har vært en gradvis utvikling gjennom stadig mer komplekse spillformer, fra Kasparov ble slått av Deep Blue i 1997, videre til maskinen Watson's seier i Jeopardy i 2011 (der premien var 1 MUSD) og til AlphaGo slo den ledende mesteren i Go i 2017. Etter dette har disse spillene gått over i en fase der nye generasjoner av AI spiller mot sine «foreldre», og utviser en eksponentiell prestasjonskurve. Der AlphaGo hadde lært spillet gjennom å bli matet inn med samtlige trekk fra en rekke tidligere mesterskap, fikk

«barnet» AlphaGo Zero bare bruksanvisningen til Go for sine selvstudier – før den slo sin forgjenger 100-0 i en ren digital kampserie. Dette sier noe om den nærmest eksponentielle fremgangen innen forskning på AI.

Utviklingen disse årene har altså vært dramatisk, og det åpnes opp for stadig nye spørsmål etter hvert som AI tar mer plass og går inn som en integrert del i dagens samfunn. Flere slike spørsmål ligger i spennet mellom jus og etikk, der det er vanskelig å se den fulle rekkevidden og retningen av AI-generasjonene som ligger foran oss. Det amerikanske patentkontoret (USPTO) kom nylig med en avgjørelse som berører to patentsøknader, der den samme AI'en var ført opp som oppfinner i begge patentsøknadene. Det var søkt om patent på en innretning for å oppbevare mat, samt for en blinkende varsel-lampe. I den konkrete avgjørelsen i søknadssaken USPTO 16/524,350 kom USPTO til at klage om pålegg om å rette søknaden ikke kunne føre frem.

De samme to søknadene har tidligere blitt avvist av det Europeiske Patentkontoret (EPO) og Storbritannias patentkontor (IPO), og det skal ligge flere tilsvarende søknader inne i flere jurisdiksjoner, f.eks. Israel. Bak alle disse søknadene står «The Artificial Inventor Project» (AIP), som har fremmet søknadene på vegne av DABUS, som står for

Device for the Autonomous Bootstrapping of Unified Science. I søknadsfeltet for fornavn var det ført opp DABUS, mens feltet for etternavn lød «*Invention generated by artificial intelligence*». Patentsøker var angitt som en navngitt privatperson som sto bak DABUS. Selv om DABUS står oppført som oppfinner, er det altså ikke slik at bakmennene ønsker å gi AI'er like rettigheter som mennesker i denne sammenheng. I stedet er fokus på den rollen som et datasystem har, og spesielt hvilken rolle slike systemer kan forventes å ha i fremtiden, ved frembringelsen av nye oppfinnelser. Et viktig spørsmål i denne sammenheng er hvem som skal anses å være oppfinner av nye tekniske innovasjoner som frembringes av en AI. Her vil det kunne være et utall av variasjoner, fra der en AI selv frembringer en oppfinnelse, til ulike samarbeidsformer for eksempel der en eller flere personer mater inn opplysninger eller forutsetninger som grunnlag for arbeidet. AIP er av den oppfatning at det i mange situasjoner vil være riktig å tilskrive den eller de som har frembragt den aktuelle AI som rettighetshavere til eventuelle patenter som frembringes av systemet.

Formålet med de to søknadene var altså i stor grad å skape debatt og oppmerksomhet rundt denne problemstillingen, som inngår i en bredere debatt knyttet til AI og rettigheter innenfor flere områder. 30. oktober 2019 publiserte USPTO under tittelen «*Request for Comments on Intellectual Property Protection for Artificial Intelligence Innovation*» en rekke spørsmål knyttet til eksisterende regelverk og bruk av AI, der publikum ble invitert til å inngi sine meninger. Disse spørsmålene omfattet problemstillinger knyttet til opphavsrett, varemerker og andre lignende rettigheter, og kom som et supplement til tilsvarende spørsmål publisert 27. august 2019 med spørsmål knyttet direkte opp mot

patentretten¹. USPTO oppretter såkalte «*initiatives*», fokusområder for spesielt viktige områder som vies ekstra oppmerksomhet. For tiden er det to slike fokusområder: «*Artificial Intelligence*» og «*Expanding Innovation*». Dette forteller oss at AI er et viktig og dagsaktuelt tema. USPTO har i denne forbindelse samlet innhold og ressurser knyttet opp mot AI på en egen dedikert nettside.²

I den konkrete saken var det altså ikke var ført opp en person som oppfinner, og det ble dermed gitt varsel om at skjemaet «*does not identify each inventor by his or her legal name*» med frist for retting. Søkeren klaget over dette, men ble møtt med ytterligere et varsel om å rette søknadsskjemaet. Klagen fra søker ble avvist, og søker påklaget deretter vedtaket i egen klage av 20. januar 2020. I denne klagen ble det særlig fremhevet at oppfinnelsen rent faktisk var gjort av DABUS, og at «... *this «creativity machine» is programmed as a series of neural networks that have been trained with general information in the field of endeavor to independently create the invention*». Det ble videre vist til at DABUS ikke var innrettet mot å løse et angitt eller på forhånd konkretisert problem, og at det var DABUS selv som vurderte oppfinnelsen til å ha nyhet og oppfinnelseshøyde. På denne bakgrunn ble det anført at status som oppfinner ikke kan begrenses til kun å gjelde mennesker, og at angivelsen av DABUS som oppfinner måtte være riktig fremgangsmåte i søknaden.

USPTO la derimot til grunn at regelverket forutsetter at søkeren er en enkeltperson, og legger i dette at søkeren må være et menneske. I avgjørelsen er det vist til definisjonen i 35 U.S.C. §§ 100(f), som angir at begrepet inventor betyr: «...*the indi-*

vidual or, if a joint invention, the individuals collectively who invented or discovered the subject matter of the invention». Tilsvarende heter det i 35 U.S.C. § 101 «**Whoever** invents or discovers any new and useful process, machine, manufacture, or composition of matter... may obtain a patent therefore, subject to the conditions and requirements of this title. (uthevelse fra avgjørelsen)»

I avgjørelsen er det fremhevet at ord som «*individual*» og «*whoever*» konsekvent benyttes ved beskrivelsen av oppfinneren, og at dette oppfattes som uttrykk for at oppfinneren forutsettes å være et menneske.

USPTO viser i denne sammenheng også til at oppfinneren i tråd med 35 U.S.C. § 115(b) skal signere en erklæring, og at ordlyden her igjen forutsetter menneskelige søkere ved bruken av pronomen som «*himself*» og «*herself*». USPTO konkluderer på dette grunnlag med at en rent språklig tilnærming viser at regelverket konsekvent forutsetter at oppfinneren er et menneske.

USPTO viser også til rettspraksis knyttet til oppfinnerbegrepet, som inneholder formuleringer og betraktninger som forutsetter at oppfinneren er en person. Det vises blant annet til sak for U.S. Court of Appeals for the Federal Circuit, University of Utah vs Max Planck Gesellschaft zur Forderung Wissenschaften e.V. (734 F.3d 1315 (2013):

«We hold that a State has no core sovereign interest in inventorship. The inventors of a patent are “the individual or, if a joint invention, the individuals collectively who invented or discovered the subject matter of the invention.” 35 U.S.C. § 100(f). It is axiomatic that inventors are the individuals that conceive of the invention:

Conception is the touchstone of inventorship, the completion of the mental part of invention. It is the formation in the mind of the inventor, of a definite and permanent idea of the complete and operative invention, as it is

1 <https://www.govinfo.gov/content/pkg/FR-2019-10-30/pdf/2019-23638.pdf>

2 <https://www.uspto.gov/initiatives/artificial-intelligence>

hereafter to be applied in practice. Conception is complete only when the idea is so clearly defined in the inventor's mind that only ordinary skill would be necessary to reduce the invention to practice, without extensive research or experimentation. [Conception] is a mental act....

Burroughs Wellcome Co. v. Barr Labs., Inc., 40 F.3d 1223, 1227-28 (Fed. Cir. 1994) (internal quotation marks and citations omitted). To perform this mental act, inventors must be natural persons and cannot be corporations or sovereigns. And because States cannot be inventors, it follows that inventorship is not a core sovereign interest of the States.»

Slike sitater fra regelverk og rettspraksis går imidlertid ikke direkte på spørsmålet om oppfinneren må være et menneske, sistnevnte sitat er fra en sak der spørsmålet som drøftes er i hvilken grad nasjonalstaten kan stå som oppfinner. Uttalelsene må forstås ut i fra riktig kontekst og bakgrunn. USPTO erkjenner også dette i avgjørelsen, men viser til at de underliggende forutsetninger om «*formation in the mind of the inventor*» og «*mental act*» er krav som må stilles til alle oppfinnere – og som kun mennesker kan innfri. Dermed blir konklusjonen på dette punkt at den angitte oppfinner i søknadsskjemaet må være en person.

I klagen var det vist til saksbehandlingen for EPO, og anført at EPO hadde anerkjent at oppfinnelsen var gjort av DABUS, men at DABUS likevel ikke kunne stå oppført som oppfinner. I dette argumentet ligger at regelverket må suppleres og fortolkes utvidende til å gjelde *de facto* oppfinnere enten dette er menneske eller maskin. USPTO viser i avgjørelsen kort til at saken til behandling utelukkende gjaldt oppføring av riktig person som oppfinner, ikke spørsmålet om hvem som hadde gjort oppfinnelsen. Det ble i tillegg vist til at EPO og andre tilsvarende utenlandske organer må håndheve egne regelverk, som ikke uten videre får be-



tydning for håndhevelsen av de amerikanske reglene.

Dette er åpenbart et sakskompleks der det gjenstår flere kapitler i flere ulike jurisdiksjoner, og der vi i et større perspektiv kan forvente å se problemstillinger knyttet til AI og rettigheter bli stadig mer aktuelle.

Når det gjelder argumentasjonen i saken som er omtalt i denne artikkelen, vil det fort kunne oppstå et spørsmål i forlengelsen av hvem som skal stå som oppfinner og hvem som er rettighetshaver der AI-systemet utvikler seg selv. Et viktig kjennetegn på en GKI, altså en sterk og generell AI, er nettopp evnen til å kombinere en slags menneskelig evne til å resonnerer med datasystemets fordeler når det gjelder hurtighet, datalagring og så videre, som omtalt ovenfor. I forlengelsen av dette vil man kunne se for seg at en AI som er i stand til å handle kreativt og utvikle nye oppfinnelser, også vil være i stand til å utvikle nye og forbedrede versjoner av seg selv. Det skal ikke mange iterasjoner eller AI-generasjoner til før man kan stille seg spørsmålet om den eller de mennesker som utviklet

førstegenerasjonen rimeligvis kan stå som eiere eller rettighetshavere til oppfinnelser gjort av etterkommende generasjoner utviklet av det opprinnelige datasystemet.

Dette er bare ett i en hel rekke av nye og spennende problemstillinger som ligger i vår nære fremtid. I innledningen overfor er det vist til Watson, IBM's datamaskin som deltok i TV-programmet Jeopardy. Konseptet i dette programmet er at programlederen gir et svar, og deltakeren skal komme med det riktige spørsmålet til dette svaret. Da Watson deltok var programlederens oppgave og svar i den avsluttende runden «William Wilkinson's 'an account of the principalities of Wallachia and Moldavia' inspired this authors' most famous novel». Watson svarte først av de tre deltakerne, og ga riktig spørsmål som løsning på oppgaven: «Who is Bram Stoker». Deltakeren Ken Jennings, et ekte menneske og ikke minst mester i Jeopardy, avga det samme svaret på noe lengre tid. Han hadde dog en tilføyelse på sin løsning, som fremgår av bildet ovenfor: «I for one welcome our new computer overlords.»



It-kontraktret, 2. udgave

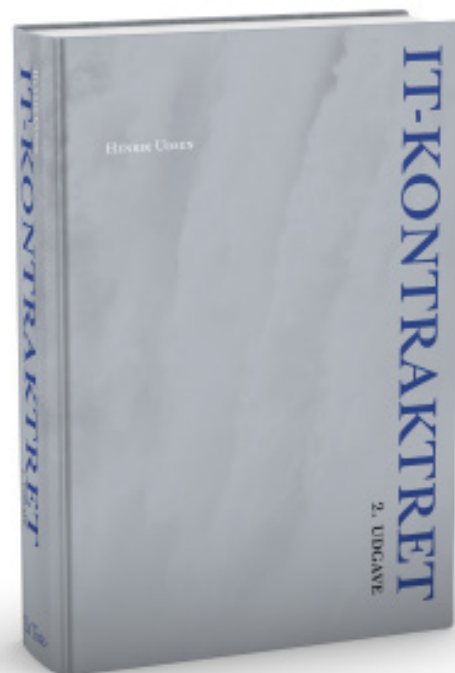
Henrik Udsen, *It-kontraktret, 2. udgave*.

Ex Tuto Publishing, 2020.

576 sider indbundet. ISBN: 978-87-420-0035-9

2. udgaven af Henrik Udsens

It-kontraktret er udkommet. Bogen er bl.a. opdateret med omtale af og eksempler fra den danske standardkontrakt for it-drift, D17. Endvidere er bogens databeskyttelsesretlige afsnit udvidet og tilpasset databeskyttelsesforordningen (GDPR), og der er tilføjet et nyt afsnit om databeskyttelsesretlige relateret til it-udvikling. Antallet af domme, der behandles i bogen, er væsentligt udvidet, herunder med omtale af en række norske domme. I forbindelse med udgivelsen af 2. udgaven offentliggøres en it-kontraktretlig domsdatabase, der samler domme omtalt i bogen. Domsdatabasen vil være tilgængelig fra www.it-kontraktret.dk.





Gorrissen Federspiel

Tue Goldschmieding

1. Datatilsynet udtaler kritik af databehandlers manglende sikkerhedsforanstaltninger i forbindelse med overtagelsen af udviklings- og testmiljø fra en anden leverandør

Det danske datatilsyn ('Datatilsynet') afsagde den 13. februar 2020 afgørelse med journalnummer: 2019-431-0036, i en sag vedrørende en dansk it- og software-virksomheds overtagelse af et udviklings- og testmiljø fra en anden leverandør. Virksomheden fik i 2017 overdraget it-løsningen i forbindelse med et virksomhedskøb, men undlod at påse om denne indeholdt personoplysninger. Serveren var oprindeligt klassificeret som en intern udviklingsserver, uden personoplysninger og blev derfor ikke undergivet virksomhedens ordinære driftssikkerhedssetup, indeholdende bl.a. patch- og sikkerhedspolitik.

I forbindelse med virksomhedens udviklingsarbejde var serveren opkoblet til internettet, hvor serveren i april 2019 var blevet kompromitteret og uretmæssigt udnyttet til at udvinde kryptovalutaen Bitcoin. Efter at den uretmæssige brug var konstateret, blev det fastslået, at serveren indeholdt personoplysninger fra flere dataansvarlige. Datatilsynet fandt, at virksomheden havde overtrådt Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningens') artikel 32, ved at behandle personoplysninger, uden forinden at have implementeret passende tekniske foranstaltninger til

sikring mod uretmæssig brug af personoplysningerne.

Der blev lagt vægt på, at bruddet kunne have været undgået, hvis der havde været indført almindelige tekniske sikkerhedsforanstaltninger, såsom firewall-regler, og at de etablerede sikkerhedsforanstaltninger ikke kunne anses som tilstrækkelige, da den foretagne risikovurdering alene var baseret på beskrivelsen »intern server« uden personoplysninger.

Det kan udledes af afgørelsen, at der ved brug af produktionsdata i forbindelse med test og udvikling, gælder de samme krav til sikkerheden, som det man vurderer er passende i driftssetuppet. Der skal her ved etableres en passende sikkerhed for de registreredes rettigheder, inden behandlingen går i gang, og hvor risikoen for de registrerede måtte være høj, skal der være foretaget en konsekvensanalyse.

Læs hele afgørelsen her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/feb/ny-afgoerelse-manglende-sikkerhed-omkring-en-udviklingsserver/>

2. Datatilsynet vurderer, at oplysninger med generelt lav risikoprofil, i konkrete tilfælde kan indebære en høj risiko

Det danske datatilsyn ('Datatilsynet') har samlet behandlet to lignende sager, j.nr. 2019-441-1578 og 2019-441-1581, om brud på persondatasikkerheden. Sagerne drejede sig om to virksomheder, der havde registreret homogene oplysninger såsom navn, kontakt- og adresseop-

lysninger samt købshistorik. Da virksomhederne ikke havde etableret en tilstrækkelig adgangskontrol til deres hjemmeside, kunne oplysningerne tilgås ved at indtaste et gyldigt ordrenummer, hvorefter man fik adgang til de registrerede oplysninger om den pågældende kunde.

Virksomhederne havde som dataansvarlige ikke fundet det nødvendigt at underrette de i alt mere end 250.000 registrerede i deres databaser om databruddet, da de ikke fandt, at bruddet indebar en høj risiko for de berørte personers rettigheder.

Datatilsynet vurderede derimod, at der burde være foretaget en særskilt vurdering for de registrerede, som kunne påtænkes at være i en særlig risikogruppe, herunder de registrerede, der havde hemmelig adresse. Efter Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningens'), artikel 34, vil dataansvarlige være forpligtet til at underrette registrerede, hvis sikkerhedsbruddet sandsynligvis vil indebære en høj risiko for de registreredes rettigheder. Datatilsynet fandt, at virksomhederne ikke havde foretaget en konkret vurdering efter databeskyttelsesforordningens artikel 34. Datatilsynets samlede vurdering af databruddet var, at der konkret var en høj sandsynlighed for at sikkerhedsbruddet havde berørt datasubjekter, for hvem eksponering af deres adresse kunne have en høj konsekvens, og at bruddet som følge heraf udgjorde en høj

risiko for disse datasubjekter. Virksomhederne blev derfor påbudt at underrette de registrerede, som måtte have hemmelig adresse.

Det fremgår af afgørelserne i de to sager, at den risikovurdering, som den dataansvarlige foretager, i forhold til hvorvidt der skal ske underretning til de registrerede, efter databeskyttelsesforordningen artikel 34, skal afspejle individuelle forhold. Afgørelsen fastslår således, at der selv i homogene behandlinger af oplysninger, som generelt ikke har en høj risikoprofil, kan være forhold for enkelte registrerede, der indebærer en høj risiko, som vil kræve underretning.

Læs datatilsynets afgørelser i de to relaterede sager her:

Nemlig.com:

<https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/dec/brud-paa-persondatasikkerheden-bos-nemlig-com-as/>

Intervare:

<https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/dec/brud-paa-persondatasikkerheden-bos-intervare-as/>

3. Datatilsynet udtalte alvorlig kritik af virksomheds behandling af personoplysninger i forbindelse med automatiske overførsler mellem pengeinstitutter

Det danske datatilsyn ('Datatilsynet') indledte af egen drift en undersøgelse af, om der i forbindelse med automatiske pengeoverførsler mellem pengeinstitutter blev medsendt personoplysninger. Datatilsynet blev bekendt med sagen i forbindelse med, at en række banker og sparekasser, jf. Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') artikel 33, anmeldte, at der i perioden fra før 25. maj 2018 til den 22. august 2019 i en række tilfælde var sket videregivelse af adresseoplysninger for personer, som var registreret med beskyttet adresse i Det Centrale

Personregister (CPR), hvilket var et brud på persondatasikkerheden fra den dataansvarlige, som i denne sag var Bankernes EDB Central A.M.B.A (BEC).

Efter en gennemgang af sagen lagde Datatilsynet til grund, at BEC uberettiget ved fremsendelse af adresser med oplysninger om betalingsafsenderen havde videregivet adresseoplysninger for personer til uvedkommende, og derved ikke havde levet op til reglerne om integritet og fortrolighed i databeskyttelsesforordningens artikel 5, stk. 1, litra f. Dertil kom, at BEC ved at anvende en ældre IT-løsning heller ikke havde levet op til reglerne i databeskyttelsesforordningens artikel 32, stk. 1 om behandlingssikkerhed. Datatilsynet begrundede bl.a. deres afgørelse med, at BEC ikke havde implementeret tilstrækkelige og passende tekniske eller organisatoriske foranstaltninger for at sikre tilstrækkelig sikkerhed for de pågældende oplysninger. BEC havde heller ikke sikret en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af disse foranstaltninger.

Datatilsynet udtalte i den forbindelse generelt, at der ved behandling af personoplysninger skal ske test og løbende opfølgning, der sikrer, at personoplysningerne behandles med vedvarende fortrolighed, integritet, tilgængelighed og robusthed.

Tilsynet anså det som en skærpende omstændighed, at de kunder, hvis adresseoplysninger var blevet videregivet, var registreret som beskyttede i CPR. Det var også en skærpende omstændighed, at fejlen i BEC's systemer havde eksisteret siden 2015, uden at dette var blevet opdaget. Over for dette anså Datatilsynet det som en formildende omstændighed, at Europa-Parlamentet og Rådets forordning (EU) 2015/847 af 20. maj 2015 om oplysninger der skal medsendes ved pengeoverførsler, og LBK nr. 646 af 2. juni 2017 ('CPR-loven') inde-

holder modstridende regler, hvilket kunne have været medvirkende til, at BEC ikke kunne afgøre, om adresseoplysningerne skulle medsendes i betalingstransaktionerne.

Læs hele afgørelsen her:

<https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/feb/videregivelse-af-beskyttede-adresseoplysninger/>

4. Datatilsynet indstiller to kommuner til bøder for brud på persondatasikkerheden

Det danske datatilsyn ('Datatilsynet') annoncerede den 10. marts 2020, at to kommuner er indstillet til bøder med påstået størrelse på henholdsvis 100.000 dkr. og 50.000 dkr. Indstillingerne følger af, at Datatilsynet har vurderet, at kommunerne ikke har levet op til kravene om et passende sikkerhedsniveau efter Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen').

Efter anmeldelser om brud på personsikkerheden i forbindelse med tyverier af de to kommuners computere, blev Datatilsynet opmærksom på kommunernes utilstrækkelige sikkerhedsforanstaltninger.

Ingen af kommunerne havde beskyttet computerne med kryptering, hvilket datatilsynet fandt havde udgjort en unødigt høj risiko for borgerne. De stjålne computere indeholdt personoplysninger, herunder personoplysninger af følsom karakter, om henholdsvis 20.620 borgere og ca. 1.600 medarbejdere.

Datatilsynet udtalte, at kommuner gennem deres virke behandler store mængder af personoplysninger, herunder oplysninger af følsom karakter. Da borgeren ikke har mulighed for at fravælge denne behandling, vil kommunernes ansvar for at beskytte personoplysninger være stort. Yderligere udtalte Datatilsynet, at den manglende kryptering var særdeles uforsigtig.

Efter lov nr. 502 af 23. maj 2018 ('den danske databeskyttelseslov')

§ 41, stk. 6 kan også offentlige myndigheder ifalde straf på samme vis som private aktører. Dog er bødeløfterne lavere for offentlige myndigheder, sammenlignet med de som fremgår af databeskyttelsesforordningens artikel 86, stk. 4-6 for private.

De påståede bødestørrelser er begrundet i overtrædelsens karakter, manglende behandlingssikkerhed, og at manglende kryptering af kommunernes computere var en generel foranstaltning. Dertil er kommunernes indbyggertal og samlede driftsbevilling indgået i grundlaget for vurderingen af bødestørrelsen.

Læs hele udtalelsen her:

<https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/mar/to-kommuner-indstillet-til-boede/>

5. EDPB og Datatilsynet udtaler sig om behandling af personoplysninger i forbindelse med udbruddet af COVID-19

Det Europæiske Databeskyttelsesråd (EDPB) og det danske datatilsyn (Datatilsynet) udgav henholdsvis den 19. marts og den 5. marts 2020 udtalelser om behandling af personoplysninger i forbindelse med udbruddet af COVID-19.

Udtalelserne fra EDPB og Datatilsynet gennemgår, under hvilke forudsætninger, der kan behandles personoplysninger i anledning af COVID-19 udbruddet inden for rammerne af Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (databeskyttelsesforordningen).

For offentlige myndigheder, herunder sundhedsmyndigheder, gælder, at disse vil kunne behandle såvel almindelige som følsomme personoplysninger efter artikel 6 og 9 i databeskyttelsesforordningen, uden at det kræver samtykke fra den registrerede, i det omfang at behandlingen sker på baggrund af national lovgivning eller efter betingelserne i databeskyttelsesforordningens artikel 6, stk. 1, litra d eller

e eller artikel 9, stk. 2, litra b, c eller i.

For arbejdsgivere gælder, at disse i visse tilfælde vil kunne behandle personoplysninger om ansatte i relation til COVID-19 udbruddet på baggrund af retlige forpligtelser, herunder særligt forpligtelser i forhold til at sikre sundhed og sikkerhed på arbejdspladsen, og forpligtelser der følger af samfundets interesse i at begrænse smittespredning.

Datatilsynet udtaler, at en arbejdsgiver i vidt omfang inden for rammerne af databeskyttelsesforordningen vil kunne registrere og videregive oplysninger i forbindelse med COVID-19 udbruddet, når oplysningerne ikke er så specifikke, at de udgør helbredsoplysninger, under forudsætning af at situationen nødvendiggør en sådan registrering eller videregivelse.

Som eksempler på oplysninger, som det ifølge Datatilsynet vil være muligt, at behandle om medarbejdere i relation til COVID-19, er oplysninger om, at en ansat er hjemvendt fra et »risikoområde«, at en ansat er i hjemmekarantæne (uden nærmere at angive årsagen hertil) eller at en ansat er syg (uden nærmere at angive årsagen).

Arbejdsgiveren vil også være berettiget til at behandle følsomme personoplysninger uden samtykke, såfremt det er nødvendigt af hensyn til samfundsinteresser på folkesundhedsområdet, jf. databeskyttelsesforordningens artikel 9, stk. 2, litra i, når det sker på grundlag af unionsretten eller national lovgivning eller behandlingen sker for at beskytte den registrerede eller en anden fysisk persons vitale interesser, når den pågældende ikke er i stand til selv at samtykke, jf. databeskyttelsesforordningens artikel 9, stk. 2, litra c.

Såfremt en arbejdsgiver registrerer eller videregiver følsomme personoplysninger, eksempelvis om at en medarbejder er smittet med COVID-19, skal der ligge saglige argu-

menter til grund herfor. Endvidere skal arbejdsgiveren sikre, at der alene registreres og videregives oplysninger, der er nødvendige for at opfylde formålet med behandlingen.

Datatilsynet påpeger i udtalelsen, at arbejdsgiveren i forbindelse med registreringen eller videregivelsen af følsomme personoplysninger bør overveje, om der er en god grund til at registrere eller videregive oplysningerne, om det er nødvendigt at specificere oplysningerne, eller om formålet med behandlingen kunne være opnået ved at »fortælle mindre«. Endvidere skal det overvejes, om det er nødvendigt at nævne navnet på den registrerede.

I udtalelsen fra EDPB berøres tillige spørgsmålet om, under hvilke forudsætninger, der kan anvendes lokationsdata fra individers mobiltelefoner i forbindelse med COVID-19 udbruddet, herunder til kontrol af menneskemængder og overvågning af smittespredning.

EDPB udtaler i den forbindelse, at anvendelsen af lokationsdata skal ske i overensstemmelse med den nationale lovgivning, som implementerer Europa-Parlamentets og Rådets Direktiv 2002/58EF af 12. juli 2002 (E-databeskyttelsesdirektivet).

I Danmark er E-databeskyttelsesdirektivet blandt andet implementeret ved lovbekendtgørelse nr. 128 af 7. februar 2014 (den danske telelov). Ifølge den danske telelov, kan lokationsdata kun benyttes, hvis dataene anonymiseres, eller hvis den registrerede samtykker i anvendelsen. Medlemsstaterne kan dog, i medfør af e-databeskyttelsesdirektivets artikel 15, indføre regler, der giver grundlag for at behandle ikke-anonymiserede personoplysninger, når det er nødvendigt og proportionelt med hensynet til den offentlige sikkerhed.

Læs EDPB's udtalelse her:

https://edpb.europa.eu/sites/edpb/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

Læs Datatilsynets udtalelse her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/mar/hvordan-er-det-med-gdpr-og-coronavirus/>

6. Tv-overvågning af ansat var uberettiget og udløste godtgørelse for tort

Den danske Højesteret (Højesteret) afsagde d. 2 marts 2020 dom i sagen BS-27 412/2019-HJR mellem Fagligt Fælles Forbund (3F) og X ApS (X).

Sagen angik, hvorvidt der var sket uberettiget tv-overvågning af C under udførelsen af hendes arbejde i E's restaurant. Tv-overvågningen fandt sted i restauranten og i fællesrum, hvor arbejdet blev udført, og parterne var enige om, at det var lovligt at opsætte kameraerne. Højesteret lagde efter bevisførelsen til grund, at tv-overvågningen bl.a. var blevet anvendt til at disciplinere C og kontrollere, om hun udførte sit arbejde korrekt. Højesteret lagde til grund, at denne anvendelse af tv-overvågningen over for C havde haft et betydeligt omfang og var foregået løbende, både når E var til stede på arbejdspladsen, og når han ikke var der.

Højesteret fandt, at E ikke godtgjorde, at der forelå saglige og proportionale grunde (i form af arbejdsmæssige eller sikkerhedsmæssige forhold) til at anvende tv-overvågningen over for C som sket. E overtrådte på den baggrund grænserne for, hvad der var tilladt efter arbejdsgiverens ledelsesret og efter den tidligere gældende lov nr. 429 af 31. maj 2000 (den dagældende danske persondatalovs) § 5, stk. 1-3.

Herefter tog Højesteret stilling til, om C som følge af den uberettigede anvendelse af tv-overvågningen havde krav på godtgørelse for tort efter lov nr. 1070 af 14. august 2018, (den danske erstatningsansvarslovs) § 26, stk. 1. Af forarbejderne til erstatningsansvarsloven og den tidligere bestemmelse i § 15 i lov nr. 127 af 15. april 1930 (ikraft-

trædelsesloven til den danske straffelov), som den danske erstatningsansvarslovs § 26 bygger på, udledte Højesteret, at tort forudsatte en culpøs krænkelse af en vis grovhed, og at krænkelsen skulle angå den pågældendes selv- og æresfølelse, dvs. vedkommendes opfattelse af eget værd og omdømme. Krænkelsen i den forelagte sag bestod i, at tv-overvågningen i et betydeligt omfang var anvendt til, uden saglig grund, løbende at kontrollere C under udførelsen af hendes arbejde. Højesteret fandt, at C som følge heraf, havde følt sig konstant overvåget på sin arbejdsplads, og at dette havde medført en stor psykisk belastning for hende.

På denne baggrund fandt Højesteret, at den uberettigede anvendelse af tv-overvågningen havde den fornødne grovhed og havde krænkelse C's selv- og æresfølelse.

C havde derfor krav på godtgørelse for tort efter erstatningsansvarslovens § 26, stk. 1.

Læs hele dommen her: <http://domstol.fe1.tangora.com/media/-300016/files/27412-dom-anonym.pdf?rev1>

7. Det danske datatilsyn udtaler alvorlig kritik af DMI's behandling af personoplysninger om hjemmesidebesøgende og udgiver ny vejledning om behandling af oplysninger om besøgende på hjemmesider

Det danske datatilsyn (Datatilsynet) traf den 11. februar 2020 afgørelse i en principiel sag vedrørende behandling af personoplysninger og visning af bannerannoncer på Danmarks Meteorologiske Instituts (DMI's) hjemmeside. Afgørelsen har affødt en ny vejledning fra Datatilsynet, hvor Datatilsynet specifikt forholder sig til behandling af personoplysninger om hjemmesidebesøgende.

Sagen tog afsæt i en klage af 29. august 2018, hvori klager overordnet anførte at DMI på deres hjemmeside viste personlige banneran-

noncer fra bl.a. annoncebørsen Google Ad Exchange, som bruger personoplysninger til personalisering af annoncer, hvorfor DMI bidrog til indsamling og videregivelse af personoplysninger om hjemmesidens besøgende til Google.

Datatilsynet fandt, at DMI sammen med Google var fælles dataansvarlige, idet Datatilsynet lagde vægt på, at DMI havde integreret bannerannoncer på hjemmesiden, og DMI sammen med Google fastlagde formålet med behandling af personoplysninger. DMI havde dog alene pligt til at sikre et gyldigt behandlingsgrundlag for de behandlingsoperationer, hvor DMI var medansvarlig, hvilket var ved indsamling og videregivelse til transmission.

Ifølge Datatilsynet var det relevante behandlingsgrundlag, for den omhandlede behandling af personoplysninger om hjemmesidebesøgende, den registreredes samtykke efter Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (databeskyttelsesforordningen) artikel 6, stk. 1, litra a.

Datatilsynet fandt ikke, at DMI's nuværende eller tidligere løsning til indhentning af samtykke til behandling af personoplysninger om de besøgende på dmi.dk opfyldte databeskyttelsesforordningens krav til samtykke i artikel 4, nr. 11, samt det grundlæggende princip om lovlighed, rimelighed og gennemsigtighed i artikel 5, stk. 1, litra a.

Datatilsynet lagde for det første vægt på, at de besøgende på dmi.dk ved at trykke »OK« til DMI's løsning til indsamling af personoplysninger gav samtykke til forskellige behandlingsformål, hvilket ikke opfyldte kravet om frivillig samtykke. Det var muligt at til- og fravælge forskellige formål, men denne mulighed var placeret »et-klik-væk«, hvorfor det ikke opfyldte databeskyttelsesforordningens krav om gennemsigtighed.

Herudover lagde Datatilsynet vægt på, at løsningen til indsamling

af personoplysninger ikke var tilstrækkeligt informeret.

Ovenstående gav anledning til alvorlig kritik af DMI's behandling af personoplysninger samt anledning til en ny vejledning vedrørende behandling af personoplysninger om hjemmesidebesøgende. Vejledningen blev udgivet den 17. februar 2020, og den gælder for organisationer, der behandler personoplysninger om hjemmesidebesøgende. Den har især fokus på samtykke som behandlingsgrundlag og gennemgår betingelserne herfor. Vejledningen indeholder illustrative eksempler.

Ifølge Datatilsynets nye vejledning er kravene for gyldigt samtykke efter databeskyttelsesforordningen blandt andet:

- at det skal være et aktivt tilvalg, når en besøgende på en hjemmeside giver lov til, at vedkommendes oplysninger behandles,
- at det skal være klart, hvilke forskellige formål den dataansvarlige gerne vil behandle oplysningerne til,
- at det skal være let for den besøgende at give samtykke til nogle formål og ikke give samtykke til andre,
- at det skal være nemt ikke at give samtykke, også rent visuelt,
- at den dataansvarlige skal kunne dokumentere, hvad en besøgende har givet samtykke til, og hvordan samtykket er indhentet.

Læs hele afgørelsen her:

<https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/feb/dmis-behandling-af-personoplysninger-om-hjemmesidebesoegende/>

Læs hele vejledningen her:

<https://www.datatilsynet.dk/press-og-nyheder/nyhedsarkiv/2020/feb/nye-retningslinjer-om-behandling-af-personoplysninger-om-hjemmesidebesoegende/>

8. Det danske datatilsyn vedtager standardkontraktbestemmelser

Det danske datatilsyn ('Datatilsynet') anmodede i april 2019 det

Europæiske Databeskyttelsesråd ('EDPB') om en udtalelse vedrørende tilsynets skabelon til databehandleraftaler med henblik på, at Datatilsynet kunne vedtage disse som standardkontraktbestemmelser i medfør af artikel 28, stk. 8 i Europa-Parlamentet og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen'). De nationale datatilsyn har i medfør af denne bestemmelse mulighed for at vedtage og udgive standardkontraktbestemmelser, som kan benyttes af dataansvarlige til at sikre, at kravene til databehandleraftaler i databeskyttelsesforordningens artikel 28, stk. 3. og 4, er opfyldt, forudsat at standardkontrakten udfyldes korrekt.

På baggrund af EDPB's udtalelse af den 9. juli 2019 ændrede Datatilsynet, sin skabelon til databehandleraftaler, således at den nu har karakter af en standardkontrakt, jf. databeskyttelsesforordningens artikel 28, stk. 8.

Brug af standardkontraktbestemmelserne har den fordel, at hvis organisationer vælger at benytte sig af disse, vil Datatilsynet som udgangspunkt ikke efterprøve standardkontraktbestemmelserne nærmere, f. eks. ved tilsynsbesøg, idet det på forhånd er vurderet, at aftalen opfylder databeskyttelsesforordningens krav til databehandleraftaler. Datatilsynet har dog i forbindelse med revideringen udtalt, at de som udgangspunkt fortsat accepterer databehandleraftaler, der er baseret på tilsynets oprindelige skabelon. Det vil derfor som udgangspunkt stadig være i overensstemmelse med databeskyttelsesforordningens regler om databehandleraftaler, hvis organisationer bibeholder databehandleraftaler, der er indgået på baggrund af denne skabelon.

Ændringerne kan findes her:

<https://www.datatilsynet.dk/press-og-nyheder/nyhedsarkiv/2019/dec/standardkontraktsbestemmelser-vedtaget-af-datatilsynet/>

9. Arbejdsmarkedets Feriefond modtager alvorlig kritik fra det danske datatilsyn som følge af manglende iagttagelse af oplysningspligt

Det danske datatilsyn ('Datatilsynet') traf den 20. december 2019 afgørelse i j.nr. 2019-32-0639, vedrørende den selvejende institution under det danske beskæftigelsesministerium, Arbejdsmarkedets Feriefonds ('fonden') behandling af personoplysninger. Datatilsynet udtalte alvorlig kritik af fondens behandling af personoplysninger, som følge af fondens manglende iagttagelse af oplysningspligten i artikel 14 af Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen').

Fonden havde registreret klagers personoplysninger, herunder cpr-nr., navn, adresse, konto nr. og oplysninger om klagers gældsforhold i forbindelse med, at klager uretmæssigt havde fået udbetalt feriepenge. Klager modtog meddelelse om registreringen den 28. januar 2019.

Den 17. februar 2019 indgav klageren en klage til Datatilsynet over fondens mangelfulde oplysning af, hvilken behandling hendes personoplysninger var genstand for, samt fondens forsøg på at indhente samtykke fra klager i forbindelse med dennes kontakt af fondens databeskyttelsesrådgiver ('DPO').

Under sagsbehandlingen oplyste fonden klager trinvist om behandlingen af personoplysninger ved fremsendelse af tre breve over en periode på 2 måneder. Det første brev blev fremsendt den 28. januar 2019 ved fondens modtagelse af personoplysningerne, det andet brev blev fremsendt den 14. februar 2019 på foranledning af henvendelse fra klager og det tredje brev blev fremsendt den 28. marts 2019 i anledning af afslutningen af fondens sag med klager.

Datatilsynet fandt, at fonden hverken i de fremsendte breve eller i fondens persondatapolitik, der

blev henvist til i fondens brev af 14. februar 2019, fyldestgørende havde oplyst klageren som foreskrevet i artikel 14, stk. 1 og stk. 2 i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen'), bl.a. ved ikke at have oplyst om retsgrundlaget for behandlingen af klagers personoplysninger.

Datatilsynet lagde derudover vægt på, at fondens oplysning af klager ikke skete som en samlet oplysning af klager i forbindelse med modtagelsen af personoplysningerne men at oplysningen i stedet var sket trinvist under sagsbehandlingen. Datatilsynet fandt derfor, at fonden hverken havde iagttaget oplysningspligten inden for fristen i artikel 14, stk. 3 i databeskyttelsesforordningen, eller truffet passende foranstaltninger til i en kortfattet, gennemsigtig, letforståelig og lettilgængelig form at give enhver oplysning omfattet af artikel 14 i databeskyttelsesforordningen, jf. artikel 12, stk. 1, i databeskyttelsesforordningen.

Datatilsynet fandt på baggrund af ovenstående grundlag for at udtale alvorlig kritik af fondens behandling af personoplysninger.

Vedrørende fondens indhentelse af samtykke, som skete i forbindelse med klagers henvendelse, tillagde Datatilsynet det vægt, at fonden allerede behandlede de konkrete personoplysninger i sagen på et andet legitimt grundlag end samtykke. Indhentelsen af samtykke var således overflødig.

Datatilsynet fandt på baggrund af dette, at fondens indhentelse af samtykket var i strid med princippet om »lovlighed, rimelighed og gennemsigtighed« i artikel 5, stk. 1, litra a i databeskyttelsesforordningen, og at der dermed var yderligere grundlag for at udtale kritik af fondens behandling af personoplysninger.

Datatilsynet tilføjede afslutningsvist, at det konkrete samtykke klageren havde afgivet ved sin kontakt af fondens DPO efter Datatilsynets

vurdering ikke var gyldigt, jf. artikel 4, nr. 11, i databeskyttelsesforordningen, eftersom der ikke var alternativer til at afgive samtykke hvis klager ville kontakte fondens DPO, og samtykket dermed måtte anses for ufrivilligt.

Læs hele afgørelsen her:

<https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/dec/arbejds-markedets-feriefonds-iagttagelse-af-oplysningspligt-og-brug-af-samtykke/>

10. Det danske datatilsyn udtaler alvorlig kritik af databehandlers leverandør, der behandlede data i ikke-sikre tredjelande

Det danske datatilsyn ('Datatilsynet') traf den 19. december 2019 afgørelse i sagen j.nr. 2019-442-3996. Sagen omhandlede, hvorvidt det skulle betragtes som et brud på persondatasikkerheden, at en databehandler havde anvendt en ikke godkendt underleverandør.

Anmelderen af bruddet, Herning Kommune, anvendte et økonomistyringssystem kaldet ØS Indsigt. Herning Kommune ejede systemet sammen med to regioner og 10 øvrige kommuner ('Ejerkredsen'). Kommunerne og regionerne var fælles dataansvarlige, Ejerkredsen var databehandlere og leverandøren EG A/S ('EG') var underdatabehandler.

Herning Kommune anmeldte den 3. september 2019 et brud på persondatasikkerheden, da kommunen blev opmærksom på, at EG anvendte en underleverandør, ServiceNow, der ikke fremgik af databehandleraftalen mellem Ejerkredsen og EG. Det fremgik endvidere af databehandleraftalen, at EG ikke måtte anvende underdatabehandlere, medmindre dette fremgik af databehandleraftalen. Bruddet omfattede ifølge Herning Kommune oplysninger om navn, fødselsdato, kontaktoplysninger og personnummer på ca. 500 personer.

EG oplyste under sagen, at de i forbindelse med driften af ØS Ind-

sigt anvendte underleverandøren ServiceNow, som var hjemmehørende i Holland. ServiceNow havde ligeledes afdelinger i tredjelandene USA, Indien og Australien. Som udgangspunkt behandlede ServiceNow ikke personoplysninger uden for EU, men ServiceNow kunne ikke garantere, at der ikke var sket en behandling i et af de nævnte tredjelande.

Den mulige behandling skyldtes, at ServiceNow's medarbejdere i de nævnte tredjelande kunne være ansvarlige for at implementere globale sikkerhedsopdateringer, og derfor også kunne have behandlet personoplysninger for EG.

EG anførte, at der ikke var tale om et brud på persondatasikkerheden, da der ikke var sket en hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse eller adgang til personoplysninger. EG mente endvidere, at de var berettiget til at benytte ServiceNow som underleverandør, da det fremgik af tilbudsmaterialet og var blevet drøftet med Ejerkredsen, at EG ville anvende ServiceNow som underleverandør i forbindelse med driften af ØS Indsigt.

EG anførte ligeledes, at det var tvivlsomt, hvorvidt der var sket en overførsel til tredjelande, eftersom behandlingen i tredjelandene kun omfattede system- og sikkerhedsopdateringer, hvorfor en evt. behandling ikke ville være omfattet af aftaleforholdet mellem Ejerkredsen og EG. Såfremt Datatilsynet kom frem til, at der var foretaget en behandling, anførte EG, at de i kraft af den databehandleraftale EG havde indgået med ServiceNow, havde hjemmel i Privacy Shield og i EU-kommissionens standardaftaler til at overføre oplysningerne til tredjelandene.

Datatilsynet fandt, at EG ved selv at havde fastlagt formålet med behandlingen var at betragte som dataansvarlig for videregivelsen af oplysninger, jf. Europa-Parlamentets og Rådets Forordning (EU)

2016/679 af 27. april 2016 ('databeskyttelsesforordningen') artikel 28.

Datatilsynet fandt ligeledes, at personoplysningerne var kommet til uvedkommendes kendskab, i kraft af ServiceNow's adgang til oplysninger, som ikke var en godkendt underleverandør. Som underdatabehandler havde EG overtrådt databeskyttelsesforordningens artikel 28, stk. 2, ved at have anvendt en underleverandør uden forudgående skriftlig tilladelse.

Ydermere havde EG, i kraft af deres rolle som dataansvarlig for videregivelsen, overtrådt databeskyttelsesforordningens artikel 6, stk. 1 samt lov nr. 502 af 23. maj 2018 ('den danske databeskyttelseslov') § 11, stk. 2, ved ikke at have haft hjemmel til behandlingen.

Herudover havde EG ikke hjemmel til at overføre oplysningerne til tredjelandene, jf. databeskyttelsesforordningens artikel 44, stk. 1. Datatilsynet fastslog, at overførsler til tredjelande kun kan ske såfremt betingelserne i databeskyttelsesforordningens kapitel 5 er opfyldt, med forbehold for overholdelsen af forordningens øvrige bestemmelser.

Datatilsynet valgte således at udtale alvorlig kritik af EG for ikke at have overholdt databeskyttelsesreglerne. Datatilsynet lagde vægt på, at der var tale om et højt antal berørte, at behandlingen blandt andet vedrørte personnumre, samt at der var sket en uhjemlet overførsel til tredjelande. Datatilsynet understregede, at det forhold, at EG selv havde indgået en underdatabehandleraftale med ServiceNow ikke kunne føre til et andet resultat. Dette skyldtes, at EG ikke havde hjemmel til at overføre oplysningerne til ServiceNow, på grund af manglende overholdelse af databeskyttelsesforordningens artikel 28, stk. 2.

Læs hele afgørelsen her:
<https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/dec/databehandlers-behandling-af-personoplysninger-uden-for-instruks/>

11. Det danske datatilsyn udgiver ny bekendtgørelse om videregivelse af personoplysninger i statistisk eller videnskabeligt øjemed

Den 1. januar 2020 trådte bekendtgørelse nr. 1509 af 18. december 2019 om videregivelse af personoplysninger i statistisk eller videnskabeligt øjemed ('bekendtgørelsen') i kraft. Det danske datatilsyn ('Datatilsynet') udgav samtidig deres vejledning til bekendtgørelsen.

Bekendtgørelsen finder anvendelse i de tilfælde, hvor der sker en videregivelse af personoplysninger i statistisk eller videnskabeligt øjemed efter lov nr. 502 af 23. maj 2018 ('den danske databeskyttelseslov') § 10, stk. 1, og Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') artikel 6, stk. 1, litra e.

Bekendtgørelsen regulerer både den afgivende og modtagende dataansvarliges forpligtelser. Ifølge Datatilsynet defineres en videregivelse som en overførsel til en ny selvstændig dataansvarlig. Såfremt overførslen sker til en databehandler finder bekendtgørelsen ikke anvendelse.

Bekendtgørelsen indeholder en række henvisninger til databeskyttelsesforordningen, der skal minde de dataansvarlige om deres forpligtelse efter denne. Eksempelvis fremgår det af bekendtgørelsens § 7 og § 13, at der skal foretages en risikovurdering i overensstemmelse med databeskyttelsesforordningens artikel 32.

Den afgivende dataansvarlige har en række forpligtelser i forbindelse med videregivelsen af oplysningerne. Det følger af bekendtgørelsens § 2, stk. 1, at oplysningerne kun må videregives, når det er nødvendigt for den modtagende dataansvarliges statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig karakter.

Det fremgår af Datatilsynets vejledning, at den afgivende dataan-

svarlige skal foretage en vurdering (og kunne dokumentere denne vurdering) af hvilke oplysninger, der er nødvendige, for at den modtagende dataansvarlige kan udføre den statistiske eller videnskabelige undersøgelse. Datatilsynet fastslår i den forbindelse, at den afgivende dataansvarlige tildele et betragteligt skøn i forhold til hvilke oplysninger, der er nødvendige.

Af bekendtgørelsens § 2, stk. 2, følger det, at de videregivne oplysninger ikke senere må behandles i et andet videnskabeligt eller statistisk øjemed, og bestemmelsen skal ses i forlængelse af bestemmelsen om formålsbegrænsning i den danske databeskyttelseslovs § 10, stk. 2. Datatilsynet anfører, at der således kun kan ske videregivelse såfremt den videregivende dataansvarlige har behandlingshjemmel i den danske databeskyttelseslovs § 10, stk. 1, eller databeskyttelsesforordningens art. 6, stk. 1 litra e. Herudover kan hverken den afgivende eller modtagende dataansvarlige benytte oplysninger til andre formål end statistisk eller videnskabeligt øjemed.

Ifølge bekendtgørelsens § 2, stk. 3, må der ikke ske videregivelse såfremt den registrerede er blevet oplyst om, at der ikke ville ske en videregivelse af oplysningerne. Sådanne oplysninger kunne eksempelvis være i afgivet til den registrerede i forbindelse med indsamlingen, jf. databeskyttelsesforordningens artikel 13.

Den dataansvarlige er som udgangspunkt forpligtet til at pseudonymisere oplysningerne, således at de ikke er umiddelbart personhenførbare, jf. bekendtgørelsens § 3. Såfremt det er strengt nødvendigt for den statistiske eller videnskabelige undersøgelse, at den enkelte registrerede kan identificeres, kan supplerende oplysninger videregives, således at modtageren kan identificere den enkelte registrerede, jf. bekendtgørelsens § 4.

Datatilsynet anfører i deres vejledning, at den afgivende og modta-

gende dataansvarlige skal samarbejde om at foretage en fælles, konkret og særkilt vurdering af nødvendigheden af de supplerende oplysninger.

Ifølge Datatilsynet vil det være strengt nødvendigt at videregive de supplerende oplysninger, såfremt undersøgelsen ikke ville kunne udføres uden de supplerende oplysninger. Dette kunne eksempelvis være såfremt formålet med videregivelsen er at berige øvrige oplysninger om den registrerede. Datatilsynet anfører, at pragmatiske hensyn og ressourcehensyn ikke i sig selv kan begrunde, at oplysninger ikke skal pseudonymiseres, eller at supplerende oplysninger skal udleveres.

Den afgivende dataansvarlige skal, jf. bekendtgørelsens § 8, forud for videregivelsen sikre at oplysningerne kun videreanvendes til statistiske eller videnskabelige formål, og skal jf. § 9 kunne dokumentere dette. Den afgivende dataansvarlige skal ligeledes påse at modtageren vil overholde bestemmelserne i § 10 til § 14, som opstiller forpligtelser for den modtagende dataansvarlige.

Den modtagende dataansvarlige skal, jf. bekendtgørelsens § 10, sikre, at det kun er autoriserede personer,

som får adgang til oplysningerne. Personer må kun autoriseres, hvis de reelt har behov for at beskæftige sig med personoplysninger. Den modtagende dataansvarlige skal ligeledes sikre, at de personer, der er autoriserede til at behandle oplysningerne, er i stand til at behandle oplysningerne i overensstemmelse med databeskyttelsesreglerne, jf. bekendtgørelsens § 11.

Der må ikke behandles flere oplysninger, end hvad der er nødvendigt for at udføre undersøgelsen, jf. bekendtgørelsens § 12. Unødvendige oplysninger skal enten slettes, tilintetgøres eller tilbageleveres. Den modtagende dataansvarlige er også forpligtet til ved afslutningen af undersøgelsen, at slette, anonymisere, tilintetgøre eller tilbagelevere oplysningerne, jf. bekendtgørelsens § 14. Det gælder dog ikke, hvis oplysningerne må opbevares efter reglerne i lovbekendtgørelse nr. 1201 af 28. september 2016 ('den danske arkivlov').

Datatilsynet anfører, at forpligtelsen efter bekendtgørelsens § 14 indtræder, når den statistiske eller videnskabelige undersøgelse afsluttes.

Dette sker efter Datatilsynets opfattelse, når der ikke længere er et konkret eller sagligt formål med be-

handlingen. Datatilsynet anfører i forlængelse heraf, at bekendtgørelsens § 12 ikke er til hinder for, at undersøgelsen ligeledes omfatter nye spørgsmål af statistisk eller videnskabelig karakter, såfremt disse har et konkret og sagligt formål, ligesom det gælder, at afslutningen af et indledende stadie af undersøgelsen ikke medfører, at slettepligten indtræder. Datatilsynet anfører slutteligt, at det ikke ses som et konkret og sagligt formål, at oplysningerne rent hypotetisk kunne være relevante for en fremtidig undersøgelse.

Læs hele bekendtgørelsen her:
<https://www.retsinformation.dk/Forms/R0710.aspx?id=212264>

Læs hele vejledningen her:
<https://www.datatilsynet.dk/media/7952/videregivelsesvejledning.pdf>

Læs pressemeddelelsen her:
<https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2019/dec/ny-bekendtgørelse-om-videregivelse/>

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



Wiersholm

Carl Emil Bull-Berg og Line Helen Haukalid

Datatilsynets årsrapport for 2019

Den 4. april 2020 publiserte Datatilsynet sin årsrapport for 2019. Rapporten oppsummerer fjorårets viktigste tall og tendenser for Datatilsynets virksomhet. I denne artikkelen vil vi kort redegjøre for utvalgte punkter fra rapporten, samt si noe om Datatilsynets fokus i 2020.

Avviksmeldinger

I 2019 registrerte Datatilsynet 1916 avviksmeldinger. Til sammenligning var tallet fra år 2015 på 86. Den betydelige økningen skyldes neppe en drastisk oppgang i antall sikkerhetsbrudd, men snarere at GDPR stiller strengere krav til melding av brudd på personopplysningsikkerheten, samt at fokuset på personvern har økt etter ikrafttredelsen av GDPR.

Kun 16 prosent av avviksmeldingene ble gjenstand for videre saksbehandling fra Datatilsynet. Øvrige saker ble avsluttet som følge av at risikoen for enkeltindivider ble vurdert som lav, samt at virksomheten har gjort tiltak for å informere de berørte.

Avvikene varierer fra menneskelige feil som rammer få personer til alvorlige hackerangrep med flere tusen rammede. Statistikken viser at den vanligste årsaken bak avvik er at personopplysninger er sendt til feil mottaker. Hele 43 prosent av avviksmeldingene oppgir dette som begrunnelse. Denne type avvik utløser som regel ingen reaksjoner fra

Datatilsynet, idet virksomheten i slike tilfeller allerede har iverksatt tiltak for å lukke avviket og begrense skaden når Datatilsynet mottar avviksmeldingen.

Videre er 22 prosent av innmeldte avvik klassifisert under kategorien «Annet». Denne kategorien utgjør den nest største, og omfatter brudd som ikke er meldepliktige, brudd der type overtredelse er uklart på meldetidspunktet eller brudd som ikke lar seg kategorisere i andre kategorier. Dette kan tilsi at et betydelig antall brudd som meldes til Datatilsynet faktisk ikke er omfattet av meldeplikten.

Andre årsaker til avvik er manglende eller feil i virksomhetens tilgangsstyring, utilsiktet publisering av personopplysninger, at opplysninger om feil person er vist frem, hacking, tap av papirdokumenter og phishing.

Datatilsynet presenterer også statistikk over hvilke områder avviksmeldingene kom fra. Hele 30 prosent av avviksmeldingene kom fra finanssektoren. Ellers er offentlige virksomheter, som kommuner og statlige forvaltningsforetak/Forsvaret, godt representert i denne statistikken, med henholdsvis 23 og 12 prosent av avviksmeldingene.

Overtredelsesgebyr

I 2019 ila Datatilsynet tre overtredelsesgebyr etter GDPR. Bergen og Oslo kommune ble ilagt gebyr på

henholdsvis 1,6 og 1,2 millioner kroner. Begge gebyrene gjaldt brudd på personopplysningsikkerheten ved behandling av personopplysninger i skolen. Det siste overtredelsesgebyret i 2019 ble ilagt Oslo kommune v/ Sykehjemsetaten for lagring av helseopplysninger utenfor journalsystemet.

Det ble også ilagt syv overtredelsesgebyr etter reglene i gammel personopplysningslov fra 2000. Dette fordi GDPR ikke har tilbakevirkende kraft. Disse gjaldt ulovlig innsyn i e-post på arbeidsplassen, kredittvurderinger uten saklig behov og ulovlig publisering av bilder fra overvåkningskamera.

Tilsyn

Ifølge rapporten prioriterte ikke Datatilsynet å gjennomføre tilsyn i 2019. Datatilsynet har i stedet lagt ned ressurser i å utvikle en ny tilsynsmetodikk, som innebærer bruk av retningslinjer for revisjon av ledelsessystemer som grunnlag for å strukturere og effektivisere tilsynsvirksomheten. Nye planverk for tilsynsvirksomheten er dermed etablert, og det er derfor grunn til å tro at kontroll- og tilsynsvirksomheten vil trappes opp i 2020.

Internasjonalt samarbeid

GDPR skal tolkes likt i hele EØS, og praksis fra andre europeiske land og det europeiske Personvernrådet (European Data Protection Board



– EDPB) kan derfor påvirke Datatilsynets handlingsrom. Av den grunn har Datatilsynet deltatt i internasjonale prosesser for å fremme bedre personvern. Herunder har Datatilsynet hatt hovedansvaret for utarbeidelse av Personvernrådets felleseuropeiske retningslinjer for innebygd personvern og personvern som standardinnstillinger, samt felleseuropeiske retningslinjer om avtale som behandling av personopplysninger i kontekst av digitale tjenester.

I såkalt grenseoverskridende behandling av personopplysninger må alle berørte datatilsynsmyndigheter identifiseres, og en ledende datatilsynsmyndighet bli utpekt etter nærmere regler. Sammen skal tilsynsmyndighetene forsøke å komme til enighet. Formålet er å sørge for en konsekvent praktisering og håndheving av GDPR. I 2019 ble Datatilsynet identifisert som berørt tilsynsmyndighet i 459 saker og ledende

datatilsynsmyndighet i 8 saker. Sakene var fremdeles åpne ved årsskiftet.

Stadig flere norske virksomheter søker om bindende virksomhetsregler (Binding Corporate Rules – BCR) for overføringer av personopplysninger ut av EØS. Ved utgangen av 2019 hadde Datatilsynet til behandling fjorten søknader om godkjenning av BCR. Dette er det femte høyeste antallet søknader i Europa. Foreløpig har ikke Datatilsynet ferdigbehandlet noen av søknadene, ettersom BCR først må fremlegges Personvernrådet for uttalelse.

Fokus fremover

I 2020 planlegger Datatilsynet å gjennomføre flere kontroller. Mens mye av fokuset i 2019 har vært på offentlige virksomheter, herunder helse og utdanning, vil Datatilsynet i tiden som kommer også gjennomføre kontroll og etterlevelse av per-

sonvernregelverket i privat sektor. I rapporten antydes det at ikrafttredelsen av Payment Service Directive 2 (PSD2) kan medføre at bank- og forsikringsvirksomhet kan bli høyere prioritert i 2020. Det samme gjelder for samferdselssektoren, dersom en utredning om veipricing iverksettes.

I rapporten uttales det at dersom kontrollvirksomheten minner ut i overtredelsesgebyr, er Datatilsynet forberedt på å bli utfordret rettslig på en annen måte enn Datatilsynet har opplevd hittil. Mye tyder dermed på at antall ilagte gebyrer vil øke og at vi vil kunne få etterlengtede avklaringer i rettspraksis.

Carl Emil Bull-Berg er advokatfullmektig hos Advokatfirmaet Wiersholm.

Line Helen Haukalid er fast advokat i Advokatfirmaet Wiersholm.



Delphi

Christina Björn och Asta Schulz

Utfärdad sanktionsavgift mot Statens servicecenter

Statens servicecenter ("SSC") behandlar på uppdrag av ett antal myndigheter personuppgifter i lönesystemet Primula. Efter att Datainspektionen mottagit flera anmälningar rörande systemet från myndigheter som SSC är personuppgiftsbiträde åt, genomfördes en tillsyn mot SSC. Efter genomförd granskning beslutade Datainspektionen att utfärda en sanktionsavgift på sammanlagt 200 000 kronor. Detta innebär att det är den första sanktionsavgiften som Datainspektionen har utfärdat på grund av bristande incidenthantering samt även den första sanktionsavgiften som utfärdas till ett personuppgiftsbiträde. Anledningen till sanktionsavgiften är att SSC har agerat för långsamt gällande en inträffad personuppgiftsincident. Först efter fem månader meddelade SSC de personuppgiftsansvariga myndigheterna som SSC varit personuppgiftsbiträde åt, vilket enligt Datainspektionen inte kan anses vara utan onödigt dröjsmål. Dessutom dröjde det drygt tre månader innan SSC anmälde personuppgiftsincidenten i egenskap av personuppgiftsansvarig, vilket också ansågs vara en överträdelse av dataskyddsbestämmelserna.

Bakgrund

Det var den 28 mars 2019 som SSC fick vetskap om, från en myndighet som SSC agerar personuppgiftsbiträde åt, att det gick att komma åt personuppgifter som tillhörde andra personuppgiftsansvariga myndigheter via lönesystemet. Därefter inkom 37 anmälningar om personuppgiftsincidenter i Primula från myndigheter som SSC agerat personuppgiftsbiträde åt. Kategorierna av personuppgifter som gick att komma åt var bland annat personnummer, namn, uppgift om kön, uppgift om skyddad adressuppgift, ekonomisk eller finansiell information, anställningstid etc. Vissa av uppgifterna omfattades av sekretess och var av integritetskänsligt slag. SSC upprättade en intern incidentrapport, men avvaktade med att underrätta de andra personuppgiftsansvariga myndigheterna, totalt 47 stycken, för att det inte ansågs finnas tillräcklig information om och hur incidenten hade inträffat. Av samma anledning gjordes heller ingen anmälan till Datainspektionen för det fall som SSC agerade som personuppgiftsansvarig, dvs. för de personuppgifter som rörde den egna personalen. Det var inte förrän den 25 juni 2019 som SSC lämnade en anmälan till Datainspektionen om personuppgiftsincidenten, och då avsåg anmälan endast den del där

SSC varit personuppgiftsansvarig. Den 20 augusti 2019 underrättades de övriga personuppgiftsansvariga myndigheterna om den inträffade incidenten, alltså närmare fem månader efter den inträffade incidenten.

Skyldighet att underrätta personuppgiftsansvariga samt anmäla till Datainspektionen

SSC har inom ramen för beslutet uppträtt i två olika roller, som personuppgiftsbiträde respektive personuppgiftsansvarig. Ett personuppgiftsbiträde ska enligt artikel 33.2 i dataskyddsförordningen ("GDPR") underrätta den personuppgiftsansvarige utan dröjsmål efter det att biträdet har fått vetskap om att en personuppgiftsincident har inträffat. Biträdet ska inte göra en bedömning av eventuell sannolikhet för vilka risker som finns för de registrerades fri- och rättigheter, utan det är den personuppgiftsansvariges uppgift. Datainspektionen bedömde att SSC hade tillräcklig information för att underrätta de personuppgiftsansvariga myndigheterna och att tiden som det tog för SSC att underrätta dessa var betydligt längre än vad som kan anses vara godtagbart, även om en kortare undersökning skulle göras för att skaffa mer information om incidenten. Datainspektionen konstaterade

också att den anmälan som SSC gjorde i egenskap av personuppgiftsansvarig, gjordes cirka två månader innan underrättelsen till de personuppgiftsansvariga myndigheterna gjordes, vilket SSC har saknat anledning till enligt Datainspektionens bedömning.

Utöver skyldigheten i egenskap av personuppgiftsbiträde att underrätta den personuppgiftsansvarige, föreligger det även en skyldighet enligt artikel 33.1 GDPR att som personuppgiftsansvarig anmäla en personuppgiftsincident till Datainspektionen utan onödigt dröjsmål och inte senare än 72 timmar efter vetskap om den. Om det inte finns möjlighet att tillhandahålla all information samtidigt, kan den personuppgiftsansvarige komplettera sin anmälan. Som nämnts ovan dröjde det alltså närmare tre månader från det att SSC fick vetskap om incidenten, till att en anmälan gjordes till Datainspektionen. Även i det fallet konstaterade Datainspektionen att det tog betydligt längre tid än vad som kan tänkas vara nödvändigt.

Vidare konstaterar Datainspektionen att SSC i egenskap av personuppgiftsansvarig inte har dokumenterat väsentliga omständigheter kring personuppgiftsincidenten och de korrigerande åtgärder som vidtagits. Detta innebär en överträdelse av artikel 33.5 i GDPR som stadgar att en personuppgiftsansvarig ska dokumentera alla omständigheter, effekter och korrigerande åtgärder som vidtagits i händelse av en personuppgiftsincident.

Utfärdade sanktioner

Antalet registrerade som omfattades av den incident som SSC inte underrättade de 47 myndigheterna om, uppgick till omkring 282 000 stycken. I sin bedömning vägrade Datainspektionen in det faktum att incidenten rörde ett stort antal registrerade, att det dröjde flera månader innan SSC underrättade myndigheterna samt att var och en av de 47 myndigheterna skulle ha underrät-

tats var för sig utan onödigt dröjsmål. Eftersom det inte var fråga om en mindre överträdelse med den nästan fem månader långa perioden innan myndigheterna underrättades, ansåg Datainspektionen att det inte var tillräckligt med en reprimand, utan en sanktionsavgift påfördes. Personuppgiftsincidenten som omfattade SSC:s egen personal, rörde omkring 1 800 anställda, och även här gick det för lång tid innan Datainspektionen underrättades om incidenten. Datainspektionen fann därför inte skäl till att ersätta sanktionsavgiften med en annan åtgärd här heller.

Sammantaget beslutade Datainspektionen att överträdelserna skulle resultera i en administrativ sanktionsavgift på 150 000 kronor för att SSC underlät att utan onödigt dröjsmål underrätta de personuppgiftsansvariga myndigheterna, samt 50 000 kronor för att SSC som personuppgiftsansvarig inte anmälde personuppgiftsincidenten till Datainspektionen utan onödigt dröjsmål.

Vad gäller SSC:s brister i dokumentationen konstaterade Datainspektionen att bristerna inte utgjort en mindre överträdelse av artikel 33.5 i GDPR eftersom Datainspektionen inte har kunnat använda sig av dokumentationen för att kontrollera efterlevnaden av artikel 33. Sammantaget bedömde Datainspektionen dock att bristen inte varit av sådan grad att en sanktionsavgift var befogad. SSC förelades därför att upprätta rutiner för dokumentation av personuppgiftsincidenter som möjliggör för Datainspektionen att kontrollera efterlevnaden av artikel 33 och se till att dessa rutiner följs.

Övrigt

Det kan även noteras att Datainspektionen i sitt beslut konstaterade att SSC inte hade ett personuppgiftsbiträdesavtal med driftleverantören av lönesystemet i enlighet med artiklarna 28.3 och 28.4 i GDPR. Däremot hade SSC och leverantören tidigare ingått ett avtal i

enlighet med de gamla bestämmelserna i personuppgiftslagen. Parterna höll på att uppdatera avtalet för att det skulle överensstämma med GDPR:s nya krav, och därför fann inte Datainspektionen någon anledning att även denna överträdelse skulle resultera i en särskild sanktionsavgift eller annan korrigerande åtgärd.

Avslutande kommentar

Vi anser att tillsynsbeslutet ger upphov till ett par intressanta reflektioner. Inledningsvis kan konstateras att den utdömda sanktionsavgiften är låg i relation till antalet berörda registrerade samt det faktum att det dröjde så länge innan SSC informerade de personuppgiftsansvariga myndigheterna samt Datainspektionen efter vetskap om personuppgiftsincidenten. Det kan här noteras att det högsta beloppet för en sanktionsavgift en myndighet kan påföras är lägre än vad som gäller för privata aktörer, men det utdömda beloppet bör ändå betraktas som förhållandevis lågt i förhållande till de försvärande omständigheter som förelegat.

Den andra reflektionen som kan göras rör SSC:s avsaknad av ett, enligt GDPR, godkänt personuppgiftsbiträdesavtal. Datainspektionen fann inte skäl att påföra en sanktionsavgift eftersom personuppgiftsbiträdesavtalet var upprättat i enlighet med personuppgiftslagen och höll på att uppdateras utifrån GDPR. Det kan konstateras att SSC haft relativt god tid på sig att uppdatera det aktuella personuppgiftsbiträdesavtalet och uppenbart överträtt artiklarna 28.3. och 28.4 i GDPR, men trots detta har varken en sanktionsavgift eller annan korrigerande åtgärd påförts.

Christina Björn är associate i Advokatfirman Delpbi, Stockholm.

Asta Schulz är associate i Advokatfirman Delpbi, Stockholm.



Gorrissen Federspiel

Tue Goldschmieding

1. Ommærkning af parallelimporterede lægemidler kunne ikke forbydes

Den 18. februar 2020 afsagde den danske Sø- og Handelsret ('Sø- og Handelsretten') kendelse i sagen BS-37 578/2019-SHR mellem sagsøger Essential Pharma Limited (Essential Pharma) og sagsøgte Orifarm A/S.

Sagen omhandlede, hvorvidt Orifarm A/S ved parallelimport til Danmark af et lægemiddel, som i eksportlandet, Belgien, af varemærkeindehaveren Essential Pharma blev solgt under varemærket 'Zarontin', var berettiget til at ommærke lægemidlet til 'Zarondan', som var det registrerede varemærke, som Essential Pharma markedsførte lægemidlet under i Danmark.

Orifarm A/S ansøgte i august 2018 den danske Lægemiddelstyrelse om markedsføringstilladelse til parallelimport af Zarontin. De fik imidlertid afslag herpå, grundet en forvekslingsrisiko med lægemidlet Saroten. Orifarm A/S foreslog herefter navnet Zarondan, hvilket de fik markedsføringstilladelse til i oktober 2018. Orifarm A/S påbegyndte herefter markedsføringen i marts 2019.

Spørgsmålet var, om den manglende adgang til at anvende eksportlandets varemærke i Danmark automatisk medførte en adgang til at anvende importmedlemsstatens varemærke, eller om det dertil var en betingelse, at det var objektivt nødvendigt at anvende lige præcis navnet Zarondan i stedet for et hvilket som helst andet navn.

Sø- og Handelsretten henviste til dommen U 2003.1807/2 H og Generaladvokatens forslag til afgørelse i sagen Upjohn C-112/89 1991, hvoraf fremgår, at hvis parallelimportøren ikke har mulighed for effektiv markedsføring uden ommærkning, foreligger der en markedsopdeling, hvilket vil berettige importøren til at ommærke. Hvis dette er grundet regler i importmedlemsstaten, vil varemærkeindehaveren ikke kunne bruge varemærkeretten til at forhindre importøren i at bruge det varemærke, som indehaveren bruger for de samme varer i importstaten. Dette berettiger til ommærkning fra det mærke, som varemærkeindehaveren anvender i eksportstaten, til det mærke, som indehaveren anvender i importstaten.

Orifarm A/S var derfor berettiget til at anvende varemærket Zarondan i Danmark til det parallelimporterede lægemiddel, idet eksportmedlemsstatens varemærke Zarontin ikke kunne anvendes på grund af forvekslingsrisiko.

Læs hele dommen her:

http://domstol.fe1.tangora.com/media/-300_011/files/Kendelse_BS-37_578-2019.pdf?rev1

2. EU-domstolen tager stilling til præjudicielle spørgsmål om varemærkers manglende klarhed og præcision og varemærkeregistreringer indgivet i ond tro

EU-Domstolen afsagde den 29. januar 2020 dom i sagen C-371/2018 mellem Sky plc og dets tyske og engelske filialer ('Sky') og SkyKick Inc.

og dets engelske filial ('SkyKick'). Sagen, der var en præjudiciel forelæggelse fra højesteretten i England og Wales, drejede sig om fortolkningen af bestemmelserne om absolutte ugyldighedsgrunde.

EU-Domstolen skulle under sagen tage stilling til tre spørgsmål vedrørende fortolkningen af artikel 7 og 51 i Rådets forordning (EF) nr. 40/94 af 20. december 1993 om EF-varemærker ('varemærkeforordningen') og artikel 3 i Rådets direktiv 89/104/EØF af 21. december 1988 om indbyrdes tilnærmelse af medlemsstaternes lovgivning om varemærker ('varemærkedirektivet').

I sagen havde Sky anlagt sag imod SkyKick for krænkelsen af fire registrerede figurvaremærker. For højesteretten i England og Wales havde SkyKick gjort gældende, at de omhandlede varemærker var registreret for en række varer og tjenesteydelser, som ikke var angivet med tilstrækkelig klarhed og præcision, herunder kategorien »computersoftware.«

Det første spørgsmål angik, om et varemærke kan erklæres helt eller delvist ugyldigt under henvisning til manglende klarhed og præcision i beskrivelsen af de varer og tjenesteydelser, som varemærket er registreret for. Hertil svarede EU-Domstolen, at kravene om klarhed og præcision alene gælder for identificeringen af de tegn, der kan udgøre et varemærke. Der kan ikke heraf udledes, at lignende krav skulle gælde for ord, der anvendes til at udpege de varer og tjenesteydelser, som varemærket er registreret for. EU-Domstolen anførte i denne for-

bindelse, at et sådant krav ikke var omfattet af de udtømmende ugyldighedsgrunde oplyst henholdsvis artikel 7 stk. 1 og 51 i varemærkeforordningen samt artikel 3 i varemærkedirektivet. Det andet spørgsmål angik, om en

varemærkereгистраering er indgivet i ond tro, når der ikke foreligger nogen hensigt til brug af varemærket inden for de varer og tjenesteydelser, som registreringen angår.

EU-Domstolen statuerede indledningsvist, at der ved fortolkningen af begrebet ond tro skal tages hensyn til den specifikke varemærkeretlige sammenhæng samt formålet med de EU-retlige varemærkereregler. Formålet med reglerne er at bidrage til en ordning med loyal konkurrence, hvori enhver virksomhed ved hjælp af registrering af varemærker, der gør forbrugeren i stand til at adskille varen eller tjenesteydelsen fra andre, kan opbygge en fast kundekreds. På denne baggrund udtalte EU-Domstolen, at ond tro skal forstås som tilfælde, hvor en varemærkeansøgning er indgivet uden det formål at deltage loyalt i konkurrence, men med hensigt om at skade tredjemands interesser på en måde der ikke er i overensstemmelse med redelig markedsføringsskik.

Slutteligt skulle EU-Domstolen vurdere, om en national bestemmelse, hvorefter en varemærkeansøger skulle erklære, at varemærket aktuelt bruges eller påtænkes brugt til de varer og tjenesteydelser der er omfattet af registreringsansøgningen, er afskåret som følge af varemærkedirektivet. Hertil svarede EU-Domstolen, at varemærkedirektivet ikke var til hinder for den nævnte slags bestemmelse. EU-Domstolen henviste i denne forbindelse til femte betragtning i varemærkedirektivet, hvorefter medlemsstaterne fuldt ud bevarer deres frihed til at fastsætte procedureregler vedrørende registrering, fortabelse og ugyldighed.

Læs hele dommen her:

<http://curia.europa.eu/juris/document/document.jsf?text=ejendomsret&do->

[cid=222824&pageIn-
dex=0&doclang=DA&mode=req&
dir=&occ=first&part=1&
cid=3579300#ctx:1](http://curia.europa.eu/juris/document/document.jsf?text=ejendomsret&do-)

3. EU-Domstolen annullerer afgørelse fra EUIPO som følge af manglende iagttagelse af begrundelsespligt

Den 19. december 2019 afsagde EU-domstolen dom i sagen T-690/18, mellem Sony Interactive Entertainment Europe Ltd (Sony Entertainment) og Den Europæiske Unions Kontor for Intellectuel Ejendomsret (EUIPO).

Sagen omhandlede en afgørelse afsagt af EUIPO's Femte Appellkammer af 12. november 2015, mellem Sony Entertainment og Vieta Audio, SA, vedrørende fortabelse af retten til brug af EU-ordmærket Vita i medfør af artikel 51, stk. 1, litra a), i Forordning nr. 207/2009 ('Forordning om EF-varemærker').

Vieta Audio, SA indgav en begæring om fortabelse af varemærket »Vita«, for alle de varer, som var omfattet af varemærket. Vieta Audio, SA gjorde gældende, at »Vita« ikke have været genstand for reel brug i den Europæiske Union i den relevante periode fra den 14. oktober 2006 til den 13. oktober 2011, og at der ikke forelå nogen rimelig grund til denne manglende brug. Ved afgørelse af 30. juni 2014 erklærede annullationsafdelingen »Vita« som fortabt for så vidt angik alle de varer, som det var registreret for.

Sony Entertainment Europe klagede den 28. august 2014 over annullationsafdelingens afgørelse til EUIPO. Ved afgørelse i sag R 2232/014-5 af 12. november 2015 stadfæstede Femte Appellkammer ved EUIPO annullationsafdelingens afgørelse og gav afslag på klagen.

Sony Entertainment indbragte sagen for EU-domstolen, der annullerede afgørelsen ved dom af 12. december 2017, Vita (T-35/16, ikke trykt i Sml., EU:T:2017:886). Retten fandt, at afgørelsen ikke var tilstræk-

keligt begrundet, idet det ikke fremgik, hvorfor Sony Entertainment ikke havde påvist, at der var gjort reel brug af det anfægtede varemærke.

EU-domstolen henviste sagen til EUIPO's Fjerde Appellkammer, der afgjorde sagen den 10. september 2018 (den anfægtede afgørelse). Afgørelsen stadfæstede den tidligere afgørelse afsagt af Femte Appellkammer. Fjerde Appellkammer lagde vægt på, at EU-domstolen havde tiltrådt Femte Appellkammers konklusioner vedrørende varigheden af, stedet for og formen af brugen af varemærket, og at de dermed var blevet endelige.

Sony Entertainment indbragte herefter igen sagen for EU-domstolen, med påstand om annullering af den anfægtede afgørelse. Sony Entertainment anførte, at det var med urette at den anfægtede afgørelse havde lagt vægt på, at EU-Domstolen havde tiltrådt Femte Appellkammers konklusioner. Dommen af 12. december 2017 havde alene konkluderet, at den tidligere afgørelse var behæftet med en manglende begrundelse. Tværtimod havde EU-Domstolen ikke undersøgt de anbringender og beviser, som Sony Entertainment havde fremført, og den medgav dermed ikke, at nogen af parternes argumenter var velbegrundede.

EU-domstolen fandt i dommen af 19. december 2019, at Fjerde Appellkammer med urette ikke havde foretaget en ny prøvelse af Sony Entertainments anbringender og beviser. Femte Appellkammers konklusioner var ikke blevet endelige som følge af dommen af 12. december 2017. Heller ikke de af anbringenderne, EU-Domstolen havde fastslået var tilstrækkeligt begrundede, kunne anses for at have opnået materiel retskraft. Fjerde Appellkammer var dermed ikke bundet af disse præmisser i den tidligere afgørelse, og kunne derfor heller ikke undlade prøvelse i den anfægtede afgørelse.

Den anfægtede afgørelse blev derfor annulleret i det hele, idet EUIPO ikke havde iagttaget begrundelsespligten, ved ikke at prøve alle de relevante spørgsmål.

Læs hele dommen her:

<http://curia.europa.eu/juris/document/document.jsf?text=ejudomsret&docid=221769&pageIn-dex=0&doclang=DA&mode=req&dir=&occ=first&part=1&cid=455905#ctx1>

4. Selfiekamera udgjorde ikke nærgående efterligning

Den danske Sø- og Handelsret afsagde den 5. marts 2020 dom i sagen BS-48 560/2019-SHR mellem Myselfie ApS ('Myselfie') og Selfiecam ApS ('Selfiecam'). Sagen angik spørgsmålet, om Myselfies photobooth var beskyttet efter lov nr. 426 af 3. maj 2017 (den danske markedsføringslovs) § 3 eller Rådets forordning (EF) nr. 6/02 af 12. december 2001 om EF-design ('EF-designforordningens') artikel 19 stk. 2.

På en messe i januar 2018 blev indehaveren af Myselfie opmærksom på Selfiecams selfiekamera, som havde samme funktionalitet og størrelse af lampe og skærm som Myselfies selfiekamera. For at distancere sig fra Selfiecams produkt, lancerede indehaveren af Myselfie en ny version af sin fotoboks. I den nye version blev frontpladen udskiftet med en større model der havde afrundede hjørner. På samme tid var Selfiecam imidlertid også i gang med at lancere en ny version af deres selfiekamera, der også skulle have afrundede hjørner. Indehaveren af Myselfie blev opmærksom herpå i juli 2019 og fremsatte efterfølgende anmodning om nedlæggelse af fagedforbud.

Den danske Sø- og Handelsret fandt, at Myselfies selfiekamera ikke havde beskyttelse efter EF-designforordningens artikel 19 stk. 2 som et ikke-registreret design, eftersom nyhedskravet i artikel 4 ikke var opfyldt. Derimod fandt retten, at My-

selfies selfiekamera var beskyttet mod efterligninger efter den danske markedsføringslovs § 3, eftersom de trufne designmæssige valg ikke udelukkende var funktionsbestemte.

De anvendte designelementer i fotoboksen var imidlertid af enkel karakter og hyppigt forekommende for elektroniske skærmprodukter, hvorfor beskyttelsen måtte anses for snæver. Henset til forskellene i de to selfiekameraers visuelle udtryk, herunder med hensyn til materialevalg og skærmstørrelse, fandt retten imidlertid ikke, at der var tale om en så nærgående efterligning, at den danske markedsføringslov § 3 var overtrådt. Myselfies anmodning om fagedforbud blev derfor ikke taget til følge.

Læs hele dommen her:

<http://domstol.fe1.tangora.com/media/-300011/files/Kendelse-BS-48-650-2019.pdf>

5. Forbrugerombudsmanden informerer virksomheder om, at 'linkbuilding' omfattes af forbuddet mod skjult reklame

Den danske forbrugerombudsmand har den 10. marts 2020 informeret virksomheder omkring det retlige standpunkt til konceptet »linkbuilding« efter lov nr. 426 af 3. maj 2017 ('den danske markedsføringslov'), lov nr. 227 af 22. april 2002 ('den danske e-handelslov') og lov bekendtgørelse nr. 763 af 23. juli 2019 ('den danske selskabslov').

Linkbuilding foregår ved, at en virksomhed, mod betaling, linker fra sin hjemmeside til en anden virksomheds hjemmeside, for dermed at skabe mere trafik for den anden hjemmeside, der følgelig opnår en højere placering i Googles søgeresultater.

Forbuddet mod skjult reklame, jf. den danske markedsføringslovs § 6, stk. 4, indebærer, at kommercielle hensigter skal være tydelige for forbrugeren. Har indehaveren af en hjemmeside aftalt med en anden virksomhed at linke til dennes hjemmeside, vil dette udgøre en

kommerciel hensigt, som vil være strafbar, i det omfang den kommercielle hensigt ikke er tydelig for forbrugeren.

Tekster der linker til andre virksomheders hjemmesider, skal derfor tydeligt markeres med fx »annonce« eller »reklame«, for derved at bekendtgøre den kommercielle hensigt, og dermed undgå at forbrugeren vildledes til at tro, at indholdet har redaktionelt indhold.

Efter den danske markedsføringslovs §§ 5-6 forbydes virksomheder at vildlede forbrugerne. Herefter forpligtes virksomheder til klart at oplyse den kommercielle hensigt med enhver form for handelspraksis. Af pkt. 11 i bilag 1 til den danske markedsføringslov følger, at det vil blive anset som vildledende såfremt redaktionelt indhold i medierne anvendes til at promovere et produkt, hvor en erhvervsdrivende har betalt for denne promovering, uden at dette tydeligt fremgår af indholdet på en måde, så forbrugeren let kan identificere dette.

Forbrugerombudsmanden henviser yderligere til den danske e-handelslov § 9, stk. 1, 2. pkt., hvorefter det skal fremgå, hvem der er afsender af indholdet på en hjemmeside, hvilket vil kunne modvirke at forbrugeren vildledes omkring, hvem den egentlige afsender af hjemmesiders indhold er som følge af linkbuilding.

I tillæg hertil gælder der en række oplysningskrav efter henholdsvis den danske e-handelslovs § 7 og den danske selskabslovs § 2, stk. 4. Således forpligter den danske e-handelslov tjenesteydere som udbyder kommercielle tjenester online at oplyse navn, fysisk adresse, e-mail og CVR-nummer. Dertil forpligtes kapital-selskaber efter den danske selskabslov til at oplyse navn, hjemsted og CVR-nummer på deres hjemmeside.

Læs hele udtalelsen her:

<https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/>

pressemdelelser/2020/forbrugerombudsmanden-orienterer-om-forbud-mod-skejult-reklame-ved-linkbuilding/

6. Forbrugerombudsmanden fandt målrettet markedsføring af lån til hasardspillere for ulovlig

Selskabet Sky Connect ApS ('Sky Connect') ønskede at afprøve de muligheder, Facebook tilbød inden for målrettet annoncering, og målrettede derfor sin markedsføring af låneportalen »Favoritlån« mod mænd i alderen 28 til 45 år der havde vist interesse for 'online games' og 'online poker'. Den danske Forbrugerombudsmand modtog henvendelse herom fra en klager, og vurderede efterfølgende at markedsføringen var i strid med god markedsføringsetik jf. lov nr. 426 af 3. maj 2017 (den danske markedsføringslovs) § 3 stk. 1.

Efter den danske markedsføringslovs § 3 stk. 1 skal erhvervsdrivende udvise god markedsføringsetik, herunder iagttage forbrugerhensyn, andre erhvervsdrivendes interesser samt almene samfundshensyn. Markedsføringen af Favoritlån var i strid med almene samfundshensyn såsom social ansvarlighed og etisk adfærd, da der i de udvalgte kategorier kunne være personer med spillegæld, hvorfor markedsføringen var ulovlig.

Den danske Forbrugerombudsmand udtalte, at virksomheder med den seneste teknologiske udvikling inden for dataindsamling har fået bedre værktøjer til at målrette deres markedsføring mod udvalgte grupper af forbrugere. Dette medfører imidlertid et større ansvar for, at kravet om god markedsføringsetik overholdes, herunder navnlig at markedsføringen ikke er i strid med almene samfundshensyn, social ansvarlighed og etisk adfærd.

Læs hele udtalelsen her:

<https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemdelelser/2020/markedsfoering-af-laan-til-hazardspillere-var-ulovlig/>

7. Forbrugerombudsmanden fandt, at en kundeaftale ikke var tilstrækkelig til, at undtagelsen til spamforbuddet kunne anvendes

Den danske forbrugerombudsmand ('Forbrugerombudsmanden') afgav den 5. december 2019 sin vurdering af, hvorvidt undtagelsen til spamforbuddet i lov nr. 426 af 3. maj 2017 ('den danske markedsføringslovs') § 10, stk. 2, kunne finde anvendelse i en konkret sag. Herefter vil en virksomhed kunne sende markedsføring til en tidligere kunde, hvis en række betingelser er opfyldt.

Vurderingen skete efter anmodning fra en virksomhed, som ønskede oplyst, hvorvidt det var lovligt, at sende markedsføringsmateriale ud til sine kunder på baggrund af en indgået kundeaftale, hvor virksomheden havde modtaget kundens mailadresse, men hvor der endnu ikke, nødvendigvis, var sket et salg.

Forbrugerombudsmanden vurderede, at undtagelsen ikke fandt anvendelse ved oprettelsen af en kundeaftale, når der ikke samtidig med oprettelsen af kundeaftalen skete salg af et produkt. Vurderingen havde grundlag i, at undtagelsen til spamforbuddet i den danske markedsføringslovs § 10, stk. 2 alene fandt anvendelse, hvis mailadressen var oplyst i forbindelse med et køb. Dertil fremhævede Forbrugerombudsmanden også, at kunden i forbindelsen med købet skulle have muligheden for at frabede sig markedsføring tilsendt mailadressen.

Læs hele udtalelsen her:

<https://www.forbrugerombudsmanden.dk/find-sager/markedsfoeringsloven/sager-efter-markedsfoeringsloven/spam/en-kundeftale-var-ikke-i-sig-selv-nok-til-at-undtagelsen-til-spamforbuddet-kan-anvendes/>

8. Virksomheds reklamebrug af landsholdsspillere i rød/hvide fodbolddragter udgjorde en krænkelse af markedsføringsloven

Den danske Sø- og Handelsret ('Sø- og Handelsretten') afsagde den 27.

januar 2020 dom i sagen BS-38 371/2018-SHR, mellem sagsøger DBU A/S og sagsøgte LeoVegas Gaming p.l.c (LeoVegas). Sagen drejede sig om hvorvidt LeoVegas, ved visning af reklamer med landsholdsspilleren Nadia Nadim, havde krænkert DBU's immaterielle og kommercielle rettigheder.

Den 14. maj 2018 indgik LeoVegas en reklameaftale med en af de mest kendte landsholdsspillere for det danske kvindefodboldlandshold, Nadia Nadim. Iført rød/hvid fodboldtrøje skulle hun således være den nye frontfigur i en reklamekampagne, der skulle løbe op til og under VM i fodbold i 2018. Den 20. maj rettede DBU henvendelse til LeoVegas vedrørende den nylancerede kampagne og anførte, at reklamekampagnen krænkede DBU's kommercielle og immaterielle rettigheder efter lovbekendtgørelse nr. 88 af 29. januar 2019 ('den danske varemærkelov') og lov nr. 426 af 03. maj 2017 ('den danske markedsføringslovs'), og henviste i denne forbindelse til Landsholdsaftalen mellem Nadia Nadim og DBU.

Sø- og Handelsretten lagde indledningsvist til grund, at Landsholdsaftalens pkt. 5.17 lægger rammerne for, hvilke begrænsninger den enkelte landsholdsspiller er underlagt ved sine muligheder for at indgå reklameaftaler. Af bestemmelsen fremgår, at spillerne ikke kan indgå personlige aftaler, hvor reklameaktiviteten relateres til landsholdet, ligesom de ikke uden om DBU kan anvende landsholdsdragten.

Retten fandt, at reklamerne, hvori Nadia Nadim umiddelbart forud for VM stod foran et dannebrogflag iført den rød/hvide dragt, gav sådanne associationer til det danske landshold, at DBU's rettigheder hertil var krænkert. Reklamerne snyltede på den goodwill, som var oparbejdet forhold til landsholdet, og dette udgjorde en overtrædelse af den danske markedsføringslovs § 3 om god

markedsføringssskik. Der var ikke godtgjort et tab, og retten fastsatte derfor skønsmæssigt et rimeligt vederlag til DBU på 500.000 kr. under hensyntagen til den betydelige og langvarige eksponering samt reklamekampagnens samlede udgifter, der beløb sig til 2-3 mio. kr.

Læs hele dommen her:

http://domstol.fe1.tangora.com/media/-300_011/files/Dom38_371-18.pdf

9. »Piratvejledning« udgjorde strafbar medvirken til ophavsretskrænkelser

Den danske Højesteret afsagde den 14. januar 2020 dom i sagen 135/2019 mellem Anklagemyndigheden og Tiltalte. Tiltalte var i tidligere instanser blevet fundet skyldig i medvirken til ophavsretskrænkelser af særlig grov karakter efter Lovbekendtgørelse nr. 976 af 17. september 2019 ('den danske straffelov') § 299b ved på sin hjemmeside, www.popcorn.dk, at have opfordret til brugen af programmet Popcorn Time, som anvendes til ulovlig streaming af film.

For den danske Højesteret angik sagen spørgsmålet, om de ophavsretskrænkelser Tiltalte havde medvirket til, var tilstrækkeligt konkretiseret i såvel anklageskriftet som i relation til vurderingen af Tiltaltes ansvar for medvirken. Derudover skulle den danske Højesteret tage stilling til, om de opnåede reklameindtægter fra besøg på hjemmesiden skulle konfiskeres.

Tiltalte gjorde under sagen gældende, at anklageskriftet led af mangler, da det ikke var tilstrækkeligt konkretiseret, hvilke ophavsretskrænkelser han havde medvirket til. Derudover gjorde han gældende, at der ikke var tale om strafbar medvirken, eftersom anvisningerne på hjemmesiden rettede sig mod en ubestemt personkreds, og ikke mod konkrete personers brud på ophavsrettigheder eller deres forberedelse hertil.

Den danske Højesteret fandt, at anvisningerne på hjemmesiden var specifikt rettet mod brug af programmet Popcorn Time, og dermed de film som var tilgængelige heri, samt at det ikke var afgørende, at der ikke forelå oplysninger om de enkelte brugere og udbydere af Popcorn Time og disses ophavsretskrænkelser. Tiltaltes formål med at skrive om Popcorn Time på hjemmesiden var at opnå store reklameindtægter, og Højesteret fandt derfor, at der var en så nær sammenhæng mellem de strafbare handlinger og reklameindtægterne, at indtægterne skulle konfiskeres i medfør af den danske straffelovs § 75 stk. 1.

Læs hele dommen her:

http://domstol.fe1.tangora.com/media/-300_016/files/135-19-anonym.pdf

10. Anvendelse af Louis Vuittons velkendte varemærke udgjorde en krænkelse

Den danske Sø- og Handelsret ('Sø- og Handelsretten') afsagde den 6. januar 2020 dom i sagen BS-43 965/2018-SHR mellem Rich-Ycled Scandinavia IVS ('Rich-Ycled') og Louis Vuitton Malletier S.A.S ('Louis Vuitton'). Sagen angik, hvorvidt Rich-Ycled var berettiget til at anvende Louis Vuittons' forretningskendetegn og varemærker i forbindelse med genanvendelse, markedsføring og salg af brugte Louis Vuitton beklædningsgenstande.

Retten fandt, at Louis Vuitton var indehaver af en lang række varemærkerrettigheder, herunder det registrerede EU-varemærkenummer 009 844 391, der viste Louis Vuittons velkendte monogram.

Rich-Ycled havde anvendt materiale, der ikke var originalt Louis Vuitton-materiale og som ikke stammede fra originale, brugte Louis Vuitton-produkter, til at producere deres produkter, herunder beklædningsgenstande. Retten tog derfor ikke stilling til, hvorvidt der var tale om berettiget genanvendelse

af originale Louis Vuitton-produkter eller rækkevidden af principet om konsumtion.

På baggrund af ovenstående udtalte retten, at Rich-Ycleds produktion, markedsføring og salg af de omhandlende sko og T-shirts udgjorde en krænkelse af Louis Vuittons varemærkerrettigheder samt en krænkelse af Louis Vuittons rettigheder efter Lov nr. 426 af 3. maj 2017 ('den danske markedsføringslov'), idet brugen uden rimelig grund medførte en utilbørlig udnyttelse af Louis Vuitton-mærkernes renommé og skadede dette i strid med god markedsføringssskik, jf. Europa-Parlamentets og Rådets forordning (EU) 2017/1001 af 14. juni 2017 om EU-varemærker ('varemærkeforordningens') artikel 9, stk. 2, litra c, og den danske markedsføringslovs § 3, stk. 1 og § 22.

Den omstændighed, at de omhandlende T-shirts var påført ordene »I am Not«, og at T-shirtene ikke umiddelbart var forvekslelige med Louis Vuittons produkter, var ikke i sig selv tilstrækkeligt til at berettige Rich-Ycleds brug af Louis Vuittons varemærker og forretningskendetegn.

Louis Vuitton blev følgelig tildelt erstatning og godtgørelse, og Rich-Ycled blev påbudt ikke at markedsføre de omhandlende produkter samt at destruere disse.

Læs hele dommen her:

http://domstol.fe1.tangora.com/media/-300_011/files/Dom_43_965-2018.pdf

11. Præjudiciel forelæggelse for EU Domstolen vedrørende digital konsumtion

EU-Domstolen afsagde den 19. december 2019 dom i sag C-263/18 mellem to ophavsrettighedsorganisationer, Nederlands Uitgeversverbond og Groep Algemene Uitgevers, overfor Tom Kabinet Internet BV mfl. i en præjudiciel afgørelse forelagt af den hollandske retsbank Den Haag. I sagen tog EU-Domstolen stilling til, hvorvidt

der gjaldt et generelt princip om digital konsumtion, hvorefter ophavsmandens eneret til spredning af et digitalt værk blev udtømt efter det beskyttede værk første gang lovligt var blevet bragt i omsætning, med den konsekvens at ophavsmanden ikke ville kunne modsætte sig, at erhververen af et digitalt værk videresælger dette.

Sagen udsprang af en tvist mellem rettighedsorganisationerne og Tom Kabinet, som drev virksomhed med handel af »brugte« e-bøger. Rettighedsorganisationerne havde nedlagt påstand om, at videresalget udgjorde en »overføring til almenheden« i henhold til Europa-Parlamentets og Rådets direktiv 2001/29/EF af 22. maj 2001 (»infosoc-direktivet«) artikel 3, stk. 1, som vil kræve rettighedshavers tilladelse. Hertil påstod Tom Kabinet, at videresalget var omfattet af spredningsretten efter infosoc-direktivets artikel 4. Af reglen følger en konsumptionsregel, hvorefter erhververe af lovlige eksemplarer frit kan videresælge værket uden tilladelse fra rettighedshaver.

EU-Domstolen tog stilling til det præjudicielle spørgsmål om videresalg af e-bøger var omfattet af spredningsretten efter infosoc-direktivets artikel 4, hvorefter videresalg kunne ske uden tilladelse fra rettighedshaver, eller om et sådan videresalg ville udgøre en »overførsel til almenheden« efter direktivets artikel 3, som ville kræve rettighedshavers tilladelse.

EU-Domstolen fastslog først ud fra en fortolkning af formålet med infosoc-direktivet, at begrebet »spredning til almenheden«, som anvendt i infosoc-direktivet, alene skal omfatte værker, som indgår i et fysisk medium. Således kunne digitale værker såsom e-bøger ikke omfattes af begrebet.

Herefter fastslog EU-Domstolen, at videresalg af e-bøger udgjorde en »overføring til almenheden«, i henhold til infosoc-direktivets artikel 3, stk.1. Dermed blev retten til

videresalg af e-bøger ikke konsumeret, når rettighedshaveren gør et eksempel af værket tilgængeligt på en onlinetjeneste.

Derefter konkluderede EU-Domstolen samlet, at videresalg af e-bøger krævede rettighedshavers samtykke. Fraværet af et digitalt konsumptionsprincip blev af EU-Domstolen begrundet med, at digitale værkers form ville medføre, at brugtmarkedet for digitale værker kunne undergrave rettighedshavernes mulighed for at opnå indtægter fra deres værker.

Dommen fjerner den usikkerhed om hvorvidt der efter Useds-oft-dommen, sag C-128/11, hvor EU-Domstolen fandt, at ophavsmanden til software ikke kunne modsætte sig videresalg af brugte softwarelicenser, måtte gælde et tværgående konsumptionsprincip, som kunne udstrækkes udover Europa-Parlamentets og Rådets direktiv 2009/24/EF af 23. april 2009 (»software-direktivet«) til også at rumme videresalg af andre digitale værker end software, herunder e-bøger.

Den nærværende dom fastslår, at der ikke gælder et sådant tværgående konsumptionsprincip, da e-bøger ikke kan videreoverdrages uden samtykke fra rettighedshaver. Antageligvis vil dommen have tilsvarende betydning for andre digitale værker, såsom musik og film, således at der ej heller vil gælde et digitalt konsumptionsprincip for disse, hvorfor videreoverdragelse af disse også vil kræve rettighedshavers samtykke.

Læs hele dommen her:
<http://curia.europa.eu/juris/document/document.jsf?text=&docid=217552&pageIndex=0&doclang=da&mode=req&dir=&occ=first&part=1&cid=8867960>

12. 66 stole benyttet på restaurant udgjorde en efterligning af Wegners 'The Chair'

Den danske Sø- og Handelsret (»Sø- og Handelsretten«) afsagde d. 10 januar 2020 dom i sagen BS-46 669/2018-SHR mellem PP Møbler ApS (»PP«) og Bryggeriet Skive ApS (»BS«). Sagen angik, hvorvidt BS ved eksemplarspredning, herunder salg og offentlig visning af en række stole krænkede PP's rettigheder efter lovbekendtgørelse nr. 1144 af 23. oktober 2014 (»den danske ophavsretslov«) og lov nr. 426 af 3. maj 2017 (»den danske markedsføringslov«) til stolen PP503 (også kaldet »The Chair«) af Hans J. Wegner.

Det var i sagen ubestridt, at Hans J. Wegners stol The Chair er ophavsretligt beskyttet som brugskunst efter den danske ophavsretslovs § 1.

Knud Bjerre (»KB«) var medejer af BS, og købte i marts 2019 75 stole i Tyrkiet fra møbelfirmaet Sette. 66 af dem blev transporteret til Skive i Danmark til brug som inventar i restaurant BS. I juni 2018 blev PP opmærksom på, at BS benyttede de omhandlede stole. Det var PP's opfattelse, at stolene krænkede PP's rettigheder til The Chair.

PP rettede henvendelse til BS, og anmodede dem bl.a. om at fjerne stolene fra restauranten. Stolene forblev dog i restauranten.

Retten fandt, at Bryggeriets stol, efter en helhedsvurdering, i sit designudtryk, lå så tæt på »The Chair«, at der var tale om en meget nærgående efterligning, på trods af visse forskelle i mål, kvalitet og bredde på armlæn.

På baggrund af ovenstående, fandt retten at der var sket en krænkelse af ophavsretten til The Chair, jf. den danske ophavsretslovs § 2, som måtte tilregnes KB som uagt-som, idet han ikke forud for købet af det store antal stole foretog nogen form for undersøgelser af, om stolene kunne krænke andres rettigheder. På det tidspunkt, hvor han

overdrog stolene til BS, var han, efter bevisførelsen, ifølge PP, fuldt bekendt med, at stolene krænkede ophavsretten til »The Chair«, og den ved overdragelsen skete krænkelse måtte derfor tilregnes ham som forsættlig.

Retten fandt endvidere, at BS ved at have benyttet stolene i restauranten i Skive og vise dem på restaurantens hjemmeside og på Facebook, krænkede PP's eneret til at gøre The Chair tilgængelig for almenheden, jf. den danske ophavsretslovs § 2. Retten fandt, at denne adfærd også udgjorde en overtrædelse af den danske markedsføringslovs § 3.

Retten bestemte, at det store antal krænkende stole i restauranten medførte en vis markedsforstyrrelse for PP, idet stolenes ringere håndværksmæssige kvalitet kunne skade The Chairs anseelse og dermed de fremtidige afsætningsmuligheder. BS og KB skulle derfor betale PP erstatnings for markedsforstyrrelse, jf. den danske ophavsretslovs § 83 og den danske markedsføringslovs § 24.

Retten fandt yderligere, at BS' fortsatte brug af stolene i restauranten, også efter henvendelse fra PP om at stolene blev fjernet fra restauranten, udgjorde forsættelige ophavsretskrænkelser, og at BS og KB

derfor pådrog sig bødeansvar, jf. den danske ophavsretslovs § 76, stk. 2, for BS vedkommende jf. den danske ophavsretslovs § 80.

Læs hele dommen her:

[http://domstol.fe1.tangora.com/media/-300011/files/Dom_\(sambehandling\)_BS-46669-2018-SHR_og_BS-24.pdf?rev1](http://domstol.fe1.tangora.com/media/-300011/files/Dom_(sambehandling)_BS-46669-2018-SHR_og_BS-24.pdf?rev1)

Tue Goldschmieding er partner i Gorrisen Federspiel og en af de danske redaktorerne for Lov&Data.



Bird & Bird

Karin Söderberg och Kajsa Zenk

Skapare av "Mordpodden" fälls för upphovsrättsintrång

Inledning

Flera poddar har under de senaste åren anklagats för plagiat. Patent- och marknadsdomstolen har nyligen funnit att delar av ett avsnitt av den populära Mordpodden gjorde intrång i upphovsrätten till boken Kakelugns-mordet. Den som varit huvudansvarig för avsnittet dömdes till böter för brott mot upphovsrättslagen. Målet aktualiserar vissa principiella frågor om bevisföringen i mål om upphovsrättsintrång (Patent- och marknadsdomstolens dom den 29 januari 2020, mål B 7619-19).

Bakgrund

De två personerna bakom Mordpodden, en podd som i varje avsnitt beskriver olika verkliga mordhistorier, åtalades för brott mot upphovsrättslagen efter att författaren till boken Kakelugns-mordet anmält podden för plagiat. Skaparna av Mordpodden menade att podden utgjorde ett nytt och självständigt verk i fri anslutning till Kakelugns-mordet och att författaren till boken hade namngivits i den omfattning och på det sätt som god sed kräver. Frågan som domstolen hade att ta ställning till var således om poddav-

snittet innebar ett intrång i upphovsrätten till boken.

Rättsliga utgångspunkter

Den som skapat ett litterärt eller konstnärligt verk har upphovsrätt till verket enligt 1 § 1 st. upphovsrättslagen. En grundförutsättning för upphovsrättsligt skydd är att verket har så kallad verkshöjd, det vill säga att verket är självständigt och originellt. I upphovsrättslagens 2 § anges, med vissa undantag, upphovsmannens uteslutande rätt att förfoga över verket genom exemplarframställning och genom att

göra det tillgängligt för allmänheten. Framställning av exemplar innefattar enligt upphovsrättslagen 2 § 2 st. varje direkt eller indirekt samt tillfällig eller permanent framställning av ett exemplar av verket oavsett i vilken form eller med vilken metod det sker och oavsett om det sker helt eller delvis. Enligt 2 § 3 st. görs ett verk tillgängligt för allmänheten när verket överförs till allmänheten på trådbunden eller trådlös väg från en annan plats än där allmänheten kan ta del av verket.

I 3 § upphovsrättslagen fastställs att upphovsmannen ska anges i den omfattning och på sådant sätt som god sed kräver då ett exemplar av ett verk framställs eller görs tillgängligt för allmänheten.

Den som bearbetat ett verk eller överfört verket till ett annat medium tillerkänns enligt upphovsrättslagens 4 § st. 1 upphovsrätt till verket i den nya gestaltningen, men har inte rätt att förfoga över det bearbetade verket i strid med upphovsrätten till originalverket. Upphovsrätten till ett bearbetat verk blir dock inte beroende av originalverket enligt upphovsrättslagen 4 § 2 st. om någon i fri anslutning till ett verk har åstadkommit ett nytt och självständigt verk.

Patent- och marknadsdomstolens avgörande

Patent- och marknadsdomstolen börjar med att utreda om boken *Kakelugns mordet* har upphovsrättsligt skydd. Domstolen påpekar att kravet på verkshöjd inte ställs särskilt högt i förhållande till litterära verk. Utredningen i målet ger enligt domstolen tydligt stöd för att *Kakelugns mordet*, även om boken bygger på verkliga händelser, är så originellt och självständigt att den anses ha upphovsrättsligt skydd.

Därefter går domstolen vidare till frågan om intrång har skett i författarens upphovsrätt till boken. Domstolen påpekar att även en poddsändring innebär en exemplarframställning och att publi-

cering av en podd på en digital plattform tillgänglig för allmänheten utgör överföring till allmänheten. De åtalade har bekräftat att de framställt exemplar av poddavsnittet och även att det tillgängliggjorts för allmänheten, vilket enligt domstolen också understöds av utredningen i målet. Domstolen gör dock bedömningen att det inte finns tillräckligt med underlag i målet för att dra slutsatsen att poddavsnittet gjort intrång i hela boken. Varken hela boken eller hela poddavsnittet har åberopades som bevisning. De generella likheter som framkommit genom målsägandens uppgifter är allmänt hållna och det har även framkommit att stora delar av bokens innehåll inte berördes i poddavsnittet. Domstolen påpekar också att det dessutom får anses naturligt att en bok och ett poddavsnitt som beskriver samma verkliga händelse har vissa likheter.

För att en exemplarframställning och tillgängliggörande för allmänheten av delar av ett verk ska utgöra upphovsrättsintrång krävs att delarna i sig själva anses ha verkshöjd. Domstolen gör bedömningen att även de enskilda delarna av verket är resultatet av ett originellt och självständigt skapande. Även delarna uppfyller därmed kravet på verkshöjd och har således upphovsrättsligt skydd. Vidare påpekar domstolen att delarnas skyddsomfång inte ska anses vara alltför snävt utan omfatta mer än bara rena avskrifter.

Domstolen fortsätter med att framhålla att upphovsrätten inte skyddar fakta och idéer och att vissa av de exempel på likheter som lagts fram innehåller sådana faktauppgifter. Domstolen finner dock vid en jämförelse mellan längre sammanhängande avsnitt att det tydligt framgår att poddavsnittet, i de delar som bygger på boken, på ett mycket närgånget sätt följer bokens struktur. Enligt domstolen använder poddavsnittet samma eller snarlika ord och uttryck som boken och

återanvänder bokens berättartekniska grepp. Likhetsjämförelsen mellan delarna av poddavsnittet och boken medför enligt domstolen att poddavsnittet inte är ett nytt och självständigt verk. Eftersom författaren inte samtyckt till användningen av boken har poddsändringen inneburit ett intrång i författarens upphovsrätt.

Angående författarens rätt till namngivelse påpekar domstolen att denna rätt inte påverkas av att poddsändringen inneburit ett intrång i författarens upphovsrätt. Då en ljuduppspelning av poddsändringen inte getts in som bevisning utgår domstolen från att namngivelsen gjorts i omedelbar anslutning till att berättelsen avslutats och varit hörbar och tydlig, även om författaren gjort gällande att musik spelades före namngivelsen och att denna gjordes "i förbifarten". Det finns vidare ingen utredning i målet till stöd för vad som är god sed vid namngivelse i poddsändringar. På grund av detta konstaterar domstolen att det inte finns stöd för att namngivelsen borde ha skett på något annat sätt än som gjorts.

Domstolen går sedan vidare och bedömer ansvaret för intrånget. Det krävs antingen uppsåt eller grov oaktsamhet för att de två som driver podden ska dömas till ansvar. Eftersom de båda är journalister anför domstolen att det bör ställas relativt höga krav på att de känner till och respekterar det upphovsrättsliga regelverket. Domstolen gör bedömningen att intrånget inte skett med uppsåt då den inte finner någon anledning att ifrågasätta ambitionen att framställa ett eget självständigt verk och det i övrigt saknas omständigheter i målet som ger stöd för ett uppsåtligt intrång. Däremot borde den av personerna som haft det huvudsakliga ansvaret för poddavsnittet, på grund av de återanvända skönlitterära beskrivningarna och berättartekniska greppen samt de identiska eller snarlika orden och uttrycken, ha förstått att

poddavsnittet riskerade att göra intrång i författarens upphovsrätt. Domstolen anser således att hon har agerat grovt oaktsamt och dömer ut böter. Åtalet mot den andra personen som driver podden ogillas eftersom domstolen finner att hon inte haft någon särskild anledning att misstänka att avsnittet skulle göra intrång i boken.

Reflektioner

Domen berör ett intressant upphovsrättsligt område och domskälen tangerar bedömningar kring upphovsrättsintrång i ett verks innersta kärna. Den återopade bevisningen, eller snarare avsaknaden av återopad bevisning, medför dock att uttalanden kring dessa frågor från domstolens sida blir tämligen begränsade. Hade poddavsnittet och boken återopats som bevisning i sin helhet skulle domstolen möjligen kunnat göra mer utförliga och intressanta resonemang kring dessa aspekter i domskälen.

Både åklagaren och de åtalade hänvisar till god sed vad gäller namngivelse av författaren till boken i podden. Dessvärre är ytterligare en följd av bevisföringen i målet att domstolen missar chansen att förtydliga vad som utgör god sed i den bemärkelsen. Eftersom poddar är ett relativt nytt verktyg för att förmedla information och framställa upphovsrättsligt skyddade verk kan det ifrågasättas om någon god sed på området har hunnit etableras. Det faktum att namngivelser i poddar generellt sker på ett visst sätt, eller att det finns en eta-

blerad branschpraxis, innebär inte nödvändigtvis att förfarandet ska anses vara förenligt med god sed. En prövning av vad som faktiskt ska anses vara god sed vid namngivelser i poddsändningar skulle således vara välkommen.

De delar av boken som återopas som bevisning i målet är i stor utsträckning en redogörelse för verkliga händelser. Det torde således ligga nära till hands att en beskrivning av händelserna, oavsett om det sker i en bok eller i en poddsändning, har vissa likheter. Betydelsen av att innehållet utgör redogörelser av verkliga händelser presenteras dock inte helt tydligt av domstolen. Domstolen påpekar förvisso, utan att närmare motivera detta, att utdragen ur boken ska anses ha ett skyddsomfång som sträcker sig längre än rena avskrifter. Vidare uttalar domstolen att utdragen trots att de bygger på verkliga händelser anses ha upphovsrättsligt skydd. Dessa uttalanden ger intryck av att böcker kan antas ha ett inte helt försumbart upphovsrättsligt skydd även om de bygger på verkliga händelser. Domstolens slutsats att poddsändningen gör intrång i boken när poddsändningen beskriver samma verkliga händelse som boken, men inte utgör en ren uppläsning av boken, får anses förstärka detta antagande. Denna slutsats ter sig intressant, särskilt eftersom idéer och fakta inte skyddas av upphovsrätten, utan endast verk som har en viss konkret utformning.

Som nämnts i inledningen till den här artikeln har flera poddar

anlagats för plagiat de senaste åren. Kanske kan Mordpodden-målet få den följd att flera poddskapare vidtar försiktighet då de hämtar inspiration från andra verk till innehållet i sina poddar. Särskilt då målet visar exempel på att straff kan utdömas för personerna bakom podden vid plagiering. Då det gäller utdömande av straff kan dock domstolens uttalande att det faktum att personerna bakom Mordpodden är journalister medför att höga krav kan ställas på att de känner till och respekterar det upphovsrättsliga regelverket noteras. Uttalandet kan motsatsvis tolkas så att poddskapare som inte är journalister, eller av någon annan anledning har särskild anledning att känna till upphovsrättsreglerna, har lägre krav på sig att känna till var gränserna för intrång i andras upphovsrättigheter går. Att bevisa uppsåt, eller grov oaktsamhet, kan kanske bli svårare då det gäller poddskapare som saknar sådan relevant utbildning eller tidigare erfarenhet från branschen.

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

Kajsa Zenk är Associate och arbetar i Bird & Birds IP-grupp, brett med olika immaterialrättsliga frågor. Hon tog examen vid Uppsala universitet 2018 och är IP-gruppens sannaste tillskott.



simonsen vogtviig

Rune Ljostad og
Hedda Baumann Heier

Dom om rett til oppfinnelse og bruk av vitenskapelige artikler i patentsøknad

Borgarting lagmannsrett avsa den 17. desember 2019 dom i en sak mellom en tidligere stipendiat ved Universitetet i Oslo (UiO) og Staten v/UiO. Saken har saksnummer LB-2018-77 812 og ble omtalt i *Nytt i immaterialretten*-spalten i forrige nummer av Lov&Data (nr. 141 1/2020).

Høyesterett besluttet 3. april 2020 at anken over lagmannsrettens dom tillates delvis fremmet. Anken tillates fremmet hva gjelder kravet om godtgjøring etter arbeidstakeroppfinnelsesloven § 7. Forhandlingene begrenses slik at det foreløpig ikke forhandles andre spørsmål enn om hvorvidt UiO (som arbeidsgiver) ervervet retten til oppfinnelsen på «annet grunnlag», jf. arbeidstakeroppfinnelsesloven § 7.

Saken har saksnummer 20-030 257SIV-HRET i Høyesterett. Det er i skrivende stund ikke kjent når saken skal opp til behandling.

Ny lov om vern av forretningshemmeligheter er sanksjonert av Kongen i statsråd

Lov om vern av forretningshemmeligheter ble sanksjonert av Kongen i statsråd den 27. mars 2020. Lovforslaget er tidligere omtalt i Lov&Data nr. 141 1/2020. Det er i skrivende stund uavklart når loven trer i kraft.

Les lovteksten i Lovdatas database. Loven har referanse LOV-2020-03-27-15.

Ny proposisjon om endringer i varemerkeloven og tolloven mv.

Regjeringen har den 14. februar 2020 fremlagt forslag til endringer i varemerkeloven og tolloven mv. i Prop. 43 LS (2019-2020). Lovforslaget gjennomfører det nye varemerkedirektivet, direktiv (EU) 2015/2436, hvilket erstatter direktiv 2008/95/EF. For å bringe norsk rett på linje med direktivets regelverk foreslås visse endringer i varemerkeloven, foretaksnavneloven, designloven, patentloven og panteloven. Det foreslås også endringer i tolloven og tvisteloven for å styrke tollmyndighetenes kontroll med varer som gjør inngrep i immaterialrettigheter. Nedenfor omtales kort noen av forslagene som fremsettes i proposisjonen, men redegjørelsen er på ingen måte uttømmende.

For å samsvare med EU-direktivet inneholder proposisjonen blant annet et forslag om at kravet til grafisk gjengivelse i varemerkelovens § 14 erstattes med et krav om at varemerket må kunne gjengis på en «klar og tydelig» måte. Departementet presiserer at dette vil åpne for muligheten å søke om registrering av et varemerke som består av en digital video- eller lydfil.

Departementet foreslår å innføre egne registreringshinder for de tilfeller der et varemerke søkes registrert i såkalt ond tro, og for de tilfellene der en agent eller representant søker å registrere et varemerke uten samtykke fra merkehaveren.

Det foreslås også enkelte klargjøringer og endringer i varemerkelovens bestemmelser om enerettens innhold og begrensninger, blant annet når det gjelder forholdet mel-

lom varemerker og foretaksnavn og bruk av varemerker i sammenliknende reklame.

De foreslåtte endringene i tolloven innebærer at adgangen til tilbakehold av varer utover 10 dager, som tidligere var forbeholdt domstolene, også gis tollmyndighetene. I tillegg innføres det et forenklet system for ødeleggelse av varer, og det legges også opp til at tollmyndighetene skal kunne holde tilbake varer der bare avsenderen opptrer i næringsvirksomhet.

Videre foreslås det endringer i panteloven som innebærer en adgang til å pantsette særskilte registrerte varemerker uavhengig av merkehavers virksomhet. Reglene som foreslås innført likner reglene om særskilt pantsettelse av patenter og planteforedlerrettigheter som ble inntatt i panteloven allerede i 2015.

Samtidig med forslag til lovendringer bes det om Stortingets tillatelse til at Norge tiltrer Singaporetraktaten om varemerkerett. Norsk rett oppfyller i stor grad kravene til traktaten, men det kreves likevel enkelte endringer i varemerkeloven for at norsk rett skal samsvare med reglene i traktaten. Proposisjonen inneholder også et forslag om godkjenning av EØS-komiteens beslutning om innlemmelse av direktiv (EU) 2015/2436 i EØS-avtalen.

Proposisjonen er i skrivende stund til behandling hos Næringskomiteen på Stortinget. Fristen for Næringskomiteens avgivelse av innstilling er 12. mai 2020.

Les lovforslaget Prop. 43 LS (2019-2020) her: <https://www.regjeringen.no/no/dokumenter/prop.43-ls-2019-2020/id2690400/>

Følg saksgangen på Stortinget her: <https://www.stortinget.no/no/Saker-og-publikasjoner/Saker/Sak/?p=78832>

Rune Ljostad er partner i Advokatfirmaet Simonsen Vogt Wiig AS, Oslo.

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



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 hel-dig regulering? Covid-19-pandemien og de medfølgende restriksjonene offentlige myndigheter har innført av smittevern hensyn 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 artikkelforfatterens 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



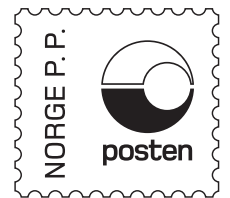
dekker de situasjoner en force majeure-klausul typisk sett er ment å ivareta. Det kan selvfølgelig innvendes at en del IT-leveranser er av en slik karakter at det nettopp er meningen at ytelsen skal leveres 24/7/365, uansett. Det er vi ikke uenige i. Det er imidlertid ikke det samme som at en leverandør skal dekke hele regningen når ekstraor-

dinære 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.



Returadresse:
Lovdata
Postboks 2016 Vik
NO-0125 Oslo
Norge

Nytt fra

LD LOVDATA

Sammen med Lovdatas hjelpetekster finner du korte filmer som viser hvordan du bruker noen av de viktigste funksjonene i Lovdata Pro.

Du finner alle Lovdatas hjelpefilmer på
<https://lovdata.helpscoutdocs.com>

