Lov & Data

Nr. 141
Mars 2020

Nr. 1/2020

Innhold








Lov&Data

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

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

Ansvarlig redaktør er Jarle Roar Sæbø, juridisk direktør i HPE, Oslo og leder for Domeneklagenemnda.
Medredaktører er Sandra Stenersen Henden og Ida Marie Vangen, 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/*

MILJØMERKET TRYKKERI 01 MEDIA – 2041 0379
TRYKT I NORGE NO-145
Miljøfyrtårn®

Leder

GDPR – Betydningen af bestemmelsen om begunstiget tredjepart i det danske datatilsyns nye standardkontraktsbestemmelser og Datatilsynets holdning til databehandleraftaler baseret på tilsynets tidligere skabelon til en databehandleraftale

Den 10. december 2019 offentliggjorde det danske datatilsyn ('Datatilsynet'), at Datatilsynet har vedtaget standardkontraktsbestemmelser i overensstemmelse med databeskyttelsesforordningen (GDPR) artikel 28, stk. 8. Standardkontraktbestemmelserne udgør en databehandleraftale, som kan anvendes mellem en dataansvarlig og en databehandler og derved sikre overholdelse af GDPR artikel 28, stk. 3. Standardkontraktbestemmelserne findes på både dansk og engelsk. Før Datatilsynets vedtagelse, har standardkontraktbestemmelserne være forelagt Det Europæiske Databeskyttelsesråd (EDPB), hvorefter Datatilsynet reviderede standardkontraktbestemmelserne og endeligt vedtog disse.

Klausul om begunstiget tredjepart

De nye standardkontraktbestemmelser indeholder blandt andet en klausul, der går videre end de krav, der følger af GDPR artikel 28, stk. 3. Bestemmelsen findes i standardkontraktens punkt 6.2, og fastslår, at den dataansvarlige skal sikre, at dennes databehandler i sine aftaler med underdatabehandlere, indføjer den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således, at den dataansvarlige kan indtræde i databehandlerens rettigheder over for underdatabehandlerne.

I sin gennemgang af Datatilsynets standardkontraktbestemmelser påpegede EDPB, at et krav om, at den dataansvarlige skal indføjes som begunstiget tredjemand ved databehandlerens konkurs, ikke følger af GDPR artikel 28. EDPB fremhævede dog, at de godt kunne se værdien i klausulen, da den blandt andet var med til at opretholde den dataansvarliges rettigheder og ansvar. EDPB påpegede dog, at Datatilsynet burde tydeliggøre formålet med

bestemmelsen, således at det tydeligt fremgår, at underdatabehandleren påtager sig et ansvar direkte over for den dataansvarlige ved databehandlerens konkurs.

Kravet om bestemmelse i aftaler mellem databehandleren og dennes underdatabehandlere om, at den dataansvarlige er en begunstiget tredjemand, medfører dog en række spørgsmål i forbindelse med brugen af Datatilsynets standardkontraktbestemmelser. Først og fremmest må man se på de ofte forekommende tilfælde, hvor store internationale selskaber, såsom Amazon, Google og Microsoft, er underdatabehandlere. Her er det vigtigt at have i mente, at bestemmelsen om, at den dataansvarlige skal indføjes som begunstiget tredjemand ikke er et krav i henhold til GDPR. Det er derfor tvivlsomt, om en databehandler, uagtet, at databehandleren over for den dataansvarlige *gerne* vil indføje klausulen, har mulighed for at forhandle klausulen på plads med sine underdatabehandlere, særligt hvor der er tale om store modparter, der leverer standardiserede ydelser på vilkår, der sjældent kan forhandles.

Ydermere kan der stilles spørgsmålstegn ved, hvordan Datatilsynet vil vurdere databehandleraftaler baseret på standardkontraktbestemmelserne, hvor denne bestemmelse om begunstiget tredjemand ikke er medtaget. Datatilsynet anfører selv i forbindelse med vedtagelsen af standardkontraktbestemmelserne, at Datatilsynet i forbindelse med tilsynsbesøg ikke vil efterprøve indhold af databehandleraftaler, der baseres på standardkontraktbestemmelserne.

EDPB har anført i deres udtalelse til Datatilsynets standardkontraktbestemmelser, at modificerede standardkontraktbestemmelser ikke kan betegnes som en standardkontrakt godkendt af en national tilsynsmyndighed, da den godkendte standardkontrakt skal ses »*as is*«.

Det er således uklart, hvordan Datatilsynet vil fortolke en databehandleraftale, der ikke indeholder den pågældende klausul. Det må i hvert fald stå klart, at Datatilsynet har mulighed for at efterprøve forholdet ved et evt. tilsyn. Idet klausulen ikke ker et rav i henhold til GDPR, må det dog antages, at Datatilsynet ikke vil udtale kritik eller underkende en databehandleraftale, der ikke indeholder klausulen, såfremt parterne ikke i øvrigt har foretaget ændringer til databehandleraftalen, som strider mod GDPR artikel 28. Dog mister virksomheder, der fjerner bestemmelsen, den beskyttelse, der ligger i at bruge standardkontraktbestemmelser.

Datatilsynets holdning til databehandleraftaler baseret på tilsynets tidligere skabelon

Datatilsynet udfærdigerede i efteråret 2017 en skabelon til en databehandleraftale, som var tilgængelig på tilsynets hjemmeside. I forbindelse med bemærkninger fra EDPB til standardkontraktbestemmelserne, som disse blev forelagt EDBP, stod det klar, at denne skabelon ikke til fulde opfyldte kravene til en databehandleraftale under GDPR artikel 28.

Datatilsynet har i forbindelse med vedtagelsen af standardkontraktbestemmelserne anført, at denne skabelon kun var udtrykt for Datatilsynets forståelse af mindstekravene i GDPR artikel 28 på daværende tidspunkt, og derfor ikke længere er tilsvarende gældende. Datatilsynet har ligeledes udtalt, at de har besluttet *»i vidt omfang og som et udgangspunkt fortsat at acceptere aftaler, der er baseret på tilsynets oprindelige skabelon, og som er indgået inden dags dato (red. 10 december 2019)«.*

Uagtet, at udmeldingen højst sandsynligt er ment som beroligende i forhold til alle de virksomheder, der har indgået en databehandleraftale på baggrund af den gamle skabelon, er det som anført af Datatilsynet kun et *udgangspunkt* der kun følges *i vidt omfang*. Det vil derfor ikke kunne udelukkes, at Datatilsynet underkender en databehandleraftale, selvom den er indgået på baggrund af Datatilsynets gamle skabelon.

Som virksomhed bør man under alle omstændigheder vurdere, om indholdet af virksomhedens nuværende databehandleraftaler er baseret på den gamle skabelon, og få et overblik over, hvor man bør foretage ændringer for at sikre overholdelse af GDPR artikel 28.

I forhold til, hvornår ændringerne bør foretages, må det antages, at i det omfang kontrakter, hvorunder databehandleraftalen er baseret på Datatilsynets gamle skabelon, enten genforhandles, eller hvor der indgås nye kontrakter, bør parterne sørge for at få opdateret databehandleraftalen. Yderligere bør virksomheder vurdere, om databehandleraftaler i kontrakter, hvorunder, der sker behandling af personoplysninger, som udgør en høj risiko, allerede nu bør genforhandles, således at aftalerne opfylder GDPR.

Endeligt, i lyset af EDPBs generelle udtalelse om, at databehandleraftaler, der blot gengiver kravene i GDPR artikel 28, stk. 3, ikke lever op til GDPR, må parter, der blot har henvist eller gengivet kravene i GDPR artikel 28, stk. 3, som minimum få dokumenteret, hvordan kravene opfyldes, eller opdatere nuværende databehandleraftaler med specificering af, hvordan kravene i GDPR artikel 28 sigtes opfyldt.

Tue Goldschmieding, Gorrissen Federspiel

Strängare krav på reklammarkering vid influencer marketing i sociala medier

Av Sara Hovstadius

I ett nytt avgörande från Patent- och marknadsöverdomstolen (”**PMÖD**”) den 5 december 2019 fastställde PMÖD strängare krav på reklammarkering vid användande av influencer markering i sociala medier.

Bakgrund

I maj 2016 stämde Konsumentombudsmannen (KO) Alexandra Media Sweden AB (”**Alexandra Media**”) och Tourn Media AB (”**Tourn Media**”) för överträdelser av marknadsföringslagens (2008:486) (”**MFL**”) krav på reklamidentifiering och sändarangivelse. Stämningen avsåg totalt två stycken av Alexandra Media publicerade blogginlägg och ett Instagraminlägg, samtliga innehållandes marknadsföring för en tjänst förmedlad av bolaget Mobilåtervinning i Sverige AB (”**Mobilåtervinning**”).

KO valde att föra talan mot bolagen Alexandra Media som via ägaren och infleuncern Alexandra Nilsson utformat och publicerat inläggen på sin blogg respektive Instagramkonto, samt Tourn Media som i egenskap av influencer nätverk hade förmedlat reklamuppdraget och agerat webbhotell för Alexandra Medias blogg. KO menade att bolaget Mobilåtervinning var huvudansvarig för marknadsföringen och att Alexandra Media och Tourn Media väsentligen bidragit till marknadsföringen enligt 23 § 2 st 3 p MFL och därför också kunde hållas ansvariga för den otillbörliga marknadsföringen. Syftet med stämningen var att genom ett domstolsavgörande få tydligare praxis och implementering avseende reklam-

Sara Hovstadius

markering i sociala medier och KO valde därför att endast stämma Alexandra Media och Tourn Media.

I dom meddelad av Patent- och marknadsdomstolen (”**PMD**”) den 31 januari 2018 gick PMD på KO:s linje i förhållande till det första blogginlägget samt Instragraminlägget. Inläggen som PDM valde att fälla hade reklammarkerats med texten ”I samarbete med” respektive ”#samarbete”. Enligt PDM hade dock inte reklammakeringen givits en tillräckligt framträdande roll. Vidare anförde PDM att inläggen inte hade utformats på sådant sätt att inläggen genom färg, form eller på annat sätt skiljde sig från övrigt innehåll i Alexandra Medias inlägg. Till följd av detta ansåg PDM att inläggen inte uppfyllde MFL:s krav på reklamidentifiering och sändarangivelse och förbjöd Alexandra Media, vid vite om 100 000 kr, att vid marknadsföring på blogg och Instagram medverka till att utforma framställning på sådant sätt att framställningen inte tydligt kan identifieras som marknadsföring och inte visar vem som svarar för marknadsföringen. Det blogginlägg som PDM däremot valde att fria hade reklammarkerats med ”sponsored post” och markeringen hade enligt PDM en framträdande placering bland annat tack vare en svagt rosa list runt blogginlägget som tydligt skiljt marknadsföringen från övrigt innehåll på bloggen. PDM friade Tourn Media från ansvar då PDM ansåg att Tourn Media visserligen genom sitt agerande i viss utsträckning bidragit till den otillbörliga marknadsföringen, bland annat genom lämnande av förslag till Alexandra Media på hur inläggen skulle utformas, men inte haft något bestämmande inflytande över den slutliga utformningen eller publiceringen av inläggen och därför inte kunde hållas ansvarig.

KO valde att överklaga domen till överinstansen Patent- och marknadsöverdomstolen (”**PMÖD**”) som meddelade prövningstillstånd. PMÖD fastställde i dom den 5 december 2019 PMD:s dom i förhållande till de av PDM fällda inläggen, men valde att även fälla det av PDM friade blogginlägget. Även PMÖD friade Tourn Media från medverkansansvar. PMÖD:s dom är inte möjlig att överklaga och är således prejudikatbildande.

Domstolens bedömning avseende brist i reklamidentifiering (9 § 1 st MFL)

PMÖD inledde med att konstatera att det var utrett i målet att det på

Alexandra Medias blogg och Instagram varvas betalda inlägg med icke kommersiella och redaktionella inlägg. Enligt PMÖD måste det därför ställas höga krav på marknadsföringens utformning för att genomsnittskonsumenten ska kunna skilja på kommersiella och redaktionella inlägg och kunna förstå när ett inlägg innehåller reklam. Avseende bestämning av genomsnittskonsumenten ansåg PMÖD att PMD hade gjort en för snäv bedömning. Med hänvisning till statistik från Google Analytics som Alexandra Media och Tourn Media hade åberopat kom PMD fram till att genomsnittskonsumenten i målet skulle bestämmas till en kvinna i åldern 18–34 år som är en van användare av sociala medier och återkommande läsare av Alexandra Medias blogg och Instagramkonto. För att inte undergräva en hög konsumentskyddsnivå bestämde dock PMÖD istället att genomsnittskonsumenten ska bestämmas till en ung kvinna i Sverige som generellt sett inte har samma erfarenhet som en äldre person, men som tack vare sin erfarenhet av att använda olika sorters sociala medier har en vana att ta till sig information från dessa kanaler och därför får antas ha en medvetenhet om att många influencers verksamhet på sociala medier åtminstone i viss mån är kommersiell. Av utredningen i målet ansåg vidare PMÖD det vara klarlagt att genomsnittskonsumenten ofta tar del av inlägg på sociala medier på ett ganska selektivt sätt och scrollar sig igenom text och bilder för att stanna till vid det som väcker intresse. Även detta selektiva sätt på vilket genomsnittskonsumenten tar till sig innehåll på sociala medier talar enligt PMÖD för att kraven på reklammarkering måste ställas högt. Detta anser PMÖD är särskilt viktigt i en digital miljö eftersom det finns möjlighet för en konsument att enkelt och snabbt fatta olika former av affärsbeslut genom att till exempel via en länk ta sig till en näringsidkares webbplats och genomföra ett köp.

PMÖD gick sedan vidare till att pröva om vart och ett av de aktuella inläggen uppfyller de högt ställda kraven på reklammarkering eller inte. I prövningen gjorde PMÖD en strängare bedömning än PMD och fällde samtliga blogg- och Instagraminlägg. PMÖD ansåg inte att utformningen av varken det första eller andra blogginlägge på något nämnvärt sätt skiljer sig från övriga redaktionella inlägg då inläggen var utformade med samma layout på rubrik och text som Alexandra Medias redaktionella inlägg. Den textuella reklammarkering som hade gjorts på det första blogginlägget i form av texten ”Inlägget är i samarbete med” ansåg PMÖD visserligen kunna sägas utgöras en reklammarkering, men ansågs innehålla flertalet brister och till följd därav inte ansågs tillräckligt tydlig. Bristerna som PMÖD identifierat var att det inte angavs med vem samarbetet var utfört samt var otydligt i fråga om det var ett betalt samarbete eller inte. Vidare hade reklammarkeringen placerats längst ner i inlägget och med liten teckenstorlek, vilket sammantaget enligt PMÖD innebär att inlägget inte var utformat på ett sådant sätt att det för genomsnittskonsumenten redan efter en flyktig kontakt framgår att inlägget är marknadsföring.

Avseende valet av den textuella utformningen av reklammarkeringen hade Alexandra Media och Tourn Media åberopat en marknadsundersökning där det framkom att majoriteten av respondenterna ansåg att markeringen ”I samarbete med” var en tydlig eller mycket tydlig reklammarkering. PMÖD ansåg dock att undersökningen hade ett begränsat värde. Detta eftersom undersökningen medför att konsumenten blir mer uppmärksam på frågor om betalning och reklam än i ett verkligt sammanhang och att det vidare måste antas att konsumenterna som deltog i undersökningen utgick från att det skulle framgå med vilket företag som samarbetet var. Av samma anledning underkände PMÖD, till skillnad från PMD, även reklammarkeringen ”sponsored post”. Den rosa listen runt blogginlägget som PDM ansåg avskilde det aktuella blogginlägget från övrigt innehöll fäste vidare inte PMÖD samma avseende vid. PMÖD ansåg istället att valet av en ljusrosa list inte gör att genomsnittskonsumentens uppmärksamhet styrs till reklammarkeringen utan till andra mer framträdande delar i inlägget. PMÖD fäste även bland annat avseende vid att reklammarkeringen inte hade placerats i början av inlägget och dessutom i en väsentligt mindre teckenstorlek än huvudrubriken.

Det i målet aktuella Instagraminlägget hade Alexandra Media reklammarkerat genom att avsluta inlägget med markeringen ”#samarbete”. Även denna reklammarkering underkände PMÖD med hänvisning till den föregående bedömningen om att det av begreppet ”samarbete” inte framgår om betalning eller någon annan ersättning utgår från annonsören till influencern. PMÖD hänvisade även till att Instagram under år 2017 tog fram en ny funktion för reklammarkering för åtminstone vissa av sina användare och att det då hade valts utformningen ”Betalt samarbete med … [företagets namn]”. Från Alexandra Medias och Tourn Medias sida hade även lyfts fram att upplysning som infogats i Instagraminlägget om att ”Länk till sidan finns i bion” är sådan att den bidrar till att genomsnittskonsumenten uppfattar att det är fråga om marknadsföring. PMÖD ansåg dock att en sådan upplysning i sig inte är tillräcklig för att genomsnittskonsumenten redan vid en flyktig kontakt ska förstå att inlägget utgör marknadsföring.

Domstolens bedömning avseende brist i sändarangivelse (9 § 2 st MFL)

När det gällde frågan om bristande sändarangivelse inledde PMÖD med att konstatera att den rättsliga utgångspunkten för denna bedömning är om bristerna varit sådana att genomsnittskonsumenten har saknat väsentlig information som hon behövt för att kunna fatta ett välgrundat beslut. Enligt PMÖD:s bedömning följer det av bristerna i reklamidentifiering att genomsnittskonsumenten inte redan efter en flyktig kontakt uppfattar vilken näringsidkare som ligger bakom marknadsföringen. PMÖD ansåg dock att utredningen ändå inte ger stöd för att denna brist i marknadsföringen, sedd för sig, har medfört att genomsnittskonsumenten saknat sådan väsentlig information som hon behövt för att fatta ett välgrundat beslut. Som exempel lyfte PMÖD att utredningen inte visade att genomsnittskonsumenten skulle ha avstått från att ta sig till Mobilåtervinnings webbplats mobilpengar.se om det i inlägget funnits information om att det var just Mobilåtervinning som låg bakom marknadsföringen har inte presenterats. Inte heller var omständigheterna sådana att genomsnittskonsumenten skulle kunna förväxla Mobilåtervinning med någon annan mer känd näringsidkare som tillhandahåller en liknande tjänst. PMÖD kom således fram till att marknadsföringen inte var att bedöma som otillbörlig i fråga om bristande sändarangivelse.

Domstolens bedömning avseende Tourn Medias medverkansansvar (23 § 2 st 3 p MFL)

PMÖD delade PMD:s bedömning att Tourn Media inte kunde åläggas något ansvar för den otillbörliga marknadsföringen. PMÖD konstaterade att utredningen inte gav stöd för att Tourn Media till följd av avtal mellan parterna haft ett sådant övergripande ansvar för marknadsföringens slutgiltiga utformning att bolaget kunde åläggas ett marknadsföringsrättsligt ansvar för just den bristfälliga reklamidentifieringen. PMÖD ansåg det visserligen klarlagt att Tourn Media varit involverad i framställningen på olika sätt, men att det var Alexandra Media som haft kontroll och slutlig bestämmanderätt över om marknadsföringen överhuvudtaget skulle komma till stånd. Det innebar enligt PMÖD att Alexandra Media också hade ansvaret och bestämmanderätten över inläggens layoutmässiga och visuella utformning, inklusive hur inläggen skulle utformas för att leva upp till de marknadsföringsrättsliga kraven på reklamidentifiering. PMÖD kom således fram till att endast Alexandra Media ska meddelas förbud enligt 23 § MFL att medverka till den otillbörliga marknadsföringen.

Kommentar

Genom PMÖD:s dom har det fastställts tydligare och strängare krav på hur marknadsföring i sociala medier ska utformas för att uppfylla kraven på reklamidentifiering, vilket förhoppningsvis kommer bidra till ett starkare konsumentskydd och skydd mot smygreklam i sociala medier. Domen har redan fått till följd att KO den 4 februari 2020 publicerade en ny vägledning för marknadsföring i sociala medier som kan tas del av kostnadsfritt via KO:s hemsida. Förekomsten av smygreklam på sociala medier har reducerats under de senaste åren men förekommer fortfarande i hög utsträckning. Det ska bli intressant att se i vilken utsträckning de strängare kraven på reklamidentifiering som nu har fastställts av PMÖD kommer att få effekt i närtid för hur influencer väljer att reklamidentifiera sina reklamsamarbeten med annonsörer.

I svensk media har det dock uppstått visst mått av missförstånd avseende frågan om ett influencer nätverk kan hållas ansvarigt för otillbörlig marknadsföring avseende reklamuppdrag som sådant nätverk har förmedlat. Enligt PMÖD:s domskäl valde PMÖD att fria Tourn Media för att utredningen inte kunde visa att Tourn Media till följd av vare sig uttryckligt eller underförstått avtal haft ett sådant övergripande ansvar för marknadsföringens slutliga utformning för att kunna åläggas ett medverkansansvar. PMÖD har således enligt min mening inte uteslutit att influencer nätverk under andra omständigheter än de som var aktuella i målet kan hållas ansvarigt för bristande reklamidentifiering. Från annonsörens perspektiv är det mot denna bakgrund viktigt att annonsören ingår avtal med såväl den aktuella influencern som det eventuella influencer nätverket som förmedlat reklamuppdraget enligt vilket både influencern och nätverket åläggs ett ansvar för att säkerställa att de inlägg som ska publiceras uppfyller MFL:s krav. Det bör i avtalet även skrivas in att annonsören ska ha rätt att förhandsgodkänna samtliga inlägg innan publicering så att annonsören kan säkerställa att inlägget uppfyller avtalade krav i praktiken.

Sara Hovstadius är advokat och arbetar i Cirios grupp för strategiska kontrakt.

Norske myndigheter trolig på tynn is vedrørende kommunikasjonsvern-direktivet krav om samtykke til «cookies»

Av Ove A. Vanebo

1 Innledning

1.1 Artikkelens tema

Ekomloven regulerer krav til samtykke for å plassere «cookies» på kommunikasjonsutstyr.

«Cookies» betegner et stykke data i form av en liten tekst eller binær data, som lastes ned og lagres på en brukers datautstyr når brukeren åpner en nettside. Ofte omtales cookies også som «informasjonskapsler».

Cookies brukes for eksempel til å lagre innloggingsdetaljer, registrere hvor brukeren beveger seg rundt på nettstedet, eller huske handlekurv i nettbutikker. Den som står bak informasjonskapselen kan tilpasse tjenestene sine ut fra informasjonen som lagres. Cookies kan også brukes for å analysere brukeradferd eller målrette markedsføring i sosiale medier ut fra brukeres preferanser, noe som har høy kommersiell verdi. Cookies kan kategoriseres på ulike måter, bl.a. ut fra om de plasseres av et nettsteds eier (førstepartscookie) eller en annen enn den som driver nettstedet (tredjepartscookie). Av plasshensyn vil jeg avstå fra utdyping på dette punkt.

Artikkelens tema er hvorvidt norske myndigheter, her særlig i form av Samferdselsdepartementet og Nasjonal kommunikasjonsmyndighet (heretter omtalt som «Nkom»), har lagt til grunn en korrekt forståelse av kommunikasjonsverndirektivets samtykkekrav for bruk av «cookies». Som jeg vil utdype under, mener jeg det er tvilsomt om myndighetenes tilnærming i forarbeider og senere uttalelser kan forenes med løsningen i tungtveiende rettskilder – særlig direktivets ordlyd. Dette fremkommer ikke minst i lys av EU-domstolens avgjørelse i den såkalte Planet49-saken, se under i punkt 2.2.[1] Konkret mener jeg at myndighetene uttrykker en gal forståelse av samtykkekravet, og har en for enkel tilnærming til hva som kreves for å samtykke gjennom innstillinger i nettlesere.

1.2 Nærmere om den aktuelle reguleringen

Bruk av samtykke til såkalte «cookies» har vært omdiskutert helt siden vedtakelsen av ny lovregulering gjennom ekomloven i 2013. Cookie-bruk er regulert i den norske ekomloven § 2-7 b, som slår fast at:

«*Lagring av opplysninger i brukers kommunikasjonsutstyr, eller å skaffe seg adgang til slike, er ikke tillatt uten at brukeren er informert om hvilke opplysninger som behandles, formålet med behandlingen, hvem som behandler opplysningene, og har samtykket til dette.*»

Dette er imidlertid ikke til hinder for teknisk lagring av eller adgang til opplysninger når det skjer:

1. utelukkende for det formål å overføre kommunikasjon i et elektronisk kommunikasjonsnett, eller

Ove André Vanebo

2. er nødvendig for å levere en informasjonssamfunnstjeneste etter brukerens uttrykkelige forespørsel.

Som man kan se regulerer ikke bestemmelsen cookies i snever forstand, men vil også omfatte «*[l]agring av opplysninger i brukers kommunikasjonsutstyr, eller å skaffe seg adgang til slike*».

Reguleringen i ekomloven skulle imidlertid gjenspeile kravene i kommunikasjonsverndirektivet, også kalt ePrivacy-direktivet (direktiv 2002/58/EF), nærmere bestemt endringene av det ved direktiv 2009/136/EF.[2] Hensynet bak endringene var å gi brukerne bedre kontroll over personopplysningene sine enn det som fulgte av tidligere

1 EU-domstolens dom C-673/17

2 Prop. 69 L (2012–2013) s. 12.

rett. Formålet med endringene var å styrke personvernet gjennom å beskytte terminalutstyret og informasjonen som lagres på slikt utstyr.[3]

Endringene fikk betydning for ordlyden i artikkel 5 nr. 3, som gjelder samtykke til bl.a. cookies. Bestemmelsen lyder slik vedrørende samtykke:

«*Medlemsstaterne sikrer, at lagring af oplysninger eller opnåelse af adgang til oplysninger, der allerede er lagret i en abonnents eller brugers terminaludstyr, kun er tilladt på betingelse af, at abonnenten eller brugeren har givet sit samtykke hertil efter i overensstemmelse med direktiv 95/46/EF at have modtaget klare og fyldestgørende oplysninger, bl.a. om formålet med behandlingen.*» (Min understreking.)

For ordens skyld nevner jeg at direktiv 2009/136/EF ennå ikke er innlemmet i EØS-avtalen, og flere deler av direktivet er ikke forsøkt gjennomført i norsk rett. Selv om direktivets artikkel 5 nr. 3 ble gjennomført i norsk rett,[4] har EØS-prosessen blitt utsatt i påvente av avklaring vedrørende EFTA-/EØS-landenes deltakelse i BEREC.[5] Departementet tar sikte på å komme tilbake til Stortinget når det ligger til rette for å innlemme BEREC-forordningen (EF) nr. 1211/2009 og de resterende bestemmelsen i direktiv 2009/136/EF som omhandler BEREC.[6]

2 Norske myndigheters oppfatning av reguleringen

2.1 Uttalelser i ekomlovens forarbeider

I forarbeidene til § 2-7 b drøftet departementet hva som er tilstrekkelig for at bruker ansees for å ha gitt samtykke. Departementet uttrykte da «*at en teknisk innstilling i nettleser vil kunne benyttes til å samtykke eller til å nekte samtykke, forutsatt at sluttbruker er tilstrekkelig informert om formålet med informasjonsinnsamlingen og lagringen*».[7] I tilknytning til cookie-bruk påpekte departementet eksplisitt at «*[o]gså en forhåndsinnstilling i nettleser om at bruker aksepterer informasjonskapsler anses å utgjøre et samtykke*».

Forutsetningen var at «*det finnes klar og tydelig informasjon tilgjengelig på det aktuelle nettstedet om hvilke informasjonskapsler og lignende teknikker som benyttes, hvilke opplysninger som behandles, hva formålet med behandlingen er og hvem som behandler opplysningene*».

Departementet viste til at det ville være tilstrekkelig å samtykke én gang for samme formål, men utdypet ikke hva dette innebærer.

> Departementet mener ekomlovens samtykkekrav er noe lempeligere enn personopplysningslovens

Interessant nok mente departementet «*at innholdet i kravet til samtykke av praktiske hensyn ikke vil være sammenfallende med samtykkekravet i personopplysningsloven*».[8] Dette ble begrunnet med det at «*kommunikasjonsverndirektivet artikkel 5.3 ikke har til hensikt å vanskeliggjøre bruk av lovlig teknikker som informasjonskapsler, men å sikre brukernes personvern*». Dette må forstås som at departementet mener ekomlovens samtykkekrav er noe lempeligere enn personopplysningslovens.

Departementet siktet her til personopplysningsloven av 2000. Nevnte lov gjennomførte samtykkekravet slik det fremkom i personverndirektivet (direktiv 95/46/EF) artikkel 7 bokstav a.[9] At det nå er en ny personopplysningslov av 2018, som gjør GDPR til norsk lov,[10] endrer ikke mine vurderinger. Som det vil fremkomme under i punkt 2.2, har norske myndigheter (ved Nkom) lagt til grunn at ekomlovens samtykkekrav heller ikke er det samme som etter GDPR.

Etter departementet syn retter artikkel 5 nr. 3 «*seg i hovedsak mot personvernkrenkende teknikker som spionprogram og lignende*». Endringen i regelverket «*skal forstås som en presisering av forpliktelsen til å gi brukere tilstrekkelig informasjon og valgmuligheter med hensyn til bruken av disse teknikkene*».[11] Brukerne ville derfor ha mulighet til å ivareta sine rettigheter.

2.2 Uttalelse fra Nasjonal kommunikasjonsmyndighet etter Planet49-dommen

1. oktober 2019 avsa EU-domstolen dom i Planet49-saken. Dommen klargjør kravet til samtykke etter både kommunikasjonsverndirektivet, personverndirektivet og GDPR.

Planet49 er et tysk firma, som hadde en lotterikonkurranse på nettsidene sine. For å delta i konkurransen måtte deltakeren skrive inn navn og adresse i et felt. Under feltene for adressen var det to «avkrysningsbokser». Den første boksen var ikke avkrysset, og var ment for deltakerens samtykke dersom vedkommende ønsket å bli kontaktet av opptil flere titalls sponsorer og samarbeidspartnere om ulike tilbud. Den andre boksen var forhåndsavkrysset, og ville medføre at en cookie plasseres i systemet for å sikre målrettede reklameannonser på nett.

EU-domstolen fastslår at samtykke etter kommunikasjonsverndirektivet krever en mer aktiv handling (jf. det engelske uttrykket «indication»), med en utvetydig viljesytring om hva den aktuelle personen ønsker. Manglende handling/stilltiende samtykke er ikke nok.

3 Prop. 69 L (2012–2013) s. 42.
4 Se endringene av ekomloven 1. juli 2013, jf. Prop. 69 L (2012–2013) s. 8 og 102.
5 BEREC er forkortelsen for *Body of European Regulators for Electronic Communications*.
6 Prop. 157 LS (2015–2016) s. 9.
7 Prop. 69 L (2012–2013) s. 43.
8 Samme sted.
9 Ot.prp.nr. 92 (1998-1999) s. 108.
10 Se personopplysningsloven av 2018 § 1.
11 Prop. 69 L (2012–2013) s. 43.

Kommunikasjonsverndirektivet inneholdt en henvisning til personverndirektivets samtykkekrav, og etter GDPR trådte i kraft må det legges til grunn, se min utdypning i 3.1. Domstolen påpeker også at det etter GDPR er et tydeligere, strengere krav til hva som kreves av samtykke i forhold til personverndirektivet.[12]

I tillegg til å være et frivillig og informert samtykke, må samtykket også være separat. En «bunt» med samtykker kan derfor ikke gis til en rekke ulike formål. Du kan ikke samtykke til å delta i lotteriet samtidig som du samtykker til å plassere cookies på maskinen.

Nkom kom med en uttalelse 10. oktober 2019 om at myndigheten «*vurderer behov for presiseringer i regelverket, etter EU-dom om samtykke når et nettsted bruker cookies (informasjonskapsler)*».[13] Nkom ville «*gå i dialog med Kommunal- og moderniseringsdepartementet*» for å vurdere «*behov for presiseringer i ekomlovgivningen som følge av rettsutviklingen*». I en uttalelse fra Nkom datert 27. november 2019[14] fremkommer imidlertid at det ikke foreligger grunnlag for å endre tidligere oppfatninger.

Nkom gjentar forarbeidenes oppfatning om at: «*Ekomloven § 2-7 b skal være med å sikre brukernes personvern på ekomområdet*». Etter Nkoms oppfatning «*kan samtykke avgis ved at sluttbruker benytter en teknisk innstilling i nettleser eller tilsvarende i tilfeller der dette er teknisk mulig og effektivt*». Nkom påpeker deretter at det fremkommer av «*lovens forarbeider at forhåndsinnstilling i nettleser om at brukeren aksepterer informasjonskapsler/cookies anses som samtykke*».

Videre viser Nkom til at «*det i Europa er vanlig med samtykke i tråd med personopplysningsforordningen også for cookies*», og synes å fastholde den tradisjonelle norske ordningen som innebærer at samtykke etter ekomloven er noe annet enn samtykke etter personopplysningslovgivningen. Dette kommer også frem ved at Nkom påpeker at:

> «*[D]ersom det er tvil om hvorvidt en cookie lagrer eller behandler opplysninger som faller inn under ekomloven § 2-7 b eller om det er behandling av personopplysninger som krever samtykke som oppfyller kravene i personopplysningslovgivningen bør man velge samtykke etter personopplysningslovgivningen (samtykke i tråd med GDPR) for å være på den sikre siden.*»

Oppsummert kan man etter dette slå fast at Nkom operer med ulike krav til samtykke for cookies som *ikke* innebærer behandling av personopplysninger og samtykke til behandling av informasjon gjennom cookies som utgjør personopplysningsbehandling.

Forutsetningen for at samtykke er gyldig, er ifølge Nkom at det finnes klar og tydelig informasjon tilgjengelig på det aktuelle nettstedet om hvilke informasjonskapsler/cookies som benyttes, hvilke opplysninger som behandles, formålet med behandlingen og hvem som behandler opplysningene.

Nkom slår for øvrig igjen fast at: «*Det er tilstrekkelig at brukeren samtykker én gang for det samme formålet.*»

3 Nærmere om kommunikasjonsverndirektivets samtykkekrav

3.1 Generelt om samtykkekravet

Etter min oppfatning er det tvilsomt om norske myndigheter har lagt til grunn en korrekt forståelse av direktivets samtykkeregulering.

Kommunikasjonsverndirektivet artikkel 2 bokstav f har inntatt en legaldefinisjon av «samtykke», som innebærer at «*en brukers eller en abonnents samtykke tilsvarer den registrertes samtykke i direktiv 95/46/EF [dvs. personverndirektivet]*». Interessant nok er dette ikke nevnt i ekomlovens forarbeider, og Nkom har heller ikke drøftet dette i sin uttalelse. Som nevnt har myndighetene antatt at personopplysningslovens samtykkekrav ikke samsvarer med kommunikasjonsverndirektivet. Dette synes vanskelig å forene med at personopplysningsloven gjennomførte personverndirektivets samtykkekrav, og kommunikasjonsverndirektivet uttrykker eksplisitt at det opererer med personverndirektivets samtykkedefinisjon.

Etter at personverndirektivet ble opphevet, slår personvernforordningen artikkel 94 nr. 2 fast at «*[h]envisninger til det opphevede direktiv skal forstås som henvisninger til denne forordning [dvs. GDPR]*». I to ferske uttalelser fra Personvernrådet konstateres derfor at kommunikasjonsverndirektivets samtykkekrav nå tilsvarer samtykkekravet etter GDPR.[15] Både det britiske[16] og det irske[17] datatilsynet har påpekt det samme. Ettersom GDPR har et noe strengere samtykkekrav enn det

12 Se dommens avsnitt 61, jf. også Skullerud m.fl., *Personopplysningsloven og personvernforordningen (GDPR); Kommentarutgave*, (2019) s. 161.

13 «*Nkom vurderer behov for presiseringer etter EU-dom om cookies*». Lest 11. februar 2020: *https://www.nkom.no/aktuelt/nyheter/nkom-vurderer-behov-for-presiseringer-etter-eu-dom-om-cookies*

14 «*Informasjonskapsler/cookies*». Lest 11. februar 2020: *https://www.nkom.no/teknisk/internett/cookies/informasjonskapsler-cookies*

15 Personvernrådet, *Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities*, s. 7 avsnitt 14, og Personvernrådet, *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*, s. 6 avsnitt 16 (denne utgaven er ennå ikke endelig, men er utgaven som er ute til høring).

16 The Information Commissioner Office (ICO), «*When can we rely on legitimate interests?*». Lest 10. februar 2020: *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/*

17 Data Protection Commission, «Guidance on Cookies and Similar Technologies», (2019) s. 2.

gamle personverndirektivet, blir det enda mer problematisk at norske myndigheter tar utgangspunkt i et lempeligere krav.

En mulig forklaring på norske myndigheters syn er at de har lest fortalepunkt 66 til direktiv 2009/136/EF, som slår fast at: «*Hvor det er teknisk muligt og effektivt, i overensstemmelse med de relevante bestemmelser i direktiv 95/46/EF, kan brugerens samtykke til databehandling udtrykkes gennem anvendelse af passende browserindstillinger eller andre applikationer.» (Min understrekning.)*

Dette kan ha forledet myndighetene til å tro at innstilling i nettleser er en enklere – men samtidig tilstrekkelig – måte å samtykke på enn hva som normalt kreves. Fortalepunktet er imidlertid ikke ment som et unntak fra det regulære samtykkekravet, men en påminnelse om at det i dagens teknologiske hverdag er mulig å gi samtykke på flere ulike måter.[18] Som jeg vil komme tilbake til under punkt 4, er heller ikke en slik løsning enkel å få til. At norske myndigheter bare viser til at samtykke kan gis i nettleserinnstilling, skaper ytterligere problemer.

3.2 Kan innholdet i begrepet «samtykke» variere fra stat til stat?

Ettersom norske myndigheter har forutsatt at samtykkekravet er annerledes etter kommunikasjonsverndirektivet enn personopplysningslovgivningen, kan det problematiseres om det er adgang til å utforme nasjonale særreguleringer med andre (og lavere) krav til samtykke.

Den enkelte direktivbestemmelse må tolkes for å klargjøre om den åpner for nasjonal tilpasning.[19] Som redegjort for over er det konstatert i direktivet hva som skal utgjøre et samtykke, og det er vanskelig å se at det åpnes opp for særordninger.

> Ettersom GDPR har et noe strengere samtykkekrav enn det gamle personverndirektivet, blir det enda mer problematisk at norske myndigheter tar utgangspunkt i et lempeligere krav.

Kommunikasjonsverndirektivet artikkel 1 nr. 1 slår fast at det overordnete formålet med direktivet er altså å sikre beskyttelse av grunnleggende rettigheter og friheter for personer som benytter elektroniske kommunikasjonsnettverk.[20] En slik forutsetning ville for øvrig passe dårlig med en nasjonal ordning som operer med lavere krav til samtykke enn i andre stater omfattet av direktivet. Tvert imot heter i Planet49-dommen avsnitt 47 at det:

«… *bemærkes, at det følger af såvel kravene om en ensartet anvendelse af EU-retten som af lighedsprincippet, at en bestemmelse i EU-retten, som ikke indeholder nogen udtrykkelig henvisning til medlemsstaternes ret med henblik på at fastlægge dens betydning og rækkevidde, normalt skal undergives en selvstændig og ensartet fortolkning i hele Unionen …*»

Det er for øvrig lite som tyder på at departementet ønsket å innføre en særegen nasjonal regulering. Alt trekker i retning av at departementet oppfattet samtykket etter kommunikasjonsverndirektivet som annerledes enn samtykket etter personopplysningslovgivningen. Forarbeidene til ekomloven presiserer for øvrig at *«§ 2-7 b gjennomfører artikkel 5.3 i direktiv 2002/58/EF om vilkårene knyttet til lagring av opplysninger i kommunikasjonsutstyr m»*.[21]

Interessant nok har datatilsynet i Liechtenstein inntatt den posisjon at landet ikke tar hensyn til EU-domstolens avgjørelse i Planet49-saken:

«*I det konkrete tilfellet tolket EU-domstolen en bestemmelse i direktiv 2009/136/EF, som EU-landene måtte implementere i sine nasjonale lover. Det skal imidlertid bemerkes at dette direktivet ikke er blitt innlemmet i EØS-retten, som Liechtenstein er underlagt. Dette betyr at bestemmelsene i dette EU-direktivet 2009/136/EF ikke er blitt gjort til liechtensteinsk rett og mangler derfor i den liechtensteinske kommunikasjonsloven.*» (Min oversettelse fra tysk.)

Datatilsynet i Liechtenstein mener landet fremdeles bare må vurderes i henhold til det opprinnelige direktiv 2002/58/EF, som ble vedtatt i EØS-rett, samt den europeiske generelle databeskyttelsesforordningen (GDPR).[22] Denne holdningen gjenspeiler imidlertid at landet i motsetning til Norge ikke har forsøkt å gjennomføre direktivet i sin nasjonale lovgivning.

4 Problemer med å gi et gyldig samtykke i nettleserinnstilling

4.1 Innledning

I tillegg til at jeg mener norske myndigheter har misforstått innholdet i samtykkekravet etter kommunikasjonsverndirektivet, er jeg også kritisk til uttalelsene om samtykke gjennom nettleserinnstillinger. Selv om det er riktig at samtykke *i prinsippet* også kan gis gjennom nettleserinnstillinger, fremstår tilnærmingen som unyansert. Dette kan henge sammen med at myndighetene nettopp har lagt til grunn en

18 Artikkel 29-gruppa, *Opinion 2/2010 on online behavioural advertising, WP 171*, s. 13.

19 NOU 1997: 19 s. 38.

20 Personvernrådet, *Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities*, s. 8 og 11.

21 Prop. 69 L 2012–2013 s. 102

22 Datenschutzstelle Fürstentum Liechtenstein, «*Informationen zum Umgang mit Cookies in Liechtenstein*», (2019). Lest 11. februar 2020: *https://www.datenschutzstelle.li/aktuelles/informationen-zum-umgang-mit-cookies-liechtenstein*

for lempelig tilnærming til hva som kreves for å avgi gyldig samtykke.

Etter dagens personvernforordning vil et gyldig samtykke kreve en «*frivillig, spesifikk, informert og utvetydig viljesytring fra den registrerte der vedkommende ved en erklæring eller en tydelig bekreftelse gir sitt samtykke til behandling av personopplysninger som gjelder vedkommende*».[23] Også etter det gamle personverndirektivet av 1995 måtte et samtykke være en «*frivillig, spesifikk og informert viljesytring om at den registrerte gir sitt samtykke til at personopplysninger om vedkommende blir behandlet*».[24] Både med dagens forordning og det tidligere direktivet, er det problematisk å få et samtykke gjennom nettleserinnstilling, se punktene 4.2 til 4.5.

> I tillegg til at jeg mener norske myndigheter har misforstått innholdet i samtykkekravet etter kommunikasjonsverndirektivet, er jeg også kritisk til uttalelsene om samtykke gjennom nettleserinnstillinger.

4.2 Kravet til spesifikt samtykke

Både personverndirektivet og -forordningen legger opp til at registrerte personer skal kunne samtykke til bestemte behandlinger og formål. Dette har også en side til kravet om frivillighet, jf. at det i personvernforordningens fortalepunkt 43 heter at: «*Samtykket antas å ikke være gitt frivillig dersom det ikke er mulig å gi separat samtykke for forskjellige behandlingsaktiviteter, selv om det er hensiktsmessig i det enkelte tilfellet […]*». En sentral utfordring her er at de fleste nettleserne ikke har innstillinger eller løsninger som muliggjør et tilstrekkelig spesifikt samtykke.

For det første vil et utvetydig samtykke kreve at det er avgrenset hva en person samtykker til. Ulike former for «blankofullmakter» er vanskelig å forene med spesifikasjonskravet.[25] En rekke nettlesere har imidlertid ikke tilstrekkelig «finmaskede» innstillingsmuligheter som gjør at brukeren kan justere presist hva det samtykkes til. Ofte vil nettlesere akseptere alle eller ingen cookies.

Som det britiske datatilsynet, ICO, påpeker i sin veiledning: «*You cannot assume that each visitor to your online service can configure their browser settings to correctly reflect their preferences in relation to the setting of cookies.*»[26]

4.3 Aktivt valg

Kommunikasjonsverndirektivet artikkel 5 nr. 3 krever altså at brukeren må ha «*givet sit samtykke*», noe som tilsier en aktivitet for å uttrykke samtykke. Ettersom også både personverndirektivet og GDPR krever tilkjennegivelse av en viljesytring, og denne må være utvedtydig, vil det oppstå problemer med tanke på hvorvidt samtykket er skjedd gjennom et aktivt valg. Artikkel 29-gruppa[27] har påpekt at et gyldig samtykke bare kan innhentes «*[w]here the website operator can be confident that the user has been fully informed and actively configured their browser or other application […]*».[28]

Kravet til aktivitet var som nevnt også en sentral problemstilling i Planet49-dommen. Gabriela Fortuna-Zandfir påpeker at et kritisk forhold som ble tatt opp i dommen, er at «*it appears impossible in practice to ascertain objectively whether a website user had actually given his or her consent to the processing of his or her personal data by merely continuing with his or her activity on the website visited (continuing browsing or scrolling) […]*».

Enkelte nettlesere vil imidlertid som standardinnstilling akseptere cookies, slik at brukeren må gå inn og endre dette selv. Verken departement eller Nasjonal kommunikasjonsmyndighet har dvelt ved problemstillingen knyttet til aktivitet, men bare konstatert at en teknisk innstilling i nettleser kan være nok.

> Verken departement eller Nasjonal kommunikasjonsmyndighet har dvelt ved problemstillingen knyttet til aktivitet.

4.4 Informasjonskravet

Uten at jeg skal gå i dybden av informasjonskravet i forbindelse med samtykke, forvansker også dette kravet muligheten til å avgi et gyldig samtykke: Reguleringen oppstiller kumulative krav til samtykke, ved at den krever både tilstrekkelig informasjon og at gyldig samtykke gis i samsvar med persondatalovgivningen.[29] Det må forstås slik at brukeren av et nettsted må motta informasjonen *før* cookies plasseres/lagres i brukerens utstyr gjennom samtykke.[30] I mange tilfeller vil nettleserens samtykkemekanisme avgi samtykke til dette før brukeren har blitt informert på tilstrekkelig vis. Et ytterligere kompliserende forhold er spesifikasjonskravet som er nevnt over: Informasjonen må tydeliggjøre hva det samtykkes til, og

23 Personernforordningen artikkel 4 nr. 11.

24 Personverndirektivet artikkel 2 bokstav h.

25 Artikkel 29-gruppa, *Working Document 02/2013 providing guidance on obtaining consent for cookies*, s. 3.

26 ICO, *Guidance on the use of cookies and similar technologies*, (2019) s. 29.

27 Artikkel 29-gruppa var et uavhengig rådgivende EU-organ i spørsmål vedrørende personopplysningsvern og personvern. Arbeidsgruppa er nå erstattet av Personvernrådet (EDPB).

28 Artikkel 29-gruppa, *Working Document 02/2013 providing guidance on obtaining consent for cookies*, s. 4.

29 Artikkel 29-gruppa, *Opinion 2/2010 on online behavioural advertising, WP 171*, s. 13

30 Samme sted.

det kan ikke gis en for generell informasjon.

4.5 Oppsummerende betraktninger

Min gjennomgang viser at det selv med et samtykke gjennom nettleser vil være svært upraktisk – og kanskje umulig – å gi et gyldig samtykke etter kommunikasjonsverndirektivets løsning.

Allerede i 2010 påpekte Artikkel 29-gruppa den store majoriteten av nettlesere ikke opererte med standardinnstillinger som tilfredsstilte samtykkekravet, og under enhver omstendighet ville browser-innstillinger kun klare å oppfylle kravene etter datidens personverndirektiv «*in very limited circumstances*».[31]

Rundt ti år senere er det liten grunn til å tro at det vil være realistisk å kunne benytte nettleserinnstillinger for å gi et gyldig samtykke. Det franske datatilsynet, CNIL, lagde derfor retningslinjer som kom på plass i slutten av juli 2019.[32] I retningslinjenes artikkel 4 uttrykker tilsynet at det er tvilsomt om dagens nettlesere har tilstrekkelige innstillingsmuligheter for å kunne uttrykke et lovlig samtykke, selv om dette kan endre seg med utviklingen av nye browsere. I forslag til nye anbefalinger fra CNIL, som ble sendt på høring i januar 2020, understrekes det fortsatt at moderne nettlesere ikke lar brukeren uttrykke tilstrekkelig manifestasjonen av et gyldig samtykke.[33] Et ytterligere problem, er at brukere ikke kan forventes å ha særlig med kunnskap om cookies og hvordan de virker.

5 Avsluttende merknader

Uklarheter rundt hva som kreves for å få et gyldig samtykke har preget diskusjonen helt fra endringene i kommunikasjonsverndirektivet ble utformet gjennom direktiv 2009/136/EF. Samme år som sistnevnte direktiv ble vedtatt, advarte Artikkel-29-gruppen om en «*erosion of the definition of consent and […] subsequent lack of transparency*».[34]

> Norske myndigheters oppfatning tar feil i sin vurdering av hvordan et gyldig samtykke kan oppnås

På bakgrunn av det ovenstående mener jeg norske myndigheters oppfatning tar feil i sin vurdering av hvordan et gyldig samtykke kan oppnås etter kommunikasjonsverndirektivet med endringen fra 2009. Selv om endringsdirektiv 2009/136/EF ennå ikke er innlemmet i EØS-avtalen, er det problematisk når meningen har vært å utforme en norsk lovbestemmelse som gjennomfører løsningen i ny artikkel 5 nr. 3. Allerede i 2013 advarte Datatilsynets direktør, Bjørn Erik Thon, om at den norske tilnærmingen «*er upraktisk, muligens i strid med direktivet, hemmende for utvikling av gode samtykkeløsninger og svært vanskelig for folk flest å håndtere*».[35] I ettertid er det vanskelig å være uenig i denne oppfatningen.

Ove André Vanebo er senioradvokat og er tilknyttet Kluges avdeling for prosedyre og offentlighet i Oslo.

31 Artikkel 29-gruppa, *Opinion 2/2010 on online behavioural advertising, WP171*, s. 13.

32 JORF n°0166 du 19 juillet 2019 texte n° 92.

33 CNIL, *Projet de recommandation*, av 14. januar 2020

34 Artikkel 29-gruppa, *Opinion 1/2009 on the proposals amending Directive 2002/58 on privacy and electronic communications (e-Privacy Directive), WP159*, s. 10

35 Bjørn Erik Thon, «*Cookies: Regjeringen har valgt en dårlig løsning*», 2013. Lest 11. februar 2020: *https://www.personvernbloggen.no/2013/03/05/cookies-regjeringen-har-valgt-en-darlig-losningen/*

Den ekonomiska förfoganderätten till Babblarna-figurerna förvärvad av uppdragsgivaren/arbetsgivaren

Av Karin Söderberg och Kajsa Zenk

Arbetsdomstolen meddelade nyligen sin dom i det uppmärksammade Babblarna-målet.[1] Målet rörde frågan om och i vilken utsträckning ett bolag förvärvat rätten att förfoga över vissa upphovsrättsligt skyddade prestationer som en illustratör skapat under sin tid som uppdragstagare och anställd vid ett bolag. Utfallet bekräftar tidigare praxis på området, men visar också på det lagstiftningsbehov som det nya upphovsrättsdirektivet kan komma att läka.

Bakgrund

En illustratör var först uppdragstagare och sedan anställd hos ett bolag för att utföra olika uppdrag avseende konceptet Babblarna. Uppdragen avsåg bland annat att formge figurerna i Babblarna, skapa illustrationer till bilderböcker och arbete med ett spel och en webbplats. Flertalet muntliga uppdragsavtal ingicks mellan 2005-2008 och 2012-2014. År 2014 ingicks ett muntligt anställningsavtal, vilket efterföljdes av ett skriftligt anställningsavtal som undertecknades i januari 2017. I maj 2017 undertecknades ett nytt anställningsavtal med en klausul som angav att bolaget skulle äga alla rättigheter till allt material illustratören skapat, skapar och producerar inom ramen för anställningen.

Illustratören fick fast ersättning och lön samt en rörlig ersättning som benämndes royalty. Vid omförhandling av royaltyavtalet var parterna inte eniga, vilket ledde till att illustratören sade upp sig. I samband med uppsägningen meddelade illustratören bolaget att han inte längre samtyckte till att bolaget förfogade över hans upphovsrättsligt skyddade material.

Karin Söderberg

Kajsa Zenk

Parterna var överens om att illustratören genom sitt arbete har gjort upphovsrättsligt skyddade prestationer. Tvisten rörde således frågan om och i vilken utsträckning bolaget förvärvat rätten att förfoga över vissa upphovsrättsligt skyddade prestationer avseende konceptet Babblarna, inklusive rätten att ändra och vidarelicensiera dessa, som illustratören skapat under sin tid som dels uppdragstagare och dels anställd vid bolaget.

Rättsliga utgångspunkter för verk skapade inom ramen för uppdragsavtal respektive anställningsavtal

Arbetsdomstolen (AD) börjar med att redogöra målets rättsliga utgångspunkter. Domstolen konstaterar att när ett upphovsrättsligt skyddat verk skapas inom ramen för ett uppdragsavtal utan att beställaren och uppdragstagaren kommer över-

1 Dom nr 53/19 den 27/11 2019 i mål nr A 69/18.

ens om vilken rätt till verket som ska tillkomma beställaren, har beställaren redan genom uppdragsavtalet förvärvat åtminstone viss rätt till verket. Omfattningen av denna rätt får enligt AD närmare avgöras mot bakgrund av omständigheterna i samband med uppdragsavtalets tillkomst och tillämpning samt parternas agerande. I denna bedömning anger arbetsdomstolen vissa i doktrin åberopade omständigheter som kan ha betydelse för tolkningen och som bör beaktas när beställarens förfoganderätt över upphovsrättsligt skyddade verk som uppstått till följd av uppdraget bedöms. Avtalets ändamål, de specifika dragen av uppdragsavtalet, och arten av det verk som skapas kan vara av betydelse. Även övriga faktorer, som betalningsformen, betalningens storlek, branschpraxis och parternas ställning kan få betydelse för den sammantagna bedömning som ska göras.

Vidare anger AD, med hänvisning till äldre praxis (AD 2002 nr. 87), att när verk skapas inom ramen för anställningsavtal och inget uttryckligen avtalats om rätten till upphovsrättsliga verk som arbetstagaren presenterat inom ramen för anställningen kan en övergång i vissa fall underförstått följa genom anställningsförhållandets beskaffenhet. Ledning ska då sökas i anställningsförhållandets art samt branschens allmänna villkor och sedvänjor. Det som är avgörande är hur utnyttjandet av verk av det aktuella slaget förutsatts ske med hänsyn till företagets normala verksamhet. AD hänvisar till en i litteraturen antagen tumregel som anger att en arbetsgivare inom sitt verksamhetsområde och sin normala verksamhet får utnyttja sådana verk som tillkommit som ett resultat av tjänsteåligganden och särskilda åtaganden gentemot arbetsgivaren och som kan förutses när verket tillkommer. Domstolen påpekar att anställningsavtalets innehåll i vissa fall kan förändras med tiden när t.ex. arbetsgivarens verksamhet utvidgas. Detta kan då komma att omfatta nya former av utnyttjanden. Om arbetstagaren då inte hävdar sina rättigheter kan rättigheter övergå till arbetsgivaren, och anställningsavtalet anses få sitt innehåll av det faktiska handlandet. Arbetsdomstolen påkallar dock restriktivitet i det avseende att sådan övergång bara bör avse rätten till sådana utnyttjanden som faktiskt förekommit. Arbetsdomstolen nämner även den så kallade specifikationsprincipen enligt vilken inte mer av upphovsrätten ska övergå än vad som uttryckligen följer av avtalet, således ska även enligt denna princip otydliga eller tysta avtal tolkas restriktivt eller inskränkande till upphovsmannens förmån.

Arbetsdomstolens avgörande

AD använder ovan nämnda bedömningsgrunder för att avgöra vilken förfoganderätt som tillkommit bolaget under de två avtalen. Domstolen anser att mycket talar för att ändamålet med det första uppdragsavtalet var att skapa ett helhetskoncept för Babblarna och att illustrationerna skapade inom ramen för avtalet skulle komma att användas för många olika produkter. Illustratören måste enligt domstolen ha insett att hans illustrationer skulle användas för de produktkategorier som uppdragsavtalet avsåg. Domstolen anser därför att uppdragsavtalet måste tolkas så att förfoganderätten till de upphovsrättsligt skyddade alster som skapades inom ramen för uppdragsavtalet avseende de produktkategorier illustratören vid denna tidpunkt kände till (bilderböcker, musikvideor, PC-spel, plastdockor och webbplatser) tillkom bolaget.

Att illustratören fick en rörlig ersättning benämnd royalty medför inte enligt AD att illustratören haft fog för att anse att bolaget gett upp någon del av den förfoganderätt bolaget förvärvat genom uppdragsavtalet. Domstolen påpekar i anslutning till detta att royaltyavtalet inte innehåller något om upphovsrätt, eller att royaltyn skulle vara en ersättning för bolagets förfoganden. Royalty har inte någon ensidig innebörd och betalas inte sällan ut av någon som redan förvärvat en förfoganderätt till annans upphovsrättsligt skyddade verk.

Domstolen anser vidare att även de efterföljande uppdragsavtalen medför en förfoganderätt för bolaget till de nya produktkategorierna. De illustrationer som gjorts under det första uppdragsavtalet användes som underlag i de nya produktkategorierna med illustratörens kännedom. Eftersom illustratören inte protesterade mot användningen anser domstolen det således vara avtalat att bolaget hade förfoganderätt för användningen av illustrationerna i de nya produktkategorierna.

När uppdragen sedermera övergick till en anställning fick illustratören kännedom om all användning bolaget gjorde av hans illustrationer. Illustratören framförde inte heller vid denna tid någon invändning mot användningen, utan snarare medverkade och underlättade illustratören användningen. Den skrivning som senare tillkom i anställningsavtalet om material och rättigheter anser domstolen inte innebär att bolaget därigenom hade för avsikt att inskränka sin förfoganderätt till illustrationer som bolaget redan förvärvat. Eftersom illustratören även medverkat till ändringar och vidarelicensiering av illustrationerna anser domstolen att bolagets förfoganderätt även ska anses innefatta en sådan rätt.

Sammanfattningsvis anser domstolen att bolaget har förvärvat rätten att förfoga över vissa upphovsrättsligt skyddade prestationer avseende konceptet Babblarna, inklusive rätten att ändra och vidarelicensiera dessa, som illustratören skapat under sin tid som uppdragstagare och anställd vid bolaget.

Reflektioner

Arbetsdomstolens slutsats ligger i linje med tidigare avgöranden på området. Även om domstolen påpekar att hänsyn ska tas till specifikationsprincipen visar domskälen på att denna princip blir av sekundär betydelse när upphovsrättsliga tvister grundas på uppdrags- eller anställningsavtal. Det läggs stor vikt vid bolagets verksamhet och vad illustratören bör ha insett om bolagets utnyttjanden av verken. Det är logiskt att större hänsyn tas till tumregeln än till specifikationsprincipen när avtal inte finns avseende immateriella rättigheters övergång. Har inget avtalats finns inget att specificera och tumregeln bör således ges en större betydelse.

För att omfattas av tumregeln ska verket ligga inom arbetsgivarens verksamhetsområde och dennes normala verksamhet. Således är det även naturligt att det läggs stor vikt vid vilka ändamål prestationerna skulle användas till. I detta ligger även att företag utvecklas, vilket medför att nya former av utnyttjanden kan komma att omfattas. Anställningsavtalet får i dessa situationer sitt innehåll av parternas faktiska handlande. Genom att illustratören varit medveten om, medverkat till, och till viss del även underlättat bolagets användning av hans illustrationer tillföll förfoganderätten bolaget. Eftersom en upprinnelse till tvisten var förhandlingarna kring royalty-ersättningen kan här tänkas att Babblarnas senare framgång, och således bolagets nya former av utnyttjanden, bidrog till att tvisten infekterades. Målets utgång i denna del visar tydligt på en sådan situation som träffas av det nya upphovsrättsdirektivets art. 20, den så kallade ”bestseller”-klausulen. Artikeln ger upphovspersoner möjlighet att omförhandla avtal och därmed få en högre ersättning om det visar sig att den ursprungliga ersättningen var oproportionerligt låg i förhållande till senare kommersialisering.

Även om det idag inte finns någon som hindrar att partnerna i efterhand förhandlar om en annan ersättning innebär det nya upphovsrättsdirektivet ökade möjligheter för upphovspersoner att kräva proportionerlig ersättning i efterhand. Implementeringen av det nya direktivet i svensk rätt är endast i startgroparna, men direktivstexten talar för att det kommer bli lättare för upphovspersoner att gå vidare rättsligt och kräva ersättning.

Utfallet av målet i AD kan alltså sägas visa på två viktiga punkter, dels att det är av vikt att uttryckligt reglera rätten till upphovsrättsligt skyddade verk i anställnings- eller uppdragsavtal och dels att det finns ett behov att införa de mekanismer som föreslås i det nya upphovsrättsdirektivet för att stärka upphovspersoners avtalsrättsliga ställning. Sammanfattningsvis stämmer ändå utgången i målet till stor del överens med tidigare praxis på området och fastställer specifikationsprincipens sekundära betydelse i förhållande till parternas handlande. Det är därför, för tillfället, av stor vikt att tydligt reglera rätten till arbetstagares och uppdragstagares upphovsrättsligt skyddade verk i anställningsavtalet respektive uppdragsavtalet. Framför allt tills det nya upphovsrättsdirektivet implementerats i svensk rätt.

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

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.

Norske varemerker trumfer indiskregistrert domenenavn

Av Sarah Wennberg Svendsen

Navnestriden om APPEAR er avgjort i Høyesterett[1]. Retten tok stilling til forholdet mellom et utenlandskregistrert domenenavn og to norske varemerker. Lagmannsretten hadde allerede fastslått at det indiske domenenavnet appear. in krenket de norske varemerkeregistreringene APPEAR, men hvilke tiltak kunne med rimelighet pålegges for å stanse krenkelsen? Er det rimelig at det indiske domenenavnet overføres til den norske varemerkeinnehaveren?

Telekommunikasjonsselskapet Appear TV, registrerte i 2009 og 2014 det kombinerte merket Appear TV og ordmerket APPEAR i Norge. Registreringene dekker blant annet apparater for overføring og gjengivelse av lyd eller bilder, databehandlingsutstyr, samt design og utvikling av datamaskiner og dataprogrammer.

Video Communications Services («VCS», tidligere Telenor Digital AS) lanserte en ny videokonferansetjeneste i 2013. Tjenesten ble markedsført i Norge under det indiske domenenavnet appear.in.

Da partene møttes i tingretten, hevdet Appear TV at bruken av det indiske domenenavnet utgjorde et inngrep i deres varemerkerettigheter. VCS svarte med å anføre at varemerkene var ugyldige på grunn av sitt beskrivende betydningsinnhold. Tingretten kom til at merketeksten APPEAR var beskrivende og uten særpreg, slik at de norske varemerkene var ugyldige. Lagmannsretten var ikke enig i dette, og fastslo at meningsinnholdet «å komme til syne» eller «å dukke opp» bare henspiller på varene og tjenestene på en suggestiv måte, slik at varemerkene var gyldig registrert. Videre kom lagmannsretten til at bruken av domenenavnene var egnet til å forveksles med varemerket APPEAR, og at domenebruken utgjorde et inngrep i varemerkeretten. Det ble utmålt erstatning tilsvarende rimelig lisensavgift, NOK 73 000.

I lagmannsretten argumenterte VCS blant annet med at norske varemerker er territorielt begrenset til Norge, og derfor ikke kan hindre domenebruk utenfor Norge. Lagmannsretten konkluderte imidlertid med at det var nødvendig og rimelig at VCS overførte domenenavnet appear.in til Appear TV. Det at appear.in var et indisk domenenavn ble ikke ansett å være til hinder for å pålegge slik overføring. Lagmannsretten la vekt på at det ikke var økonomiske eller praktiske forhold som gjorde overføring uforholdsmessig, og overføring ble ansett rimelig selv om domenebruken retter seg mot flere land enn Norge.

Det var dette siste spørsmålet som skulle bli gjenstand for vurdering i Høyesterett – om territorialprinsippet begrenser adgangen til å pålegge overføring av domenenavnet, og om overføring er nødvendig og rimelig.

For å hindre varemerkeinngrep, kan retten påby forebyggende tiltak «i den utstrekning det finnes rimelig», se varemerkeloven § 59. Valget mellom mulige tiltak skal skje ut fra en forholdsmessighetsvurdering, hvor man ser hen til «inngrepets alvorlighet, virkningene av tiltakene og tredjeparts interesser». Dersom det er bruk av et domenenavn som utgjør inngrepet, følger det av forarbeidene at sletting,

Sarah Wennberg Svendsen

eller overføring av domenenavnet til eieren av varemerket, er vanlige forebyggende tiltak.

Territorialprinsippet går ut på at varemerker må beskyttes i hver enkelt jurisdiksjon, slik at en norsk varemerkeregistrering bare gjelder i Norge. Høyesterett kom til at dette prinsippet ikke begrenset hvilke tiltak som kunne pålegges innehaver av appear.in. Norske varemerker må «sikres den beskyttelse som varemerkeloven gir anvisning på, også der krenkelsen skjer ved bruk av domenenavn på internett». Det ble blant annet uttalt at VCS ikke hadde påberopt noen nær forbindelse til India, der domenenavnet ble registrert. Gjennom det internasjonale avtaleverket ICANN forplikter domeneinnehaver seg til å akseptere

1 *HR-2019-2213-A.*

domstolsavgjørelser om sletting og overføring av domenenavn som innebærer krenkelse av andres rettigheter.

Selv om spørsmålet om domenebruken utgjorde et inngrep ble endelig avgjort i lagmannsretten, var det naturlig at Høyesterett gikk nærmere inn på *inngrepets art*. Dette fordi krenkelsens alvorlighetsgrad kommer inn som et moment når det skal vurderes om tiltaket er formålstjenlig, rimelig og forholdsmessig.

Nettaktiviteten må rette seg mot det norske markedet for å kunne konstatere et varemerkeinngrep. Dette er blant annet uttalt i læreboken til Lassen og Stenvik (*Kjennetegnsrett*, s. 294), som det refereres til i dommen. Situasjonen var ikke den at det bare *fantes* et indisk domenenavn som var tilgjengelig for brukere i Norge; domenenavnet APPEAR.in ble *aktivt brukt i markedsføringen* av VCS sine videokonferansetjenester, og markedsføringen var *rettet mot nordmenn*. Mellom 300 og 500 nordmenn besøkte daglig nettsiden APPEAR.in. Dette var ifølge Høyesterett et «vedvarende rettsstridig inngrep». Man kan tolke utfra dette at det er lettere å konstatere et varemerkeinngrep og at inngrepet anses mer alvorlig, når domenenavnet med utenlandsk toppdomene aktivt brukes i Norge.

Etter Lagmannsrettens dom endret VCS navn på videokonferansetjenesten fra appear.in til Whereby, som nå brukes globalt. Når noen gikk inn på nettsiden appear.in ble de gjort oppmerksom på navnekonflikten og navnebyttet. En link ledet brukerne til det nye nettstedet Whereby. Men etter Høyesteretts syn var dette ikke et tilstrekkelig tiltak for å stanse varemerkeinngrepet.

Ved vurderingen av formålstjenlighet, støttet Høyesterett seg til den tidligere avgjørelsen Rt. 2004 side 1414 om domenenavnet Volvoimport.no. Domenenavnet ble brukt av en uavhengig Volvo-importør uten tilknytning til Volvo, og det ble fastslått at brukeren av domenenavnet krenket varemerket Volvo. Det hjalp ikke at det fremgikk uttrykkelig av nettsiden at virksomheten ikke hadde noen kommersiell forbindelse til Volvo. Brukerne av nettsiden ble først gjort oppmerksom på dette *etter at de var ledet inn på nettsiden*. Da hadde den uavhengige aktøren allerede dratt urimelig nytte av det kjente Volvo-navnet.

I tråd med dette konkluderte Høyesterett med at navnebyttet til Whereby og linken til den nye nettsiden ikke var tilstrekkelig til å hindre fortsatte inngrep.

Høyesterett foretok så en konkret forholdsmessighetsvurdering, slik varemerkeloven § 59 krever. Tiltaket skal være proporsjonalt med inngrepets kommersielle effekt.

Overføring av domenet til Appear TV ville ifølge retten effektivt sette en stopper for videre varemerkeinngrep i Norge. Det ble fastslått at tiltaket om overføring ikke ville skape handelsbarrierer (stengsler mot «legitimate trade»), jf. TRIPS-avtalen artikkel 41. VCS kunne jo rett og slett skifte navn, og fortsette sin markedsføring under det nye navnet. Retten anerkjente at overføringen er en *ulempe* for VCS sin forretningsdrift, men det hindret dem ikke i å utøve sin virksomhet. Tredjeparts eventuelle komplikasjoner ved å gjennomføre allerede avtalte videokonferanser, medførte heller ikke at overføringen ble ansett som uforholdsmessig.

Dommen er enstemmig, og det synes ikke som at Høyesterett har vært i tvil om at det var riktig å pålegge overføring av domenet. Avslutningsvis formulerer retten seg slik: **Med mindre domenenavnet legges dødt, står valget i realiteten mellom overføring til rettighetshaver eller fortsatte varemerkeinngrep** (til slutt i avsnitt 64). Sagt på en annen måte; for å hindre varemerkeinngrep, må domenenavnet enten slettes eller overføres.

Hvor stor betydning hadde *den aktive bruken og markedsføringen* av domenenavnet for Høyesteretts resultat? Dersom det oppstår liknende tvister, hvor det utenlandske domenenavnet bare er tilgjengelig for nordmenn, uten å være aktivt brukt her, blir det interessant å se hva domstolen måtte komme til. Som påpekt i bloggen Immaterialrettstrollet sin omtale av dommen: «Skillet mellom når et domene er brukt på en slik måte at det retter seg mot det norske markedet, og når nettsiden bare er tilgjengelig for norske brukere, synes ikke skarpt.»

Jeg tolker dommen fra Høyesterett som en stadfestelse av varemerkers sterke posisjon i norsk rett.

Det kan ved første øyekast virke strengt at en nasjonal rettighet trumfer et internasjonalt domenenavn. Men ved nærmere ettertanke mener jeg at resultatet er det eneste rette. Selv om domenenavn kan ha en viktig rolle som unike adresser til nettsteder, og selv om de kan ha en viss kjennetegnsfunksjon, (jf. Høyesterettsavgjørelsen *Popcorn-Time.no*), er det varemerkene som står sterkest i en navnekonflikt. Domenenavn gir ikke navnerettigheter i seg selv.

Dersom Høyesterett hadde kommet til motsatt resultat, ville man kunne «snike seg til» bruk av en annens varemerke ved å tilføye et utenlandsk toppdomene bak navnet. Eier av et utenlandsk domenenavn ville kunne markedsføre sine varer og tjenester under dette domenenavnet i Norge, i konkurranse med innehaver av varemerket. Det ville ikke bare gripe inn i og utvanne varemerkeretten. Dersom et nærmest identisk domenenavn og varemerke ikke samles på samme hånd, ville det også skape forvirring blant forbrukerne i markedet.

Jeg vil avslutte med et tenkt eksempel. Hvis det norske domenenavnet tatata.no brukes aktivt i reklame i hele Europa og noen i Frankrike har registrert TATATA som et fransk, nasjonalt merke, kan den norske domenehaveren bli pålagt å gi domenet fra seg til den franske varemerkeeieren. Høyesterettsdommen viser hvor viktig det er å undersøke det varemerkerettslige spillerommet i markedet før man aktivt satser på et domenenavn i markedsføringen.

Sarah Wennberg Svendsen er advokatfullmektig i Oslo patentkontor og nemndsmedlem i Domeneklagenemnda.

Sanktionsdirektivets tillämplighet vid brott mot licensavtal

Av Carl Gleisner

Frågan om ett agerande utgör ett intrång i en immateriell rättighet eller endast betraktas som ett avtalsbrott är betydelsefull eftersom ett mer kraftfullt regelkomplex är tillämpligt vid intrång. Detta regelkomplex innefattar bland annat intrångsundersökning, förbudstalan och informationsföreläggande samt stadgar särskilda beräkningsgrunder för ersättningens storlek. I avgörandet IT Development mot Free Mobile (C-666/18) prövade EU-domstolen hur datorprogram- och sanktionsdirektivet ska tolkas då ett nationellt ersättningssystem ger regler om avtalsbrott företräde vid åtgärder vilka i sig kan utgöra både avtalsbrott och intrång.

Bakgrund

Målet vid den franska domstolen gällde ett ersättningsanspråk som en mjukvaruleverantör riktade mot en licenstagare som hade gjort ändringar i den upplåtna mjukvaran i strid med licensavtalet. Mjukvaruleverantören väckte talan om ersättning på den grunden att ändringarna utgjorde intrång i upphovsrätten. Talan ogillades dock av domstolen med hänvisning till att det påstådda intrånget uppenbart utgjorde bristande fullgörelse av de förpliktelser som licenstagaren underkastat sig genom att ingå licensavtalet. Domen överklagades och mjukvaruleverantören yrkade då ersättning på såväl inom- som utomobligatorisk grund.

Det noteras att franska domstolar sedan tidigare har gjort olika bedömningar av frågan om åtgärder i strid med gällande licensavtal ska anses utgöra avtalsbrott eller upphovsrättsintrång.

Begäran om förhandsavgörande och tolkningsfrågorna

Den hänskjutande domstolen upplyste om att fransk rätt innehåller en princip som innebär att skadeliden-

Carl Gleisner

de är hänvisade till att stödja anspråk på inomobligatorisk grund när denna grund konkurrerar med en utomobligatorisk grund, t.ex. intrång i upphovsrätten. I sin begäran om förhandsavgörande ställde domstolen åtskilliga frågor om olika typer av åtgärder skulle utgöra intrång eller avtalsbrott. Med tanke på de gränsdragningsproblem som uppstår när ett agerande ska klassificeras som intrång eller endast avtalsbrott hade det varit intressant om EU-domstolen svarat på dessa frågor.

EU-domstolen omformulerade dock de ställda frågorna till att enbart avse den mer EU-rättsligt relevanta frågan om huruvida sanktions- respektive datorprogramdirektivet[1] ska tolkas så, att ett brott mot en klausul i ett licensavtal för ett datorprogram som [avser] immateriella rättigheter omfattas av begreppet ”immaterialrättsintrång”, i den mening som avses i sanktionsdirektivet, och att rättighetsinnehavaren följaktligen måste kunna åtnjuta de garantier som föreskrivs i sanktionsdirektivet, oberoende av vilket ersättningssystem som är tillämpligt enligt nationell rätt.

EU-domstolens avgörande

Domstolen konstaterade inledningsvis att intrång enligt datorprogramdirektivet inte förutsätter förekomsten av något brott mot ett

1 Direktiv (EG) 2004/48 om säkerställande av skyddet för immateriella rättigheter och direktiv (EG) 2009/24 om rättsligt skydd för datorprogram.

licensavtal.[2] Såvitt gällde sanktionsdirektivet fann domstolen att direktivet enligt artikel 2(1) är tillämpligt vid ”varje intrång i immateriella rättigheter” och att det är uppenbart av lydelsen att direktivet även måste omfatta intrång som följer av ett avtalsbrott som härrör ur ett brott mot en avtalsklausul som är hänförlig till utnyttjandet av en immateriell rättighet.[3] Domstolen fann att slutsatserna rörande sanktionsdirektivet bekräftades av såväl ändamålen med direktivet som det sammanhang som artikel 2(1) ingår i.[4]

Slutligen uttalade domstolen att medan sanktionsdirektivet fastslår de åtgärder, förfaranden och sanktioner som medlemsstaterna ska tillförsäkra rättighetsinnehavare, så föreskrivs inte närmre hur detta ska ske eller vilket ersättningssystem som ska tillämpas.[5] Medlemsstaterna är kompetenta att närmre reglera utformningen av ersättningssystemet, under förutsättning att det inte på något sätt hindrar rättighetsinnehavare från ett effektivt skydd för sina immateriella rättigheter enligt datorprogramdirektivet och sanktionsdirektivet.[6] Det åligger medlemsstaterna att tolka sina ersättningssystem direktivkonformt i den utsträckning det är möjligt. Baserat på franska statens upplysningar om den nationella rätten bedömde EU-domstolen att en direktivkonform tolkning skulle vara möjlig.[7]

Kommentar

Det kan noteras att den svenska skadeståndsrätten, i likhet med den franska, åtminstone tidigare har innefattat en allmän huvudregel där en skadelidande är hänvisad till den inomobligatoriska grunden i handelse av konkurrerande ansvarsgrunder. Rättsläget är samtidigt under utveckling och det är oklart vad som kan sägas gälla i allmänhet.[8]

Inom upphovsrätten gäller däremot redan sedan tidigare att bristande fullgörelse av licensvillkor som rör själva förfoganderätten utgör upphovsrättsintrång, vilket medför rätt till skälig ersättning och ersättning för skada enligt upphovsrättslagen. Brott mot avtalsvillkor som mer indirekt rör förfoganderätten, exempelvis sen betalning av royalty, anses inte utgöra intrång och kan därför bara grunda skadeståndsansvar för avtalsbrott.[9] De gränsdragningsproblem som finns på detta område kvarstår trots avgörandet i *IT Development mot Free Mobile*. Det svenska nationella ersättningssystemet vid samtidigt upphovsrättsintrång och licensavtalsbrott är alltså som sådant förenligt med unionsrätten.

Carl Gleisner är biträdande jurist på Wesslau Söderqvist Advokatbyrå i Stockholm

2 Punkt 32-34.
3 Punkt 36.
4 Punkt 37.
5 Punkt 43.
6 Punkt 46.
7 Punkt 47-48f.
8 Hellner och Radetzki, Skadeståndsrätt (10 uppl.), 4.4, med där gjorda hänvisningar.
9 Olsson, Copyright (10A uppl.), kapitel 8; Bengtsson och Lyxell, Åtgärder vid immaterialrättsintrång (2006), s. 50.

Personvern og tiltak mot hvitvasking: – Særlig om screening mot sanksjonslister

Av Christopher Sparre–Enger Clausen og Hugo-A. B. Munthe-Kaas

1 Introduksjon

Den norske personopplysningsloven og GDPR var ikke de eneste regelverkene som trådte i kraft i 2018. I 2018 trådte også ny lov om tiltak mot hvitvasking og terrorfinansiering («hvitvaskingsloven») av 01.06.2018 nr. 23. med forskrift av 14.9.2018 nr. 1324 i kraft. Hvitvaskingsloven gjennomfører store deler av EUs fjerde anti-hvitvaskingsdirektiv, og både endrer og presiserer tidligere lovverk fra 2009 på dette området.

Hvitvaskingsloven gjelder for «rapporteringspliktige» etablert i Norge, inkludert filialer av utenlandske foretak.[1] Etter hvitvaskingsloven § 4 vil blant annet banker, kredittforetak, finansieringsforetak, verdipapirforetak og forsikringsforetak være rapporteringspliktige.[2] Hvitvaskingsloven pålegger rapporteringspliktige en rekke plikter. Rapporteringspliktige er blant annet forpliktet til å (i) ha rutiner for å håndtere identifisert risiko og etterleve kav i hvitvaskingslovgivningen, (ii) gjennomføre kundetiltak og løpende oppfølging, (iii) undersøke forhold som kan indikere at midler blir benyttet til hvitvasking eller terrorfinansiering, samt (iv) rapportere forhold som gir grunnlag for mistanke om hvitvasking eller terrorfinansiering til Økokrim.[3] For å etterleve de til dels omfattende kravene etter hvitvaskingsloven, benytter mange rapporteringspliktige digitale støtteverktøy og -overvåkingssystemer.[4] Disse støtteverktøyene benyttes blant annet til å utføre elektroniske sjekker («screening») av om kunder (og andre) er oppført på sanksjonslister.

Christopher Sparre-Enger Clausen

Hugo-A. B. Munthe-Kaas

På samme måte som personvernlovgivningen, verner hvitvaskingsloven om viktige samfunnsmessige interesser:

> *«Tiltakene i loven skal beskytte det finansielle og økonomiske systemet samt samfunnet som helhet ved å forebygge og avdekke at rapporteringspliktige brukes eller forsøkes brukt som ledd i hvitvasking eller terrorfinansiering»*[5]

Med stadig strengere krav til tiltak mot blant annet hvitvasking pålegges rapporteringspliktige å gjennomføre til dels omfattende undersøkelser av kunder og andre som er involvert i finansielle transaksjoner. Dette innebærer i praksis at store mengder personopplysninger blir

1 Jf. hvitvaskingsloven § 3 første ledd, jf. § 4.

2 Jf. hvitvaskingsloven § 4, jf. § 2 første ledd bokstav c.

3 Jf. hvitvaskingsloven § 8, kapittel 4, samt §§ 25 og 26.

4 Banker, kredittforetak og finansieringsforetak plikter å ha elektroniske overvåkingssystemer for å avdekke forhold som kan indikere hvitvasking og terrorfinansiering, jf. hvitvaskingsloven § 38. Disse foretakene håndterer store transaksjonsvolumer og vil vanskelig klare å overvåke disse transaksjonene uten elektroniske systemer.

5 Jf. hvitvaskingsloven § 1 andre ledd.

behandlet for slike formål. Personopplysningsloven og GDPR setter på sin strenge regler for hvordan personopplysninger behandles, og brudd på dette lovverket kan få alvorlige konsekvenser gjennom blant annet bøter og tap av renommé.

I denne artikkelen vil vi belyse og kommentere enkelte utfordringer og problemstillinger rapporteringspliktige møter når de forsøker å etterleve både personvernlovgivningen, hvitvaskingsloven og internasjonal sanksjonslovgivning. Vi vil i denne sammenheng særlig fokusere på rapporteringspliktiges screening mot sanksjonslister.

2 Inneholder sanksjonslister særlige kategorier av personopplysninger og personopplysninger om straffbare forhold?

Sanksjoner og sanksjonslister er virkemidler i internasjonal politikk for å få individer, selskaper, grupper eller stater til å endre politikk eller handlemåte.[6] I Norge er FNs og EUs sanksjonslister i stor grad gjennomført gjennom Utenriksdepartementets forskriftsverk.[7]

Det vil kunne være ulike årsaker til at individer blir sanksjonert og oppført på en sanksjonsliste av FN, EU eller Norge. En viktig problemstilling i denne sammenheng fra et personvernperspektiv er om listeføringen av det aktuelle individet også gir informasjon om «*rasemessig eller etnisk opprinnelse, politisk oppfatning, religion eller filosofisk overbevisning*», jf. GDPR artikkel 9 (1), eller informasjon om «*straffedommer, lovovertredelser eller tilknyttede sikkerhetstiltak*», jf. GDPR artikkel 10. Bakgrunnen for dette er at behandling av særlige kategorier av personopplysninger eller personopplysninger om straffbare forhold krever særskilt hjemmel i henholdsvis GDPR artikkel 9 (2) og artikkel 10.

Noen listeføringer på slike sanksjonslister vil ikke gi informasjon av denne typen som omtales i GDPR artikkel 9 (1) og GDPR artikkel 10. Listeføringer kan imidlertid noen ganger inneholde informasjon om «*straffedommer*, *lovovertredelser eller tilknyttede sikkerhetstiltak*». Det kan også diskuteres om for eksempel listeføringer begrunnet med tilhørighet i visse terrorgrupper vil anses som personopplysninger om «*politisk oppfatning*». Dette vil i så fall innebære at man etter GDPR må ha hjemmel i et av unntakene i artikkel 9 (2) for å kunne behandle denne typen opplysninger.

En slik hjemmel vil man også ha for screening av norske og europeiske sanksjonslister hjemlet i norsk rett eller i EU retten (som blant annet også implementerer FNs sanksjonslister innenfor sine respektive jurisdiksjoner), jf. GDPR artikkel 10, samt GDPR artikkel 9 (2) litra g som bestemmer at behandling av særlige kategori av personopplysninger kan skje når:

> *«Behandlingen er nødvendig av hensyn til viktige allmenne interesser, på grunnlag av unionsretten eller medlemsstatenes nasjonale rett som skal stå i et rimelig forhold til det mål som søkes oppnådd, være forenlig med det grunnleggende innholdet i retten til vern av personopplysninger og sikre egnede og særlige tiltak for å verne den registrertes grunnleggende rettigheter og interesser.»*

Hvitvaskingsforskriften § 6-1 gir også rapporteringspliktige hjemmel til å behandle sensitive personopplysninger «når dette er nødvendig for å overholde plikter i hvitvaskingsloven eller forskrift med hjemmel i loven».

Det er imidlertid mer uklart om disse hjemlene også vil kunne bli benyttet for screening mot amerikanske eller andre tredjelands sanksjonslister, i den grad disse skulle inneholde personopplysninger som omtales i GDPR artikkel 9 (1) og GDPR artikkel 10.

En særlig utfordring for norske rapporteringspliktige (og andre) er at enkelte slike sanksjonslister, slik som de amerikanske, kan ha ekstraterritoriell virkning. Videre er mange rapporteringspliktige avhengig av å ikke bryte nettopp amerikanske sanksjoner for å kunne gjøre transaksjoner i amerikanske dollar, samt å handle med amerikanske aktører.

Hvitvaskingsloven § 24 krever at rapporteringspliktige skal løpende følge opp kundeforhold. Dette skal blant annet omfatte «*å overvåke at transaksjoner som utføres i kundeforholdet, er i samsvar med den rapporteringspliktiges innhentede opplysninger om kunden, kundens virksomhet og risikoprofil, midlenes opprinnelse og kundeforholdets formål og tilsiktede art.*» I følge Finanstilsynet innebærer plikten også å screene mot FN og EUs sanksjonslister.[8] Muligens kan man argumentere for at dette også må gjelde tredjelands sanksjonslister i den grad dette kan gi informasjon om risikobildet ved en person. Muligens vil man også kunne hjemle søk i tredjelands sanksjonslister gjennom aktsomhetsplikten som oppstilles i blant annet straffeloven § 340 som forbyr uaktsom hvitvasking. Noen selskaper har også søkt Datatilsynet om særskilt tillatelse til å behandle særlige kategorier av personopplysninger og personopplysninger om straffbare forhold for å utføre integritetsundersøkelser («Integrity Due Diligence» – «IDD»).[9] Erfaringsmessig vil slike IDD-tillatelser også hjemle screening mot amerikanske og andre tredjelands sanksjonslister.

6 Utenriksdepartementet og Finanstilsynet. «Finansielle sanksjoner: Veiledning om frysbestemmelsene.» 16. April 2018.

7 I Norge betegnes EUs «sanksjoner» vanligvis som «restriktive tiltak». Vi vil for enkelthetens skyld også omtale disse «restriktive tiltakene» som «sanksjoner».

8 Jf. punkt 4.11 i Finanstilsynets veileder til hvitvaskingsloven, publisert 31. mai 2019 (korrigert 27. juni 2019).

9 Jf. § 6 fjerde ledd i forskrift av 29.03.2019 nr. 401. Se også personopplysningsloven § 7, jf. § 10.

I praksis er det uansett ingen tvil om at rapporteringspliktige (og andre) i Norge og i EU screener sine kunder og transaksjoner opp mot amerikanske og andre lands sanksjonslister, da nedsiden ved å ikke gjøre dette, for eksempel vil kunne være at man i verste fall risikerer å ikke lenger kunne gjøre transaksjoner i amerikanske dollar, eller på annen måte bli utestengt fra markeder i andre tredjeland. Videre er det liten grunn til å tro at GDPR har hatt til hensikt å begrense norske selskapers adgang til å operere i utenlandske markeder på denne måten, eller til å gjøre aktsomme valg i lys av norsk straffelovs hvitvaskingsbestemmelser.

Forholdet mellom hvitvaskingslovens forpliktelser og personvernlovgivningen drøftes grundig i det siste høringsnotatet datert 1. november 2019 fra Finanstilsynet knyttet til gjennomføring av EUs femte hvitvaskingsdirektiv mv.[10] Problemstillingen om screening mot tredjestaters sanksjonslister berøres imidlertid ikke særskilt. Uklarheten rundt hjemmelssituasjonen for screening av individer mot tredjestaters sanksjonslister, samt den avgjørende betydningen slik screening har for at norske rapporteringspliktige (og andre bedrifter) skal kunne operere i et internasjonalt marked, taler imidlertid klart for at det bør foretas en klargjøring på dette området. Av hensyn til både rapporteringspliktiges, norsk næringslivs og registrertes forutberegnelighet bør en slik presisering skje i lovverket og ikke håndteres gjennom Datatilsynets adgang til å gi IDD-tillatelser.

10 Høringsnotat – forslag til endringer i hvitvaskingsloven og hvitvaskingsforskriften, 01.11.2019.

Christopher leder Thommessens faggruppe for Teknologi og Personvern. Christopher jobber hovedsakelig med teknologikontrakter og personvern.

Hugo leder Thommessens kompetansegruppe innen compliance og granskning og har bred juridisk erfaring innen corporate compliance og tvisteløsning. Hugo bistår klienter særlig med spørsmål knyttet til internasjonal handel, internasjonale sanksjoner, anti-korrupsjon, anti-hvitvasking og eksportkontroll.

Halvor Manshaus

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

Spørsmål om behandlingsgrunnlag – omtaler av helsepersonell på *legelisten.no*

For å ta en god beslutning er det nødvendig med relevant informasjon. På internett florerer det med tjenester som tilbyr kjøpshjelp, ofte i så stor grad at det i praksis kan bli vanskelig å ta den endelige beslutningen. Det kan rett og slett bli for mye informasjon. Enten man skal kjøpe en mobiltelefon eller en vaskemaskin så har man tilgang til et nærmest endeløst hav av vurderinger, omtaler og tester. Dette gjelder ikke bare varer, men også tjenester av ulike slag. Et eksempel er søkemotoren Google, som i resultatlisten viser relevante virksomheter med omtaler fra tidligere kunder. Det eksisterer også mer spesialiserte oversikter, slik som den norske tjenesten *legelisten.no* som gir evalueringer av norsk helsepersonell.

Oslo tingrett avsa nylig dom i saken om *legelisten.no*, en kommersiell nettbasert tjeneste som oppfordrer pasienter til å dele sine erfaringer etter behandling hos helsepersonell. Pasienter som vurderer besøk hos samme behandler kan da på forhånd gjøre seg kjent med omtalen og vurderingen som foreligger på *legelisten.no*. På denne bakgrunn kan det gjøres et informert valg om hvilken person man ønsker å gå til for behandling.

Tilgang til omtalene og vurdering av den enkelte behandler ligger åpent tilgjengelig på tjenesten. I skrivende stund tilbys det søk på tannlege, kiropraktor, gynekolog, psykolog og fastlege under mottoet «hjelper deg å finne gode leger». Den enkelte vurdering bygger på et karaktersystem der man innenfor hver kategori kan gi 1 til 5 stjerner. De aktuelle kategoriene er tilgjengelighet, tillit og kommunikasjon, service og en overordnet samlet vurdering. For hver enkelt kategori kan det også legges til en utfyllende kommentar i eget tekstfelt.

Det fremgår av dommen at *legelisten.no* har gjennomgått en gradvis utvikling og modning frem mot den løsningen som eksisterer i dag. Når det i dag legges inn en vurdering mottar brukeren en e-post som ber om bekreftelse på innlegget. Deretter går vurderingen til intern vurdering hos *legelisten.no* før den eventuelt publiseres. Helsepersonell kan ikke på generelt grunnlag reservere seg mot omtale på tjenesten, men der man kan dokumentere «spesielt tungtveiende grunner» vil det blir vurdert særskilt. I dommen er det vist til at det er gjort 41 slike reservasjoner der helsepersonell er holdt utenfor tjenesten.

Det er interessant å se på dommens beskrivelse av trafikken på denne tjenesten. Det skal være publisert over 84000 vurderinger, av totalt 119000 innsendte forslag. Det er videre vist til opplysninger fra *legelisten.no* om at nettsiden har 3,5 millioner besøk årlig, med en samlet brukermasse på om lag 2 millioner personer.

Den kommersielle delen av tjenesten bygger på en abonnementsordning. Det koster 95 kroner for et abonnement som varer 3 måneder for deretter å opphøre automatisk. Så lenge abonnementet er aktivt får man da tilgang til blant annet sjekk av reaksjoner fra Helsetilsynet overfor konkret behandler og varsling ved ny vurdering av samme behandler.

Legeforeningen reagerte på tjenesten allerede ved oppstart, og Datatilsynet har vært inne i bildet ved flere anledninger. Dommen omhandler punkt 1 i vedtak fra Datatilsynet av 8. november 2017, som går på hvorvidt tjenesten har behandlingsgrunnlag etter personopplysningsloven § 8 litra f. I vedta-

ket ble legelisten.no pålagt å innføre en egen reservasjonsadgang, ettersom det ble lagt til grunn at tjenesten ellers ville mangle behandlingsgrunnlag.

Som en konsekvens av vedtaket mottok legelisten.no henvendelser fra 1100 leger om reservasjon mot tjenesten. Vedtaket fra Datatilsynet ble imidlertid påklaget til Personvernnemnda, og tilsynet ga på denne bakgrunn vedtaket oppsettende virkning. Legelisten.no innførte således ikke noen reservasjonsadgang etter det opprinnelige vedtaket.

Da Personvernnemnda skulle behandle saken var i mellomtiden personvernforordningen GDPR trådt i kraft, og saken ble dermed løst under GDPR artikkel 6 nr. 1. Bestemmelsen gjør behandling av personopplysninger lovlig dersom ett av de etterfølgende vilkår er oppfylt. Nemnda viste til litra f og vilkåret om at:

> *«behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn»*

Nemnda konkluderte med at dette var tilstrekkelig hjemmel for opplysningene som ble behandlet gjennom legelisten.no, og fant det ikke påkrevd å pålegge noen generell reservasjonsadgang. Legeforeningen brakte saken videre til Oslo tingrett, og krevde dom for at dette punktet i vedtaket måtte bli kjent ugyldig. Spørsmålet for tingretten ble dermed hvorvidt legelisten.no hadde behandlingsgrunnlag etter GDPR artikkel 6 nr. 1 litra f, samt om det var nødvendig å innføre en generell adgang til å reservere seg mot omtale på tjenesten.

Tingretten gjør innledningsvis en viktig avgrensning ved sin vurdering, i det GDPR artikkel 21 nr. 1 ikke får anvendelse i saken. Bestemmelsen gir *«den registrerte»* rett til å protestere mot behandling av personopplysninger med hjemmel i artikkel 6 nr. 1 litra f. Tingretten viser til at en slik protest må begrunnes i *«vedkommendes særlige situasjon»*, altså at det kreves en konkret og individualisert vurdering. Det heter i dommen at det er uklart om Legeforeningen har påberopt seg artikkel 21 direkte, men retten finner at dette uansett ikke er avgjørende ettersom artikkel 6 nr. 1 litra f gir en generell hjemmel for behandling av gruppen av helsepersonell som sådan. Som omtalt ovenfor var det for øvrig 41 personer som faktisk hadde blitt fjernet fra tjenesten grunnet *«spesielt tungtveiende grunner»*.

I saken var det anført fra Legeforeningen at artikkel 6 nr. 1 litra f utgjorde et svakt behandlingsgrunnlag, mens Staten inntok et motsatt standpunkt. Det er alltid interessant å se hvordan domstolene behandler slike spørsmål, som i realiteten går på lovtolkningen. Retten uttaler at det avgjørende må være den konkrete vurderingen av om behandlingsgrunnlaget er tilstrekkelig. En veiledning knyttet opp mot bestemmelsens rekkevidde må altså leses ut av rettens etterfølgende drøftelse, som tar utgangspunkt i interesseavveiningen mellom hensynet til den behandlingsansvarliges formål satt opp mot hensynet til den registrerte.

Retten berører flere interessante spørsmål i den videre drøftelsen. Det nevnes blant annet at anonymitet for pasientene som skriver omtaler er nødvendig, ettersom krav til identifikasjon ville kunne medføre at det ikke i samme grad ble skrevet omtaler. Dette omtales gjerne som en *«chilling effect»*. Videre legger retten til grunn at en generell reservasjonsrett i praksis ville innebære at legelisten.no mistet sin informasjonsverdi, og peker på at Datatilsynets vedtak om reservasjonsrett medførte at 1100 helsepersonell tok kontakt for å reservere seg.

Retten gir klart uttrykk for at det avgjørende momentet i totalvurderingen er pasientenes ytringsfrihet. I denne forbindelse viser retten også til utformingen av legelisten.no, som har innført tiltak for å bedre kvaliteten på omtalene. Det vises her blant annet til at omtalene er gjenstand for kvalitetskontroll før publisering på tjenesten, samt at det ved særlige behov er gitt reservasjon for helsepersonell etter en behovsprøving.

> Samtidig gjelder omtalene ikke legens privatliv, men profesjonsrollen som helseutøver, slik at hensynet til legen må vurderes som en profesjonell part i en offentlig rolle

Legeforeningen hadde en interessant anførsel knyttet til det som i dommen betegnes som *«portvokterrollen»*. Begrepet sikter til legens rolle som forvalter av felles samfunnsressurser som kun tildeles etter en behovsprøving. Det kan tenkes at en lege som frykter negativ omtale på legelisten.no vil kunne ta beslutninger overfor pasienten som ikke kan forsvares medisinsk. Eksempler på dette kan være at legen skriver ut en sykemelding eller skriver ut resept på medisiner som pasienten ikke skulle ha fått etter en objektiv faglig vurdering. På sikt vil strenge leger som håndhever en faglig etablert norm eller terskel motta flere negative omtaler enn andre leger, og miste pasienter. Legen kan heller ikke velge bort en pasient som gir fortløpende negative omtaler, ettersom legen har plikt til å yte medisinsk bistand. Retten mener slike forhold ikke bare er konkurransemessige betraktninger, men også har betydning for interesseavveiningen fordi det for den enkelte lege vil

kunne oppleves som en krenkelse av personvernet. Samtidig gjelder omtalene ikke legens privatliv, men profesjonsrollen som helseutøver, slik at hensynet til legen må vurderes som en profesjonell part i en offentlig rolle.

Retten drøfter også hvilken «informasjonsverdi» som ligger i tjenesten fra legelisten.no. På dette punktet legger retten vekt på en uttalelse fra Forbrukerrådet i anledning saken, og konkluderer med at tjenesten har en ikke ubetydelig informasjonsverdi:

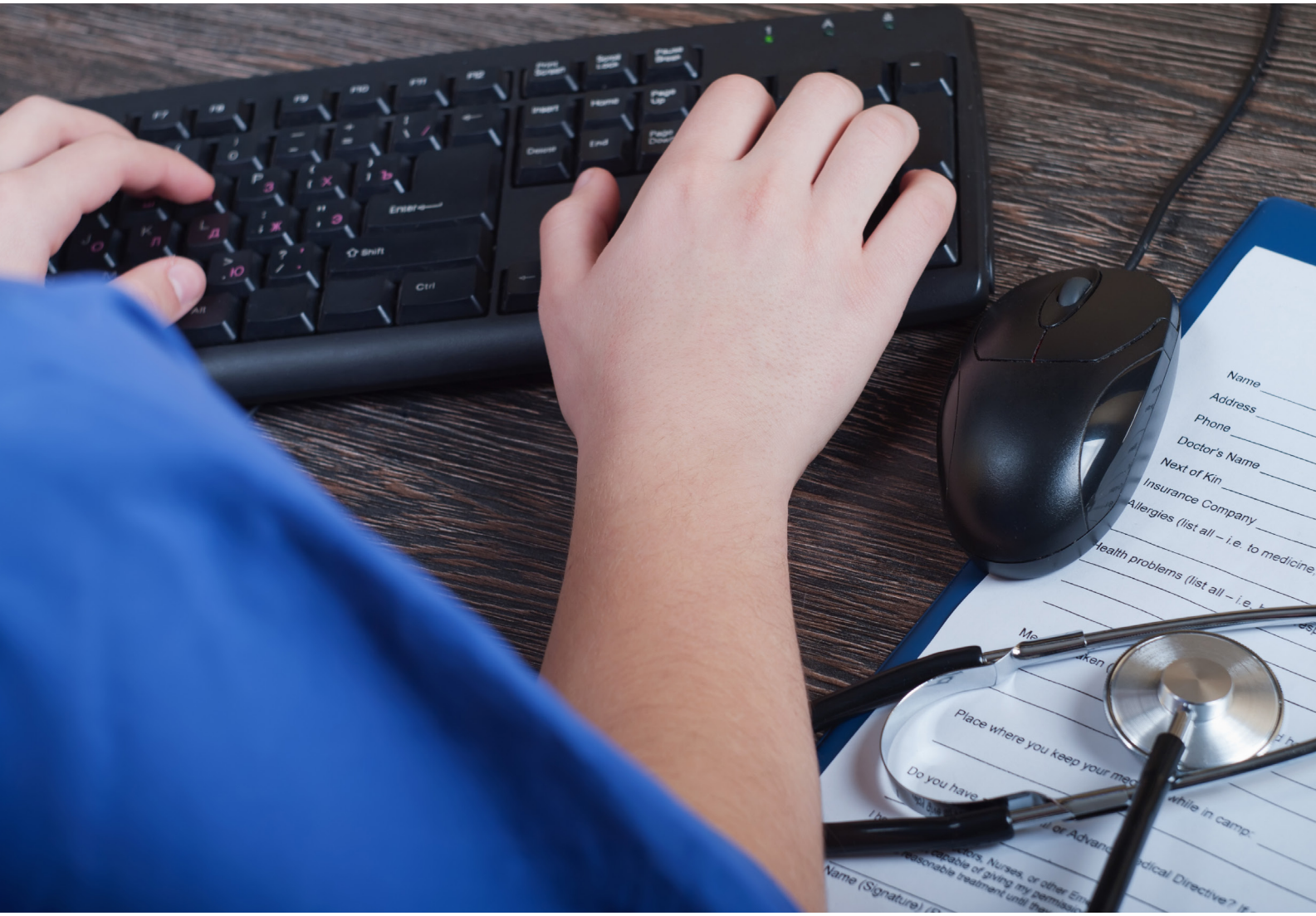
«Ved interessevurderingen legger derfor retten også til grunn at Legelisten har informasjonsverdi og at den ikke er ubetydelig. Retten viser her til blant annet Forbrukerrådets innlegg til Personvernnemnda datert 26. januar 2018 som blant annet uttaler «Vi mener det foreligger en sterk allmenninteresse i formidlingen av slike opplysninger». Forbrukerrådet mener denne type informasjon fortjener «et sterkt vern», og at forbrukere har stor forståelse for hva slike vurderingssider er, med sine styrker og svakheter. Dette er i tillegg det eneste stedet hvor denne type informasjon er tilgjengelig, som gir informasjonen ytterligere verdi.»

Det fremgår av dommen at et underliggende vurderingstema har vært graden av seriøsitet knyttet til tjenesten. Retten legger altså betydelig vekt på at det er innført tiltak som bidrar til å fjerne useriøse innlegg og at tjenesten anses å ha allmenninteresse. I vurderingen opp mot personvernet viser retten også til at det i det enkelte forhold mellom pasient og lege normalt vil være pasienten som er den svake part:

«Retten ser de personvernulemper som er fremhevet, men mener at de allmenne interessene som er nevnt ovenfor her må veie tyngre. De ytringene som pasientene ønsker å komme med, og som ligger innenfor retningslinjene til Legelisten, er ytringer helsepersonell må tåle. Ved vurderingen er det sentralt at helsepersonellet er den profesjonelle og sterke part i forholdet mellom behandler og pasient.»

Retten konkluderte i dommen med at legelisten.no hadde behandlingsgrunnlag for å samle inn og publisere subjektive vurderinger av helsepersonell etter artikkel 6 nr. 1 litra f. Vedtaket fra Personvernnemnda ble med andre ord ikke funnet ugyldig.

Dommen er anket til lagmannsretten.



Gorrissen Federspiel

Tue Goldschmieding

Det danske datatilsyn udsteder nye retningslinjer for behandlingsgrundlag efter databeskyttelsesforordningens artikel 9, stk. 1

Det danske datatilsyn ('Datatilsynet') udstedte den 7. november 2019 nye retningslinjer for behandlingen af følsomme personoplysninger jf. Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen'), artikel 9.

Datatilsynet fastslår, at dataansvarlige, der behandler følsomme personoplysninger omfattet af databeskyttelsesforordningens artikel 9, stk. 1, efter Datatilsynet opfattelse skal have hjemmel både i databeskyttelsesforordningens artikel 9, stk. 2 og artikel 6.

Datatilsynets nye retningslinjer er udstedt i forbindelse med en holdningsændring fra Det Europæiske Databeskyttelsesråd ('EDPB).

Dog har Datatilsynet vurderet, at såfremt en af undtagelserne i databeskyttelsesforordningens artikel 9, stk. 2 er opfyldt, vil betingelserne i databeskyttelsesforordningens artikel 6 sædvanligvis ligeledes være opfyldt. Ændringen får derfor som udgangspunkt ikke den store praktiske betydning, men databehandlere bør dog overveje, om de ligeledes har gyldig hjemmel i artikel 6, forud for behandlingen af følsomme personoplysninger.

Datatilsynet har vurderet at ændringen hovedsageligt vil have betydning for vurderingen af indsigelser efter databeskyttelsesforordningens artikel 21.

Læs hele udtalelsen her:

https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2019/nov/behandling-af-foelsomme-oplysninger/

EU-Kommissionen godkender tredje gennemgang af Privacy Shield-ordningen

En af EU-Kommissionens opgaver er at føre løbende kontrol med Privacy Shield-ordningen, jf. Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april ('databeskyttelsesforordningens') artikel 45, stk. 6. På baggrund heraf har EU-kommissionen den 23. oktober 2019 udgivet deres tredje årlige gennemgang af Privacy Shield-ordningen.

EU-Kommissionen udstedte i forbindelse hermed en rapport baseret på møder med repræsentanter for alle de amerikanske regeringsafdelinger med ansvar for Privacy Shield, og med input fra flere interessenter, herunder virksomheder, NGO'er samt repræsentanter fra EU's uafhængige databeskyttelsesmyndigheder.

Rapporten fastslår, at USA fortsat sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger, som overføres under Privacy Shield-ordningen. Gennemgangen af Privacy Shield-ordningen fokuserede på erfaringerne fra den praktiske implementering samt den daglige brug af Privacy Shield-ordningen.

Følgende forbedringer i Privacy Shield-ordningen forhold til forrige rapport blev fremhævet: (i) at det amerikanske handelsministerium i højere grad end tidligere sikrer det nødvendige tilsyn på en mere systematisk måde, (ii) at håndhævelsestiltag er forbedret, (iii) at et stigende antal EU-borgere anvender deres rettigheder under Privacy Shield-ordningen, (iv) at de relevante klagemuligheder er velfungerende, og (v) at der er udnævnt en fast ombudsperson samt at de sidste to ledige stillinger i Privacy and Civil Liberties Oversight Board ('Tilsynsrådet'). Tilsynsrådet er en uafhængig myndighed i USA hvis opgave delvis er rådgivende og delvis tilsynsførende med relevant retsområder, herunder databeskyttelse, er blevet udfyldt.

EU-Kommissionen anfører ligeledes i rapporten, at de i forbindelse med EU-Domstolens kommende domsafsigelse i *Schrems-II-dommen*, vil gennemgå dommen og dommens eventuelle konsekvenser for Privacy Shield-ordningen.

Læs hele rapporten her:

https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6134

EU-Domstolen fastslår, at brug af cookies forudsætter en aktiv handling

EU-Domstolen afsagde den 1. oktober 2019 dom i sagen C637/17, mellem Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV ('Verbraucherzentrale') og Planet49 GmbH ('Planet49').

Sagen omhandlende besvarelsen af to præjudicielle spørgsmål, herunder hvordan et gyldigt samtykke kan afgives i forbindelse med brug

af cookies, samt omfanget af hjemmesideindehaverens oplysningspligt ved brug af cookies.

Planet49 havde afholdt en konkurrence på en af deres hjemmesider, hvoraf der var to afkrydsningsfelter. Det første afkrydsningsfelt var ikke forudafkrydset og omhandlede samtykke til markedsføring. Det andet afkrydsningsfelt var derimod forudafkrydset og omhandlede samtykke til indsamling af cookies.

Såfremt brugeren ikke ønskede, at der skulle afgives samtykke til indsamlingen, skulle brugeren foretage en aktiv fravælgelse af samtykket. EU-Domstolen blev derfor spurgt om et forudafkrydset samtykke kunne anses for at være et aktivt samtykke, både i henhold til Europa-Parlamentet og Rådets Direktivets 2002/58/EF af 12. juli 2002 ('E-databeskyttelsesdirektivet') artikel 5, stk. 3 og Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april ('Databeskyttelsesforordningen') artikel 6, stk. 1 litra a.

EU-Domstolen lagde til grund, at et gyldigt samtykke indebar en frivillig, specifik, informeret og utvetydig viljestilkendegivelse, hvor der stilles krav om aktiv adfærd i denne henseende.

EU-Domstolen bemærkede, at indretningen af tilmeldingen ikke muliggjorde en objektiv mulighed for at fastslå, om brugeren faktisk havde afgivet sit samtykke aktivt, eller om brugeren havde læst den ledsagede information eller havde misforstået indholdet.

På baggrund heraf anførte EU-Domstolen, at samtykket ikke kunne anses for gyldigt afgivet, da dette må betinges af, at der faktisk var afgivet et aktivt samtykke. EU-Domstolen fastslog således, at gyldigt samtykke til brug af cookies ikke kan bygge på en opt-out model.

Herefter behandlede EU-Domstolen det andet spørgsmål, som relaterede sig til hjemmesideindehaveres pligt til at tilvejebringe fyldestgørende oplysninger for brugeren ved brug af cookies. Spørgsmålet angik, hvorvidt hjemmesideindehaverens oplysningspligt indebar, at hjemmesideindehaveren skal oplyse om en cookies funktionsvarighed, og om tredjeparters mulighed for at få adgang til disse cookies.

EU-Domstolen fastslog, at fyldestgørende oplysninger indebærer, at brugeren er i stand til, uden besvær, at bestemme følgerne af det eventuelle samtykke, og at oplysninger er tilstrækkeligt let forståelige og detaljerede til, at brugeren kan forstå den anvendte cookiefunktionalitet. EU-Domstolen konkluderede derfor, at en cookies funktionsvarighed og tredjeparters mulighed for at få adgang til den pågældende cookie er blandt de klare og fyldestgørende oplysninger, som hjemmesideindehaverne er forpligtet til oplyse om, når de benytter sig af cookies.

EU-Domstolens afgørelse vil få stor betydning for de hjemmesideindehavere, der har indrettet deres hjemmesider på en sådan måde, hvor en opt-out model for samtykke til cookies benyttes. Løsningen med forudafkrydsede felter kan således ikke anvendes længere.

Læse hele dommen her:
http://curia.europa.eu/juris/document/document_print.jsf?docid=218462&text=&dir=&doclang=DA&part=1&occ=first&mode=req&pageIndex=0&cid=1710106

Datatilsynet ændrer praksis angående offentliggørelse af billeder på internettet

Den 26. september 2019 ændrede det danske datatilsyn ('Datatilsynet') deres praksis angående offentliggørelse af billeder af identificerbare personer på internettet, uden personens samtykke.

Datatilsynets hidtidige praksis har været, at vurderingen af, om der kan ske offentliggørelse uden samtykke, afhang af, hvorvidt billedet var et situationsbillede eller et portrætbillede.

Dette udgangspunkt forlader Datatilsynet med udtalelsen, og fremadrettet vil Datatilsynet basere vurderingen på en helhedsvurdering af billedet og formålet med offentliggørelsen.

Den dataansvarlige skal sikre, at der foreligger en gyldig hjemmel til at behandle billedet. Behandlingen kan eksempelvis tage udgangspunkt i interesseafvejningsreglen i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') artikel 6, stk. 1, litra f.

Ved benyttelsen af interesseafvejningsreglen skal der foretages en vurdering af, om der foreligger en legitim interesse, og om denne interesse overstiger hensynene til den registrerede i at behandlingen ikke sker. Ifølge Datatilsynet indeholder vurderingen blandt andet følgende elementer: karakteren af billedet, hvor og hvorfor billedet er taget, i hvilken sammenhæng billedet er taget, samt formålet med offentliggørelsen. Alderen af personerne på billedet, vil ligeledes indgå som et moment i vurderingen, da der er et større beskyttelseshensyn af børn.

Datatilsynet fremhæver ligeledes at et afgørende element i vurderingen er, at de identificerbare personer ikke med rimelighed må føle sig udstillet, udnyttet eller krænket, eksempelvis. i forbindelse med kommerciel udnyttelse af billedet.

Datatilsynet har oplistet følgende eksempler på hvornår interesseafvejningsreglen som udgangspunkt kan benyttes, og offentliggørelsen derfor kan ske uden samtykke: billeder af publikum til en koncert, billeder af besøgende i en zoologisk have eller lignende.

Datatilsynet anfører, at interesseafvejningsreglen som udgangspunkt ikke vil kunne bruges som behandlingsgrundlag i følgende situationer: billeder af besøgende hos lægen, kunder i banken og i fitnesscentret eller lignende, billeder af besøgende på en bar, natklub, diskotek eller lignende, samt billeder af ansatte på

arbejde i en privat virksomhed eller i en offentlig myndighed.

Læs hele udtalelsen her:

https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2019/sep/aendret-praksis-i-forhold-til-billeder-paa-internettet/

Læs den opdaterede vejledning om brug af billeder på internettet her:

https://www.datatilsynet.dk/emner/internet-og-apps/billeder-paa-internettet/

Det danske datatilsyn udtaler kritik af behandlingssikkerheden hos kontorfællesskab af advokatfirmaer

Det danske datatilsyn ('Datatilsynet') traf den 5. november 2019 afgørelse i sag j.nr. 2019-41-0029, og udtalte kritik af et kontorfællesskab af advokatfirmaers ('kontorfællesskabet') behandlingssikkerhed, herunder kryptering af e-mails, og manglende efterlevelse af kravene i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»databeskyttelsesforordningen«) artikel 32, stk. 1, og artikel 5, stk. 2, jf. stk. 1, litra f, jf. artikel 32, stk. 1 og stk. 2.

I forbindelse med sit tilsyn undersøgte Datatilsynet, hvorvidt kontorfællesskabet havde foretaget en risikoanalyse i forbindelse med fremsendelsen af personoplysninger via e-mail, og hvorvidt kontorfællesskabet overholdt Datatilsynets krypteringskrav ved fremsendelse af personoplysninger via e-mail.

Kontorfællesskabet havde forud for tilsynet fremsendt en risikovurdering for kontorfællesskabets generelle behandling af personoplysninger. Datatilsynet fandt, at kontorfællesskabet ikke i tilstrækkeligt grad havde godtgjort, at den udarbejdede risikovurdering indeholdte en vurdering som påviste risikoen forbundet med fremsendelse af fortrolige og følsomme personoplysninger via e-mail, hvilket den dataansvarlige er forpligtet til, jf. databeskyttelsesforordningens artikel 5, stk. 2, jf. stk. 1, litra f, jf. artikel 32, stk. 1 og stk. 2.

Datatilsynet lagde endvidere vægt på, at kontorfællesskabet ikke havde indført procedurer, som sikrede at modtageren af personoplysningerne sendt via e-mail understøttede kryptering på transportlaget via TLS ved fremsendelse af fortrolige og følsomme personlysninger.

I forbindelse med gennemgangen af kontorfællesskabets krypteringsløsning, fastslog Datatilsynet, at brugen af end-to-end kryptering med S/MIME certifikater i forbindelse med fremsendelse af e-mails til domstolene, politikredse, anklagemyndigheden, styrelser og nævn, udgjorde et tilstrækkeligt sikkerhedsniveau.

I forhold til kontorfællesskabets e-mailkommunikation med klienter, fastslog Datatilsynet, at kontorfællesskabet anvendte opportunistisk TLS (kryptering på transportlageret), såfremt modtageren ikke understøttede den anvendte end-to-end kryptering. Kontorfælleskabet havde dog ikke fastsat procedurer, der sikrede, at TLS kun blev anvendt såfremt modtagerdomænet understøttede TLS.

Datatilsynet udtalte kritik af kontorfællesskabet for den manglende udarbejdelse af risikovurderingen vedrørende fremsendelse af personoplysninger via e-mail, samt de manglende procedurer i forbindelse med anvendelse af TLS kryptering.

Læse hele afgørelsen her:

https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/nov/tilsyn-med-behandlingssikkerhed-hos-kontorfaellesskab-af-advokatfirmaer/

Det danske datatilsyn udtaler kritik og meddeler påbud mod dansk fagforening i forbindelse med tilsyn

Det danske datatilsyn ('Datatilsynet') udtalte den 5. november 2019 kritik angående behandlingssikkerheden hos Kristelig Fagforening ('Krifa'), særligt i henhold til kryptering af e-mails, og dermed manglende efterlevelse af kravene i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') artikel 32 og artikel 33.

Datatilsynets tilsyn omhandlede især, hvorvidt Krifa havde udarbejdet en risikoanalyse, og hvorvidt Krifa havde overholdt krypteringskravene i forbindelse med fremsendelse af personoplysninger over internettet.

Datatilsynet fandt, at Krifa i overensstemmelse med databeskyttelsesforordningens artikel 5, stk. 2, jf. stk. 1, litra f, jf. artikel 32, stk. 1 og 2, havde udarbejde en fyldestgørende risikovurdering.

Datatilsynet fastslog, at en oplysning om medlemskab af Krifa, ikke i sig selv udgør en følsom oplysning. Datatilsynet påpeger, at dette skyldes, at Krifa består af både en A-kasse og en fagforening, hvoraf det er muligt at være medlem af den ene, uden at være medlem af den anden.

Ved behandling af oplysninger over internettet anvendte Krifa end-to-end kryptering, hvilket ifølge Datatilsynet var i overensstemmelse med databeskyttelsesforordningens artikel 32.

I tilfælde, hvor modtageren ikke understøttede end-to-end kryptering, anvendte Krifa systemet Sikker@Mail. Ved brug af Sikker@Mail systemet, sendes den oprindelige meddelelse krypteret til Krifas servere, hvorefter modtageren notificeres og får tilsendt et link til meddelelsen. Denne fremgangsmåde var som udgangspunkt i overensstemmelse med artikel 32.

Når modtageren tilgår meddelelsen via Sikker@Mail skal modtageren benytte et kodeord for at tilgå meddelelsen. Kodeordet var enten modtagerens personnummer, eller et engangskodeord, der blev fremsendt via SMS.

Som udgangspunkt var kodeordet modtagerens personnummer, og modtageren skulle aktivt frasige sig

dette, såfremt modtageren ønskede et engangskodeord via SMS. Datatilsynet fandt, at det var i strid med databeskyttelsesforordningen at anvende modtagerens personnummer som kodeord.

Datatilsynet påbød Krifa at ophøre med at anvende modtagerens personnummer som kodeord. Påbuddet blev meddelt med hjemmel i databeskyttelsesforordningens artikel 58, stk. 2, litra d.

Datatilsynet fandt derudover, at Krifa havde overtrådt databeskyttelsesforordningens artikel 32 og artikel 33 ved at have sendt fire e-mails til modtagere, der ikke understøttede end-to-end kryptering og hvor Sikker@Mail ikke var benyttet, og hvori det var muligt at udlede oplysninger om fagforeningsmæssigt tilhørsforhold, uden at anmelde dette til Datatilsynet.

Krifa mente at de med hjemmel i databeskyttelsesforordningens artikel 33, 2. led, kunne undlade at anmelde hændelsen til Datatilsynet med den begrundelse, at de pågældende e-mails var fremsendt med opportunistisk TLS, og at Krifas statistik for marts 2019 viste, at mindst 99,74 % af de sendte mails var blevet sendt krypteret.

Datatilsynet tiltrådte ikke Krifas argument og fastslog, at de burde have anmeldt hændelsen til Datatilsynet. En dataansvarlig har således ikke mulighed for at undlade at melde et muligt brud til Datatilsynet, ved at henvise til, at den statistiske sandsynlighed for, at bruddet rent faktisk indebar en risiko for fysiske personers rettigheder, var lav. En dataansvarlig må således i forhold til det specifikke tilfælde konkret kunne godtgøre, at det konkrete brud ikke har indebåret en risiko for fysiske personers rettigheder.

Læs hele afgørelsen her:
https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/nov/tilsyn-med-behandlingssikkerhed-hos-fagforening/

Kommunes behandling af personoplysning ved *type-ahead* søgefunktion var lovlig

Det danske datatilsyn ('Datatilsynet') traf den 25. oktober 2019 afgørelse i sag j.nr. 2019-32-0910, og fandt, at der i den konkrete sag var et lovligt grundlag for at behandle borgerens navn i forbindelse med en søgefunktion på kommunens hjemmeside.

En borger klagede over, at en kommune behandlede oplysninger om borgeren gennem en »type-ahead«-søgefunktion på hjemmesiden. Type-ahead funktionen medførte, at ved indtastning af dele af borgerens navn foreslog søgefunktionen automatisk klagers navn i forbindelse med to resultater i søgemaskinen. Det første resultat forekom i forbindelse med en udgivelse, som ingen forbindelse havde til klager. Det andet resultat fremkom i forbindelse med en publikation, der indeholdt klagers navn.

Kommunen anførte, at behandlingen skete i overensstemmelse med artikel 6, stk. 1, litra e, i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen'). Kommunen anførte derudover, at formålet med søgefunktionen var, at yde bedre service for kommunens borgere, og at »type-ahead« ikke behandler personoplysninger, men blot gemmer det indtastede søgeord i søgemaskinen som tekststrenge, hvorfor at funktionen ikke skelner mellem personnavne og øvrig tekst. Der er en funktionalitet i søgemaskinen, som sikrer, at personnumre ikke vises.

Med hjemmel i databeskyttelsesforordningens artikel 6, stk. 1, litra e, kan behandling af personoplysninger ske, såfremt behandling er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse.

Datatilsynet fandt herefter ikke grundlag for at tilsidesætte kommunens vurdering af, at behandlingen skete inden for rammerne af den relevante bestemmelse i databeskyttelsesforordningen. Datatilsynet lagde vægt på, at søgefunktionen blev anvendt som et redskab, der skulle understøtte kommunens overholdelse af sin almindelige vejledningspligt over for borgerne.

Datatilsynet fandt derudover, at behandlingen var i overensstemmelse med de grundlæggende behandlingsprincipper i databeskyttelsesforordningens artikel 5, herunder princippet om dataminimering i databeskyttelsesforordningens artikel 5, stk. 1, litra c.

Læs hele afgørelsen her:
https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/okt/klage-over-soegefunktion-paa-kommunes-hjemmeside/

Københavns Kommunes løbende abonnering på personoplysninger i CPR var i strid med databeskyttelsesreglerne

Det danske datatilsyn ('Datatilsynet') traf den 25. oktober 2019 afgørelse i en sag j.nr. 2018-32-0232. Sagen omhandlede, hvorvidt Københavns Kommune ('KK') overtrådte Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') ved at abonnere på den registreredes personoplysninger i Det Centrale Personregister ('CPR').

Den registrerede indgav den 30. maj 2018 en klage over KKs abonnering på den registrerede i CPR. Forud for klagen havde den registrerede henvendt sig til KK den 17. januar 2018, og anmodet om en forklaring på, hvorfor KK abonnerede på den registrerede i CPR. Den registrerede var fraflyttet kommunen den 1. februar 1999.

KK oplyste som svar på henvendelsen, at de ikke længere havde behov for at abonnere på den registrerede, hvorfor abonnementet ville blive slettet.

Grundet den registreredes henvendelse gentegnede KK abonnementet. Dette skete automatisk i forbindelse med oprettelsen af en sag i KKs journaliseringssystem. KK informerede den registrerede om gentegningen den 12. april 2018, hvorefter den registrerede bad KK om at slette det nye abonnement. KK afslog denne anmodning den 9. maj 2018.

Datatilsynet fandt, at KK i perioden fra februar 1999 til 17. januar 2018, uden fornøden hjemmel havde abonneret på CPR-oplysninger om den registrerede. Datatilsynet anførte, at abonneringen på personerne i CPR omfatter behandling af ikke-følsomme personoplysninger, hvorfor KK skulle have hjemmel i databeskyttelsesforordningens artikel 6, stk. 1, litra a til f, til at foretage behandlingen.

KK havde påberåbt sig artikel 6, stk. 1, litra e, som behandlingshjemmel. Databeskyttelsesforordningens artikel 6, stk. 1, litra e giver hjemmel til nødvendige behandlinger af personoplysninger i samfundets interesse eller opgaver angående den offentlige myndighedsudøvelse som myndigheden har fået pålagt.

KK anførte, at litra e hjemlede abonneringen af oplysninger på både nuværende og forhenværende borgere. Derudover gjorde KK gældende, at de var berettiget til at gentegne abonnementet med henblik på at understøtte kommunens myndighedsudøvelse, herunder pligten til at kunne håndtere aktindsigtsanmodninger.

Datatilsynet fandt, at KK ikke havde hjemmel til behandlingen af oplysningerne i databeskyttelsesforordningens artikel 6, stk. 1, litra e. Datatilsynet anførte, at litra e kun kan benyttes som behandlingsgrundlag, såfremt behandlingen er nødvendig. Datatilsynet konkluderede, at det ikke var nødvendigt at tegne et abonnement på den registrerede, alene med det formål at håndtere eventuelle aktindsigts- eller rettighedsanmodninger.

Datatilsynet lagde vægt på, at KK havde mulighed for at foretage enkeltopslag i CPR for at bliver oplyst om ajourførte oplysninger om borgeren, såfremt dette blev aktuelt. I forbindelse med sagen fastslog Datatilsynet, at abonnementet ligeledes var i strid med databeskyttelsesforordningens artikel 5, stk. 1, litra c, om dataminimering.

Datatilsynet valgte at udtale kritik af både Københavns Kommunes abonnering på personoplysninger i perioden fra den 1. februar 1999 til den 17. januar 2018, og i perioden efter den 17. januar 2018, da Københavns Kommune efter Datatilsynets opfattelse ikke havde haft en gyldig behandlingshjemmel.

Læs hele afgørelsen her: https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/okt/kommunes-cpr-abonnement-var-i-strid-med-databeskyttelsesreglerne/

Det Europæiske Databeskyttelsesråd udgiver sin endelige vejledning om kontrakter som behandlingsgrundlag

Den 8. oktober 2019 udgav Det Europæiske Databeskyttelsesråd ('EDPB') deres endelige vejledning om kontrakter som behandlingsgrundlag i forbindelse med salg af online ydelser.

Vejledningen gennemgår, hvornår Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningens') artikel 6, stk. 1, litra b kan anvendes. EDPB fastslår, at behandlingen skal være nødvendig af hensyn til at opfylde kontrakten.

Tilfælde, hvor en behandling er nødvendig for at opfylde kontrakten, skal ifølge EDPB begrænses til tilfælde, hvor behandlingen er objektiv nødvendig. Dette medfører, at såfremt formålet kan opnås med mindre indgribende midler, kan litra b ikke benyttes som behandlingsgrundlag.

EDPB anfører ligeledes, at den dataansvarlige skal foretage en vurdering af, om en behandling er nødvendig forud for, at behandlingen bliver udført. Hvorvidt en behandling er nødvendig af hensyn til kontrakten, skal vurderes uafhængigt af eventuelle standardvilkår. Eventuelle standardvilkår ændrer ikke på, hvilken behandling, der er objektiv nødvendig i henhold til kontrakten, ligesom standardvilkår ikke kan udvide den kontraktuelle forpligtelse til at omfatte andre behandlinger end objektivt nødvendige behandlinger.

EDPB illustrerer dette med følgende eksempel: Såfremt en forbruger bestiller en forsendelse, kan databeskyttelsesforordningen artikel 6, stk. 1, litra b anvendes til at behandle adresseoplysningen. Såfremt pakken ikke skal leveres til forbrugerens adresse, men i stedet afhentes på posthuset, kan firmaet ikke længere behandle adressen med hjemmel i artikel 6, stk. 1, litra b, og må for at behandle adressen finde et selvstændigt behandlingsgrundlag for denne behandling.

I forbindelsen med vurderingen af, om databeskyttelsesforordningens artikel 6, stk. 1, litra b kan anvendes, har EDPB opstillet følgende spørgsmål, som kan benyttes som rettesnor:

(a) Hvilken karakter har ydelsen af natur? Hvad er kontraktens særlige karakter?
(b) Hvad er rationalet bag kontrakten?
(c) Hvad er kontraktens vigtigste bestanddele?
(d) Hvilke gensidige perspektiver og forventninger har parterne til kontrakten? Herunder hvordan ydelsen er blevet reklameret, samt hvorvidt en almindelig oplyst bruger af ydelsen, ville forvente at den pågældende behandling ville finde sted?

EDPB fastslår, at brugen af artikel 6, stk. 1, litra b som behandlingsgrundlag ikke hindrer, at ydelser

samles, da det står den dataansvarlige frit for selv at indrette sin virksomhed i henhold til gældende lov.

Da vurderingen af om artikel 6, stk. 1, litra b kan benyttes, tager udgangspunkt i de enkelte ydelser i henhold til nødvendigheden af kontrakten, kan artikel 6, stk. 1, litra b, ikke benyttes som særskilt behandlingsgrundlag for ydelser, der ikke er objektivt nødvendige for at opfylde kontrakten. Såfremt flere ydelser samles til en ydelse, kan litra b kun benyttes som hjemmel med henblik på objektive nødvendige behandlinger i forhold til kontrakten, mens de øvrige ydelser må have deres eget selvstændige behandlingsgrundlag.

Læse hele vejledningen her:

https://www.datatilsynet.dk/media/6971/edpb-guideline-2-2019-article-6-1-b.pdf

Det danske datatilsyn udsteder nye vilkår for henholdsvis kreditoplysningsbureauers behandling af personoplysninger og behandling af oplysninger i form af advarselsregistre og spærrelister

Det danske datatilsyn ('Datatilsynet') udstedte den 8. oktober 2019 nye vilkår om behandling af oplysninger til bedømmelse af økonomisk soliditet og kreditværdighed med henblik på videregivelse, samt en vejledning om de nye vilkår. Vejledningen gælder for dataansvarlige, der behandler information om økonomisk soliditet og kreditværdighed med henblik på videregivelse.

Man bør være opmærksom på, at vilkårene supplerer databeskyttelsesforordningen og den danske databeskyttelseslov, og at disse finder anvendelse i det omfang forhold ikke er reguleret af vilkårene.

Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') regulerer ikke særskilt behandling af kreditoplysninger. Det følger dog af lov nr. 502 af 23. maj 2018 ('den danske databeskyttelseslov') § 26, stk. 1, nr. 2, at forinden iværksættelse af en behandling med henblik på erhvervsmæssig videregivelse af oplysninger til bedømmelse af økonomisk soliditet og kreditværdighed, der foretages for en privat dataansvarlig, skal Datatilsynets tilladelse indhentes. Det følger endvidere af den danske databeskyttelseslovs § 26, stk. 4, at Datatilsynet kan udstede nærmere vilkår for behandlingen.

Datatilsynets vilkår for behandling af kreditoplysninger berører følgende områder:

(e) Behandlingsregler
(f) Oplysningspligt
(g) Urigtige/vildledende oplysninger
(h) Sletning af oplysninger
(i) Anmodninger fra en registreret
(j) Sikkerhed

Ændringer og ophør

(k) De nye vilkår supplerer den danske databeskyttelseslovs kapitel 5 (§ 19 til § 21) og § 26, som i øvrigt regulerer behandlingen af kreditoplysninger.

De nye vilkår omfatter blandt andet hvornår registreringen af oplysninger om gæld, som ikke opfylder betingelserne for summarisk form, jf. den danske databeskyttelseslovs § 21, stk. 3, kan ske. Datatilsynet fastslår, at følgende tre kumulative betingelser skal være opfyldt før behandlingen af oplysninger i summarisk form kan behandles: (1) inden registreringen skal der være sendt mindst tre rykkere til debitor, (2) i forbindelse med fremsendelse af tredje rykker skal den dataansvarlige gøre opmærksom på at manglende betaling medfører indberetning til et kreditoplysningsbureau, og (3) kravet må ikke være bestridt.

Datatilsynet har den 22. november 2019 udstedt vilkår for dataansvarliges brug af advarselsregistre og spærrelister. Vilkårene er fastsat med hjemmel i den danske databeskyttelseslovs § 26, stk. 4. Vilkårene berører i høj grad de samme emner som vilkårene for behandling af kreditoplysninger. Datatilsynet har ligeledes udgivet vejledninger om behandlingen af henholdsvis advarselsregistre og spærrelister.

Fælles for vilkårene for brug af advarselsregistre og spærrelister er, at der er tale om standardvilkår til brug for meddelelse af tilladelse til behandling, jf. den danske databeskyttelseslovs § 26, stk. 1, nr. 1. Datatilsynet oplyser, at vilkårene tilpasses i nødvendigt omfang til det enkelte registers særlige karakter.

Læs vilkårene og vejledningerne her:

Kreditoplysningsbureauer:

https://www.datatilsynet.dk/media/7922/vilkaar-for-kreditoplysningsbureauer.pdf

https://www.datatilsynet.dk/media/7921/kreditoplysningsbureauer.pdf

Advarselsregistre:

https://www.datatilsynet.dk/media/7935/vilkaar-for-advarselsregistre.pdf

https://www.datatilsynet.dk/media/7938/vejledning-om-advarselsregistre.pdf

Spærrelister:

https://www.datatilsynet.dk/media/7936/vilkaar-for-spaerrelister.pdf

https://www.datatilsynet.dk/media/7937/vejledning-om-spaerrelister.pdf

Det danske datatilsyn opdaterer vejledning om samtykke som behandlingsgrundlag

Det danske datatilsyn ('Datatilsynet') har den 2. september 2019 opdateret tilsynets vejledning for, hvornår der foreligger et gyldigt samtykke efter Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('Databeskyttelsesforordningen') artikel 6, litra a.

Opdateringen sker på baggrund af en opdatering af Det Europæiske Databeskyttelsesråd vejledning om samtykke. Vejledningen indeholder en tjekliste, som den dataansvarlige kan bruge i forbindelse med indhentelsen af et samtykke, samt for at efterse, hvorvidt et allerede indhentet samtykke er i overens-

stemmelse med Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen').

Vejledningen gennemgår betingelserne for, hvornår der foreligger et gyldigt samtykke og retsvirkninger af et tilbagekaldt samtykke.

Vejledningen indeholder nu ligeledes et krav om granularitet (opdeling). Kravet om granularitet knytter sig til kravet om, at samtykket skal være specifikt og frivilligt, jf. databeskyttelsesforordningens artikel 7, stk. 4. Det følger af vejledningen, at et samtykke ikke antages at være frivilligt, såfremt samtykket afgives til flere forskellige behandlingsaktiviteter, uden mulighed for at afslå de enkelte behandlingsaktiviteter.

Datatilsynet illustrerer dette med følgende eksempel: I forbindelse med et køb af varer over internettet, anmoder en forretning om samtykke til både aktiviteter i forbindelse med levering, til markedsføringsmæssige formål og til at oplysningerne deles med tredjeparter. Samtykket kan kun gives til alle tre formål. Samtykket er ikke granulat, da de enkelte formål ikke kan udskilles, og individuelt accepteres eller afslås.

Såfremt en behandling tjener flere formål, skal den dataansvarlige indhente særskilt samtykke for hvert formål. Dette kan eksempelvis ske ved brug af en samlet erklæring, hvor det er muligt for den registrerede enkeltvis at markere, hvilke af formålene, der gives samtykke til.

Den nye vejledning har ligeledes et øge fokus på den dataansvarliges forpligtelser i tilfælde af, at den registrerede tilbagekalder sit samtykke, jf. databeskyttelsesforordningens art. 7, stk. 3. Datatilsynet anfører, at behandlingen skal ophøre hurtigst muligt efter tilbagekaldelsen, og at opbevaring i sig selv udgør en behandling.

Som udgangspunkt kan den dataansvarlige ikke skifte behandlingsgrundlag i forbindelse med tilbagetrækningen af samtykket.

Datatilsynet påpeger således, at det derfor er vigtigt, at den dataansvarlige fra behandlingens start anvender det mest hensigtsmæssige behandlingsgrundlag. Såfremt der er hjemmel til at behandlingen forsætter med et andet formål end det oprindelige formål, kan behandlingen stadig finde sted efter samtykket er trukket tilbage. Datatilsynet tilføjer dog, at dette nye behandlingsgrundlag ikke kan være interesseafvejningsreglen i databeskyttelsesforordningens artikel 6, stk.1, litra f.

Læs vejledningen her:
https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2019/sep/vejledning-om-samtykke-er-opdateret/

Det danske datatilsyn finder at afvisning på indsigt i personoplysninger (cookies) var korrekt, men kritiserer håndtering af anmodning

Den 18. november 2019 traf det danske datatilsyn ('Datatilsynet') afgørelse i sag j.nr. 2019-32-0670. Sagen omhandlede, hvorvidt Danske Statsbaner ('DSB') som dataansvarlig havde besvaret en registreret indsigtsanmodning korrekt.

Den registrerede havde den 29. januar 2019 bedt om *»indsigt i alt, hvad I har registreret om mig«*. DSB udleverede den 8. februar 2019 en række af de anmodede oplysninger. Klager mente, at de fremsendte oplysninger ikke var tilstrækkelige, og indgav herefter en klage til Datatilsynet den 3. marts 2019. Datatilsynet rettede henvendelse til DSB i forbindelse med klagesagen, og på baggrund af dette udleverede DSB de manglende oplysninger til den registrerede den 11. april 2019. DSB oplyste i forbindelse hermed, at DSB ikke havde mulighed for at udlevere videooptagelser af den registrerede samt personoplysninger indsamlet gennem cookies.

Datatilsynet fandt, at DSB ikke havde behandlet indsigtsanmodningen i overensstemmelse med Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen'), artikel 12, stk. 2. Datatilsynet lagde vægt på, at DSB på tidspunktet for den første anmodning lå inde med videooptagelser af klager.

Datatilsynet indskærpede over for DSB, at der ikke kan stilles krav om særskilt anmodning om indsigt i videooptagelser. DSB havde anført, at de havde undladt at tage stilling til, hvorvidt den registrerede kunne få indsigt i videooptagelserne, da den registrerede ikke udtrykkeligt havde anført, at anmodningen ligeledes omfattede videooptagelser.

Datatilsynet anførte endvidere, at såfremt den dataansvarlige er i tvivl om omfanget af en indsigtsanmodning, eller der foreligger en betydelig mængde oplysninger, har den dataansvarlige mulighed for at kontakte den registrerede, med henblik på at få specificeret anmodningen. Såfremt den registrerede ikke ønsker at oplyse om yderligere forhold, skal den dataansvarlige opfylde anmodningen i det omfang det er muligt.

Datatilsynet fandt således på denne baggrund, at DSB overtrådte databeskyttelsesforordningens artikel 12, stk. 2, da DSB ikke i tilstrækkelig grad gav klager mulighed for at udøve sine rettigheder, da videomaterialet efterfølgende var blevet slettet og således ikke kunne udleveres til den registrerede. Ydermere fandt Datatilsynet, at den endelige udlevering af oplysningerne (den efterfølgende udlevering d. 11 april) var sket senere end en måned efter, at anmodningen var fremsendt. Hvorfor Datatilsynet fandt, at DSB ligeledes havde overtrådt databeskyttelsesforordningens § 12, stk. 3.

For så vidt angår udleveringen af oplysningerne indsamlet ved hjælp af cookies påpegede Datatilsynet, at en dataansvarlig ikke er forpligtet til at beholde, indhente, eller behandle yderligere oplysninger for at kunne identificere den registrerede alene med det formål at overholde forordningen, såfremt formålene med

behandlingen ikke eller ikke længere kræver, at den registrerede kan identificeres af den dataansvarlige, jf. databeskyttelsesforordningens artikel 11, stk. 1.

Datatilsynet påpegede endvidere, at det følger af databeskyttelsesforordningens artikel 11, stk. 2, at den dataansvarlige skal kontakte den registrerede ved tilfælde omfattet af stk. 1, hvor den dataansvarlige påviser ikke længere at kunne identificere den registrerede.

Datatilsynet lagde vægt på, at formålene med behandlingen, hvor DSB anvendte cookies, ikke krævede, at DSB konkret kunne identificere den registrerede, samt at DSB ikke var i besiddelse af oplysninger, der kunne koble klager med oplysningerne, som behandles ved hjælp af cookies. Datatilsynet fandt, at DSB i overensstemmelse med artikel 11, stk. 2, havde kontaktet den registrerede og informeret den registrerede om, at DSB ikke kunne identificere oplysningerne om den registrerede uden yderligere information.

Datatilsynet valgte på baggrund af håndteringen af anmodningen om videomaterialet at udtale alvorlig kritik af DSB. Datatilsynet fandt ikke grundlag for at udtale kritik af den manglende udlevering af personoplysninger indsamlet ved hjælp af cookies.

Læs vejledningen her:
https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/nov/indsigt-i-personoplysninger-hos-dsb/

Det danske datatilsyn finder at Visitdenmarks udsendelse af brev med Digital Post var i overensstemmelse med databeskyttelsesreglerne, men ikke oplysningspligten

I april 2019 indledte det danske datatilsyn ('Datatilsynet') af egen drift en sag mod Visitdenmark. Datatilsynet blev bekendt med Visitdenmarks behandling af personoplysninger i forbindelse med udsendelse af breve med Digital Post under emnet' *Vigtig information til dig med sommerhus'*.

Datatilsynet traf afgørelse i sagen den 21. november 2019.

I forhold til Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') artikel 6, stk. 1. og § 11, stk. 1, i lov nr. 502 af 23. maj 2018 ('den danske databeskyttelseslov') fandt Datatilsynet, at Visitdenmarks behandling af personoplysninger i forbindelse med udsendelse af brev med Digital Post var sket inden for rammerne af de nævnte regler.

Datatilsynet fastlagde indledningsvist, at Visitdenmark i henhold til lov nr. 648 af 15. juni 2010 om Visitdenmark ('den danske lov om Visitdenmark'), er en offentlig myndighed. Visitdenmark var på baggrund af en aftale indgået i det danske folketing den 17. maj 2018, blevet pålagt at tilrettelægge en kampagne rettet mod at få flere danskere til at leje deres sommerhus ud. Datatilsynet fandt derfor, at der ikke var grundlag for at tilsidesætte Visitdenmarks vurdering af, at behandlingen af personoplysningerne var nødvendig af hensyn til udførelse af en opgave, som henhørte under offentlig myndighedsudøvelse. Datatilsynet vurderede også, at behandlingen var foretaget i overensstemmelse med den danske databeskyttelseslov § 11 og de grundlæggende principper i databeskyttelsesforordningens artikel 5, herunder princippet om formålsbegrænsning i databeskyttelsesforordningens artikel 5, stk. 1, litra b.

I forhold til databeskyttelsesforordningens artikel 14 om myndigheders oplysningspligt, inddelte Datatilsynet deres begrundelse i to dele.

Første del vedrørte oplysningspligt ved indsamling af navn og BBR-oplysninger. Her udtalte Datatilsynet, at i tilfælde hvor personoplysninger ikke er indsamlet hos den registrerede, følger det af databeskyttelsesforordningens artikel 14, stk. 1, at det påhviler den dataansvarlige at give den registrerede meddelelse om en række oplysninger. Efter databeskyttelsesforordningens artikel 14, stk. 2, skal den dataansvarlige give den registrerede meddelelse om yderligere oplysninger, som er nødvendige for at sikre en rimelig og gennemsigtig behandling. Visitdenmark havde ved indsamlingen af de pågældende personoplysninger, ikke givet meddelelse til de registrerede. Datatilsynet fandt derfor, at Visitdenmark ikke havde iagttaget myndighedens oplysningspligt efter databeskyttelsesforordningens artikel 14 stk. 1, og 2.

Anden del vedrørte oplysningspligt ved indsamling af personnumre i CPR-registre. Datatilsynet bemærkede, at det af databeskyttelsesforordningens artikel 14, stk. 5, litra c, fremgår, at oplysningspligten ikke finder anvendelse, hvis regler for indsamling eller videregivelse er udtrykkelig fastsat i EU-ret eller i national ret i den medlemsstat, som den dataansvarlige er underlagt. Datatilsynet fandt derfor, at oplysningspligten i forbindelse med indsamling af personnumre i CPR-registret kunne undtages med henvisning til lov nr. 528 af 11. juni 2012 om Digital Post fra offentlige § 7, stk. 1, som bestemmer, at offentlige afsendere er berettigede til at anvende Digital Post til kommunikation med fysiske personer.

Læs afgørelsen her:
https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/nov/breve-i-e-boks-fra-visitdenmark/

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


Wiersholm

Line Haukalid og Marthe Femanger Pettersen

Ansiktsgjenkjenning – stadig mer aktuelt

Det svenske datatilsynet, Datainspektionen, har ilagt sitt første overtredelsesgebyr etter GDPR. Overtredelsesgebyret er på 200 000 svenske kroner og knytter seg til testing av et ansiktsgjenkjenningsverktøy i en videregående skole. Vedtaket illustrerer at ansiktsgjenkjenning blir stadig mer aktuelt.

I denne artikkelen ser vi nærmere på hva ansiktsgjenkjenning er, hva det kan brukes til og hva man må være oppmerksomme på i innhentingen av samtykke.

Hva er ansiktsgjenkjenning og biometriske opplysninger?

Ansiktsgjenkjenning benytter seg av biometriske kjennetegn for å identifisere enkeltpersoner. Biometriske opplysninger er i GDPR definert som «*personopplysninger som stammer fra en særskilt teknisk behandling knyttet til en fysisk persons fysiske, fysiologiske eller atferdsmessige egenskaper, og som muliggjør eller bekrefter en entydig identifikasjon av nevnte fysiske person, f.eks. ansiktsbilder eller fingeravtrykksopplysninger*». Datatilsynet beskriver biometriske kjennetegn som kjennetegn som utgår fra kroppen, som er unike for deg som enkeltperson og samtidig permanente eller stabile over tid.

Ansiktsgjenkjenning kan både brukes for å identifisere hvem noen er og for å verifisere at noen er den de utgir seg for å være, for eksempel slik vi bruker Face ID på mobiltelefoner (autentisering). I forarbeidene til personopplysningsloven av 2000 var bruken av biometriske personopplysninger antatt å falle inn under § 12, uten at dette eksplisitt fremgikk av ordlyden. Bestemmelsen oppstilte et krav om saklig behov for sikker identifisering, samt at metoden var nødvendig for å oppnå slik identifisering.

Etter ikrafttredelsen av GDPR er behandlingen av biometriske opplysninger eksplisitt definert og regulert. Artikkel 9 i GDPR oppstiller i utgangspunktet et forbud mot bruk av biometriske opplysninger, ettersom biometriske opplysninger er særlige kategorier av personopplysninger som kun kan behandles på nærmere bestemte vilkår. Det mest praktiske behandlingsgrunnlaget for bruk av biometriske opplysninger er samtykke.

Utfordringer ved bruk av samtykke til ansiktsgjenkjenning

Et samtykke til behandling av personopplysninger må være frivillig, spesifikt, informert, dokumenterbart, utvetydig og gitt gjennom en aktiv handling. I tillegg må samtykket kunne trekkes tilbake.

Avgjørelsen fra den svenske Datainspektionen bekrefter at man må vurdere styrkeforholdet mellom virksomheten og den som personopplysningene gjelder nøye før samtykke brukes som behandlingsgrunnlag. En svensk kommune hadde innhentet samtykke fra de aktuelle elevene til test av et ansiktsgjenkjenningsverktøy til oppmøteregistrering. Før innhenting av samtykket var det gitt full informasjon om bruken av personopplysningene og om retten til å trekke tilbake samtykket. Datainspektionen konkluderte imidlertid med at det ikke er adgang til å bruke samtykke som behandlingsgrunnlag i et tilfelle som dette, hvor elevene er i en avhengighetssituasjon overfor skolen. Av samme grunn kan det ofte være problematisk for en arbeidsgiver å bygge på samtykke fra sine ansatte.

Bruk av ansiktsgjenkjenning er derfor mer aktuelt i andre sammenhenger, gjerne i forholdet mellom en virksomhet og dens kunder. En finansinstitusjon vil for eksempel kunne innhente samtykke fra sine kunder for å kunne ta i bruk ansiktsgjenkjenning til sikker innlogging i nettbanken.

Andre betenkeligheter

Betenkelighetene ved bruk av ansiktsgjenkjenning dukker kanskje særlig opp når et kamera kan identifisere personer på avstand uten at man vet at man er identifisert, eller når ansiktsgjenkjenningssystemer

blir matet med utallige bilder samlet inn fra internett og sosiale medier uten vår tillatelse eller kunnskap. I Kina er bruken av ansiktsgjenkjenning utbredt. Her blir ansiktsgjenkjenning angivelig brukt til å kontrollere tilstedeværelse i skolen og til å kontrollere innbyggernes bruk av papir på offentlige toaletter. Ved utgangen av 2020 forventes det å være satt opp over 600 millioner kameraer med ansiktsgjenkjenning. Denne overvåkingen er knyttet tett sammen med Zhima Credit-systemet, som kinesiske myndigheter er i ferd med å utvikle. Systemet skal standardisere vurderingen av innbyggernes og virksomheters økonomiske og sosiale omdømme. Hva innbyggerne fortar seg skal visstnok være med på å gi dem en sosial score, som for eksempel kan påvirke muligheter for jobb, skolegang og hvor de kan bo.

> ikke er adgang til å bruke samtykke som behandlingsgrunnlag i et tilfelle som dette, hvor elevene er i en avhengighetssituasjon overfor skolen

Riktig bruk gir muligheter

Å bruke ansikt som mekanisme for identifikasjon eller autentisering blir stadig mer utbredt. Ansiktsgjenkjenning kan brukes av politiet til å finne mistenkte personer i folkemengder. En lege vil kunne bruke teknologien for å gjenkjenne endringer i ansiktsuttrykk og på den måten forutsi sykdomsforløp. Flere flyplasser har tatt i bruk teknologi som gir reisende anledning til å gå gjennom sikkerhetskontrollen uten å måtte vise frem dokumenter. På konserter og andre arrangementer vil ansiktsgjenkjenning kunne gjøre bruk av billetter overflødig. I de kommende olympiske leker i Tokyo skal ansiktsgjenkjenning brukes til å identifisere autoriserte personer og gi dem automatisk adgang. Ansiktsgjenkjenning gir med andre ord mange muligheter, forutsatt at det brukes i tråd med regelverket.

Line Helen Haukalid er advokat og jobber i Wiersholms team for teknologi og immaterielle rettigheter med særlig vekt på personvern og GDRP.

Marthe Femanger Pettersen er advokatfullmektig og jobber og jobber i Wiersholms team for teknologi og immaterielle rettigheter med særlig vekt på personvern og GDRP.

Delphi

Rebecka Harding och Adam Odmark

eSams inställning om myndigheters outsourcing av IT-funktioner ger upphov till diskussion

En fråga som fått alltmer uppmärksamhet i Sverige under de senaste åren är om och hur myndigheter kan göra uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (”OSL”) tillgängliga för en IT-leverantör utan att samtidigt anses ”röja” uppgifterna till leverantören, dess underleverantörer eller tredje part. Frågan har fått särskilt stor uppmärksamhet sedan CLOUD Acts ikraftträdande i USA 2018. Detta eftersom CLOUD Act gör det möjligt för amerikanska brottsbekämpande myndigheter att i vissa fall direkt begära att vissa IT-leverantörer som står under amerikansk jurisdiktion lämnar ut data, oavsett var i världen den lagras av leverantören, samtidigt som OSL föreskriver att det som utgångspunkt är förbjudet att röja sekretessbelagda uppgifter till utländska myndigheter.

Efter CLOUD Acts ikraftträdande publicerade eSam, samma år, ett rättsligt utlåtande om röjande av sekretesskyddade uppgifter enligt OSL vid användning av vissa typer av molntjänster. eSam är ett program för samverkan mellan myndigheter och Sveriges kommuner och regioner (”SKR”) (tidigare Sveriges

kommuner och landsting/SKL), som organiserar Sveriges samtliga kommuner och regioner. Syftet med programmet är att ta tillvara digitaliseringens möjligheter inom det offentliga. eSam har bland annat publicerat flera icke-bindande rekommendationer i såväl juridiska som mer praktiska frågor av betydelse i samband med outsourcing av IT-funktioner riktade till aktörer inom det offentliga.

Bland annat framgår följande av eSams utlåtande från 2018:

”*Om sekretessreglerade uppgifter görs tekniskt tillgängliga för en tjänsteleverantör som till följd av ägarförhållanden eller annars är bunden av regler i ett annat land, enligt vilka tjänsteleverantören kan bli skyldig att överlämna information utan att internationell rättshjälp anlitats eller annan laglig grund föreligger enligt svensk rätt, får uppgifterna anses vara röjda. Anledningen är att det inte längre är osannolikt att uppgifterna kan komma att lämnas till utomstående*.” (vår understrykning)

Uttalandet ovan föreskriver att en myndighet alltså ska göra en sannolikhetsbedömning av om uppgifter som omfattas av sekretess kan komma att lämnas ut till utomstående innan de görs tekniskt tillgängliga för en tjänsteleverantör som är bunden av lagstiftning likt CLOUD Act.

Uttalandet gav upphov till diskussion i Sverige om det över huvud taget är möjligt för en svensk myndighet att tillgängliggöra sekretesskyddade uppgifter till en molntjänstleverantör som står under amerikansk jurisdiktion. Uttalandet har även mötts av viss kritik för att vara alltför kategoriskt och för att inte vila på tillräcklig kunskap om hur CLOUD Act och amerikansk processuell lagstiftning fungerar. Kritiken har delvis tagit sikte på om CLOUD Act verkligen innebär att ”*det inte längre är osannolikt att uppgifterna kan komma att lämnas till utomstående*”.

I december 2019 publicerade eSam en ny vägledning om sekretess och dataskydd i samband med outsourcing av IT-funktioner. Vägledningen innehåller bland annat avsnitt som följer upp eSams utlåtande från 2018 om röjande av sekretessreglerade uppgifter vid användning av vissa typer av molntjänster. I 2019 års vägledning menar eSam att en sannolikhetsbedömning enligt 2018 års uttalande aldrig blir aktuell om myndigheten gör bedömningen att ”*tjänsteleverantören på grund av regler i en främmande rättsordning [kan] bli tvungen att lämna ut uppgifter*”. I så fall ska myndighetens sekretesskyddade uppgifter enligt eSam anses röjda i OSL:s mening. eSam specificerar inte till vem uppgifterna ska anses röjda men vi får anta att eSam syftar på myndigheter i det främmande landet, till vilka det som utgångspunkt är förbjudet enligt OSL att röja sekretesskyddade uppgifter.

Kommentar

De rättskällor som tydligast behandlar tolkningen av begreppet ”röjande” enligt OSL är ett rättsfall från Högsta domstolen (NJA 1991 s. 103) och ett från Arbetsdomstolen (AD 2019 nr 15). Enligt dessa domar krävs inte att någon de facto tagit del av en uppgift för att den ska anses röjd. Det avgörande ska vara om uppgiften har blivit tillgänglig för någon obehörig under sådana omständigheter att man måste räkna med att den obehörige kommer att ta del av uppgiften. Enligt vår mening ger dessa rättsfall visst fog för 2018 års uttalande där eSam talar om en sannolikhetsbedömning. Uttalandet i eSams vägledning från 2019 om att en sannolikhetsbedömning aldrig blir aktuell om tjänsteleverantören på grund av regler i en främmande rättsordning kan bli tvungen att lämna ut uppgifter tycks däremot sakna tydligt stöd i de rättskällor som finns att tillgå idag. Det ska i sammanhanget även noteras att SKR (som är en betydelsefull aktör i sammanhanget) valde att inte ställa sig bakom 2019 års vägledning.

Om man tar fasta på att det är korrekt att göra en sannolikhetsbedömning enligt 2018 års uttalande är frågan i så fall om lagstiftning som CLOUD Act verkligen innebär att det inte längre är osannolikt att myndigheterna i det främmande landet kommer att ta del av de sekretessreglerade uppgifterna så som eSam skriver. Den statistik om utlämnanden som finns att tillgå från stora molntjänstleverantörer som Amazon och Microsoft, kombinerat med riktlinjer från det amerikanska justitiedepartementet om att i första hand begära ut data direkt från dess ägare, indikerar enligt vår uppfattning att det kanske inte är särskilt troligt att en svensk myndighets sekretesskyddade uppgifter kommer att hamna hos amerikanska myndigheter – åtminstone inte med stöd av just CLOUD Act.

Den svenska regeringen har tillsatt en utredning som bland annat ska tydliggöra de rättsliga förutsättningarna för det offentligas outsourcing av IT-funktioner, vilket vi ser positivt på då det är uppenbart att behovet och efterfrågan av tydliggöranden finns. Denna del av utredningen ska redovisas senast den 31 augusti 2020 och vi ser fram emot att läsa utredningens betänkande när det kommer.

Rebecka Harding är senior associate/advokat och Adam Odmark är associate vid Advokatfirman Delphi, Stockholm.

Gorrissen Federspiel

Tue Goldschmieding

Fogedforbud ikke fremmet da sagsøgers muligheder for at opnå sin ret ikke ville forspildes ved at afvente almindelig rettergang

Den danske sø- og handelsret ('Sø- og Handelsretten') afsagde den 18. november 2019 dom i sagen BS-31266/2019-SHR mellem sagsøger Hejs.dk A/S ('Hejs.dk') og sagsøgte TS Platform & Hejs ApS og TS Stilladsmontage A/S ('TS'). Sagen angik, hvorvidt Hejs.dk kunne opnå midlertidigt forbud og påbud efter lov nr. 938 af 10. september2019 ('den danske retsplejelov') § 411 stk. 1, mod sagsøgtes brug af »TS Hejs.dk« i dennes markedsføring for at krænke Hejs.dk's påståede varemærke.

TS Platform & Hejs ApS og TS Stilladsmontage A/S, der begge var ejet af TS Group Holding ApS, drev begge virksomhed med udlejning af arbejdsplatforme, herunder også stilladser ligesom Hejs.dk.

Hejs.dk rettede den 17. maj 2017 og den 2. august 2017 henvendelse til sagsøgte med påtale af brugen af »TS Hejs.dk« som led i virksomhedens markedsføring – begge gange nægtede TS at stoppe brugen. Den 17. juni 2019 henvendte Hejs.dks advokat sig med endnu et påbud om den fortsatte brug. Dertil blev det varslet, at manglende efterkommelse ville medføre retslige skridt. Virksomheden afviste endnu engang påbuddet og Hejs.dk indgav derefter anmodning om nedlæggelse af midlertidigt forbud og påbud.

Der var forløbet godt 1 år og 10 måneder inden Hejs.dk gjorde indsigelse mod brugen af navnet, såvel som der yderligere var gået 1 måned før der var indleveret forbudsbegrænsing til domstolen. Sø- og Handelsretten fandt derfor, at Hejs.dk ikke havde godtgjort eller sandsynliggjort, at virksomhedens muligheder for at opnå sin ret ville forspildes ved at afvente tvistens afgørelse ved en civil sag. Betingelsen i den danske retsplejelovs § 413 nr. 3 var således ikke opfyldt, og der kunne følgelig ikke nedlægges midlertidigt forbud og påbud mod brugen af det påståede varemærke.

Læs hele dommen her:
http://domstol.fe1.tangora.com/media/-300011/files/Kendelse_BS-31266-2019-SHR.pdf?rev1

Den danske markedsføringslov og varemærkelov, samt EF-designforordningen var krænket ved import, markedsføring og salg i Danmark

Den danske sø- og handelsret ('Sø- og Handelsretten') afsagde den 4. november 2019 dom i sagen BS-18539-SHR mellem Telebrands Corporation og International Edge Inc. ('sagsøger') og Bilablau ApS, samt tre ledende personer i virksomheden ('sagsøgte')).

Sagsøgtes forretningsmodel var baseret på »dropshipping«-konceptet. Dette indebar, at sagsøgte ikke nødvendigvis havde samtlige varer på lager, men derimod videresendte kundens ordre til grossisten, der i stedet leverede direkte til kunden.

Sagen angik, hvorvidt sagsøgte i deres markedsføring af en række importerede produkter havde krænket sagsøgers rettigheder efter lov nr. 426 af 3 maj 2017 ('den danske markedsføringslov'), lovbekendtgørelse nr. 88 af 29. januar 2019 ('den danske varemærkelov') og Rådets forordning (EF) nr. 6/2002 af 12. december om EF-design ('EF-designforordningen'). Dertil angik sagen, hvorvidt tre ledende personer i virksomheden var personligt ansvarlige for krænkelserne.

Retten fastslog indledningsvist, at sagsøgtes brug af sagsøgers produktbilleder i deres onlinemarkedsføring udgjorde en ophavsretlig krænkelse. Dertil fandt Retten, at sagsøgte havde importeret og solgt et produkt, som udgjorde en nærgående efterligning af sagsøgers produkt'Pocket Hose', der bar tilstrækkelig særpræg til at opnå beskyttelse efter den danske markedsføringslov. Yderligere var det en krænkelse af sagsøgers, i sagen ubestridte, designret efter EF-designforordningen, da produktet gav det samme helhedsindtryk som Telebrands EF-design.

Retten fandt, at sagsøgte som følge af krænkelserne skulle betale sagsøger et rimeligt vederlag og erstatning for det yderligere tab, som krænkelserne havde påført sagsøger. Retten fastsatte skønsmæssigt beløbet til 150.000 danske kr. På trods af, at sagsøgte havde modtaget advarselsbreve fra sagsøger vedrørende krænkelserne, var sagsøgte fortsat med at markedsføre krænkende produkter. Retten vurderede derfor, at de tre ledende skikkelser, grundet deres ledende roller i virksomheden, måtte hæfte solidarisk med Bilablau ApS.

Læs hele dommen her:
http://domstol.fe1.tangora.com/media/-300011/files/Dom18539-18.pdf

Frakke fra Baum und Pferdgarten A/S nød beskyttelse som ikke-registreret EF-design

Den danske sø- og handelsret ('Sø og Handelsretten') afsagde den 4. november 2019 dom i sagen BS-42938/2018-SHR mellem Baum und Pferdgarten A/S ('Baum') og DK Company Vejle A/S ('DK Company'). Sagen angik, hvorvidt en frakke fra Baum, med stylenavnet »Bellona«, var beskyttet som et ikke-registreret EF-design, og i så fald om DK Company ved markedsføring og salg af en lignende frakke, »ICHI«, havde krænket designet efter Rådets Forordning (EF) Nr. 6/2002 af 12. december 2001 ('EF-designforordningen') og lov nr. 426 af 3. maj 2017 ('den danske markedsføringslov').

Ifølge EF-designforordningen nyder et design beskyttelse som et ikke-registreret EF-design i tre år fra offentliggørelsen, hvis det kan karakteriseres som nyt og individuelt, jf. artikel 4, 5 og 6. Retsvirkningen heraf er, at indehaveren har eneret til at bruge det pågældende design og således kan forbyde tredjemand at udøve en sådan brug, jf. artikel 19 stk. 2.

Sø- og Handelsretten fandt, at frakken »Bellona« var sammensat af designelementer på en sådan ny og individuel måde, at frakken opfyldt betingelserne for at nyde beskyttelse som et ikke-registreret EF-design i tre år fra offentliggørelsen. Frakken »ICHI« udgjorde en så nærgående efterligning af »Bellona«, at det ikke kunne formodes, at DK Company havde udviklet den i en selvstændig proces uden kendskab til den anden frakke.

Retten fandt derfor, at DK Company havde krænket Baums rettigheder efter EF-designforordningens artikel 19 stk. 2. Eftersom DK Company iværksatte designarbejdet med »ICHI« blot få måneder efter ophøret af Baums markedsføring af »Bellona«, havde selskabet tillige handlet i strid med god markedsføringsskik efter den danske markedsføringslovs § 3 stk. 1.

Læs hele dommen her:
http://domstol.fe1.tangora.com/media/-300011/files/Dom-BS-42938-2018.pdf

Domænet »*jobindekset.dk*« skulle overføres til klageren

Det danske klagenævn for domænenavne ('Klagenævnet for Domænenavne') afsagde den 18. september 2019 afgørelse i sag j.nr. 2019-1037, mellem Jobindex A/S ('klager') og Rentbuyestate.com A/S ('indklagede'), hvorefter Klagenævnet for Domænenavne tilpligtede indklagede at overføre domænet »*jobindekset.dk*« til klager.

Klager gjorde gældende, at dennes hjemmeside havde været i drift siden 1996, og udgør en af Danmarks største websites, samt at klager selv fandt på kendetegnet »Jobindex«, og har ordmærket »JOB-INDEX« registreret som varemærke. Klager gjorde gældende, at indklagede krænkede klagers varemærket.

Indklagede gjorde gældende, at klageren ikke havde varemærketten til ordet »jobindekset«, og at registreringen derfor ikke var i strid med god domænenavnsskik.

Indklagede meddelte i duplikken, at denne havde afregistreret domænet, hvorfor det stod klager frit for, at registrere domænet »jobindekset.dk«. Sagen kunne derefter løses i mindelighed.

Klagenævnet valgte dog uagtet at udtale, at en opretholdelse af indklagedes registrering efterfølgende ville være en overtrædelse af god domænenavnsskik i medfør af § 25, stk. 1 i lov nr. 164 af 26. februar 2014 ('den danske domænelov'). Afgørelsen er således et eksempel på, at klagenævnet ikke er underlagt forhandslingsmaksimen, og at Klagenævnet således kan tage stilling til ikke fremførte anbringender.

Domænet blev følgelig overdraget til klager.

Læs hele afgørelsen her:
https://www.domaeneklager.dk/sites/default/files/2019-09/2019-0137-R%20-%20jobindekset.dk_.pdf

Domænet »*pdfprinter.dk*« skulle ikke overføres til klageren

Det danske klagenævn for domænenavne ('Klagenævnet for Domænenavne') traf den 10. oktober 2019 afgørelse i sagen j.nr. 2019-0088, mellem enkeltmandsvirksomheden Wilken IT ('klager') og ITEKSOFT ('indklagede'). Sagen angik, hvorvidt domænet'pdfprinter.dk' skulle overføres til klager.

Klager gjorde gældende, at han havde en stærk interesse i at anvende domænet til forhandling af software til fremstilling af pdf-dokumenter, hvilket domænet tidligere har været brugt til af en tidligere domæneindehaver. På klagetidspunktet stod domænet fortsat ubenyttet på venteposition, efter domænet var blevet overdraget til indklagede i starten af 2014.

Klager gjorde gældende, at registreringen var i strid med god domænenavnsskik, efter lov nr. 164 af 26 februar 2014 ('den danske domænelov') § 25, stk. 1, da domænet stod ubenyttet hen. Klager mente derfor, at domænet skulle overdrages til den næste på ventelisten: klagers firma (eller klager som privatperson).

Klagenævnet for Domænenavne fandt, at klager havde en naturlig kommerciel interesse i at benytte domænet: »pdfprinter.dk«. Imidlertid fandt klagenævnet, at også indklagede havde en kommerciel interesse i domænet. Til trods for, at indklagede først efter klagens indgivelse etablerede en hjemmeside under det omstridte domæne, »pdfprinter.dk«, fandt klagenævnet, at der ikke er tilstrækkeligt grundlag for at fastslå, at indklagede ikke havde en loyal interesse i at opretholde registreringen af domænenavnet »pdfprinter.dk«.

Klagenævnet for Domænenavnes foretagne interesseafvejning faldt

derfor ud til fordel for indklagede, da klagenævnet ikke fandt at klagers interesse væsentligt oversteg indklagedes interesse i domænet »pdfprinter.dk«. Klagenævnet konkluderede derfor, at indklagedes fortsatte registrering af domænet ikke var i strid med god domænenavnsskik, jf. den danske domænelov § 25, stk. 1. Domænet skulle derfor ikke overføres til klager.

Læs hele afgørelsen her:

https://www.domaeneklager.dk/sites/default/files/2019-10/2019-0088%2C%20pdfprinter.dk_.pdf

Den danske forbrugerombudsmand fastslår, at et selskab anvendte vildledende og aggressiv markedsføring ved telefonsalg af antivirusprogrammer

Den danske forbrugerombudsmand ('Forbrugerombudsmanden') afgav den 28. oktober 2019 sin vurdering i sag nr. 18/06780. Sagen vedrørte et selskab, der havde anvendt telefonsalg til salg af antivirusprogrammer. Selskabet ringede forbrugerne op uden forudgående samtykke og undlod at oplyse forbrugerne om, hvorvidt der gjaldt en fortrydelsesret.

Forbrugerombudsmanden vurderede, at selskabet ved telefonsalget havde anvendt vildledende markedsføring og aggressiv handelspraksis over for forbrugere, som stred med lov nr. 426 af 3 maj 2017 ('den danske markedsføringslov') § 6, stk. 1 og § 7, sammenholdt med § 8.

Dertil fandt Forbrugerombudsmanden, at selskabets undladelse af at oplyse forbrugerne om fortrydelsesrettens bortfald i forbindelse med telefonsælgerens installering af antivirusprogrammet på forbrugerens computer stred med lov nr. 1457 af 17. december 2013 ('den danske forbrugeraftalelov') § 8, stk. 1, nr. 9.

Selskabets indhentede samtykker til at kontakte forbrugerne telefonisk, var opnået i forbindelse med forbrugernes deltagelse i forskellige konkurrencer på internettet. Forbrugerombudsmanden fandt ikke, at selskabets dokumentation for samtykkerne var tilstrækkelig. Dokumentationen var fremsendt i form af links til konkurrencer, der ikke længere var aktive, eller ikke længere så ud, som de gjorde på tidspunktet for forbrugernes deltagelse. Forbrugerombudsmanden fandt herefter, at selskabet havde handlet i strid med den danske forbrugeraftalelov § 4, stk. 1, da dokumentationen ikke kunne udgøre bevis for forbrugernes samtykke til telefoniske henvendelser.

Læs hele udtalelsen her:

https://www.forbrugerombudsmanden.dk/find-sager/markedsfoeringsloven/sager-efter-markedsfoeringsloven/vildledning/telefonsalg-var-i-strid-med-markedsfoerings-og-forbrugeraftaleloven/

Den danske Sø- og handelsret finder, at markedsføring af miljømæssige fordele stred med markedsføringsloven

Den danske sø- og handelsret ('Sø- og Handelsretten') afsagde den 11. november 2019 dom i sagen BS-44586-SHR mellem ELLEPOT A/S ('Ellepot') og Sungrow A/S ('Sungrow'). Sagen vedrørte, hvorvidt Sungrows brug af udsagn såsom »100 % nedbrydelighed« i markedsføringen af papirpotten PlantPaper U1 udgjorde misligholdelse af et tidligere retsforlig mellem parterne, som forbød sagsøgte at benytte visse udsagn i dennes markedsføring, og hvorvidt Sungrows markedsføring i øvrigt stred med lov nr. 426 af 3. maj 2017 ('den danske markedsføringslov').

Sø- og Handelsretten konkluderede indledningsvist, at Sungrow ikke havde overholdt det retsforlig, som parterne havde indgået ved en tidligere sag, da de i deres efterfølgende markedsføring fortsat gjorde brug af udsagn, som de efter forliget ikke måtte benytte.

Retten vurderede derefter, at Sungrow ikke tilstrækkeligt havde dokumenteret, at deres papirpotter kunne nedbrydes i jorden. Derimod havde Sungrow alene dokumentation for, at papirpotterne var nedbrydelige såfremt de senere blev gravet op igen og anbragt i et industrielt komposteringsanlæg. Sø- og Handelsretten fandt derfor, at Sungrow havde udeladt væsentlige informationer i deres markedsføring, som følgelig var egnet til at vildlede og til at påvirke andre erhvervsdrivendes økonomiske adfærd eller skade konkurrenter. Markedsføringen var derfor i strid med den danske markedsføringslov § 20, stk. 1.Retten konkluderede, at Sungrow måtte forbydes at benytte sig af de omtvistede udsagn i deres markedsføring, såfremt Sungrow ikke samtidigt angav, at PlantPaper U1 alene kunne nedbrydes i et industrielt komposteringsanlæg. Dertil påbød Retten, at Sungrow i et år fra domsafsigelsen, på deres hjemmeside, skulle offentliggøre en berigtigelse af deres hidtidige markedsføring.

Læs hele afgørelsen her:

http://domstol.fe1.tangora.com/media/-300011/files/Deldom_BS-44586-2018-SHR.pdf

Der forelå ikke uberettiget videreudvikling eller kopiering af sofaer i strid med sagsøgers rettigheder

Den danske Sø- og Handelsret ('Sø- og Handelsretten') har afsagt dom i sag BS-25746/2018-SHR den 25. november 2019, mellem sagsøger BRUUNMUNCH FURNITURE ApS og sagsøgte Danish Design Supply ApS (også benævnt »Icons of Denmark«) samt Barreth Holding ApS. Tvisten angik hvorvidt sagsøgte uberettiget havde videreudviklet eller kopieret møbler i strid med sagsøgers designrettigheder.

Sagsøger havde nedlagt påstand om erstatning, forbud mod salg af de påståede krænkende modeller samt overdragelse af de udviklede produkter. Sagsøgte havde som

modsvar påstået frifindelse såvel som de havde nedlagt selvstændig påstand om, at sagsøgte skulle betale erstatning.

Parterne havde i 2016 indgået en samarbejdsaftale omkring overdragelse af rettighederne til produktion, markedsføring og salg af en række sofamodeller. Af aftalen fremgik, at såfremt designeren udarbejdede en model, som fremtrådte som en videreudvikling af de overdragne modeller, skulle modellen først tilbydes BRUUNMUNCH FURNITURE ApS.

BRUUNMUNCH FURNITURE ApS gjorde gældende, at aftalen indebar en loyalitetsforpligtelse som sagsøgte overtrådte ved at levere til en af sagsøgers væsentligste kunder. Yderligere gjorde sagsøger gældende, at der var foretaget en videreudvikling en sofamodel omhandlet i samarbejdsaftalen.

Sø- og Handelsretten fandt på baggrund af skønserklæringen og sagens oplysning, at BRUUNMUNCH FURNITURE ApS ikke havde godtgjort, at sofaerne var lig hinanden og dermed i strid med samarbejdsaftalen.

Sø- og Handelsretten fandt derfor, at der ikke forelå en uberettiget videreudvikling eller kopiering i strid med sagsøgers rettigheder. Følgelig frifandt retten sagsøgte, mens sagsøger blev tilpligtet at betale sagens omkostninger.

Læs hele dommen her:

http://domstol.fe1.tangora.com/media/-300011/files/Dom-25746-18.pdf?rev1

Præjudiciel forelæggelse for EU-Domstolen omkring overgangen fra designbeskyttelse til ophavsretlig beskyttelse

EU-Domstolen afsagde den 12. september 2019 dom i sag C-683/17 mellem Cofemel – Sociedade de Vestuário SA ('Cofomel') og G-Star Raw CV ('G-Star') på baggrund af en præjudiciel forelæggelse fra den portugisiske Supremo Tribunal de Justiça.

Sagen udsprang fra en tvist mellem to tøjproducenter, hvoraf Cofomel havde produceret og markedsført tøjmodeller, der lå tæt op af G-Stars modeller ARC og ROWDY. G-Star anså modellerne som værende originale intellektuelle frembringelser, der som designværker skulle nyde ophavsretlig beskyttelse.

De præjudicielle spørgsmål omhandlede, hvilke kriterier et designværk skal opfylde, før det kan ydes ophavsretlig beskyttelse i medfør af artikel 2, litra a) i Europa-Parlaments og Rådets direktiv 2001/29/EF af 22. maj 2001 ('infosoc-direktivet'), der harmoniserer aspekter af ophavsretslovgivningen blandt medlemsstaterne.

EU-Domstolen fastslog indledningsvist, at begrebet »værk« som omhandlet i artikel 2, litra a) i infosoc-direktivet er et selvstændigt EU-retligt begreb, der skal fortolkes og anvendes ensartet. Begrebet forudsætter, efter EU-Domstolens faste praksis, at der foreligger en original genstand i den forstand, at denne er ophavsmandens egen intellektuelle frembringelse.

For at en genstand kan anses som original, er det både nødvendigt og tilstrækkeligt, at den afspejler ophavsmandens personlighed ved at give udtryk for dennes frie og kreative valg. Der er således tale om en objektiv standard. Hvis frembringelsen derimod er bestemt af tekniske hensyn, regler eller andre begrænsninger for ophavsmandens kreative frihed, vil genstanden ikke kunne anses for at have den nødvendige originalitet for at kunne udgøre et værk.

Det var den forelæggende retsinstans opfattelse, at en særegen og karakteristisk visuel effekt måtte være påkrævet for, at et værk kunne opfattes som originalt. Dette krav blev imidlertid afvist af EU-Domstolen, idet et sådant æstetisk kriterie lægger op til en subjektiv vurdering af værket.

EU-Domstolen konkluderede således, at der i medfør af artikel 2, litra a) i infosoc-direktivet ikke efter medlemsstaternes nationale ophavsretslovgivning kan stilles krav om et værks æstetisk kvaliteter, førend det kan betragtes som originalt og dermed nyde ophavsretlig beskyttelse.

Læs hele dommen her:

http://curia.europa.eu/juris/document/document.jsf;jsessionid=76125C217D7BA-1394BE3098A73957B-8F?text=&docid=217668&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=5394037

Den danske Sø- og handelsret nedlægger forbud mod firmas fremstilling af urskiver lavet af maleriet '*Paris chic*' af kunstneren Tal R

Den danske sø- og handelsret ('Sø- og Handelsretten') har afsagt kendelse i sag BS-51005/2019-SHR den 2. december 2019, mellem den danske kunstner Tal Rosenzweig ('Tal R') og KANSKE DENMARK ApS ('Kanske'). Sø- og Handelsretten nedlagde forbud mod Kanskes fremstilling af urskiver lavet af maleriet »*Paris Chic*« af Tal R i overensstemmelse med § 413 i lovbekendtgørelse nr. 938 af 10. september 2019 ('den danske retsplejelov').

Sagen omhandlede, hvorvidt Tal R kunne få nedlagt et midlertidigt forbud mod, at firmaet Kanske fremstillede ure med dele udskåret af maleriet »*Paris Chic*«, som Tal R havde ophavsretten til, men som Kanske havde købt af tredjemand. Sagen var af principiel karakter, og angik både kunstnerisk ytringsfrihed samt forholdet mellem ophavsretshaver og den reelle indehaver af værket.

Det var ubestridt at »*Paris Chic*« var et ophavsretligt beskyttet værk. De økonomiske rettigheder, som Tal R besad som ophavsmand, omfattede blandt andet eneretten til at gøre værket tilgængeligt for almenheden i ændret skikkelse, jf. § 2, stk. 1, i lovbekendtgørelse nr. 1144 af

23. oktober 2014 ('den danske ophavsretslov').

Sø- og Handelsretten fandt, at Kanskes projekt mod Tal Rs rettigheder udgjorde en ændring af værket, og dermed var i strid med § 2, stk. 1 i den danske ophavsretslov, da værket blev gjort tilgængeligt for almenheden i ændret skikkelse. Gengivelsen af værket på virksomhedens hjemmeside udgjorde derudover en selvstændig overtrædelse af § 2, stk. 1 i den danske ophavsretslov.

Sø- og Handelsretten fandt derudover, at den påtænkte ændring af værket udgjorde en overtrædelse af Tal Rs ideelle rettigheder, jf. § 3, stk. 2 i den danske ophavsretslov, og dermed var krænkende over for ophavsmandens kunstneriske anseelse eller egenart.

Sø- og Handelsretten fandt yderligere, at Kanske ved deres markedsføring uretmæssigt havde snyltet på Tal Rs markedsposition og uretmæssigt anvendt dennes forretningskendetegn i strid med § 3, stk. 1, og § 22 i lov nr. 426 af 3. maj 2017 (den danske markedsføringslov').

Følgelig blev Kanske forbudt at opskære, klippe eller på anden måde ændre værket Paris Chic til brug for fremstilling og markedsføring af ure i Danmark.

Læs hele dommen her: http://domstol.fe1.tangora.com/media/-300011/files/Kendelse51005-19.pdf?rev1

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

simonsen vogtwiig

Hedda Baumann Heier og
Cecilia Orheim

Høring om gjennomføring av EUs direktiv om kollektiv rettighetsforvaltning mv.

Den 6. desember 2019 sendte Kulturdepartementet ut et høringsbrev og -notat med forslag til gjennomføring av direktiv 2014/26/EU i norsk rett, eller det såkalte CRM-direktivet. Stortinget har forpliktet seg til gjennomføringen av direktivet gjennom vedtak 10. desember 2018, jf. Innst. 90 S (2018–2019).

Som et overordnet mål skal direktivet modernisere systemet med kollektiv forvaltning av opphavsrett og nærstående rettigheter i medlemslandene. For norsk retts vedkommende vil direktivet etablere en rettslig ramme for slik forvaltning, dvs. virksomhet der kollektive forvaltningsorganisasjoner forvalter rettigheter på rettighetshavernes vegne.

Moderniseringen skal for det første skje gjennom harmonisering av regler om bedre forvaltning (good governance) og økt åpenhet og innsyn (transparancy) i kollektive forvaltningsorganisasjoners virksomhet. For det andre stiller direktivet strenge krav til rapportering, åpenhet om forvaltning og om medlemmenes medbestemmelsesrett.

Direktivet skal på denne måten bidra både til at rettighetshaverne kan føre en mer effektiv kontroll med organisasjonene, og til at forvaltningen av disse rettighetene effektiviseres.

Direktivet skal også legge til rette for og forenkle multiterritoriell lisensiering av musikkverk for bruk på nettet. Direktivet har regler om hvordan slik lisensiering skal skje, slik at man enklere kan klarere musikkrettigheter over landegrenser.

I norsk rett er ikke kollektive forvaltningsorganisasjoner særlig regulert. Åndsverksloven (lov 15. juni 2018 nr. 40 om opphavsrett til åndsverk mv.) regulerer i hovedsak selve rettighetene, men i mindre grad hvordan disse skal forvaltes. Videre er kollektive forvaltningsorganisasjoner underlagt forskjellige generelle rettsregler, alt ettersom hvilken juridisk organisasjonsform de har.

På bakgrunn av dette er det etter departementets vurdering mest hensiktsmessig å gjennomføre direktivet i en egen lov om kollektiv forvaltning av opphavsrett mv., slik de andre nordiske landene har gjort.

Høringen gjelder også direktivets forhold til eksisterende godkjenningsordninger for organisasjoner som kan inngå avtalelisenser (åndsverkloven § 63) og åndsverklovens rekkevidde for nærstående rettigheter (åndsverkloven § 114).

Høringsfristen er 7. februar 2020.

Les høringsbrevet og -notatet her: *https://www.regjeringen.no/no/dokumenter/horing---gjennomforing-direktiv-kollektiv/id2680857/*

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

Borgarting lagmannsrett avsa den 17. desember 2019 dom i saken mellom en tidligere stipendiat ved Universitetet i Oslo (UiO) og Staten v/UiO.

Saksforholdet var i korte trekk at et svensk firma hadde patent i Europa, USA og Japan på en oppfinnelse som en doktorgradsstipendiat ved UiO arbeidet med som ledd i doktorgraden. Stipendiaten var ikke oppgitt som oppfinner eller medoppfinner i det svenske firmaets patentsøknader.

Spørsmålet for lagmannsretten var for det første om stipendiaten var oppfinner eller medoppfinner av oppfinnelsen, og i så fall om hun hadde rett på godgjøring etter arbeidstakeroppfinnelsesloven § 7. For at dette skulle være tilfelle, måtte UiO som arbeidsgiver ha erervet oppfinnelsen i tråd med lovens § 4 eller «på annet grunnlag», jf. § 7.

For det andre måtte lagmannsretten vurdere om UiO var erstatningsansvarlig overfor stipendiaten etter arbeidsgiveransvaret (skadeerstatningsloven § 2-1). Dette som følge av at veilederen ved UiO hadde gjort artikkelutkast tilgjengelige for patentterververen, som hadde publisert disse i strid med stipendiatens opphavsrett.

Etter en vurdering av stipendiatens arbeid sett opp mot innholdet i patentsøknadene, kom lagmannsretten under tvil til at stipendiaten var å anse som medoppfinner. Imidlertid kom lagmannsretten til at UiO i dette tilfellet ikke hadde «disponert over oppfinnelsen på en måte som omfattes av arbeidstakeroppfinnelseslovens regler om rett til godtgjøring». Arbeidsgiveren kunne av den grunn ikke anses å ha ervervet stipendiatens medoppfinnerrettigheter, og stipendiaten hadde ikke rett til godtgjøring etter § 7.

> Etter en vurdering av stipendiatens arbeid sett opp mot innholdet i patentsøknadene, kom lagmannsretten under tvil til at stipendiaten var å anse som medoppfinner

I spørsmålet om erstatning etter arbeidsgiveransvaret, kom lagmannsretten til at UiO var ansvarlig. Det var uaktsomt av veilederen å samarbeide med patentterververen bak stipendiatens rygg. Veilederen hadde på denne måten bidratt til bruddet på opphavsretten, noe UiO måtte svare for.

Når det gjaldt utmåling av erstatning, uttalte lagmannsretten at det bare var «den konkrete utformingen av tekst og figurer/tabeller mv. som er beskyttet etter åndsverkloven», og at loven ikke gir beskyttelse av vitenskapelige ideer.

Lagmannsretten fant at det i saken ikke var ført tilstrekkelig bevis for at det forelå et økonomisk tap som kunne føres tilbake til krenkelsen av opphavsretten, og fant derfor ikke grunnlag for å utmåle erstatning for økonomisk tap etter åndsverkloven § 55.

Les dommen i Lovdatas database med saksnummer LB-2018-77812. Dommen er anket til Høyesterett og er derfor i skrivende stund ikke rettskraftig.

For ordens skyld gjøres det oppmerksom på at Advokatfirmaet Simonsen Vogt Wiig AS representerte det svenske firmaet som er eier av patent på den omtvistede oppfinnelsen. Saken ble imidlertid avvist for det svenske selskapets vedkommende på grunn av manglende norsk domsmyndighet, jf. LB-2016-135328 jf. HR-2017-803-U.

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

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

Dan Sørensen

Statens standardavtaler gjennomgår en større revisjon

Statens standardavtaler skal blir mer fleksible og brukervennlige ved å gjøre reguleringene modulbaserte og tilpasset flere leveransemodeller og leveransetyper.

Difi startet arbeidet med en større revisjon av Statens standardavtaler (SSA) i 2019, og det nye Digitaliseringsdirektoratet (Digdir) viderefører dette arbeidet i 2020. Digdir ble opprettet 1. januar 2020 som et resultat av en sammenslåing av Difi, Altinn og deler av Brønnøysundregistrene. Fra 1. september 2020 vil anskaffelsesavdelingen, som forvalter SSAene, blir overført fra Digdir til Direktoratet for forvaltning og økonomistyring (DFØ). Disse endringene kommer i kjølvannet av regjeringens ønske om økt digitalisering av offentlige tjenester.

I forbindelse med revisjonsarbeidet gjennomførte Difi en brukerundersøkelse rettet mot både kunde- og leverandørsiden samt opprettet en referansegruppe. Målet var å analysere hvordan dagens SSAer blir benyttet og få innspill til revisjonsarbeidet. Ifølge Digdir ved seniorrådgiver Charlotte Lindberg, som er prosjektleder for SSA-revisjonen, var de fleste tilbakemeldingene knyttet til behovet for enklere avtaler og mer veiledning.

Det var også tydelige tilbakemeldinger fra leverandørsiden om at avtalen for løpende tjenestekjøp (SSA-L) ble brukt til tjenesteleveranser den ikke er egnet for. Digdir ser at det er behov for en skytjenesteavtale som både kan brukes til mer sammensatte og komplekse leveranser og en enklere avtalevariant som er egnet til kjøp av standardiserte skytjenester.

Undersøkelsen viste også at oppdragsgiverne ofte bruker flere avtaler i samme anskaffelse. Det er særlig vedlikeholdsavtalen (SSA-V) som brukes sammen med kjøpsavtalen (SSA-K) eller tilpasnings- og utviklingsavtalen (SSA-T). I en del anskaffelser brukes i tillegg driftsavtalen (SSA-D). Tilbakemeldingene fra leverandørsiden tyder på at oppdragsgiverne strever med å velge riktige avtaler. Dette medfører at brukerne ofte velger avtaler som ikke passer til den faktiske leveransen.

Tilbakemeldingene Digdir har fått stemmer overens med vår egen erfaring når vi bistår i anskaffelsesprosesser. Spesielt når SSA-L skal benyttes til en eller annen form for kjøp av skybaserte løsninger bruker vi mye tid på veiledning og tilpasning samt innarbeidelse av tredjepartsvilkår for standardleveranser.

Digdirs ambisjon med den pågående revisjonen er å utarbeide mer fleksible avtaler som bygges opp av modulbaserte reguleringer, slik at avtalene kan tilpasses de ulike leveransemodellene og leveransetypene. Målet er å lage en veileder som inneholder en digital avtalebygger. Avtaleutkastet genereres da ved å sette sammen ulike moduler basert på ulike valg som brukerne gjør i veilederen. En slik veileder vil nok kunne hjelpe brukerne med å velge riktig avtalestruktur, men den vil neppe bli utviklet med det første.

I mellomtiden vil Digdir likevel utarbeide nye standardavtaler i tradisjonelt format. Disse vil inneholde standardiserte reguleringer som kan brukes på tvers av de ulike avtaletypene. I tillegg vil Digdir fokusere på klart språk og forenkling av reguleringene. Digdir har også en målsetting om at avtalene løpende blir forbedret og videreutviklet basert på tilbakemelding fra brukerne og fra innspill i fremtidige brukerforum som skal opprettes. Digdir forteller at de nå arbeider med å utvikle en mer omfattende avtale for skytjenester som blant annet skal omfatte integrasjonstjenester. Dette blir den første avtalen som blir tilgjengelig i revidert format.

Det blir interessant å se hva som kommer ut av Digdirs pågående revisjon, og hvordan de nye avtalene blir sett opp mot IKT-Norges nye standardavtaler, som har hentet mye inspirasjon fra SSAene. IKT-Norge publiserte nylig engelske utgaver av sine nye standardavtaler. Til slutt nevner jeg at Digdir i januar 2020 publiserte en standard databehandleravtale med bilag.

Dan Sørensen er senioradvokat i avdelingen for HITEK i Advokatfirmaet Selmer, Oslo.

Returadresse:
Lovdata
Postboks 2016 Vika
NO-0125 Oslo
Norge

Nytt fra

LOVDATA

Lovdata tilbyr maskinlesbare data gjennom API

Ved å bruke strukturert regelverk fra Lovdata gjennom API-tjenesten kan man utvikle nye digitale tjenester.

Hva er tilgjengelig?
Lover
Opphevede lover
Sentrale forskrifter
Stortingsvedtak
Delegeringer
Instrukser
Lokale forskrifter
Opphevde forskrifter
Statens personalhåndbok

Prismodell
Tjenesten prises ut fra mengden informasjon man har tilgang til gjennom tjenesten, og telles pr. tusen tegn pr. år. Utover dette telles ikke selve bruken av tjenesten, det vil f.eks. si at man kan laste ned så mye og så ofte man ønsker uten at dette påvirker prisen.

API-nøkkel kr 15 000,- per år
Tekst kr 18,90 per tusen tegn per år

Alle dokumenter foreligger i et XML-format med strukturer som f.eks. kapitler, paragrafer, ledd og setninger.

Lovdata holder den maskinlesbare versjonen av konsoliderte lover og forskrifter a jour parallelt med publiseringen på lovdata.no og Lovdata Pro slik at man alltid har siste versjon tilgjengelig.

Ta kontakt med marked@lovdata.no for mer informasjon om API-tjenesten.

Application programming interface

Produksjon: 07 Media