Lov & Data

Nr. 144
Desember 2020
Nr. 4/2020

Innhold

Lov&Data

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

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

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

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

Abonnementspriser for 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-123
Miljøfyrtårn®

Leder

Det arbeides for tiden med en ny app for smittesporing i Norge, og målet er at den skal være klar i slutten av desember. I november ble det publisert en befolkningsundersøkelse i forbindelse med dette utviklingsarbeidet. Undersøkelsen kartla befolkningens holdninger til å installere og aktivere en ny app for smittesporing. Svaret viste at kun en tredjedel av befolkningen ville installere en slik app, og den desidert største begrunnelsen var personvern.

Det er noe gledelig og noe bekymringsverdig ved dette. Det gledelige er at en stor andel av befolkningen er oppmerksomme på de betenkeligheter som knytter seg til innsamling av store mengder personopplysninger. Isolert sett kan vi feire dette som en stor fremgang, for bevisstløs deling av personopplysninger er et samfunnsproblem. Dersom noen skulle betvile dette, kan man eksempelvis undersøke hvordan Cambridge Analytica bistod Donald Trump i valgkampanjen i 2016. Cambridge Analytica brukte da opplysninger innhentet via en Facebook-app, og det er vel trygt å anta at mange av brukerne ville avstått fra å bruke appen dersom de kjente til at opplysningene ville brukes til å fremme Donald Trump sin valgkampanje.

Selv om det er gledelig å se at folk er bevisst på disse betenkelighetene, er det også noe paradoksalt ved situasjonen. Det er min antakelse at en stor andel av de samme menneskene, de som ikke vil installere Smittestopp, ikke har gjennomført en grundig gjennomgang av personverninnstillingene på egen mobiltelefon, Facebook-profil, etc. Vi deler fortsatt enorme data uten å vite om det, fordi vi godtar standardinnstillingene på de ulike enhetene og tjenestene vi benytter. I denne situasjonen er det altså at så mye som to tredjedeler av befolkningen vil avstå fra å installere den nye Smittestopp, dog skal det erkjennes at mange også har andre grunner enn personvern, eksempelvis batteritid.

Det er sannsynlig at appens forhistorie er en viktig del av begrunnelsen for dette. Det var mange som mente at appen innhentet mer informasjon enn det som var nødvendig for smittesporing, og Datatilsynets foreløpige vurdering gikk i samme retning, se *Varsel om vedtak om midlertidig forbud mot å behandle personopplysninger* datert 12. juni 2020. I

tillegg viste Datatilsynet til at appen også samlet inn data til forskningsformål, og at appen ikke ga mulighet til å samtykke til smittesporing uten å også samtykke til forskning.

En rapport fra Amnesty hevdet at den norske appen for smittesporing var verdens dårligste på personvern, sammen med appene som ble lansert i Kuwait og Bahrain. Dette kan det nok være delte meninger om, og rapporten ble imøtegått av Simula og mange andre, men i ettertid er det iallfall liten tvil om at personvernet kunne og burde være bedre ivaretatt i Smittestopp.

Smittestopp ble altså utviklet av Simula som et hastearbeid etter utbrudd av pandemien. Alle arbeidet under stort tidspress, alle hadde gode intensjoner, og alle gjorde så godt de kunne. I forbindelse med utlysningen av arbeidet med en ny app for smittesporing, uttalte Simula at «*Siden Simula er en forskningsinstitusjon og ikke en IT-utvikler, vil vi ikke legge inn anbud på en ny løsning. Smittestopp ble utviklet av Simula fordi Norge var i en krisesituasjon...*», se deres rapport *Sammenligning av alternative løsninger for digital smittesporing* (udatert rapport publisert på deres hjemmeside).

Det er nå en ny leverandør som skal forsøke seg, og det er ingen tvil om at mange venter spent. Den nye appen skal visstnok også hete Smittestopp, noe jeg tror er uklokt på grunn av forhistorien. Befolkningen har allerede en formening om hva Smittestopp var for noe, og mange håper at den nye appen er noe helt annet. Et nytt navn kunne vært med å signalisere dette.

Jarle Roar Sæbø

Hvordan beskytte virksomheten mot digitale angrep i koronatider?

Av Marthe Famanger Pettersen og Line Haukalid

Organisasjoner står overfor en stadig lengre rekke av sikkerhetstrusler, for eksempel datasvindel, spionasje og sabotasje. Cyberkriminelle tar kontinuerlig i bruk nye verktøy og metoder som krever at alle virksomheter jevnlig bør holde seg oppdatert, kjenne til nye trusler og sårbarheter, og vurdere om man har etablert tilstrekkelig sikring. Det kan også se ut til at koronapandemien har blitt utnyttet til det fulle.

I oktober 2020 ble Nasjonal sikkerhetsmåned arrangert for 10. gang i Norge. Dette er en årlig kampanje for å øke kunnskapen om informasjonssikkerhet. Norsk senter for informasjonssikring (NorSIS) koordinerer denne kampanjen i Norge på vegne av Justis- og beredskapsdepartementet. Datatilsynet, NOKIOS og Visma er eksempler på aktører som bidro med foredrag og delte sine erfaringer.

Marthe Femanger Pettersen

Line Helen Haukalid

Trusselbildet under koronapandemien

Truslene som har blitt rapportert under koronapandemien er de samme som før, men NorSiS sine undersøkelser viser at det rapporteres om flere og mer målrettede og avanserte digitale angrep. Grunner til dette kan være påbud om hjemmekontor, samt at cyberkriminelle utnytter befolkningens frykt og behov for informasjon.

Hjemmekontor kan utgjøre en trussel for alle bedrifter fordi det oppstår sikkerhetsutfordringer når man logger seg på bedriftens løsninger hjemmefra. Ansatte som jobber hjemmefra er ikke lengre beskyttet bak organisasjonens brannmurer, men bak sine egne hjemme-rutere, med begrenset eller ingen sikkerhet. Hjemmenettverk er generelt enkle mål for hackere, sammenlignet med sikrere internettinfrastrukturer på arbeidsplassen.

> Hjemmekontor kan utgjøre en trussel for alle bedrifter fordi det oppstår sikkerhetsutfordringer når man logger seg på bedriftens løsninger hjemmefra.

Førstelektor i Cyber Security hos Noroff, Francois Mouton, har nylig forsket på økningen av cyberangrep under koronapandemien. I forskningsartikkelen antydes det at vi vil se flere og flere ondsinnede nettsider, falske nyheter og phishing-forsøk. Eksempler på dette kan være eposter med emnefelt som «*Covid-19 testene dine har ankommet*» eller «*Endelig har ditt gratis Covid-19 testsenter åpnet, klikk her for å bestille time*». Ved første øyekast kan slike svindeleposter fremstå som sikre, ved at de tilsynelatende sendes fra troverdige avsendere som for eksempel Folkehelseinstituttet.

NorSIS publiserte i februar 2020 rapporten «Trusler og trender 2019-2020». Rapporten gjennomgår trusselbildet for små og mellomstore bedrifter i perioden 2019-2020, og redegjør for både enkelte cyberhendelser fra 2019 og de ti største digitale truslene vi står overfor i dag, som løsepengevirus, phishing, datainnbrudd og verdikjedeangrep. I tillegg fremgår det av rapporten at hele én av fire virksomheter tror at de nærmest er immune mot dataangrep.

Både rapporten fra NorSIS og forskningsrapporten fra Francois Mouton konkluderer med at god opplæring av de ansatte vil løse mange av problemene. Det er ofte enkle grep den enkelte arbeidstaker

kan ta for å bli tryggere på nett. Det handler om alt fra å kunne gjennomskue en svindelkampanje til å avsløre falske nyheter. Forhåpentligvis har Nasjonal sikkerhetsmåned bidratt til å øke kompetansen.

Tiltak for å beskytte personopplysninger i virksomheten

Personopplysninger er spesielt sårbare i dataangrep. Datainnbruddet hos Stortinget 24. august 2020 er et godt eksempel. Her ble e-poster, kontonumre, personnumre, bankinformasjon og andre personopplysninger fra ansatte og stortingspolitikere stjålet i et omfattende dataangrep.

Misbruk av personopplysninger kan ha omfattende skadevirkninger for den det gjelder, og virksomheter må derfor beskytte disse på en tilfredsstillende måte. Det følger av GDPR at dersom en virksomhet behandler personopplysninger, har den en plikt til å implementere et system for styring av informasjonssikkerhet i virksomheten. Grunnleggende krav for å oppnå et tilfredsstillende sikkerhetsnivå er risikovurderinger og etablering av tekniske og organisatoriske tiltak.

Hva som er tilfredsstillende sikkerhetsnivå må ta utgangspunkt i risikoen forbundet med behandlingen av personopplysninger i den enkelte virksomhet. En virksomhet som behandler store mengder sensitive personopplysninger (for eksempel helseopplysninger), trenger flere og sterkere sikkerhetssystemer enn en virksomhet som behandler mer trivielle personopplysninger i begrenset omfang. Risikovurderinger må foretas regelmessig, slik at de tar hensyn til endringer i trusselbildet, sårbarhet og hvilke personopplysninger man har i virksomheten.

I GDPR artikkel 32 nevnes pseudonymisering og kryptering av personopplysninger som eksempler på organisatoriske og tekniske tiltak som kan etableres i virksomheten. Det er imidlertid ikke alltid pseudonymisering og kryptering er praktisk. Andre tekniske tiltak er å sørge for antivirusbeskyttelse, totrinnsautorisasjon og at programvare er oppdatert. Nødvendige organisatoriske tiltak er tilgangsstyring basert på tjenstlig behov, taushetserklæringer, sikkerhetsinstrukser, opplæring i rutiner og bruk, og databehandleravtaler.

> Sikkerheten kan ivaretas gjennom klare og tilgjengelige rutiner som forklarer hvordan de ansatte skal koble seg til virksomhetens ressurser fra hjemmekontor.

Tiltak på hjemmekontor

En rekke enkle tiltak kan iverksettes for å bedre sikkerheten på hjemmekontor. Under årets Nasjonale Sikkerhetsmåned lanserte NorSIS, i samarbeid med og Næringslivets Sikkerhetsråd (NSR), en egen nettside med råd og tips for en tryggere digital arbeidshverdag. Tiltakene deles inn i to kategorier; tiltak som arbeidsgiver bør iverksette og tiltak som de ansatte bør iverksette.

Når det gjelder tiltak som arbeidsgiver bør iverksette, fremheves at arbeidsgiver bør sørge for at den som skal jobbe hjemmefra har tilstrekkelige ressurser til å jobbe effektivt og sikkert. Sikkerheten kan ivaretas gjennom klare og tilgjengelige rutiner som forklarer hvordan de ansatte skal koble seg til virksomhetens ressurser fra hjemmekontor. Rutinene bør også inneholde informasjon om varsling og hendelseshåndtering. Videre kan arbeidsgiver for eksempel sende ut en e-post med konkrete råd om hva den ansatte kan gjøre for å identifisere svindelmail. Et slikt råd kan blant annet være å holde musepekeren over adressen og se hvor e-posten egentlig kommer fra, og sjekke om adressen er feilstavet eller inneholder en.com-ending i stedet for. no.

Den ansatte som har hjemmekontor må være oppmerksom. Han eller hun bør unngå å blande privat IKT-utstyr, eller bruken av dette, med utstyret fra arbeidsgiver. IKT-utstyret som benyttes bør til enhver tid være oppdatert med sikkerhetsoppdateringer fra leverandøren. I tillegg må den ansatte passe på å logge av eller låse datamaskinen når den ikke brukes. Dette hindrer at barn eller andre i husstanden får tilgang til virksomhetens dokumenter, og for eksempel sletter eller publiserer noe ved et uhell.

De digitale truslene vil ikke forsvinne med det første. Alle virksomheter må fortsette med å styrke kunnskapen og bruke erfaringene de opparbeider seg. Å foreta jevnlige risikovurderinger er en viktig del av dette arbeidet.

Marthe Famanger Pettersen er advokatfullmektig i Advokatfirmaet Wiersholm.

Line Helen Haukalid er fast advokat i Advokatfirmaet Wiersholm.

Vil Bidens overvåkingsstat bli bedre?

Av Kristian Foss

Fra «land of the free» til «free to be watched». Og er Europa noe bedre?

Edward Snowdens avsløringer i 2013 åpnet øynene på dem som fremdeles ikke trodde USA var blitt en overvåkingsstat. Situasjonen ble ikke vesentlig bedre under Obama, på tross av idealistens uttalte visjon om åpenhet. Idet mange puster lettet ut etter valget av Joe Biden som USAs neste president, blir spørsmålet: vil overvåkingen reduseres og staten bli mer transparent?

Mageføelsen til mange er nok at Biden må være langt bedre for personvernet enn Donald Trump, men er det så sikkert?

EU-domstolen slo i sommer fast at at det er uforsvarlig å eksportere europeiske persondata til USA uten spesielle tiltak (Schrems II). Dette fordi amerikansk etterretningslovgivning tillater for store inngrep i personvernet. Europeiske borgere er ikke vernet mot de inngripende etterretningslovene i USA, ikke engang av det fjerde tillegget til den amerikanske grunnloven, som skal beskytte privatlivet. Tillegget lyder:

> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*

Amerikanerne som utformet grunnlovstillegget om privatliv hadde kjent de britiske koloniherrenes undertrykkelse på kroppen. De ønsket å unngå at staten skulle ha lov til å trenge inn i borgernes privatliv uten konkret grunn, og typisk bare etter en domstols konkrete kjennelse. Med den enorme forskjellen i makt mellom en enkeltperson og en stat, vil et slikt prinsipp bidra til å redusere risiko for overgrep mot enkeltmennesker.

Uten trygghet for at egne tanker, funderinger og private diskusjoner vil forbli private, vil mange sensurere seg selv, bevisst eller ubevisst. Kreativitet oppstår ofte i møtet med andre mennesker som også har frihet til uobservert å kunne lese og undersøke andres ideer. Derfor vil selvsensur og frykt redusere kreativitet og utvikling. Manglende trygghet for meningsutveksling vil således hemme opposisjon. Allerede nå viser undersøkelser Datatilsynet har foretatt en tydelig nedkjølingseffekt, som følge av både privat og statlig overvåking.

> Et samfunn hvor borgerne vet mest mulig om staten, mens staten ikke vet mer enn den trenger.

I likhet med Norge har USA regler om innsyn i det offentliges virksomhet. Vi har offentleglova og forvaltningsloven, USA har Freedom of Information Act. Tanken bak slike åpenhetslover er at borgerne bør vite mest mulig om hva staten gjør, for å kunne vurdere statens beslutninger, kreve korrigeringer og i siste instans vurdere hvilke politikere de vil velge. Det vil si et

Kristian Foss

redskap for å oppnå best mulig styring, herunder unngå overgrep mot enkeltpersoner.

For de av oss som ønsker reell personlig frihet og effektive tøyler på overvåkingen, blir idealet følgende: Et samfunn hvor borgerne vet mest mulig om staten, mens staten ikke vet mer enn den trenger.

Hvordan ligger USA an i forhold til dette idealet? Dessverre ikke så bra.

Amerikanske etterretningsmyndigheter kan

- **avlytte** ikke-amerikanere (uten kjennelse) og amerikanere (med kjennelse) etter Foreign Intelligence Surveillance Act (FISA) fra 1978, senere skjerpet gjennom overvåkingsloven Patriot Act (2001);
- **avlytte datatrafikk** ut og inn av USA (executive order 12 333 fra 1981, senere endret); og
- **kreve innsyn** i private data lagret av amerikanske selskaper, også i utlandet (Clarifying Lawful Overseas Use of Data (CLOUD,

2018) Act, som modifiserte Stored Communications Act).

EU-domstolen fremholder i Schrems II-dommen FISA som særlig problematisk. Overvåkingen under FISA skal i prinsippet godkjennes av den hemmelige FISA-domstolen, hvor bare etterretningsmyndighetene får lagt frem argumenter. Under Obamas regjeringstid fra 2008-2016 ble 99.06% av anmodningene godkjent av «domstolen». Under Trump har andelen faktisk gått noe ned.

> NSA kunne ikke fremlegge ett eneste eksempel på at masseovervåkingen hadde avverget terror.

Fra Europa kjenner vi til datalagringsdirektivet som skulle pålegge teleoperatører å lagre all telefontrafikk i seks til 24 måneder. Lagringen skulle omfatte abonnements-, lokasjons- og trafikkdata. Dataene ville gi informasjon om hvem man har hatt kontakt med på telefon og e-post, samt når og hvor man har hatt det. I tillegg skulle internettleverandører logge når og fra hvor man har logget seg på internett, fra PC og mobil.

Fra Norge kjenner vi til **etterretningstjenesteloven**, misvisende nok kalt lov om digitalt grenseforsvar. Datatilsynets direktør Bjørn Erik Thon uttalte at «Forslaget innebærer i realiteten at nær sagt alle kommunikasjonskanaler vi bruker i det daglige, kan bli gjenstand for overvåking».

Både datalagringsdirektivet og det det såkalte Digitale grenseforsvaret skapte sunn og sterk motstand. Begge ble vedtatt i EU og i Norge.

Er det noen som passer på?

Det er ganske tydelig at FISA-domstolen ikke gjør jobben sin. Derimot ser det ut som de alminnelige domstolene i USA har våknet opp. En appelldomstol (nest øverste domstol) avsa 2. september i år en dom som som slår fast at bevisene samlet inn fra masseovervåking av telefonsamtaler ikke var nødvendige for domfellelse for de aktuelle terroranklagene. NSA kunne ikke fremlegge ett eneste eksempel på at masseovervåkingen hadde avverget terror. Ankedomstolen slo dermed fast at overvåkingen var i strid med USAs fjerde grunnlovstillegg om rett til privatliv.

Også kongressen har i perioder vært opptatt av overvåkingen, ikke minst etter Snowdens avsløringer i 2013. Men mer til å stole på er formidable American Civil Liberties Union, som fører en rekke saker om brudd på det fjerde grunnlovstillegget.

Retten til privatliv i Norge og EU har i stor grad blitt reddet av EU-domstolen. Domstolen har i tre dommer fastslått at ukvalifisert masseinnsamling av persondata er i strid med *EU-pakten om grunnleggende rettigheter*. Pakten er en slags grunnlov for EU, som inneholder mye av det samme som Den europeiske menneskerettighetskonvensjonen. To sentrale bestemmelser i pakten er:

> Under Trump har andelen faktisk gått noe ned.

Artikel 7

Respekt for privatliv og familieliv

Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin kommunikation.

Artikel 8

Beskyttelse af personoplysninger

1. Enhver har ret til beskyttelse af personoplysninger, der vedrører den pågældende.

2. Disse oplysninger skal behandles rimeligt, til udtrykkeligt angivne formål og på grundlag af de berørte personers samtykke eller på et andet berettiget ved lov fastsat grundlag. Enhver har ret til adgang til indsamlede oplysninger, der vedrører den pågældende, og til berigtigelse heraf.

3. Overholdelsen af disse regler er underlagt en uafhængig myndigheds kontrol.

> Frykten og håpet griper tak i både befolkning og politikere, og kanskje også domstolene.

Det avgjørende i EU-domstolens vurderinger var at reglene som gjorde unntak fra retten til privatliv og privat kommunikasjon av hensyn til *nasjonal sikkerhet*, ikke satte tilstrekkelige skranker. Etter EUs (og norske) regler må unntaket være 'nødvendig, passende og forholdsmessig i et demokratisk samfunn'(kommun ikasjonsverndirektivet art. 15 (1)). EU-domstolen slo i saken som var anlagt mot James Bonds arbeidsgiver MI6, MI5, mfl. at den altomfattende masseinnsamlingen av data om lokasjon, avsender, mottager, varighet, tidspunkter, IP-adresse og all annen metadata (unntatt selve innholdet) var uforholdsmessig og ikke 'strengt nødvendig' (Privacy International (sak C-623/17 - 6. oktober 2020). Ikke bare kunne privatlivet krenkes, men også retten til ytringer, yrkesmessig taushetsplikt og vern av varslere.

I den andre dommen avsagt samme dag, 6. oktober i år, går domstolen enda mer direkte inn i grensene for hvilke unntak enkeltland kan gjøre fra reglene som skal sikre privatliv og ytringsfrihet (La Quadrature du Net and Others (sak

C-511/18)). Dommene vil stanse innføringen av den vedtatte etterretningstjenesteloven.

EU-dommen som annulerte datalagringsdirektivet ble avsagt 8. april 2014.

Hvorfor godtar vi overvåkingen?

Den klassiske driveren for å akseptere stadig mer overvåking er frykt kombinert med håpet om at overvåkingen vil gjøre oss alle tryggere. Frykten og håpet griper tak i både befolkning og politikere, og kanskje også domstolene.

I USA satte utviklingen mot en overvåkingsstat fart etter at USA ble rammet av terror 11. september 2001. Terrorangrepene ledet ikke bare til krigene i Afghanistan og Irak, men også til en enorm økning i overvåkningen, og vedtagelse av overvåkningsloven ironisk nok kalt Patriot Act. USAs National Security Agency (NSA) bygget ut enorme datasentre og påbegynte en overvåkning som mangler sidestykke. Alt dette muliggjort av nye lover og en flom av penger, tilrettelagt for av nyvalgte president George Bush jr. (2000-2008).

I Europa sparket bombeangrepet i Madrid i 2004 og angrepene på kollektivsystemet i London i 2005 overvåkingsballen i gang for alvor. Datalagringsdirektivet og en kraftig opptrapping av etterretningsorganisasjoner og praksis over hele Europa fulgte.

Ettersom frykten gradvis har sluppet taket og tankene klarnet, har spørsmålet om overvåkingen faktisk *fungerer,* meldt seg. Svaret er avgjørende fordi overvåkingen bare kan aksepteres dersom den virker. Samfunnskontrakten har vært; *overvåking mot sikkerhet.*

Svaret på spørsmålet ser ut til å være nei. I forbindelse med rettssaker i USA hvor spørsmålet om strid med den amerikanske grunnlovens vern av privatliv har kommet opp, har etterretningsmyndighetene i USA måttet legge frem bevis på at overvåkingen avverger terror. Ikke i ett tilfelle har dommerne blitt overbevist om dette, selv etter å ha fått tilgang til hemmelig dokumentasjon fra NSA.

Om situasjonen er at ukvalifisert masseovervåking ikke leverer den lovede sikkerheten, er samfunnskontrakten brutt. Resultatet må bli at de enormt inngripende (og kostbare) overvåkingsprogrammene avvikles.

> Om situasjonen er at ukvalifisert masseovervåking ikke leverer den lovede sikkerheten, er samfunnskontrakten brutt.

Hva skjedde med Obamas change?

Med president Barack Obama (2008 - 2016) kom nytt håp om *endring.* Åpenhet var en hovedparole. På hans første dag som president signerte han til og med et memorandum om åpenhet i staten. De første linjene leser:

> *Memorandum for the Heads of Executive Departments and Agencies*
>
> *Subject: Transparency and Open Government*
>
> *My Administration is committed to creating an* ***unprecedented level of openness*** *in Government. We will work together to ensure the public* ***trust*** *and establish a system of transparency, public* ***participation****, and collaboration. Openness will strengthen our democracy and promote efficiency and effectiveness in Government.*

Som senator hadde Obama også kritisert den vidtgående overvåkingsloven Patriot Act, som ble vedtatt etter terroren i 2001. Alt så dermed ut til å ligge vel til rette for redusert overvåking. Men hva skjedde når håpets og åpenhetens forkjemper og fredsprisvinner (2009) ble president?

Mye skjedde, men lite av den gode sorten, hva angikk overvåking.

NSAs uhemmede overvåking fikk i stor grad fortsette. Etterretningslovene ble i liten grad reformert. Varsleren Snowden og journalisten og aktivisten Julian Assange ble forfulgt. Pengebruken til etterretningsvesenet økte.

Stort sett ble den kritiserte etterretningspraksisen under Bush videreført. Allerede 5. mars 2009, bare uker etter Obama tiltrådte, ble hjemmelen for masseinnhenting av telefonopplysninger fornyet (Patriot act sec. 2015). Slike fornyelser ble gitt igjen og igjen.

Videre fortsatte den hemmelige FISA-domstolen sin praksis med å godkjenne nær alle anmodninger om overvåking fra NSA (over 99%).

USA påbegynte i 2010 forfølgelsen av journalisten Julian Assange, etter Wikileaks avsløringer av grove overtramp i bl.a. Irak og Afghanistan. Dokumentene avslørte blant annet drap på ubevæpnede sivile, amerikansk kjennskap til tortur av krigsfanger, 15 000 sivile dødsfall som tidligere ikke var rapportert, og at USA hadde beordret spionasje på FN-diplomater.

> Det er dypt bekymringsfullt at ytringsfriheten angripes på denne måten, fordi staten ikke liker budskapet (eller budbringeren).

Det er verdt å merke seg at Wikileaks-leder Assange ikke selv har lekket dokumentene, men kun publiserte dem. Det vil si journalistisk virksomhet. Det er dypt bekymringsfullt at ytringsfriheten angripes på denne måten, fordi staten ikke liker budskapet (eller budbringeren).

I 2013 begynte forfølgelsen av varsleren Snowden. Snowdens avsløringer beviste den ulovlige overvåkingen NSA tidligere hadde benektet. Mistankene om overvåking medførte at det ble holdt en rekke høringer i den amerikanske kongressen allerede fra 2012. Blant andre måtte NSA-sjef James Clapper stille. På direkte spørsmål om NSA samlet inn opplysninger om millioner av amerikanere, svarte han nei. Løgnen til NSA-sjefen motiverte Snowden til å avsløre omfanget av NSAs overvåking.

Snowdens avsløringer skjedde under arbeidet med GDPR, og gjorde det enklere for EUs lovgivere å motstå presset fra lobbyister for amerikanske og andre særinteresser. Lobbyistene for *big data* var ikke glad i planene om de høye bøtene som til slutt ble vedtatt. I det hele tatt medvirket avsløringene til at arbeidet for vern av grunnleggende rettigheter, som for eksempel retten til privatliv, fikk medvind.

Under Obama fikk NSA mer penger og overvåkingen økte. Fra 2008 til året Obama gikk av i 2016, økte budsjettet for sivil etterretning med drøyt 11% til omkring ufattelige 485 milliarder norske kroner (53 mrd USD). Beløpet utgjorde nesten en tredjedel av det norske statsbudsjettet samme år. I tillegg kom ca. 168 milliarder norske kroner til militær etterretning.

De eneste positive tiltakene mot økt overvåking av betydning under Obamas regjering besto av en reform av FISA-domstolen og motstand mot å styrke FISA ytterligere.

I sum er det imidlertid klart at Obamas regjeringstid ikke medførte særlig forbedring for personvernet. Tvert om motarbeidet myndighetene sivilsamfunnet og kongressens forsøk å få innsyn og stanse overtrampene. Og de få som våget å varsle om forholdene ble forfulgt med alle midler.

Bidens rolle

Joe Biden var Obamas visepresident. Mest oppmerksomhet fikk trolig Bidens rolle i å tvinge flyet til den bolivianske presidenten ned i Østerrike på vei fra Moskva, ved å presse europeiske land til uhjemlet å nekte overflyvning. Amerikanerne mistenkte at Snowden var ombord.

Biden tok videre kontakt med den ecuadorianske presidenten Rafael Correa for å overtale Ecuador til å nekte Snowden politisk asyl i Ecuador, slik Snowdens plan var.

> Også idealer kan korrumperes.

Julian Assange ble på sin side etterøkt og endte med å måtte søke beskyttelse i den ecuadorianske ambassaden i London. Der ble han sittende i 7 år. Nå venter han i fengsel på dom i saken om utlevering til USA (i strid med en 2016-beslutningen av et FN-panel om vilkårlig frihetsberøvelse).

Situasjonen var med andre ord at påtroppende president, og daværende visepresident Biden under «åpenhetens president» Obama, jaget en varsler og en journalist som begge bidro til avsløringer av sjokkerende og ulovlige forhold som den amerikanske staten var ansvarlig for.

Hvorfor økte overvåkningen under Obama?

At utviklingen ble slik den ble under Obama, kunne man kanskje forstått om Trump var president i perioden. Men hvordan kunne det skje under Obama?

Makt korrumperer, heter det. Korrumpering medfører ikke nødvendigvis handlinger til egen personlig vinning. Også idealer kan korrumperes. Obamas uttalte ideal var åpenhet. Når han selv kom i en posisjon hvor åpenhet kunne hindre hans eget statsapparat i å gjøre ting det mente var fornuftig, kunne åpenhet bli en trussel.

Som president omgis man av maktpersoner. Maktpersonene vil forsøke å indoktrinere en president med hvilken skade åpenhet og begrensninger kan påføre egen maktorganisasjon. Det er jobben deres. Presidenten presenteres ikke for tilsvarende motforestillinger og motkrefter. Ingen har den jobben. Over tid er det derfor ikke overraskende at til og med en type som Obama mister egne idealer av syne.

En annen, litt mer konspiratorisk, forklaring er at organisasjoner som NSA, CIA og FBI vet så mye om deg at det kan bli ubehagelig å legge seg ut med dem. Alle mennesker har noe å skjule, selv om jeg hører noen påstå at de ikke har det. Dette «noe» trenger ikke være ulovlig eller unormalt, men likevel opplysninger du ønsker å holde privat, ikke minst for politiske motstandere. Tenk for eksempel på legebesøk, et barns psykiske problemer, dommen for fyllekjøring eller sex (TV eller PC med med kamera og mikrofon hackes enkelt). Og selv om du skulle like åpenhet om selv slike ting, vil mange andre ikke like det. Som med rettssikkerhet, må alle gis det samme vernet for at vernet skal fungere.

Med slike motkrefter, skal det rak rygg til å temme det som nærmest kan karakteriseres som et overvåkingsmonster. Resultatet er dermed at en hvilken som helst president, eller statsminister, raskt blir fanget av systemet.

Hva kan endre systemet?

Et mektig overvåkingssystem kan med andre ord neppe reformeres fra innsiden selv med en velmenende president ved roret. Så hva skal til?

I prinsippet skal maktfordelingsprinsippet løse problemet. Domstolene skal kontrollere om utførende del av staten (presidenten) etterlever reglene laget av lovgiver. Heldigvis skjer dette, om enn langsomt.

© Designer Hugh D'Andrade / EFF (Electronic Freedom Foundation)
https://creativecommons.org/licenses/by/3.0/us/

Som nevnt over har **domstoler** i både USA og Europa funnet at amerikansk og europeisk overvåkningspraksis er i strid med våre mest grunnleggende rettigheter. I Europa gjelder det ikke det bare Schrems I- og II-sakene, men også stoppordren for datalagringsdirektivet og det digitale grenseforsvaret.

Men selv om særlig EU-domstolen har vært et bolverk mot overtramp, holder det alene neppe over tid. **Sivilsamfunnet** og **folk flest** må bry seg. Politikerne som vedtar lover som krymper privatlivet vårt, må stemmes ut. Om vi som velgere kontakter våre representanter, kan det muligens også hjelpe. Kanskje må vi demonstrere i gatene. En dag dukker kanskje et parti med personvern som fanesak opp, slik miljøpartiene har.

For å komme dit må flere **journalister** våkne opp. Publiseres ikke overtrampene, glemmes de. Den fjerde statsmakten må ikke bare beskytte ytringsfriheten, men også forløperen til offentlige ytringer, nemlig private utvekslinger og funderinger - privatlivet. Hvis ikke alle kan føle seg trygge på at man kan lese, tenke, undersøke og diskutere hva man ønsker, når man ønsker og uten innsyn, vil opposisjon og utvikling sakte kveles. Da blir det ingen ytringer å forsvare.

Siden mye av våre private liv leves på nett, vil også **private selskapers** holdninger være viktige. Til og med i USA ser vi positive tendenser fra noen selskaper. Microsoft og Apple har gjort det til en fanesak å forsvare privatlivet og fulgt opp med handling.

I USA gir visse **delstaters** holdninger grunn til håp. California har knapt rukket å sette California Consumer Protection Act i kraft, før velgerne 3. november i år stemte for den nye California Privacy Rights Act. Sistnevnte vil bringe verdens sjette største økonomi mye nærmere vår egen GDPR og forhåpentlig vise vei i USA.

Obama, Trump eller Biden verst?

Obama og Biden var ikke bra for overvåkingen i sine åtte år. Trump er totalt uforutberegnelig, empatiløs og primært styrt av egeninteresse. Det er likevel interessant å merke seg at FISA-domstolen under

Trump har avslått flere anmodninger om overvåking enn under Obama, selv om reduksjonen kanskje kan tilskrives Obamas reform.

> Obama ville, men fikk lite til.

Trump uttalte også flere ganger under sin valgkamp i 2016 at han elsket Wikileaks. Grunnen var imidlertid publiseringen av Hillary Clintons eposter, neppe idealisme. Et av de første vedtakene Trump gjorde i sin nåværende periode, var videre å annullere en Federal Trade Commission-regel som påla telekomoperatører å besørge at telefondata forblir konfidensielle (slik kommunikasjonsverndirektivet gjør i Europa). Dernest sørget Trumps republikanere i kongressen for at Obamas forslag til ny personvernlov ikke ble vedtatt.

Før sitt presidentskap, uttalte Trump at Snowden burde skytes. Men i motsetning til Obama, synes Trump likevel å ville vurdere å benåde Snowden. Dessverre er trolig motivasjonen igjen rent personlig, heller enn prinsipiell. Trump mener han selv har vært overvåket. Eksemplene viser uansett Trumps prinsippløshet.

Obama ville, men fikk lite til. Biden vil neppe veldig, og har neppe kraften om han så ville. Jakten hans på Snowden i 2013 lover ikke godt. Jeg tror dermed ikke Bidens overvåkningsstat vil bli vesentlig bedre *på grunn av* Biden. Men den kan bli bedre på grunn av andre krefter, som domstolene, deler av pressen, USAs sterke sivilsamfunn og kanskje som følge av kongressens arbeid, når korona og Trumps galskap har sluppet taket. Og fordi vanlige mennesker ser at overvåking ikke gjør dem trygge.

Advokat Kristian Foss er partner i Bull & Co Advokatfirma, med over 20 års erfaring fra personvern, IT- og teknologijuss. Foss er medlem av Fagutvalget for IKT-rett i Juristenes utdanningssenter og har har vært president i IT IP Law Group Europe.

FAKTABOKS SNOWDEN OG BAKGRUNN

For dem som vil sette seg inn Snowdens historie, se dokumentaren 'Citizen Four' om Snowdens flukt, 'Snowden' (Oliver Stone), les 'No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State' (Glenn Greenwald, 2015) eller 'Systemfeil' (Edward Snowden, 2019) og tidslinjene fra Propublica.org og Electronic Frontier Foundation. The Guardian og The New York times har også hatt god dekning.

Halvor Manshaus og Inge Kristian Brodersen

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

Senioradvokat i Advokatfirmaet Schjødt AS, Oslo, med spesialisering innen IT og personvern.

I kjernen av europeisk personvern – ny veileder fra Personvernrådet om overføring av personopplysninger til tredjeland

1. Innledning

Tirsdag 10. november publiserte det europeiske Personvernrådet («European Data Protection Board» (EDPB)) en veiledning som gjelder overføring av personopplysninger til land utenfor EU (såkalte tredjeland).[1] Veiledningen, som i fulltekst heter «*Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*», følger i kjølvannet av den mye omtalte Schrems II-avgjørelsen som kom fra EU-domstolen tidligere i år.[2]

Schrems II-tematikken, herunder myndighetsovervåkning av borgere og praktiseringen av reglene om overføring av personopplysninger over landegrenser, berører helt fundamentale utgangspunkter i europeisk personvernrett. I punkt 2 og 3 nedenfor vil vi kort plassere den siste tids rettsutvikling innenfor europeisk personvern i en bredere kontekst, både i et historisk og et politisk perspektiv. Vi håper at dette vil bidra til en bedre forståelse for det konkrete innholdet i Schrems I- og II-avgjørelsene og den etterfølgende veiledningen som nå har kommet fra Personvernrådet, som oppsummeres i henholdsvis punkt 4 og 5 nedenfor.

2. Europeisk personvern – et tilbakeblikk

På personvernområdet er Europa en premissleverandør, og i andre deler av verden ser mange land på den europeiske tilnærming til personvern som en «gullstandard».[3] Hvordan er det blitt slik?

I tillegg til økt bevissthet om personvern gjennom Den europeiske menneskerettskonvensjon (EMK) og FN, har særlig Tysklands rolle vært sentral i utviklingen av europeisk personvern i etterkrigstiden. Tyskland har fra 2. verdenskrig og gjennom årene med overvåkning i regi av Stasi, det hemmelige politiet i Øst-Tyskland, levd gjennom offentlige regimer med sterk grad av overvåkning. På dette dystre bakteppet utviklet Vest-Tyskland i 1970-tallet sine første personvernlover, som ble alle tyskere til del da landet ble gjenforent i 1990.[4]

Tysklands tilnærming til personvern har hatt stor innflytelse på resten av Europa. For å adressere utfordringene ved økende datatrafikk på tvers av landegrensene, gikk EU-landene på 1990-tallet sammen om å utforme et felleseuropeisk regelverk om personvern. Samarbeidet førte til EU-direktivet fra 1995, som var utgangspunktet for en rekke nasjonale personopplysningslover i hele EU, blant annet den forrige norske personopplysningsloven fra 2000. Regler om begrensninger på mulighet for overføring av personopplysninger til tredjeland ble etablert på denne tiden. Herfra trekker vi linjen gjennom en rivende teknologisk utvikling med sosiale medier, skytjenester, adtech, kunstig intelligens osv., med ditto dramatisk økning i utveksling av personopplysninger, via Snowden og NSA, Schrems I-dommen fra 2015[5], helt

1 *https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en*

2 *http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=12312155*

3 Ref. Graham Greenleaf «The Influence of European Data Privacy Standards Outside Europe» (2012)

4 Ref. Anu Bradford «The Brussels Effect: How the European Union Rules the World» (2018), og Thomas Shaw (IAPP-artikkel fra 2013): *https://iapp.org/news/a/2013-03-01-privacy-law-and-history-wwii-forward/*

5 *http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=111441*

til EUs «General Data Protection Regulation» (GDPR) som i Norge ble innlemmet gjennom ny personopplysningslov av 2018. Den siste utviklingen i denne lange linjen er altså Schrems II-dommen.

3. Forholdet til USA

Enhver behandling av personopplysninger som tilhører europeiske borgere, er i prinsippet underlagt GDPR-regimet og har betydning for de fleste leverandører i verden som leverer tjenester til Europa. GDPR representerer i dag det strengeste og mest betydningsfulle personvernregelverket på global basis.

Europeisk personvern skaper til stadighet friksjon mot land i andre deler av verden, og i særdeleshet USA. Sett i forhold til EU, er USAs regler om personvern til dels umodne, dels vektet i favør av myndighetenes ønske om kontroll og overvåkning fra et nasjonalt sikkerhetsperspektiv og ikke minst kommersielle interesser. Tjenestene fra gigantselskapene fra USAs vestkyst (Facebook, Google, Apple, Twitter, Amazon osv.) som de fleste europeiske borgere benytter seg av, gjerne på daglig basis, innebærer en massiv innsamling av personopplysninger – og overføring av disse fra EU til USA. I boken «The Age of the Surveillance Capitalism» (2019) gjør den fremtredende amerikanske forskeren Shoshana Zuboff en vri på det orwellianske begrepet «Big Brother» og kaller den nå allestedsnærværende overvåkningskapitalismen for «the Big Other».

Det er ikke bare på personvernområdet EU blir provosert av de amerikanske gigantselskapene. EU har også iverksatt tiltak for å motvirke uønsket markedsdominans og å øke skattelegging. Sistnevnte tema var gjenstand for en egen artikkel i denne spalten helt nylig. Man skal i denne sammenheng ikke se helt bort fra at EUs tiltak mot amerikanske selskaper på personvernområdet, også kan ha en viss kommersiell og realpolitisk motivasjon.

4. Schrems I og II

Avgjørelsene er oppkalt etter den østerrikske advokaten og personvernaktivisten Max Schrems. Siden 2011 har Schrems krevet at det irske datatilsynet må stoppe overføringer av personopplysninger mellom Facebooks irske enhet og Facebooks amerikanske enhet. Kjernen i hans argumentasjon er at USA ikke tilbyr samme nivå av personvern som Europa, herunder at amerikanske myndigheter bedriver masseovervåkning av privatpersoner, som blant annet avslørt av Edward Snowden i 2013.

I den såkalte Schrems I-avgjørelsen fra 2015 besluttet EU-domstolen at den såkalte Safe Harbour-mekanismen (en form for selvsertifisering av amerikanske bedrifter) var ugyldig som grunnlag for overføring fra EU til USA. En konsekvens av Schrems I-avgjørelsen var etableringen av Privacy Shield-mekanismen, som i prinsippet skulle fylle samme funksjon som Safe Harbor, men forutsetningsvis med et tilfredsstillende sikkerhetsnivå etter europeiske regler.

Schrems slo seg ikke til ro med dette, og nå i juli falt Schrems II-dommen. EU-domstolen konkluderte i denne avgjørelsen med at Privacy Shield-mekanismen ikke sto seg. EU-domstolen viste riktignok til at et annet og praktisk overføringsgrunnlag, «EU Standard Contractual Clauses» (SCC), ikke var ugyldig som sådan. Samtidig oppstilte domstolen flere vilkår som må være oppfylt for at overføring av personopplysninger til land utenfor EU skal være lovlig. Det ble understreket at bruk av SCC-malen i seg selv ikke nødvendigvis medfører tilstrekkelig grunnlag for lovlig overføring av personopplysninger ut fra EU.

I vurderingen av hva som kreves som tilstrekkelig grunnlag for overføring, er det verdt å fremheve to sentrale premisser fra Schrems II:

1. § 702 i USAs Foreign Intelligence Surveillance Act (FISA §702) åpner for en uforholdsmessig stor grad av overvåkning, ettersom loven ikke har begrensninger for når myndighetene kan samle inn utenlandsk informasjon. FISA §702 gjelder de dataimportører som er såkalt «electronic communication service providers» («ECSP»). Dette omfatter tilbydere av ekomtjenester slik vi kjenner det fra europeiske ekomregler, men går lenger ved at skyleverandører og visse leverandører av innholdstjenester også omfattes. De som ikke regnes som ECSP etter definisjonen kan derfor avtale at utlevering etter FISA § 702 ikke skal skje.
2. Både nevnte § 702 og overvåking i henhold til USAs Executive Order 12 333 (EO 12 333) tillater innsamling av data utover hva som anses «strengt nødvendig» etter Europeisk personvernrett. EO12 333 gjelder bulkinnsamling for data som fraktes til USA, typisk via undersjøiske kabler. For å begrense amerikanske myndigheters tilgang etter EO 12 333, kan man vurdere en kombinasjon av tekniske og avtalemessige tiltak. Man kan for eksempel avtale at importøren ikke frivillig skal hjelpe amerikanske myndigheter med innhenting hjemlet i EO 12 333 og at opplysningene krypteres (med tilstrekkelig styrke) samt at nøkkelen ikke må være tilgjengelig for myndighetene.

I realiteten overlater derfor EU-domstolen til de enkelte virksomheter å gjøre komplekse risikovurderinger, herunder av andre lands lov og rett. Dommen er også skrevet i et vanskelig tilgjengelig og utpreget juridisk språk. Med tanke på det potensielt skyhøye nivået for bøter for brudd på GDPR, er Personvernrådets nye veiledning som klargjør disse forutsetningene både etterlengtet og nødvendig for at mar-

kedsaktørene skal være i stand til å opptre på riktig måte.

5. Personvernrådets veileder av 10. november

Personvernrådets nye veileder gir en detaljert oversikt over hvordan virksomheter skal håndtere overføring av personopplysninger til land utenfor EU. Veilederen er foreløpig et utkast til høring med frist for innspill 30. november, men utkastet fremstår som så omfattende og gjennomarbeidet at vi ikke forventer vesentlige endringer.

Veilederen inneholder kun anbefalinger og utgjør ikke bindende lovgivning, men utgjør det nærmeste verktøyet å gripe til per i dag. Det er ikke gitt noen utsettelse av håndheving av brudd på GDPR som følge av behov for tilpasning etter Schrems II-avgjørelsen, så i praksis anbefales samtlige virksomheter som berøres å implementere anbefalingene fra veilederen.

Veilederen gjelder overføring til alle såkalte tredjeland - ikke bare til USA som sådan. Kort sagt kan man si at Personvernrådet legger til grunn at mange land utenfor EU har dårligere personvern enn EU, ofte fordi andre lands overvåkning av kommunikasjon er større enn i EU. Personvernrådet sier derfor at bedrifter må iverksette ekstra tiltak som gjør at slik overvåkning ikke kan skje.

Veilederen omfatter seks steg som berørte virksomheter oppfordres til å følge:

1. Kartlegg hvor personopplysningene overføres, hvilke personopplysninger det gjelder og omfang.
2. Sjekk at gyldig overføringsgrunnlag foreligger.
3. Vurder relevant lovgivning og praksis i tredjelandet.
4. Identifiser og implementer ytterligere tiltak innenfor følgende kategorier:
   a. Tekniske tiltak (f.eks. kryptering, pseudonymisering mv.)
   b. Kontraktuelle tiltak (f.eks. innarbeide kontraktuell forpliktelse om å implementere tekniske tiltak, forpliktelse til å varsle ved forestående myndighetsinngrep, overholde individers rettigheter mv.)
   c. Organisatoriske tiltak (f.eks. utarbeidelse av interne «governance policies», sørge for transparens, dataminimering mv.)
5. Overhold eventuelle formelle prosedyrer, herunder eventuelt behov for godkjenning av tilsynsmyndighet mv.
6. Foreta re-evaluering med jevnlige mellomrom.

Ingen av stegene er enkle, men i praksis mener vi det nok vil være steg 3 (vurdering av tredjelandets lovgivning/praksis) og steg 4 (implementering av ytterligere tiltak) som vil volde mest hodebry.

Når det gjelder steg 3, har riktignok EU-domstolen i Schrems II-dommen allerede slått fast at overvåkningsnivået i USA er for høyt. Vurderingen må imidlertid gjøres også for andre tredjeland som er involvert, og vil i praksis være krevende for mange virksomheter. Til hjelp har Personvernrådet laget en egen veileder om «EUs Essential Guarantees for surveillance meaures»[6] som kan brukes som et «komparativt» hjelpemiddel.

Implementering av ytterlige tiltak i samsvar med steg 4 er bare relevant dersom man i vurderingen av steg 3 har kommet til at den valgte overføringsmekanismen (typisk SCC) i seg selv ikke er tilstrekkelig for at de overførte personopplysningene beskyttes tilsvarende som i EU. Ytterligere tiltak – tekniske, kontraktuelle og/eller organisatoriske - må derfor implementeres eksempelvis ved overføring til USA.

Personvernrådet gir uttrykk for å ha størst tiltro til de tekniske tiltakene (jf. avsnitt 48): «*Indeed there will be situations where only technical measures might impede or render ineffective access by public authorities in third countries to personal data, in particular for surveillance purposes.*» I veiledningens Appendix 2, drøfter veilederen ulike eksempler på aktuelle tekniske tiltak. Det listes for det første opp ulike eksempler på scenarier (Use Case 1-5) hvor EU mener det er mulig å implementere tekniske tiltak som kan medføre tilstrekkelig beskyttelse og derfor kvalifisere som adekvate ytterligere tiltak. EU lister deretter opp 2 scenarier (Use Case 6-7) hvor det etter deres syn ikke er mulig å implementere slike tiltak. Eksempelvis skriver Personvernrådet for «Use Case 1» at det kan være mulig for en dataeksportør å bruke en leverandør («hosting service provider») av lagringstjenester for back-up-formål i tredjeland, forutsatt at opplysningene underlegges streng kryptering før overføring og at krypteringsalgoritmen er tilstrekkelig sikker. Dessuten må krypteringsnøkkelen fullt ut være utenfor importørens og tredjelandets myndigheters kontroll. «Use Case 1» har sitt motstykke i «Use Case 6» på den måten at sistnevnte scenario gjelder når dataimportøren vil ha tilgang til «data in the clear», altså at skyleverandøren har tilgang til ukrypterte, «rå» personopplysninger. Her ser ikke Personvernrådet per dags dato noen mulighet for tekniske tiltak som kan motvirke dette, og kan for eksempel ikke godkjenne overføring til en skyleverandør som må ha tilgang til ukrypterte personopplysninger for å utføre tjenesten.

I tillegg har EU nettopp utgitt et eget hjelpemiddel for de «kontraktuelle» tiltakene. Utkast til nye SCC fra EU-kommisjonen ble sendt på høring 12. november, med oppdaterte avtalemekanismer som kan

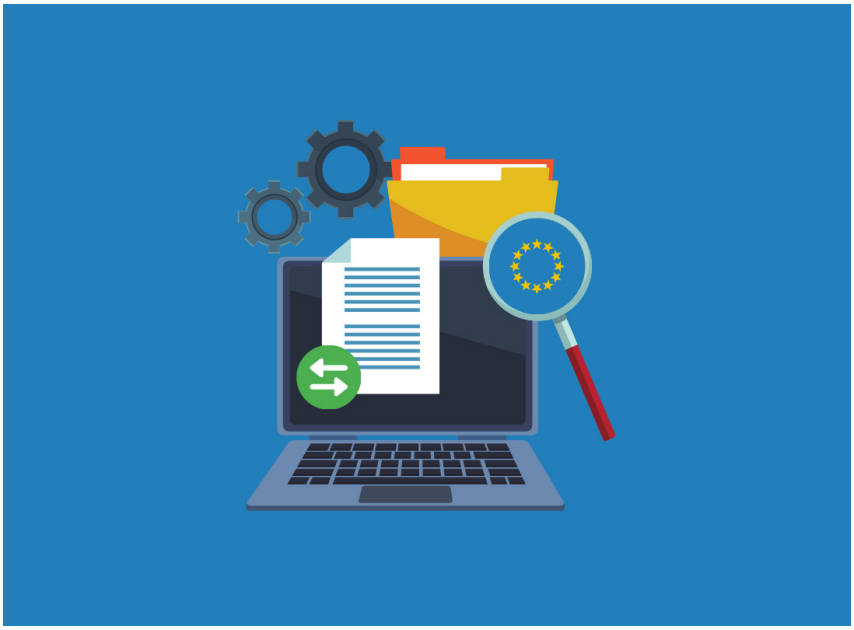
6 *https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en*

være relevante ved overføring til tredjeland.[7]

6. Avsluttende om utlevering

Veilederen er grundig og går konkret til verks - det må regnes som positivt i en situasjon som lenge har fremstått som uoversiktlig for mange aktører i markedet. Samtidig medfører veilederen til dels omfattende arbeid fra de overførende virksomheters side (dvs. eksportørene), og i mange tilfeller vil nok konklusjonen bli at overføringen ikke er lovlig. I utgangspunktet er det derfor nærliggende å tenke seg at kunder vil søke mot europeiske skytjenester (uten tilgang fra tredjeland via fjernaksess) for å unngå hele problemstillingen. Det vil i så fall kunne gå utover selskaper fra tredjeland, eller som benytter seg av tjenester fra tredjeland – ikke minst de amerikanske gigantselskapene.

Det blir interessant å følge med på hvordan typiske importørene, slik som eksempelvis leverandører av skytjenester, vil tilpasse seg situasjonen, og i hvilken grad de for eksempel vil komme opp med nye tekniske løsninger som kan bidra til økt beskyttelse av europeiske personopplysninger.



Illustrasjon: https://dataprivacymanager.net/

Situasjonen har for lengst skapt storpolitiske bølger mellom EU og USA, og det har vært snakk om etablering av en sertifiseringsmekanisme bygget på samme modell som «Safe Harbour» og «Privacy Shield». Det er berettiget å reise spørsmålet om akkurat det er en god idé, etter at begge foregående mekanismer er skutt ned av herr Schrems. I kjølvannet av presidentvalget, er uansett enkelte kommentatorer forsiktig optimistiske med tanke på et bedre og mer konstruktivt samarbeid over Atlanteren også på personvernområdet[8]. Kanskje oppnår vi tilslutt adekvat beskyttelse av europeiske personopplysninger – og unngår Schrems III. I denne spalten har vi tidligere omtalt saker i USA som har omhandlet amerikanske myndigheters rett til innsyn til data lagret innen EU. Det blir altså spennende å følge denne parallelle rettsutviklingen i tiden fremover.

7 *https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries*

8 *https://iapp.org/news/a/what-could-a-biden-administration-mean-for-privacy-cybersecurity/*

Personvernforordningen – en lærebok

Av Rolf Riisnæs

Dag Wiese Schartum, *Personvernforordningen – en lærebok*. Fagbokforlaget – 340 s. Bergen 2020 – ISBN: 978 82 450 3387 8

Innledning

Det er noen ganske få regelverk som er relevante for nær sagt alle virksomheter – offentlige og private – og som i praksis berører oss alle som enkeltpersoner. Ett av dem er personvernforordningen. Det skal godt gjøres, som praktiserende jurist, å ikke måtte forholde seg til eller bli berørt av personvernforordningen på en eller annen måte. Det er derfor svært velkomment at Dag Wiese Schartum (heretter «forfatteren») nå har skrevet en lærebok om emnet.

Det er en krevende oppgave forfatteren har løst. Personopplysningsretten er et fag det tar tid å «få tak på». Det er et typisk «systemfag» der kunnskap om enkeltbestemmelser ikke er til så stor hjelp om man ikke samtidig har grep om fagets systematikk og grunnleggende prinsipper og sammenhenger. I tillegg kommer at personvernforordningen er bygget opp på en måte som ligger langt fra norsk lovgivningstradisjon; den fremstår fragmentert, abstrakt og med et komplisert språk, og er preget av kompromisser gjennom en lang tilblivelsesprosess. At personvernforordningen har som formål å legge til rette for fri flyt av personopplysninger innenfor EØS-området, ved å fastlegge ensartede, men generelle, krav til behandlingen av personopplysninger for å sikre de berørte fysiske personers rettigheter og friheter på tvers av ulike anvendelsesområder, gjør det ikke mindre komplisert.

Forfatteren skriver selv (på s. 29-30) at: «*Personvernforordningen er på mange måter et «uhyre» av et regelverk på ca 100 sider normal tekst. Selve forordningsteksten har 99 artikler som til sammen utgjør mer enn 26.000 ord. I tillegg kommer fortalen bestående av mer enn 20.000 ord fordelt på 173 avsnitt. … Kombinert med en lovgivningsstil med til dels meget lange og innfløkte setningskonstruksjoner, vanskelig – og noen ganger inkonsistente – logiske resonnementer og en utpreget fragmentarisk regulering, er det imidlertid krevende å sette seg inn i denne viktige delen av personopplysningsretten. Riktignok er det stort sett logisk rekkefølge på kapitler og bestemmelser. Problemet er bare at det er så mange mulige, implisitte sammenhenger og samspill på kyss [!] og tvers i forordningsteksten … Med denne boken blir det forhåpentligvis litt lettere å trenge gjennom regelmaterien.*»

Forfatteren ønsker å sette leseren i stand til å resonnere selvstendig. Dette mener jeg han har løst på en utmerket måte.

Hva boken omfatter

Personvernforordningen regulerer det vi etter vært har blitt vant til å kalle «personopplysningsrett» eller «personopplysningsvern». Forfatteren redegjør innledningsvis i boken godt for hvordan personopplysningsretten forholder seg til det bredere begrepet «personvern» som også omfatter sider ved menneskerettighetene og regler om privatlivets fred mv. Deretter behandler han, relativt kort, men presist, sentrale begreper og sammenhenger, før han går løs på den betydelige oppgaven med å systematisere fremstillingen av personvernforordningens regler.

Boken er på totalt 300 sider fordelt på 10 kapitler. Det fremstår som et egnet format for en lærebok. Kapitlene varierer i omfang. Hovedvekten er lagt på behandlingen av de viktigste aktørene og deres roller (kap. 2), grunnleggende og generelle krav til behandling av personopplysninger (kap. 3), den registrertes rettigheter (kap. 4) og risikovurdering og personopplysningssikkerhet (kap. 6). Innledningsvis beskriver han (kap. 1), på en pedagogisk og god måte, hvor personvernforordningen gjelder og hvem og hva den gjelder for, og forklarer sentrale begreper som reguleringen bygger på som bl.a. «personopplysning» og «behandling». Disse delene utgjør til sammen ca 230 av bokens 300 sider.

De resterende 70 sidene er fordelt på flere emner, bl.a. den systematiske plasseringen av personopplysningsretten som del av personvernet og en (befriende) kort lovgivningshistorikk (deler av kap. 1, ca 25 sider) og overføring av personopplysninger til tredjeland (kap. 5, ca 10 sider). Kapitlene om vurdering av personvernkonsekvenser (kap. 7), tilsyn med behandlingen av personopplysninger (kap. 8), erstatningsansvar, sanksjoner og overtredelsesgebyr (kap. 9) og klagerett og

andre rettsmidler (kap. 10), er samlet presentert over ca 35 sider. For en lærebok opplever jeg denne fordelingen som stort sett velbegrunnet. For den som lurer på hvordan f.eks. bestemmelsene om erstatningsansvar, eller de mye omtalte reglene om overtredelsesgebyr, vil fungere i praksis, er det nok andre kilder som gir bedre utbytte, men fremstillingen er tilstrekkelig til å skape en grunnleggende forståelse av de rammebetingelsene som omgir de sentrale personopplysningsrettslige prinsippene og rettighetene, og som skal bidra til at de kan håndheves. Mot slutten av denne anmeldelsen kommenterer jeg likevel enkelte avgrensninger som er gjort, bl.a. noen særlige spørsmål knyttet til databehandlere og overføring av personopplysninger til tredjeland.

Det vil føre for langt å skulle oppsummere og kommentere hver enkelt del av boken som er nevnt ovenfor. Jeg har i stedet valgt ut noen enkeltområder som kan bidra til å belyse hvordan forfatteren har arbeidet med å systematisere stoffet og gjøre det tilgjengelig for leseren.

Sentrale begreper og aktører

De sentrale begrepene «behandling» og «personopplysning» er godt og grundig behandlet i bokens kap. 1.6. Begrepene favner som kjent veldig vidt, og forfatteren beskriver dette på en god måte, ikke minst kompleksiteten knyttet til indirekte identifiserbare opplysninger. I tillegg beskriver forfatteren opplysninger som (kanskje) ikke er personopplysninger, men som *kanskje kan bli det* (på s. 45). Om det høres pussig ut, så kan man tenke seg at det har å gjøre med skillet mellom *identifiserbarhet* og *individualiserbarhet*.

Personopplysninger kan være direkte eller indirekte identifiserbare. Det er grovt sagt et spørsmål om man kan knytte dem til en fysisk person direkte, basert på sitt eget innhold, f.eks. navn og fødselsdato, eller om det må suppleres med opplysninger som finnes et annet sted, f.eks. hvem som er registrert som innehaver av et bestemt registreringsnummer for kjøretøy som kan avklares ved å gjøre oppslag i et sentralt register. Man kan imidlertid også tenke seg opplysninger som på det aktuelle tidspunkt ikke kan koples til noen bestemt fysisk person, fordi det ikke finnes tilstrekkelig med identifiserende elementer – hverken direkte eller indirekte – men der arten av eller antallet opplysninger likevel er slik at de bare kan tilhøre én person – vi vet bare ikke hvem. Slike opplysninger kan beskrives som *individualiserbare* selv om de på det aktuelle tidspunktet ikke er *identifiserbare*. For en del slike opplysninger kan det imidlertid være et spørsmål om tid før man har tilgang til så mye data at indirekte identifisering likevel er mulig. Alternativt at den tekniske løsningen som gjør dem individualiserbare, men ikke identifiserbare, brytes, f.eks. ved at det man trodde var en enveisalgoritme likevel kan reverseres. Tilgangen til data (stordata) er stadig økende, og teknikken utvikler seg hele tiden. Det vil derfor være fornuftig, som forfatteren påpeker, at hvis man behandler opplysninger man antar er individualiserbare, innretter seg som om det er personopplysninger man behandler (så langt det lar seg gjøre). Det kan ellers bli svært krevende å «reparere» situasjonen hvis opplysningene på et senere tidspunkt skulle vise seg å være eller bli personopplysninger fordi indirekte identifisering plutselig blir mulig.

Sentrale aktører som den behandlingsansvarlige, databehandleren og personvernombud, beskrives godt i bokens kap. 2. Som jeg kommer tilbake til avslutningsvis, mener jeg likevel at det med fordel kunne vært spandert enda litt mer plass på å drøfte utfordringer knyttet til databehandlerrollen og bruken av databehandleravtaler.

Grunnleggende krav og prinsipper for behandling av personopplysninger

I bokens kapittel 3, behandler forfatteren grunnleggende og generelle krav til behandlingen av personopplysninger, med særlig vekt på prinsippene i art. 5 og kravet til behandlingsgrunnlag i art. 6 og art. 9. Fremstillingen av prinsippene i art. 5 dekker bl.a. viktige forhold som formålsbegrensningsprinsippet, dataminimeringsprinsippet, krav til opplysningens kvalitet (korrekthet) og lagringsbegrensningsprinsippet. Vurderingene her tar forfatteren med seg videre i boken i forbindelse med tolkningen av andre bestemmelser i personvernforordningen, se nærmere nedenfor.

Kravene til et gyldig samtykke er viet relativt mye plass sammenliknet med de øvrige behandlingsgrunnlagene i art 6, de såkalte «nødvendige grunner» til å behandle personopplysninger. Også dette fremstår som en fornuftig disponering, og de øvrige grunnlagene omtales enkeltvis på en presis og beskrivende måte, men grunnlaget «berettiget interesse», som i praksis er svært viktig, kunne nok fortjent noe mer omtale når det gjelder den interesseavveiningen som skal gjøres. Her kunne nok også noen flere praktiske eksempler vært på sin plass.

Fremstillingen av artikkel 9, om de såkalte særlige kategorier av personopplysninger, er behandlet på tilsvarende måte, og fremstår som nesten overraskende tilgjengelig kompleksiteten tatt i betraktning. Det er imidlertid litt pussig at forfatteren har valgt overskriften «Forebyggende medisin mv» i punktet som dekker art. 9(2)(h), og som bl.a. (også) gjelder det praktisk viktige området medisinsk diagnostikk og ytelse av helse- og sosialhjelp (altså bl.a. leger og sykepleieres be-

handling av helseopplysninger som nok er en praktisk problemstilling for langt flere enn spørsmålet om forebyggende medisin). På dette punktet kunne nok sammenhengen med bl.a. pasientjournalloven også fortjent omtale. Forholdet til helsepersonelloven er imidlertid behandlet. Betydningen av begrepet «helseopplysninger « kommenterer jeg kort nedenfor.

Videre i fremstillingen får forfatteren på en god måte frem hvilken betydning prinsippene i personvernforordningen art. 5 har eller kan ha ved tolkning og anvendelse av andre bestemmelser i forordningen, f.eks. i forbindelse med kravene til datakvalitet som han behandler i tilknytning til personvernforordningen art. 16 og 17 om retting og sletting. I første del av boken (på s. 87), skriver riktignok forfatteren, i et forsøk på forklare hvordan man kan se på prinsippene i art. 5, at: «*Prinsippene kan trolig best ses som en kombinasjon av «utgangspunkter for tanken» og retningslinjer: Er mothensynene sterke nok, kan de i konkrete tilfeller bli tillagt liten vekt.*» Slik han senere benytter art. 5, også ved tolkningen av andre bestemmelser, er imidlertid begrepene «utgangspunkt for tanken» og «retningslinjer» etter min oppfatning ikke veldig beskrivende. Særlig ettersom forfatteren også benytter begrepet «retningslinjer» om anbefalinger fra den tidligere Artikkel 29-gruppen (på s. 24). Det virker mer nærliggende å forstå prinsippene i art. 5 som en type grunnleggende krav og overgripende normer som både har selvstendig rettslig betydning, og som samtidig har betydning ved tolkning og anvendelse av andre bestemmelser i personvernforordningen. At prinsippene har selvstendig rettslig betydning mener jeg fremkommer f.eks. i art. 23 der det fremgår at det enkelte medlemsland, «*ved lovgivningsmessige tiltak [kan] begrense rekkevidden av forpliktelsene og rettighetene i … [bl.a.] artikkel 5* …», og av art. 83 nr. 5 der det fremgår at overtredelse av art. 5 kan medføre overtredelsesgebyr. Det samme gjelder art. 5 nr. 2 der det fremgår at den behandlingsansvarlige er ansvarlig for, og skal kunne påvise, at [prinsippene i] nr. 1 overholdes. Jeg oppfatter at det også er slik forfatteren håndterer det i praksis. Uansett fremstår grepet med å integrere art. 5 i drøftelsen av andre bestemmelser som nyttig og oppklarende.

Artikkel 5 nr. 2 behandler forfatteren sammen med art. 24 om den behandlingsansvarliges ansvar.

Den registrertes rettigheter

Forfatteren redegjør i kap. 4.2, under overskriften «Åpenhet og gjennomsiktighet», for sammenhengen mellom reglene om informasjon (art. 13-14) og rett til innsyn (art. 15). Forfatteren gir her råd om hvordan den behandlingsansvarlige kan innrette seg på en praktisk og effektiv måte bl.a. ved å synliggjøre sammenhengen mellom bestemmelsene. Han har bl.a. utarbeidet en nyttig oversikt som sammenstiller fellestrekk ved de tre bestemmelsene. Videre drøfter forfatteren forholdet til andre innsynsretter, bl.a. forvaltningslovens regler om partsinnsyn og offentleglova. Fremstillingen fremstår som både praktisk og dekkende.

Forfatteren skriver i kap. 4.3 godt om sammenhengen mellom retting og sletting (art. 16 og 17), og påpeker bl.a. at opplysninger som er ukorrekte eller mangler lovlig grunnlag for behandlingen, ikke nødvendigvis skal slettes, men i mange tilfeller korrigeres med anmerkning av de tidligere ukorrekte opplysningene. Det er bl.a. hensynet til den registrertes mulighet for (i ettertid) å få avklart hvilke opplysninger som (på et tidligere tidspunkt) faktisk har blitt behandlet, som begrunner dette, f.eks. i forbindelse med et mulig erstatningskrav. Sammenhengen mellom den registrertes rettigheter og den behandlingsansvarliges plikter knyttet til retting og sletting kommer også godt frem i dette kapittelet. Forfatteren redegjør videre for en del unntak fra sletteplikten, bl.a. av hensyn til ytrings- og informasjonsfriheten og til arkivformål.

I samme kapittel behandler forfatteren spørsmål knyttet til bl.a. den registrertes rett til å kreve begrensning av behandlingen og retten til å protestere (art. 18 og 21). Han gjør også en sammenstilling og analyse av de ulike begrepene som er benyttet i art. 16-22 (begrepene rett til å få, kreve, motta, protestere, ikke være gjenstand for). Han slår fast at det i alle bestemmelsene dreier seg om rettigheter, og drøfter om og i hvilken grad det utgjør noen realitetsforskjell at enkelte av begrepene gir anvisning på et resultat (få motta og ikke være gjenstand for), mens de andre mer har preg av en situasjonsbeskrivelse (kreve og protestere). Avslutningsvis i dette underkapittelet skriver forfatteren kort om retten til dataportabilitet (art. 20).

Risikovurdering, innebygd personvern og sikkerhet ved behandlingen (personopplysningssikkerhet)

I bokens kapittel 6 behandler forfatteren personvernforordningens bestemmelser om risikovurdering, krav til innebygd personvern og personopplysningssikkerhet (i forordningens art. 32 kalt sikkerhet ved behandlingen), samt om personvernbrudd. Bestemmelsen om sikkerhet ved behandlingen (art. 32) dekker omtrent det samme som i den tidligere personopplysningsloven (2000) ble kalt «informasjonssikkerhet», men personvernforordningens art. 32 er noe mer detaljert og det fremgår tydeligere at sikkerhetskrav skal være basert på risikovurdering.

Forfatteren er åpenbart ikke særlig imponert over den uensartede begrepsbruken i personvernforordningen når det gjelder å beskrive krav eller egenskaper knyttet til sikkerhet. Han illustrerer dette ved å sammenstille de mange ulike begrepene som er benyttet i art. 4(12), art. 5(1)(f) og art. 32(1)(b), i en tabell (i kap. 6.4.1), og som innledning til tabellen skriver han: «*Hvis vi samler og strukturerer alle disse elementene, får vi et ganske sammensatt bilde som det skal atskillig god vilje til for å bedømme som en gjennomtenkt systematikk.*» Det er lett å være enig med ham i det.

Fremstillingen av kravene til risikovurdering og sikkerhet ved behandlingen vil utvilsomt være til god hjelp for å forstå disse relativt krevende, og for mange jurister, litt «fremmede» områdene. Jeg tror også fremstillingen av kravene til innebygd personvern og personvern som standardinnstilling kan være nyttige for mange, ettersom denne reguleringen er ny i personvernforordningen. Riktignok har dette vært diskutert også i tilknytning til den tidligere personopplysningsloven (2000), men det er først med personvernforordningen at kravene er blitt formalisert.

Fremstillingen av risikovurderinger kommenterer jeg kort avslutningsvis nedenfor.

Nyttige oversikter

Forfatterens valg av systematikk, bl.a. parallelbehandlingen av beslektede bestemmelser på de enkelte områder, gir god oversikt og forståelse, og det er strukturert på en måte som gjør at et imponerende antall alternativer blir behandlet.

Boken inneholder også enkelte tabeller, oversikter og veiledninger som i enkelte tilfeller kan fungere som en slags sjekklister som nok kan komme til nytte for mange. Det gjelder bl.a. kapittel 1.4 som har tittelen «*Eksempel på hvordan viktige bestemmelser i forordningen kommer til anvendelse*», men som inneholder en nyttig liste over spørsmål som den behandlingsansvarlige bør stille seg når man vurderer å gå i gang med å registrere eller på annen måte behandle personopplysninger.

Et annet eksempel er tabellen i kap. 4.2.2 som sammenstiller kravene i personvernforordningens bestemmelser om informasjon og innsyn (art. 13-15) på en oversiktlig og god måte, og som også reflekterer mange av de ulike kravene knyttet til behandling av personopplysninger som den behandlingsansvarlige må ta stilling til.

Om avgrensninger og bruk av eksempler mv.

Det virker veloverveid å benytte så mye plass på grunnleggende krav og prinsipper, den registrertes rettigheter og personopplysningssikkerhet. For det første fordi emnene er omfattende. For det andre fordi de er sentrale for å kunne behandle og forstå andre personopplysningsrettslige spørsmål. Det er imidlertid enkelte andre valg og avgrensninger som jeg stiller meg mer spørrende til.

Om jeg skal driste meg til å foreslå noen justeringer i neste utgave av boken, ville det for det første være å benytte noen flere praktiske eksempler illustrert ved konkrete brukssituasjoner. Det er mulig det er plassen som har vært til hinder for dette, men det ville nok bidratt til ytterligere å lette tilgjengeligheten til et ganske krevende materiale. I denne sammenheng ville jeg nok også benyttet noen flere eksempler fra privat sektor. Det er mange gode eksempler å hente fra offentlig virksomhet og systemutvikling i den forbindelse, og det gjør forfatteren på en veldig god måte. Jeg mistenker imidlertid at vektleggingen av eksempler fra offentlig sektor ikke bare er faglig eller fremstillingsmessig begrunnet, men at det også er preget av forfatterens egen faglige bakgrunn og erfaring. Jeg tror det for mange kunne ha verdi om det ble benyttet flere eksempler knyttet f.eks. til behandling av personopplysninger om ansatte (som naturligvis også er relevant for ansatte i det offentlige), og om næringslivets mange «digitale kunder» innen uensartede bransjer som bank og forsikring, reise- og transportvirksomhet og mer tradisjonell detalj- og netthandel som alle har sine særtrekk. Jeg tror det ville være eksempler som mange studenter kan kjenne seg igjen i og som kunne bidra til å anskueliggjøre hva de relativt abstrakte bestemmelsene gjelder og hvordan de skal anvendes.

Det er også et par konkrete områder som jeg mener hadde fortjent mer oppmerksomhet i boken. Forfatteren presiserer selv at dette ikke er en lovkommentar eller håndbok, men en lærebok. Det innebærer at systematikk og sammenhenger står sentralt, sammen med andre forhold som kan gjøre leserne i stand til å løse rettsspørsmål på egen hånd, og at enkeltstående praktiske problemstillinger typisk må ligge. Det er imidlertid noen spørsmål som oppstår så ofte i praksis, at det nesten er litt påfallende at de ikke har fått mer omtale i boken.

Databehandleravtaler og overføring til tredjeland (land utenfor EØS-området)

Dette gjelder for det første kompleksiteten knyttet til bruk av databehandlere. IT-markedet er i stadig utvikling, og et typisk trekk er at en behandlingsansvarlig virksomhet ikke drifter sine IT-systemer selv, eller får sine IT-tjenester fra én leverandør, men fra et knippe leverandører, og/eller en kjede av leverandører. Dette innebærer i praksis atskillig flere utfordringer knyttet til bruk av databehandleravtaler, speiling av forpliktelser og oppfølging av databehandlere og underdatabehandlere, herunder underdatabe-

handlere som leverer standardiserte tjenester til et stort antall kunder, enn det man kan få inntrykk av når man leser bokens fremstilling av databehandlere og databehandleravtaler.

Det henger også sammen med et annet tema som er relativt kort behandlet, nemlig overføring av personopplysninger til land utenfor EØS-området. Overføring av personopplysninger til land utenfor EØS-området krever, som forfatteren redegjør godt for, et særskilt rettslig overføringsgrunnlag. Stadig flere virksomheter får deler av sin IT-portefølje levert som eller via en eller annen form for «skytjenester», gjerne som del av en større samlet leveranse som kanskje koordineres eller forvaltes av en lokal leverandør. Om ikke forvalteren eller leverandøren av skytjenestene selv er etablert utenfor EØS-området, vil gjerne driften av skytjenestene være organisert på en slik at måte at de gjennom døgnet følges opp av ressurser lokalisert i ulike land etter et slags «follow the sun» prinsipp. Det samme kan gjelde store enkeltstående norske og andre europeiske leverandører som har etablert seg med ressurssentre ulike steder i verden – dels på grunn av prisnivået, dels for å kunne drive døgnkontinuerlig oppfølging av driftstjenestene uten å ha et unødig stort team av ansatte som jobber nattskift i Europa. I tillegg kommer at mange norske industriselskaper har søster- og datterselskaper etablert utenfor EØS-området som det utveksles informasjon med på daglig basis. I praksis innebærer dette at spørsmålet om overføring av personopplysninger til land utenfor EØS-området er langt mer praktisk og omfattende enn man kanskje skulle tro. Jeg minner for ordens skyld om, som forfatteren også påpeker, at det å skaffe seg tilgang fra et tredjeland (fjernaksess) til systemer som behandler personopplysninger i mange tilfeller vil regnes som overføring av personopplysninger selv om overføring hverken er formålet med tilgangen eller en ønsket konsekvens av den.

Dette aktualiserer spørsmålet om rettslig overføringsgrunnlag i form av såkalte nødvendige garantier for behandling av personopplysningene. Forfatteren drøfter (i kap. 5) to av de mulige virkemidlene som er nevnt i art. 46. Det første er bare aktuelt for offentlige virksomheter. Det andre er bindende virksomhetsregler, ofte referert til ved det engelske akronymet BCR (Binding Corporate Rules) som omtales veldig kort. Her unnlater forfatteren å nevne at det i praksis vil være mange begrensninger knyttet til når bindende virksomhetsregler kan benyttes (konserninterne overføringer). Det kommer heller ikke frem at prosessen med å etablere slike bindende virksomhetsregler er relativt omfattende og tidkrevende, bl.a. som følge av at det typisk vil involvere tilsynsmyndighetene i flere land. Antakelig kunne det vært et godt eksempel for å forklare det tverrnasjonale samarbeidet mellom tilsynsmyndighetene som ellers er beskrevet relativt kort i bokens kapittel 8, men det er nok en riktig avgrensning å ikke bruke så mye plass på dette i en lærebok.

Det forfatteren derimot ikke behandler, er bruken av det personvernforordningen omtaler som standard personvernbestemmelser, også gjerne kalt modellavtaler eller standard kontraktklausuler, ofte referert til med det engelske akronymet SCC (Standard Contractual Clauses), godkjent av Kommisjonen i henhold til personvernforordningen art. 46(2)(c). Dette er i mange tilfeller de eneste reelt tilgjengelige overføringsgrunnlagene når det gjelder bruk av databehandlere også i flerleddete databehandlerrelasjoner. Eksisterende standardkontrakter, som ble godkjent av Kommisjonen under det tidligere personverndirektivet, og som gjelder overføring til databehandlere i tredjeland, er etter sin egen ordlyd et forhold mellom den behandlingsansvarlige (eksportøren) og den databehandleren som skal motta personopplysningene (importøren). I praksis vil det imidlertid ofte være slik at primærdatabehandleren er en virksomhet innenfor EØS-området der en ordinær databehandleravtale er tilstrekkelig. Databehandleren kan imidlertid ha underleverandører (underdatabehandlere) som holder til utenfor EØS-området. Da er det behov for et særskilt overføringsgrunnlag i underdatabehandlerleddet. Det har ikke de eksisterende standard kontraktklausuler vært tilpasset for. Den 12. november 2020 ble imidlertid utkast til nye standard personvernbestemmelser lagt ut på høring av Kommisjonen.[1] De skal bl.a. legge til rette for overføring mellom databehandlere innenfor og utenfor EØS.

Disse problemstillingene knyttet til bruk av flerleddete databehandlerrelasjoner og spørsmålet om overføring til tredjeland i forbindelse med helt grunnleggende tjenester som døgnkontinuerlig oppfølging av driften, vil nok treffe mange av studentene når de skal ut for å gi råd i praksis, og kan nok med fordel få litt mer plass i neste utgave av boken. På det tidspunktet får vi håpe at også de nye standard personvernbestemmelsene er blitt vedtatt. Om andre utfordringer ved bruken av standard kontraktklausuler, bl.a. i forlengelsen av EU-domstolens avgjørelse i Schrems II, er det skrevet godt og mye andre steder her i Lov&Data.

1 Se *https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries.*

Helseopplysninger

Jeg nevnte ovenfor at boken kunne nytt godt av noen flere eksempler, f.eks. knyttet til behandling av personopplysninger om ansatte. Et annet område av stor praktisk betydning, og høy kompleksitet, er behandling av helseopplysninger. Det er nok fornuftig av forfatteren å ikke trå for langt inn på dette området; det er skrevet egne bøker om dette. Jeg stusser likevel litt over at forfatteren ikke spanderer ørlite plass på å forklare begrepet helseopplysning. Det er nok mange som vil være overrasket over hvor vidt begrepet helseopplysning rekker. I og med at helseopplysninger tilhører de såkalte «særlige kategorier av personopplysninger» i art. 9, kan det ha stor betydning for den behandlingsansvarlige om en personopplysning skal regnes som en helseopplysning eller ikke.

Risikovurderinger

Et siste område jeg vil nevne, er risikovurdering. Et gjennomgående trekk ved personvernforordningen er krav om forholdsmessighet f.eks. mellom tiltak og de risikoer tiltakene skal bøte på, se f.eks. art. 24 og 32 om «egnede» tiltak. Dette vil i mange tilfeller bygge på en risikovurdering. I noen sammenhenger er kravet til risikovurdering eksplisitt uttalt, f.eks. i art 35, andre steder fremgår det mer indirekte. Risikovurdering er et område som kan oppleves som vanskelig for de fleste som ikke driver med det til daglig, kanskje først og fremst fordi man ikke helt vet hvordan man skal gripe det an. For komplekse risikovurderinger bør det nok tilkalles fagekspertise, men for de mange løpende risikovurderinger som skal gjøres, ville det være til god hjelp å få litt praktisk veiledning. Forfatteren gir virkelig gode bidrag i kap. 6.1.2, og påpeker selv at han anser det som så viktig at det er viet mer plass enn andre enkeltemner. Jeg tror likevel ingen lesere av boken vil bebreide ham om han i neste utgave går enda lenger i råd og veiledning med hensyn til praktisk dag-til-dag håndtering av risikovurderinger.

Sammenfatning og hovedinntrykk

Jeg har ovenfor pekt på noen forhold som etter min mening hadde fortjent noe mer oppmerksomhet i en lærebok om personvernforordningen. Det er for detaljer å regne.

Det er en fremragende prestasjon av forfatteren å systematisere, komprimere og gjøre tilgjengelig personvernforordningens innhold så strukturert, tydelig og dekkende, og med et så klart språk, som det er gjort i denne boken – på bare 300 sider. Jeg anbefaler den uforbeholdent; ikke bare til studenter, men også til praktikere og andre som arbeider med personopplysningsrett. Jeg føler meg sikker på at også jurister med betydelig praktisk erfaring innenfor personopplysningsretten vil ha nytte av boken, og finne støtte for egne resonnementer i forfatterens tilnærming og systematikk. Jeg tror også at de fleste vil finne nye momenter både ved første og annen gangs gjennomlesing. Det skyldes ikke at teksten er uklar, men at den på mange områder er så komprimert, og beskriver så mange alternativer, at leserens egen praktiske erfaring kan ha betydning for hvilke poenger man tar med seg fra lesingen.

Det er bare å gratulere Dag Wiese Schartum med nok et strålende arbeid!

Rolf Riisnæs er advokat dr. juris, partner i Wikborg Rein Advokatfirma AS.

Immaterialrett, kontrakter og erstatning

Harald Irgens-Jensen (red.), Camilla Vislie (red.).
Universitetsforlaget – 344 s. Oslo 2020 – ISBN: 9 788 215 030 081

Immaterialretten får større betydning for økonomi og samfunn, og den blir stadig mer kompleks. Samtidig er det viktig ikke å miste dens nære sammenheng med annen formuerett, i første rekke kontraktsretten og erstatningsretten, av syne.

Det nære forholdet mellom immaterialrett og annen formuerett ble understreket av Ragnar Knoph, norsk immaterialretts viktigste skikkelse, på 1930-tallet. I hans ånd, har denne artikkelsamlingen som mål å illustrere samspillet mellom immaterialretten, kontraktsretten og erstatningsretten fra ulike synsvinkler. Samlingen inneholder en rekke analyser av spørsmål som kan oppstå i tilknytning til ulike immaterialrettsavtaler (lisensavtaler, FoU- og tilvirkningskontrakter, overdragelser av patenter, forlagsavtaler, avtaler om bruk av opphavsrettslig materiale osv.) og til erstatningskrav for immaterialrettskrenkelser.

Bak artiklene står et knippe forfattere med bred bakgrunn: forskere, stipendiater og advokater. Temaene i samlingen vil ha interesse ikke bare for jurister som arbeider med immaterialrett, men også for dem som driver med arbeidsrett, entreprenørrett, kjøpsrett, idrettsjuss og konkursrett, i advokatfirmaer, domstoler, patentbyråer og kunstnerorganisasjoner, i selskaper engasjert i teknologiutvikling, underholdning og merkevarer, og i våre forskningsinstitusjoner.

Bidragsytere: Nora Sandvik Bratheim, Knut Jørgen Egelie, Thomas Granrud, Magnus Hauge Greaker, Harald Irgens-Jensen, Kaja Skille Hestnes, Kirsten Lange, Morten Smedal Nadheim, Haakon Thue Lie, Ole-Andreas Rognstad, Urd Sira, Camilla Vislie og Inger Berg Ørstavik.

Ytringsfrihet og medieregulering

Olav Torvund
Universitetsforlaget – 448 s. Oslo 2020 – ISBN: 9 788 215 032 955

Både jussen og medievirkeligheten har utviklet seg mye på kort tid. Blant annet har Grunnlovens hovedbestemmelse om ytringsfrihet i § 100 blitt endret. I tillegg har vi fått en ny straffelov og ny rettspraksis fra bl.a. Menneskerettsdomstolen.

«Ytringsfrihet og medieregulering» gir en innføring i medierett og behandler emner som pressens rolle, ytringsfrihetens grenser, ansvaret og de rettslige rammene for ytringsfriheten. Denne fremstillingen er hovedsakelig skrevet for det tverrfaglige bachelorprogrammet «Digitale medier» ved Universitetet i Oslo. I tillegg vil boka være et nyttig oppslagsverk for jurister og ansatte i landets mediehus.

Gorrissen Federspiel

Tue Goldschmieding

EDPB udgiver information vedr. bindende virksomhedsregler, som er godkendt af det engelske datatilsyn

Det Europæiske Databeskyttelsesråd ('EDPB') offentliggjorde den 22. juni 2020 en orienterende note om bindende virksomhedsregler med den britiske tilsynsmyndighed som ledende myndighed.

Bindende virksomhedsregler er regler, som fastlægges internt i en koncern, og som sikrer lovlig overførsel af data imellem de forskellige selskaber i en koncern, jf. Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') artikel 46, stk. 2, litra b og artikel 47, stk. 1. Bindende virksomhedsregler skal godkendes af den kompetente tilsynsmyndighed i den medlemsstat, hvori koncernens hovedsæde ligger.

Som en konsekvens af Brexit skal koncerner med bindende virksomhedsregler, der har det britiske datatilsyn som den kompetente tilsynsmyndighed, finde en ny kompetent tilsynsmyndighed beliggende i et EØS-land, inden den aktuelle Brexit-overgangsperiode slutter. Bindende virksomhedsregler, der allerede er godkendt, skal have udstedt en ny godkendelse fra den nye kompetente tilsynsmyndighed efterfulgt af en vurdering fra EDPB, før overgangsperioden slutter. Den nye godkendelse er dog ikke påkrævet, hvis de bindende virksomhedsregler er blevet godkendt af det britiske datatilsyn, da det fungerede som kompetent tilsynsmyndighed i henhold til Direktiv 95/46/EF af 24. oktober 1995, der er forgængeren til databeskyttelsesforordningen.

For at hjælpe de dataansvarlige og databehandlerne indeholdte den orienterende note en tjekliste over elementer, der skal ændres i forbindelse med ændringen af den kompetente tilsynsmyndighed.

Læs hele udgivelsen her:
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_informationnoteforgroupswithicoasbcrleadsa_20200722.pdf

Link til hjemmesiden:
https://edpb.europa.eu/our-work-tools/our-documents/other/information-note-bcrs-groups-undertakings-enterprises-which-have_en

EDPB udgiver FAQ om Schrems II-dom

Det Europæiske Databeskyttelsesråd ('EDPB') offentliggjorde den 23. juli 2020 en FAQ på baggrund af EU-Domstolens dom afsagt den 16. juli 2020 i sag C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* (Schrems II dommen). I dommen blev det vurderet hvorvidt EU-US Privacy Shield ordningen samt EU-Kommissionens standardkontraktbestemmelser (SCC'er) kan bruges som gyldigt overførselsgrundlag af personoplysninger.

Schrems II-dommen afgjorde, at EU-Kommissionens standardkontraktbestemmelser kan bruges som overførselsgrundlag, mens det for EU-US Privacy Shield ordningen blev afgjort, at denne ikke levede op til det tilstrækkelige beskyttelsesniveau, der var sikret ved Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen'). På den baggrund blev Privacy Shield ordningen erklæret ugyldig

EDPB anfører, at Schrems II-dommen, har betydning for alle, der ved elektroniske midler overfører personoplysninger til USA eller andre lande uden for EU/EØS (tredjelande), som ikke kan garantere et tilstrækkeligt databeskyttelsesniveau i henhold til databeskyttelsesforordningens artikel 46 om overførsler omfattet af fornødne garantier. I EDPB's FAQ er det angivet, hvordan virksomheder, der overfører personoplysninger til tredjelande, skal forholde sig i lyset af dommen.

Det bliver endvidere i EDPB's FAQ gjort klart, at en virksomhed, der forsat ønsker at overføre personoplysninger til USA eller andre tredjelande, skal foretage en vurdering af omstændighederne ved overførslerne, og hvilke yderligere supplerende foranstaltninger virksomheden kan indføre for at opnå det databeskyttelsesniveau, der er fastsat i databeskyttelsesforordningen.

EDPB har analyseret Schrems II-dommen og vedtog i november 2020 anbefalinger til supplerende foranstaltninger, der kan implementeres for sikre en legitim overførsel af personoplysninger til tredjelande, hvor den tilstrækkelige databeskyttelsesgaranti ikke er sikret. Dette omfatter bl.a. vejledning til hvordan en dataeksportør afklarer om de har behov for supplerende foranstaltninger, betingelser for at disse er effektive samt en liste med eksem-

pler på supplerende foranstaltninger.

Læs hele FAQ-udgivelsen her:
https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf

Læs anbefalingerne her:
https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

1.1 Nyt register over grænseoverskridende sager

Det Europæiske Databeskyttelsesråd ('EDPB') har udgivet et register, som indeholder afgørelser truffet af nationale tilsynsmyndigheder i overensstemmelse med artikel 60 i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen'). Artikel 60 statuerer, at tilsynsmyndigheden i det land, hvor en dataansvarlig har hovedsæde ('den ledende tilsynsmyndighed'), har pligt til at samarbejde med tilsynsmyndighederne i de lande, som den dataansvarliges grænseoverskridende aktivitet berører ('de berørte tilsynsmyndigheder'). Dette samarbejde betegnes som »One-Stop-Shop«-samarbejdet ('OSS-samarbejdet').

Under OSS-samarbejdet skal den ledende tilsynsmyndighed forberede udkast til afgørelser og samarbejde med de berørte tilsynsmyndigheder for at opnå enighed om afgørelsen. De ledende tilsynsmyndigheder har indtil videre (medio oktober 2020) afsagt 135 OSS afgørelser, der kan tilgås gennem det nyligt udgivne register, som tillige indeholder referater af afgørelserne på engelsk.

Registeret er relevant for praktikere som arbejder med databeskyttelse, idet det bliver muligt at få indsigt i, hvorledes de berørte tilsynsmyndigheder arbejder sammen for at håndhæve databeskyttelsesforordningen.

Informationen i registeret er blevet valideret af de relevante ledende tilsynsmyndigheder i overensstemmelse med vilkårene i national lovgivning.

Find registeret her:
https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en

Utilstrækkelig sikkerhed ved levering af inkassobreve udløste kritik fra Datatilsynet

Det danske datatilsyn ('Datatilsynet') har den 11. juni 2020 ved afgørelse i sag med journalnummer 2020-31-2260 udtalt kritik af RoestNielsen ApS ('RoestNielsen') for manglende opfyldelse af kravene om et passende sikkerhedsniveau i forbindelse med levering af inkassobreve til en borger.

Borgeren klagede den 15. september 2019 til Datatilsynet over Altektum A/S ('Alektum') der som dataansvarlig havde indgået en databehandleraftale med RoestNielsen, hvorefter konsulenter hos RoestNielsen skulle besøge og levere inkassobreve til debitorer på vegne af Alektum. Borgeren havde oplevet at naboen måtte aflevere et brev, der var havnet ude foran naboens ejendom og en anden gang havde borgeren fundet et brev, der var blevet sat løst fast på dennes hoveddør.

Datatilsynet fandt i sin afgørelse, at der ved RoestNielsens levering ikke var levet op til de databeskyttelsesretlige krav om et passende sikkerhedsniveau i art 32, stk. 1 i Europa-Parlamentet og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen'), idet en konsulent ansat ved RoestNielsen afleverede inkassobrevene, ved at placere disse ved borgerens hoveddør. RoestNielsen havde ikke leveret de to pågældende breve i overensstemmelse med den instruks, som var givet af Alektum, og som RoestNielsen som var underlagt. Datatilsynet fandt på baggrund heraf, at sagen skulle rettes mod RoestNielsen, som databehandler.

I vurderingen af sagen lagde Datatilsynet vægt på, at brevene ikke blev afleveret i borgerens postkasse, uagtet at borgeren havde en postkasse, og at RoestNielsen placerede kuverterne så tilgængeligt, at der var en stor risiko for, at de ville gå tabt i et eventuelt uvejr, eller at uvedkommende ville kunne tilgå dem. Det faktum at borgerens adresse var i et sommerhusområde, hvor postkasserne kan være centralt placeret i postkasseanlæg fritog ikke RoestNielsen. som burde have undersøgt forholdene nærmere, ved eventuelt at inspicere området omkring borgerens ejendom eller ved at undersøge, om der på ejendommene omkring adressen var opsat postkasser.

Datatilsynet lagde herudover vægt på, at der i brevene fremgik oplysninger om inkasso og gæld, og at eksponering af sådanne oplysninger kunne indebære alvorlige krænkelser for borgeren.

Læs afgørelsen her:
https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/jun/utilstraekkelig-sikkerhed-ved-levering-af-inkassobreve

Region Syddanmark får alvorlig kritik og påbud af Datatilsynet for utilstrækkelige sikkerhedsforanstaltninger

Det danske datatilsyn ('Datatilsynet') har den 12. juni 2020 ved afgørelse i sag med journalnummer 2020-442-6448, udtalt alvorlig kritik af Region Syddanmark og givet påbud om underretning af borgere, hvis personoplysninger har været genstand for sikkerhedsbrud.

Region Syddanmark anmeldte et brud på persondatasikkerheden til Datatilsynet efter at være blevet bekendt med, at et netværksdrev til midlertidig opbevaring af dokumenter, der skulle tilknyttes regionens Elektroniske Patient Journal (EPJ), ikke var beskyttet med tilstrækkelig adgangskontrol, idet alle Region Syddanmarks ca. 30.000 ansatte havde adgang til drevet og dermed dokumenterne.

Dokumenterne indeholdte almindelige, fortrolige og personop-

lysninger af særlige kategorier, herunder oplysninger vedrørende børn eller særligt udsatte grupper og registrerede med beskyttet adresse for op imod 800.000 registrerede.

Datatilsynets kritik gives på baggrund af den ovenstående manglende persondataretlige sikkerhed som udgjorde et brud på artikel 32, stk. 1 i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen'). Endvidere udtaler Datatilsynet, at den manglende logning af, hvem der tilgik oplysningerne, dannede grundlag for udstedelse af et påbud om underretning af de registrerede om bruddet på persondatasikkerheden, fordi risikoen for dem blev vurderet som høj. I sin afgørelse lagde Datatilsynet desuden særligt vægt på mængden af indeholdte oplysninger samt den fortrolige karakter som en del af disse havde.

Læs hele afgørelsen her:
https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/jun/utilstraekkelige-sikkerhedsforanstaltninger-hos-region-syddanmark

Læs Datatilsynets vejledning om håndtering af sikkerhedsbrud her:
https://www.datatilsynet.dk/media/7591/haandtering-af-brud-paa-persondatasikkerheden.pdf

Region Syddanmark får alvorlig kritik for manglende risikovurdering og test af IT-system

Det danske datatilsyn ('Datatilsynet') har den 17. juli 2020 ved afgørelse i sag med journalnummer 2018-442-0026 udtalt alvorlig kritik af Region Syddanmark for manglende risikovurdering og test under udviklingen af et IT-system, hvilket medførte et brud på persondatasikkerheden.

Region Syddanmark ('Regionen') anmeldte brud på persondata sikkerheden til Datatilsynet efter have opdaget at der ved en spørgeskemaundersøgelse blev givet uautoriseret adgang til samlet set 365 personers navn, personnummer og oplysning om graviditet.

Det fremgår af sagen, at ca. 2000 gravide kvinder blev anmodet om at udfylde et spørgeskema. Personerne havde mulighed for at se en liste med navn og personnummer på andre personer, som også var blevet anmodet om at udfylde samme spørgeskema. De berørte registrerede modtog senere elektronisk post i e-boks fra Regionen, der oplyste, at det kun var navne og personnumre, der var blevet gjort tilgængelige men i anmeldelsen til Datatilsynet tilføjede Regionen, at man ligeledes havde informeret om adgangen til oplysninger om graviditet.

Datatilsynet fandt på baggrund af hændelserne i sagen, at der var sket et brud på persondatasikkerheden, jf. artikel 4, nr. 12 i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen'). Tillige fandt Datatilsynet, på baggrund af Regionens forklaringer, at den nødvendige risikovurdering, jf. databeskyttelsesforordningens artikel 32, stk. 1 ikke havde fundet sted. Derudover vurderede Datatilsynet, at Region Syddanmark ikke havde handlet i overensstemmelse med databeskyttelsesforordningens artikel 33, stk. 5 om dokumentation af alle brud på persondatasikkerheden ved ikke at oplyse de berørte individer om alle potentielle brud.

Det var Datatilsynets vurdering, at man ved Region Syddanmarks behandling af kvindernes personoplysninger ikke underrettede de registrerede om omfanget af bruddet af persondatasikkerheden i overensstemmelse med artikel 34, stk. 2.

Datatilsynet udtalte på baggrund af ovenstående alvorlig kritik af Region Syddanmarks behandling af personoplysninger, der ikke var behandlet i overensstemmelse med databeskyttelsesforordningens artikel 32, stk. 1, artikel 33, stk. 5 og artikel 34, stk. 2.

Læs hele afgørelsen her:
https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/jul/brud-paa-persondatasikkerheden-hos-region-syddanmark

Kommune indstilles til bøde for manglende sikkerhedsforanstaltninger

Det danske datatilsyn ('Datatilsynet') har den 30. juni 2020 ved politianmeldelse indstillet Lejre Kommune til en bøde for ikke at have overholdt sin forpligtelse som dataansvarlig i henhold til Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen').

Lejre Kommune blev bekendt med en praksis i kommunens afdeling, Center for Børn og Unge, hvorefter mødereferater indeholdende følsomme personoplysninger blev uploadet på kommunens medarbejderportal. Her kunne personoplysningerne tilgås af en større del af kommunens ansatte, herunder en del medarbejdere, der ikke selv arbejdede med sager, hvor de beskyttede oplysninger indgik. Efter kommunen blev opmærksom på dette brud på persondatasikkerheden, anmeldte de det til Datatilsynet.

Datatilsynet specificerer i indstillingen til politianmeldelsen, at der i en situation, som den pågældende navnlig bør iværksættes to sikkerhedsforanstaltninger. For det første bør en adgangskontrol iværksættes, således at kun medarbejdere med et arbejdsbetinget behov for oplysningerne kan tilgå disse. For det andet må logning af de personer, der har fået vist de følsomme personoplysninger anses for en nødvendig og passende foranstaltning.

Datatilsynet har indstillet til at bøden skal beløbe sig til 50.000 kr. Ved fastlæggelsen af størrelsen på bøden er der bl.a. lagt vægt på overtrædelsens karakter, herunder at der var tale om manglende sikkerhedsbehandling, og på mængden af personoplysninger omfattet af sikkerhedsbruddet. Sagen er hos politiet,

der skal undersøge, om der er grundlag for at rejse sigtelse i sagen.

Læs hele nyheden her:
https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/jun/lejre-kommune-indstilles-til-boede

1.2 Hotelkæde indstilles til millionbøde for manglende sletning af data

Det danske datatilsyn ('Datatilsynet') indstillede ved politianmeldelse den 28. juli 2020 Arp-Hansen Hotel Group A/S ('Arp-Hansen') til en bøde på 1,1 mio. kr. i forbindelse med, at Arp-Hansens egne slettefrister ikke var blevet overholdt.

I forbindelse med et tilsyn hos Arp-Hansen gennemgik Datatilsynet en række systemer med formål om at undersøge, om Arp-Hansen havde tilstrækkelige procedurer til at sikre, at der ikke blev opbevaret personoplysninger i længere tid, end det var nødvendigt af hensyn til de formål, hvortil oplysningerne blev behandlet, jf. opbevaringsbegrænsningen i artikel 5, stk. 1, litra e i Europa-Parlamentet og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen').

Datatilsynet fandt, at særligt et bookingsystem indeholdt mange personoplysninger. Datatilsynet konstaterede at ca. 500.000 kundeprofiler eksisterede i systemet, selvom profilerne burde være blevet slettet flere år tidligere ifølge Arp-Hansens egne slettefrister.

Idet Arp-Hansen, ifølge Datatilsynet, ikke fremkom med saglige grunde til den omfattende opbevaring, indstillede Datatilsynet hotelkæden til en bøde på 1,1 mio. kr. for ikke at leve op til kravet om sletning i opbevaringsbegrænsningen.

Læs hele nyheden her:
https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/jul/arp-hansen-hotel-group-as-indstilles-til-boede

1.3 Opgavebesvarelser anset som personoplysninger, hvorved videregivelse af besvarelserne var et brud på persondatasikkerheden

Det danske datatilsyn ('Datatilsynet') afsagde den 18. juni 2020 afgørelse i sag med journalnummer 2019-431-0045 vedrørende en databehandlers videregivelse af gymnasieelevers opgavebesvarelser.

Tre gymnasier anmeldte henholdsvis den 15. og 16. august 2019 et brud på persondatasikkerheden til Datatilsynet vedrørende MaCom A/S ('MaCom'), der som databehandler havde videregivet elevers opgavebesvarelser til forskere fra Datalogisk Institut ved Københavns Universitet til brug for udviklingen af plagiatprogrammer. Dette var sket, uden at de tre gymnasier som dataansvarlige havde givet tilladelse til videregivelsen.

Datatilsynet fandt, at opgavebesvarelser kan anses for personlysninger, jf. artikel 4, nr. 1 i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen'), når en opgavebesvarelse behandles i sin helhed, idet de er udtryk for opgavebesvarerens tankegang, dømmekraft og kritiske sans. Da uddragene af opgavebesvarelserne var af et sådan omfang, at plagiatprogrammet skulle kunne genkende de enkelte besvarelser fra hinanden, havde besvarelserne en sådan karakter, at de ville kunne henføres til en bestemt registreret, ved brug af supplerende oplysninger. På den baggrund fandt Datatilsynet, at videregivelsen af opgavebesvarelserne skulle anses som behandling af pseudonymiserede personoplysninger jf. databeskyttelsesforordningens artikel 4, nr. 5.

På baggrund af dette, og idet videregivelsen var sket uden instruks fra de dataansvar-lige, fandt Datatilsynet, at der var grundlag for at udtale alvorlig kritik af, at MaCom havde behandlet personoplysninger i strid med databeskyttelsesforordningens artikel 28, stk. 3. For så vidt angår graden af kritik, lagde Datatilsynet i skærpende retning vægt på at MaCom ikke kunne redegøre for antallet af oplysninger, som var blevet stillet til rådighed og antallet af gange, videregivelsen havde fundet sted. I formildende retning lagde Datatilsynet bl.a. vægt på, at videregivelsen var sket i videnskabeligt øjemed og med et samfundstjenesteligt formål, og at videregivelsen var sket i pseudonymiseret form.

Læs hele afgørelsen her:
https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/jun/videregivelse-af-opgavebesvarelser

1.4 PrivatBo modtager alvorlig kritik og indstilles til bøde på 150.000 kr. efter to tilfælde af videregivelse af fortrolige personoplysninger

Det danske datatilsyn ('Datatilsynet') har den 4. august 2020 ved sag 2019-441-1480, udtalt alvorlig kritik af og ved politianmeldelse indstillet PrivatBo A.m.b.A. af 1993 ('PrivatBo') til en bøde på 150.000 kr. for brud på persondatasikkerheden.

PrivatBo bistod en boligfond med et påtænkt salg af tre ejendomme. I den forbindelse uddelte PrivatBo i alt 424 USB-nøgler indeholdende materiale angående ejendommene til ejendommenes lejere i overensstemmelse med tilbudspligten, jf. lovbekendtgørelse nr. 227 af 9. marts 2016 ('den danske lejelov') §§ 100-103. Dog indeholdt USB-nøglerne ved en fejl en række dokumenter med fortrolige personoplysninger, som ikke skulle have været videregivet, og som følge heraf anmeldte PrivatBo et brud på persondatasikkerheden jf. Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') til Datatilsynet den 23. december 2018.

Efter databruddet anmeldt den 23. december 2018, antog PrivatBo PwC som ekstern kvalitetskontrol for at sikre overholdensen af per-

sondatasikkerheden. Ved et nyt tilfælde efterfølgende i januar 2019 udleverede PrivatBo USB-nøgler indeholdende oplysninger om adresser, deposita, forudbetalt leje, og hvorvidt der var foretaget udlæg i nævnte deposita. Materialet blev ved en fejl udleveret til beboerne i en anden ejendom end den påtænkte. PwC havde forudgående meddelt, at materialet ikke indeholdt personoplysninger, der ikke var nødvendige af hensyn til opfyldelse af tilbudspligten. Derfor blev bruddet ikke indberettet til Datatilsynet. Datatilsynet tilslutte sig ikke vurderingen, og PrivatBo indberettede følgeligt bruddet i maj 2019.

Datatilsynet vurderede i sagen, at PrivatBo ikke havde levet op til kravene i databeskyttelsesforordningens artikel 32 om, at gennemføre passende tekniske og organisatoriske sikkerhedsforanstaltninger, i forbindelse med den førstnævnte udlevering af USB-nøgler, der ved en fejl indeholdte fortrolige personoplysninger. Datatilsynet udtalte, at PrivatBo som minimum burde have gennemgået materialet inden udleveringen. På denne baggrund anmeldte Datatilsynet PrivatBo til politiet og indstillede til en bøde på 150.000 kr. Derudover udtale Datatilsynet alvorlig kritik af, at PrivatBo ikke i forbindelse med sikkerhedsbruddet uden unødig forsinkelse og senest 72 timer efter at PrivatBo blev bekendt hermed, anmeldte bruddet til Datatilsynet, hvilket udgør en overtrædelse af databeskyttelsesforordningens artikel 33. At PrivatBo var i vildfarelse om sikkerhedsbruddet var ikke en undskyldelig omstændighed.

Datatilsynet udtalte også alvorlig kritik, af den efterfølgende utilsigtede videregivelse af oversigter over deposita, forudbetalt leje og i nogle tilfælde udlæg foretaget i disse deposita. Fejlen skyldtes manglende grundighed og indebar en risiko for registreredes omdømme. PwCs fejlagtige vurdering af karakteren af oplysningerne kunne ikke føre til et andet resultat.

Læs hele afgørelsen her:

https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/aug/afgoerelse-vedroerende-privatbo-amba-af-1993-i-forbindelse-med-brud-paa-persondatasikkerheden

https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/aug/datatilsynet-indstiller-privatbo-til-boede

1.5 EU-Kommissionen har offentliggjort informationsmateriale om Brexit

Storbritanniens overgangsperiode efter Brexit udløber den 31. december 2020 ifølge aftalen om Det Forenede Kongerige Storbritannien og Nordirlands udtræden af EU 2019/C 384 I/01 ('udtrædelsesaftalen'). Herefter vil enhver overførsel af personoplysninger til Storbritannien blive betragtet som en overførsel til et usikkert tredjeland.

EU-kommissionen har offentliggjort informationsmateriale med titlen: »Getting ready for the end of the transition period«, som skal forberede EU-landene på overgangsperiodens udløb. Informationsmaterialet indeholder information af mere generel karakter samt en meddelelse specifikt om databeskyttelse.

Meddelelsen om databeskyttelse indeholder en beskrivelse af mulighederne for overførsel af personoplysninger som beskrevet kapitel 5 i Europa-Parlamentet og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') med fokus på overførsler til Storbritannien. Herudover beskrives artikel 71 i udtrædelsesaftalen, der handler om beskyttelse af de personoplysninger, der er overført til Storbritannien mens landet stadig var en del af EU samt i overgangsperioden.

Find specifik meddelelse om databeskyttelse her: (på engelsk)

https://ec.europa.eu/info/sites/info/files/brexit_files/info_site/data_protection_en.pdf

Find hele materialet her:

https://ec.europa.eu/info/european-union-and-united-kingdom-forging-new-partnership/future-partnership/getting-ready-end-transition-period_en

Ikke i strid med reglerne at behandle oplysninger om fingeraftryk af medarbejdere

Det danske datatilsyn ('Datatilsynet') afsagde den 8. juli 2020 afgørelse i sag med journalnummer 2019-31-1650, vedrørende en virksomheds behandling af oplysninger om fingeraftryk med henblik på identifikation af medarbejdere.

Sagen omhandlede en kreaturslagterivirksomhed, der anvendte fingeraftryk som identifikation af medarbejderne for at kontrollere hvilke medarbejdere, der havde deltaget i produktionen af et givent produkt, samt sikre, at uvedkommende ikke fik adgang til produktionen. Virksomheden anførte, at nøglebrikker ikke ville give den tilstrækkelige sikkerhed for entydig identifikation, da der var risiko for tyveri eller ombytning af nøglebrikkerne.

Datatilsynet fandt, at behandlingen af fingeraftryk som udgangspunkt var omfattet af forbuddet i artikel 9, stk. 1 i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen'). Kontrolforanstaltningen kunne dog alligevel finde sted, hvis det var nødvendigt for den dataansvarliges arbejdsretlige forpligtelser, jf. databeskyttelsesforordningens artikel 9, stk. 2, litra b og artikel 5, stk. 1, litra a-c, om rimelighed, legitime formål og dataminimering.

Datatilsynet anførte, at hensynet til fødevaresikkerheden udgjorde et sagligt driftsmæssigt hensyn, og at der ikke var grundlag for at tilsidesætte virksomhedens vurdering om nødvendigheden heraf. Datatilsynet fandt det derfor foreneligt med databeskyttelsesreglerne, at virksomheden kunne anvende fingeraftryk som kontrolforanstaltning med

henblik på entydig identifikation af medarbejdere.

Læs hele afgørelsen her:

https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/jul/brug-af-fingeraftryk-ved-adgangskontrol

Datatilsynet har opdateret vejledning om fortegnelser over behandlingsaktiviteter

Det danske datatilsyn ('Datatilsynet') og Justitsministeriet offentliggjorde i februar 2018 en vejledning om fortegnelser over behandlingsaktiviteter. Vejledningen var Datatilsynets og Justitsministeriets bud på, hvad en fortegnelse skulle indeholde for at leve op til kravene i artikel 30 i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen').

Efter databeskyttelsesforordningens artikel 30, skal den dataansvarlige føre fortegnelser over behandlingsaktiviteter under dennes ansvar, herunder f.eks. formålene med behandlingen og en beskrivelse af kategorierne af registrerede og kategorierne af personoplysninger.

Datatilsynet har på baggrund af de erfaringer, som tilsynet har gjort sig efter, at databeskyttelsesforordningen trådte i kraft den 25. maj 2018, opdateret vejledningen om fortegnelser over behandlingsaktiviteter.

Datatilsynet har således præciseret, at en fortegnelse over behandlingsaktiviteter skal indeholde en tydelig kobling mellem hvilke kategorier af personoplysninger, der behandles om de enkelte kategorier af registrerede. Hvis der bliver eller vil blive videregivet personoplysninger i forbindelse med en behandlingsaktivitet, skal fortegnelsen også indeholde information om hvilke kategorier af personoplysninger, der bliver eller vil blive videregivet til den pågældende modtager. I tilknytning hertil skal det også fremgå hvilke kategorier af registrerede, de pågældende oplysninger vedrører. Dette er efter tilsynets opfattelse oplysninger, som dataansvarlige bør have viden om og dokumentation for, herunder bl.a. til brug for udarbejdelse af risikovurderinger og implementering af passende tekniske og organisatoriske sikkerhedsforanstaltninger m.v.

Find hele den opdaterede vejledning her:

https://www.datatilsynet.dk/Media/E/5/Fortegnelse.pdf

Brud på persondatasikkerheden hos Datatilsynet selv

Det danske datatilsyn ('Datatilsynet') offentliggjorde den 20. august 2020, konstateringen af et brud på persondatasikkerheden hos Datatilsynet selv. Den 11. september 2020 udtalte Datatilsynet alvorlig kritik af tilsynet selv i afgørelse vedrørende databruddet.

Datatilsynet blev i starten af august opmærksom på et brud på persondatasikkerheden ved deres lokaler i Valby. Bruddet vedrørte Datatilsynets bortskaffelse af papirmateriale, der potentielt indeholdt personoplysninger.

Sikkerhedsbruddet stod på i perioden fra februar 2020 indtil bruddets opdagelse i august 2020. Bruddet skete, idet papirmateriale, som indeholdte fortrolige og følsomme oplysninger, og som derfor skulle have været makuleret, ved en fejl blev bortskaffet som almindeligt papiraffald. Datatilsynet havde fejlagtigt afmærket en beholder med almindelig papiraffald som værende en makuleringsspand, uden at det blev kontrolleret, hvorvidt der reelt var tale om en sådan beholder. Bruddet indebar at papirmaterialet, der potentielt indeholdte personoplysninger, og som var ment til bortskaffelse ved makulering, blev behandlet som almindeligt papiraffald. Herved havde papirpateriet været tilgængeligt for bygningens servicepersonale og for vognmandsfirmaet, der afhentede og transporterede affaldet til genbrug.

Datatilsynet fandt på denne baggrund, at tilsynet havde overtrådt artikel 32, stk. 1 i Europa-Parlamentet og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen'), idet tilsynet ikke havde truffet de passende organisatoriske og teknikske foranstaltninger for at sikre et sikkerhedsniveau, der passede til de risici, der var ved tilsynets behandling af personoplysninger.

Om Datatilsynets foretagender efter bruddets opdagelse har tilsynet oplyst, at papiraffaldet efterfølgende er blevet bortskaffet på den tilsigtede måde, at Datatilsynets anmeldelse af bruddet skete et døgn for sent i forhold til fristen på 72 timer efter databeskyttelsesforordningens artikel 33, stk. 1, at Datatilsynet har underrettet de registrerede gennem nyheder på Datatilsynets hjemmeside, samt at Datatilsynet har gennemgået dets procedurer for bortskaffelse af papiraffald og indskærpet sine retningslinjer.

Læs hele afgørelsen her:

https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/sep/brud-paa-persondatasikkerheden-i-datatilsynet

1.6 Korrekt ikke at give en registreret indsigt i et dokument, der vurderer, hvorvidt en bestemt retssag mod en kunde kan vindes

Det danske datatilsyn ('Datatilsynet') afsagde den 20. august 2020 afgørelse i sag med journalnummer 2020-31-2757 vedrørende en klage over manglende indsigt.

En borger klagede den 13. februar 2020 til Datatilsynet over, at Velliv, Pension & Livsforsikring A/S ('Velliv') ikke havde meddelt indsigt i alle oplysninger, som Velliv behandlede om borgeren. Overordnet havde borgeren i sin klage anført, at vedkommende ikke havde fået fuld indsigt i de personoplysninger, som Velliv havde behandlet om borgeren i perioden fra den 6. februar 2018 til den 10. januar 2019. Borgerens forsikringsdækning ved Velliv blev bragt til ophør den 1. februar 2019.

Velliv oplyste, at Velliv i forbindelse med besvarelsen af borgerens indsigtsanmodning undtog oplysninger om et internt arbejdsdokument og en korrespondance med Vellivs advokat, som ifølge Velliv ikke var omfattet af retten til indsigt, jf. lov nr. 502 af 23. maj 2018 ('den danske databeskyttelseslov') § 22.

Det følger af den danske databeskyttelseslovs § 22, stk. 1, at artikel 15 i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen') ikke finder anvendelse, hvis den registreredes interesse i oplysningerne findes at burde vige for afgørende hensyn til private interesser, herunder hensynet til den pågældende selv. Af de specielle bemærkninger til lovens § 22, stk. 1, fremgår bl.a. at den dataansvarlige efter omstændighederne kan nægte indsigt i f.eks. et notat, der vurderer, hvorvidt der er udsigt til, at en bestemt retssag mod en kunde kan vindes. Herudover lagde Datatilsynet vægt på, at Velliv havde oplyst, at de personoplysninger, som er indeholdt i det omhandlede materiale, allerede var tilgået borgeren, og at materialet derudover ikke indeholdt oplysninger om borgeren, som er omfattet af indsigtsretten.

Vellivs behandling af personoplysninger var sket inden for rammerne af reglerne i databeskyttelsesforordningens artikel 15 og den danske databeskyttelseslovs § 22, stk. 1. Datatilsynet fandt på den baggrund, at Velliv var berettiget til at undtage det interne arbejdsdokument og korrespondancen med Vellivs advokat, hvorfor der ikke var grundlag for at udtale kritik af Velliv.

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

1.7 Videregivelse af kundeoplysninger til brug for markedsføring var lovligt

Det danske datatilsyn ('Datatilsynet') afsagde den 11. juni 2020 afgørelse i sag med journalnummer 2019-31-2211 vedrørende klage over Stofa A/S' ('Stofa') videregivelse af kundeoplysninger til Syd Energi ('SE') til brug for markedsføring.

Sagen blev indledt på baggrund af, at en kunde hos Stofa klagede til Datatilsynet over, at vedkommendes navn, adresse, telefonnummer og kundenummer var blevet videregivet til SE, der efterfølgende kontaktede klageren med henblik på indgåelse af el-aftale.

Det følger af lov nr. 502 af 23. maj 2018 ('den danske databeskyttelseslov') § 13, stk. 1, at en virksomhed ikke må videregive oplysninger om en forbruger til en anden virksomhed til brug for direkte markedsføring eller anvende oplysningerne på vegne af en anden virksomhed i dette øjemed, medmindre forbrugeren har givet sit udtrykkelige samtykke hertil. Datatilsynet vurderede sagen efter undtagelsen i den danske databeskyttelseslov§ 13, stk. 2, hvorefter videregivelse af personoplysninger om en forbruger til en anden virksomhed til brug for direkte markedsføring kan ske hvis to betingelser er opfyldt. For det første skal der være tale om generelle kundeoplysninger, og for det andet skal videregivelsen følge den interesseafvejning, som er fastsat i artikel 6, stk. 1, litra f i Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 ('databeskyttelsesforordningen').

Datatilsynet lagde ved afgørelsen vægt på, at der i forarbejderne til den danske databeskyttelseslov § 13 står, at interesseafvejningsreglen kun undtagelsesvist vil falde ud til kundens fordel ved anvendelsen af databeskyttelseslovens § 13, stk. 2. Herudover lagde Datatilsynet vægt på, at der var tale om generelle kundeoplysninger, samt at videregivelsen skete med henblik på, at kunne tilbyde kunden en el-aftale, som vil kunne føre til en besparelse. Stofas videregivelse af kundeoplysninger var derfor sket i overensstemmelse med den danske databeskyttelseslov § 13, stk. 2.

Læs hele afgørelsen her: https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/jun/videregivelse-af-kundeoplysninger-til-brug-for-direkte-markedsfoering/

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

Delphi

Christina Björn

Bakgrund

Som tillsynsmyndighet tar Datainspektionen emot klagomål från enskilda med anledning av dataskyddsförordningen, GDPR. Under hösten har myndigheten publicerat en rapport om dessa nationella klagomål som har inkommit till myndigheten från dess att förordningen började att tillämpas och två år framåt, dvs. från den 25 maj 2018 till och med den 24 maj 2020. Klagomålen utgörs till största delen av sådana som rör GDPR, men eftersom Datainspektionen därutöver är tillsynsmyndighet avseende brottsdatalagen, samt inom kamerabevakning, kreditupplysning och inkasso, inkommer även klagomål som är kopplade till dessa områden.

Ett klagomål behöver nödvändigtvis inte vara kopplat till att den enskilde själv har drabbats av en felaktig personuppgiftshantering, utan varje person kan även tipsa Datainspektionen om denne anser att ett företag, myndighet eller annan organisation har brutit mot GDPR, eller någon av de andra tillsynsområdena, i sin hantering.

Kraftig ökning av antalet klagomål sedan införandet av GDPR

Sedan GDPR trädde i kraft i maj 2018, har antalet klagomål till Datainspektionen gällande behandling av personuppgifter ökat kraftigt. En förklaring enligt rapporten är att medvetenheten hos medborgarna har ökat och därmed förväntningarna på att behandlingen av deras personuppgifter ska vara korrekt. Av de cirka 3 500 klagomål som årligen inkommer till Datainspektionen rör närmare 90 procent dataskyddsförordningen. Antalet kan jämföras med de cirka 500 klagomål som myndigheten tog emot året innan GDPR trädde i kraft, dvs. när personuppgiftslagen, PUL, fortfarande var tillämplig.

Ett syfte med de enskildas rättigheter enligt GDPR är att ge alla medborgare en bättre kontroll på hur behandlingen av deras personuppgifter sker. Ungefär en fjärdedel av de klagomål som inkommit rörande GDPR är hänförliga till de enskildas rättigheter, och ytterligare knappt en fjärdedel rör klagomål kopplat till sajter med utgivningsbevis. Drygt hälften av anmälningarna som rör de enskildas rättigheter handlar om rätten till radering. En typisk situation bland klagomålen som Datainspektionen ger som exempel i sin rapport, är när en kund har avslutat sin kundrelation och bett om att få sina personuppgifter borttagna. Trots påpekandet från kunden har företaget inte agerat. Rapporten tar upp flertalet exempel på där kunder åtskilliga gånger har kontaktat företagen, som inte tillgodoser den registrerades rättighet vad gäller radering.

En annan stor andel av klagomålen som rör den enskildas rättigheter är rätten till registerutdrag, vilket utgör en tredjedel av klagomålen hänförliga till den registrerades rättigheter. Vanliga situationer som Datainspektionen tar upp i sin rapport är, likt många klagomål som är kopplat till rätten till radering, att företaget inte tillgodoser den enskildes förfrågan. I många fall rör klagomålen att registerutdraget inte är komplett, men även att företagen inte ens svarar på den enskildes förfrågan.

Ungefär hälften av alla klagomål enligt dataskyddsförordningen som Datainspektionen fick in under den här tvåårsperioden, rör privat sektor. Den enskilt största branschen som klagomålen riktar sig mot, 25 procent, är sökmotorer.

Granskningar med anledning av de registrerades rättigheter

En del av Datainspektionens uppdrag som tillsynsmyndighet är att granska efterlevnaden av tillämpliga lagar och regler, ett sätt är att utföra granskningar av de som hanterar personuppgifter. Kort efter att rapporten publicerades i slutet av oktober 2020, meddelade myndigheten att ett antal granskningar nu ska inledas. Granskningarna kommer att vara inriktade på just de registrerades rättigheter och till skillnad från andra granskningar är detta en mer specifikt inriktad granskning med utgångspunkt i de enskildas klagomål som har kommit in.

Det kommer att bli intressant att se vad resultatet av granskningarna kommer att bli och vad den fortsatta utvecklingen kommer att resultera i, både vad gäller eventuella sanktioner som kommer utdelas till verksamheterna, men även vad gäller de enskildas medvetenhet om hanteringen av deras personuppgifter. Med tanke på den kraftiga ökningen av klagomål som har skett enbart under de senaste två åren, är detta nog bara en början som vi ser.

Christina Björn är associate i Advokatfirman Delphi, Stockholm.

Gorrissen Federspiel

Tue Goldschmieding

Indkøbsforening for cykelkæder havde ikke handlet i strid med god markedsføringsskik ved salg af cykeltilbehør

Den danske Sø- og Handelsret ('Sø- og Handelsretten') afsagde den 25. august 2020 dom i sagen BS-55 374/2019-SHR mellem GripGrab ApS ('GripGrab') og Indkøbsforeningen Fri A.m.b.a ('Indkøbsforeningen'). Sagen angik et spørgsmål om, hvorvidt en række forskellige produkter indenfor cykeludstyr var beskyttet mod efterligninger efter lov nr. 426 af 3. maj 2017 (den danske'markedsføringslov') og i så fald, hvorvidt Indkøbsforeningen, ved at have markedsført en række tilsvarende produkter, havde krænket GripGrabs rettigheder efter den danske markedsføringslovs § 3, stk. 1.

For så vidt angår spørgsmålet om beskyttelsen efter den danske markedsføringslov fandt Sø- og Handelsretten, at beskyttelsen alene kunne udstrækkes til at omfatte beskyttelse mod slaviske efterligninger, og hvad der må sidestilles hermed, jf. den danske markedsføringslovs § 3, stk. 1.

Sø- og Handelsretten fandt, at Indkøbsforeningens produkter fremstod som forholdsvis nærgående efterligninger af GripGrabs produkter og i øvrigt havde formgivningsmæssige ligheder hermed samt at især to af produkterne fra Indkøbsforeningen havde'iøjnefaldende ligheder' med de samme produkttyper fra GripGrab. Dog vurderede Sø- og Handelsretten, at produkterne ikke havde karakter af slaviske efterligninger, eller hvad der må sidestilles hermed, og der forelå dermed ikke en krænkelse af GripGrabs rettigheder efter den danske markedsføringslov.

Læs hele afgørelsen her: http://domstol.fe1.tangora.com/media/-300 011/files/Dom-55 374-2019-SHR.pdf

Der kunne ikke nedlægges midlertidigt forbud mod markedsføring af terrassevarmer

Den danske Sø- og Handelsret ('Sø- og Handelsretten') afsagde den 24. august 2020 dom i sagen BS-16 630/2020-SHR mellem Zhuhai Runwin Electric Co., Ltd ('Runwin') og Schou Company A/S ('Schou'). Runwin begærede i sagen forbud mod Schou's udbud, markedsføring, import, eksport og salg af en terrassevarmer, som Runwin påstod at have en beskyttet ret til, i henhold til lovbekendtgørelse nr. 1144 af 23. oktober 2014 ('den danske ophavsretslov'), Rådets forordning af 2001-12-12 om EF-design ('EF-designforordningen') og lov nr. 426 af 3. maj 2017 ('den danske markedsføringslov').

Om beskyttelsen af produktet efter den danske ophavsretslovs §1, fandt retten ikke, at Runwins terrassevarmer var ophavsretligt beskyttet, idet designet af terrassevarmeren fandtes at være funktionelt betinget, og kun bar ringe eller ingen præg af, at være et udtryk for frie og kreative valg, som kunne anses for en beskyttet intellektuel frembringelse I forhold til beskyttelsesomfanget for EF-designet fandt retten, at produktets udseende bar stærkt præg af, at være bestemt af dets tekniske funktion, hvilket ikke beskyttes, jf. EF-designforordningens artikel 8, stk. 1. Retten fandt det ikke bevist, at Runwins design på tidspunktet for registreringen var nyt og havde individuel karakter. Omfanget af Runwins designbeskyttelse var derfor snæver. Af disse grunde fandt retten ikke, at den informerede burger ville få et sådan helhedsindtryk af det påståede krænkende design, at der forelå en krænkelse.

Om beskyttelse af Runwins terrassevarmer efter den danske markedsføringslov udtalte retten, at Runwins terrassevarmer nød beskyttelse efter den danske markedsføringslovs § 3. Beskyttelsen er dog meget snæver og kun kan udstrækkes til nærgående efterligninger. Beskyttelsen omfatter også kun produkter, hvor der har været en egentlig markedsføringsindsats, beregnet til at give produktet en særlig markedsmæssig identitet. Med henvisning til forskellighederne mellem Runwins og Schou's produkter, og at Runwin ikke kunne dokumentere en egentlig markedsføringsindsats, fandt retten, at Schou ikke havde handlet i strid med god markedsføringsskik.

Retten fandt på baggrund af ovenstående ikke grundlag for at fremme Runwins begæring om forbud men tog i stedet Schous påstand om frifindelse til følge.

Læs hele afgørelsen her: http://domstol.fe1.tangora.com/media/-300 011/files/Kendelse-BS-16 630-2020.pdf

Tasker blev ikke krænket efter markedsføringsloven

Sø- og Handelsretten afsagde den 12. august 2020 to domme. Først

sagen BS-3143/2019-SHR mellem Depeche & Co. A/S (»Depeche«) mod Dixie ApS (»Dixie«) og dernæst de i de sambehandlede sager BS-87/2019-SHR og BS-28 774-2019-SHR mellem Depeche mod LM Noella fashion IVS og Noella Wholesale ApS (tilsammen »Noella«). De to domme omtales i det følgende samlet, da de drejer sig om samme spørgsmål.

Sagerne angik spørgsmålet om hvorvidt fem af Depeches tasker var beskyttet mod efterligninger efter lov nr. 426 af 3. maj 2017 ('den danske markedsføringslov') og Europa-Parlamentets og Rådets forordning (EF) nr. 6/2002 af 12. december 2001 ('designforordningens') regler om ikke-registrerede EF-Designs - og i så fald, hvorvidt de sagsøgte havde krænket Depeches rettigheder ved at markedsføre lignende tasker.

Sø- og Handelsretten fandt, at fire ud af fem af taskerne var beskyttede af reglerne i designforordningen. Taskerne var modeprodukter, der var sammensatte af allerede kendte elementer, men havde dog alligevel et vist særpræg, hvorfor de også nød beskyttelse mod meget nærgående eller slaviske produktefterligninger, jf. den danske markedsføringslovens § 3.Sø- og Handelsretten fandt dog ikke, at der rent designmæssigt var så stor en lighed mellem partneres tasker at det konstituerede en slavisk efterligning. Derfor var der ikke tale om en krænkelse af Depeches rettigheder, hverken efter reglerne om EF-Designs eller efter den danske markedsføringslov § 3.

De sagsøgte blev derfor frifundet af Sø- og Handelsretten.

Læs hele dommen vedr. DEPECHE & CO A/S mod DIXIE ApS her:

http://domstol.fe1.tangora.com/media/-300 011/files/Dom_BS-3143-2019.pdf

Læs hele dommen vedr. DEPECHE & CO A/S mod LM Noella fashion IVS og Noella Wholesale ApS her:

http://domstol.fe1.tangora.com/media/-300 011/files/Dom_(sambehandling)_BS-87-2019_og_BS-28 774-2019.pdf

Ikke påbud om at angive »interflora« som negativt søgeord i Google Ads

Den danske Sø- og Handelsret ('Sø- og Handelsretten') afsagde den 25. juni 2020 dom i sagen, BS-58 160/2019-SHR, mellem Interflora Danmark A/S ('Interflora') og Abella Blomster v/Jeanette Rasmussen ('Abella Blomster'). Sagen angik, hvorvidt Abella Blomster havde krænket Interfloras varemærke, og om Abella Blomster kunne blive påbudt at angive »*interflora*« som negativt søgeord i Google Ads.

Interflora gjorde i spørgsmålet om krænkelse af varemærketten gældende, at Abella Blomster indirekte gjorde brug af Interfloras varemærke ved annoncer på Goolge, idet Abella Blomster annonce blev vist, når der på Google bl.a. blev søgt på ordene *»send blomster interflora«*.

Abella Blomster havde gennem Google Ads betalt for at få vist sin annonce, når der på Google blev søgt på »*send blomster*« og andre lignende søgeord, men Abella Blomster havde ikke angivet »*interflora*« som et positivt søgeord. Det var ubestridt mellem partnerne at Abella Blomster ikke havde registreret »*interflora*« som søgeord i Google Ads. Sø- og Handelsretten anførte, at Abella Blomster derfor, allerede af den grund, ikke krænkede Interfloras varemærke efter lov nr. 88 af 29. januar 2019 ('den danske varemærkelov') § 4 og lov nr. 426 af 3. maj 2017 ('den danske markedsføringslov') § 22.

Interflora gjorde desuden gældende, at Abella Blomster skulle pålægges at angive »*interflora*« som et negativt søgeord i Google Ads. Ved at angive »*interflora*« som et negativt søgeord i Google Ads, ville Abella Blomsters annoncer ikke blive vist, når en søgning på Google indeholdt »*interflora*«, selvom søgningen også indeholdt andre søgeord, hvortil Abella Blomster ellers havde betalt for at få vist sin annonce.

Sø- og Handelsretten fandt dog uden nogen nærmere begrundelse, at der ikke var grundlag for at pålægge Abella Blomster et sådant påbud, og det ville derfor ikke stride imod den danske markedsføringslovs § 3, om god markedsføringsskik, ikke at angive »*interflora*« som et negativt søgeord i Google Ads.

Læs hele kendelsen her:

http://domstol.fe1.tangora.com/media/-300 011/files/Kendelse__BS-58 160-2019-SHR.pdf

Synoptik A/S skal betale bøde på 300.000 kr. for vildledende markedsføring

Forbrugerombudsmanden anmeldte i 2018 Synoptik A/S til politiet for vildledende markedsføring, og nu har optikerkæden accepteret, at betale en bøde på 300.000 kr.

Synoptik A/S havde i 2017 sendt reklamebreve ud til forbrugere, hvori der blev reklameret med 50 % rabat på brilleglas, men det fremgik ikke tydeligt nok, at rabatten var betinget af, at kunden tillige købte et brillestel til fuld pris. Selve reklamen blev vist med stor hvid skrift i en rød boks, og langs højre side af boksen stor med væsentlig mindre, lodret skrift: »Gælder til 30.12.17 for alle glas ved køb af stel«.

Forbrugerombudsmanden vurderede i sin behandling af sagen, at den enkelte forbruger let har kunnet overse betingelsen om køb af brillestel. Forbrugerombudsmanden henviser til lov nr. 426 af 3 maj 2017 ('den danske markedsføringslov') §§ 5 og 6 og udtaler, at forbrugere klart og tydeligt skal kunne se, hvad der bliver tilbudt i en reklame, og at såfremt reklamen fremstår som et bedre tilbud end det reelt er, foreligger der vildledende markedsføring.

Læs hele nyheden her:

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

pressemeddelelser/2020/optikerkaede-har-betalt-boede-paa-300 000-kroner-for-vildledning/

Domænenavnet »minklasse.dk« skulle ikke overdrages til klageren

Det danske klagenævn for domænenavne ('Klagenævnet for Domænenavne') afsagde den 30. juni 2o2o afgørelse i sag med journalnummer 2020-0085 vedrørende rettigheden til domænet »minklasse.dk«.

Sagen omhandlede domænets mulige overdragelse til virksomheden Min Klasse ApS ('Min Klasse'), som følge af manglende aktivitet på domænet. Min Klasse ville tillige have domænet overdraget med henblik på udviklingen af en app af samme navn, der skulle bruges til udviklingen af et socialt medie. Min Klasse henviste til lov nr. 164 af 26. februar 2014 ('den danske domænelov') § 25, stk. 1 om god domænenavnsskik og gjorde gældende, at det inaktive domæne udgjorde brud på denne.

Indklagede, som var privatperson, ('indklagede') angav derimod i svarskriftet, at domænet blev benyttet gennem en whitelisting af få IP-adresser, der gør det muligt at se indholdet på domænet. Derudover argumenterede indklagede ligeledes for, at domænet ville blive brugt med henblik på at åbne et virtuelt lokale for skoleopgaver og gjorde i den forbindelse gældende, at praksis fra klagenævnet viste, at det ikke var brud på god domænenavnsskik blot at have rettighederne til et domæne uden at bruge dette aktivt.

Klagenævnet fandt ikke, at der var grundlag for at imødekomme klagerens ønske om at få domænet overdraget, da Min Klasses interesse i domænet ikke oversteg indklagedes egen interesse i at beholde domænenavnet »minklasse.dk«. Tillige bemærkede Klagenævnet, at den manglende brug af et eksisterende domænenavn ikke i sig selv er i strid med domænelovens § 25, stk. 1 om god domænenavnsskik.

Læs hele afgørelsen her: https://www.domaeneklager.dk/sites/default/files/2020-07/2020-0085%2C%20minklasse.dk_.pdf

Domænenavnet »suspekt.dk« skulle ikke overdrages til klageren

Det danske klagenævn for domænenavne ('Klagenævnet for Domænenavne') traf den 30. juni 2020 afgørelse i sag 2020-0070, mellem SUSPEKT 2010 ApS ('klager') og privatperson ('indklagede'). Klagenævnet for Domænenavne fandt frem til, at domænet'suspekt.dk' ikke skulle overføres til klager.

Klager gjorde gældende, at klager er et af de største navne i den danske musikbranche, hvilket understøttedes af, at klager følges af 139.000 og 84.000 personer på henholdsvis Facebook og Instagram. Klager oplyste, at klager ville bruge domænenavnet til sin webshop og til at kommunikere om klagerens musiske virke. Desuden mente klager, at indklagede ikke overholdte god domænenavnsskik efter lov nr. 164 af 26. februar 2014 ('den danske domænelov') § 25, stk. 1, og klager bemærkede i denne forbindelse, at der ikke var noget indhold på »suspekt.dk«.

Indklagede gjorde blandt andet gældende, at »suspekt« er et almindeligt dansk ord, og at indklagede registrerede domænenavnet mere end 10 år inden, klager registrerede sit selskabsnavn. Desuden gjordes det gældende, at klager har brugt og brandet sig gennem domænenavnet »tabushop.dk« siden 2010. Indklagede forklarede, at »su-spekt.dk« blev registreret i slutningen af 1990'erne, idet indklagede var med i et fællesskab, der kaldte sig »Club Suspekt«, og på den baggrund registrerede indklagede domænenavnet med henblik på, at gruppens medlemmer kunne oprette anonyme e-mailadresser. I øvrigt bemærkede indklagede, at registreringen af domænenavnet ikke forhindrer klager i at udøve den ønskede virksomhed, samt at parterne ikke har sammenfaldende interesser.

Klagenævnet for Domænenavne havde i sagen foretaget henholdsvis en vurdering af om registreringen af »suspekt.dk« var i strid med den danske domænelov § 25, stk. 1, samt en interesseafvejning og en afvejning af, hvordan domænenavnet anvendtes. Klagenævnet for Domænenavne lagde i sin afgørelse vægt på, at ordet »suspekt« er et almindeligt dansk ord, der som udgangspunkt frit kan anvendes af enhver. Dette til trods for ordet »suspekt« i høj grad forbindes med denne klager som musikgruppe. Nævnet nåede ud fra parternes respektive forklaringer frem til, at begge parter havde en interesse i at kunne disponere over domænenavnet. Samtidig vurderede nævnet, at klagers interesser ikke væsentligt oversteg indklagedes interesser. Da indklagede derudover havde registreret domænenavnet flere år inden stiftelsen af klageren (som selskab) og selve musikgruppen, Suspekt, havde indklagede ikke handlet i strid med god domænenavnsskik.

Læs hele afgørelsen her: https://www.domaeneklager.dk/sites/default/files/2020-07/2020-0070%2C%20suspekt.dk_.pdf

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

Bird & Bird

Karin Söderberg

Satirikern Aron Flam frias från upphovsrättsintrång i En svensk tiger – han har skapat en parodi

Sammanfattning

Bilden *En svensk tiger* skapades av författaren och illustratören Bertil Almqvist under andra världskriget. Den togs fram åt Statens Informationsstyrelse i samband med deras vaksamhetskampanj. Kampanjens syfte var att uppmana svenskarna att hålla tyst om information som kunde skada Sverige.

Satirikern och författaren Aron Flam har med *En svensk tiger* som utgångspunkt skapat flera egna versioner. Den som fått mest uppmärksamhet är omslagsbilden till Aron Flams bok *Det här är en svensk tiger*. Boken handlar om Sveriges undfallenhet gentemot Nazityskland under andra världskriget.

Det finns väsentliga detaljer som skiljer verken åt bland annat har Flams tiger en svastika runt ena benet och det andra benet rest i en "Hitlerhälsning", den ler, blinkar med det ena ögat och har en jungiansk skugga.

En polisanmälan med påstående om upphovsrättsintrång gjordes av Beredskapsmuseet som är innehavare av de ekonomiska rättigheterna till Almqvists tiger. En förundersökning inleddes, åtal väcktes samt ansökan om förbud och yrkande om skadestånd framställdes av Beredskapsmuseet och Bertil Almqvists efterlevande i juli 2020. En upplaga av Aron Flams bok togs i beslag i juni 2020 av polisen. Efter om- och överprövning hävdes beslaget av Patent- och marknadsöverdomstolen i augusti 2020. Huvudförhandling hölls i Patent- och marknadsdomstolen i september 2020 och Aron Flam friades från upphovsrättsintrång och övriga yrkanden lämnades utan bifall i dom som meddelades i oktober 2020. Både åklagaren, Beredskapsmuseet samt Bertil Amlqvists barn har överklagat domen till Patent- och marknadsöverdomstolen.

Rättsliga utgångspunkter

Den som skapat ett litterärt eller konstnärligt verk har upphovsrätt till verket enligt 1 § 1 st. upphovsrättslagen, under förutsättning att verket är självständigt och originellt i den mening att det ger uttryck för upphovsmannens egen intellektuella skapelse. Upphovsmannen har en uteslutande rätt att förfoga över verket genom att framställa exemplar av det och göra det tillgängligt för allmänheten enligt 2 § upphovsrättslagen. Med upphovsrätten följer också ideella rättigheter, dels en rätt att bli namngiven och dels en rätt att motsätta sig vissa förändringar av verket i samband med utnyttjande av verket, vilket följer av 3 § upphovsrättslagen.

Parodiundantaget är en i svensk rätt oskriven rättsregel. Av förarbetena till upphovsrättslagen framgår att det av gammal hävd har ansetts tillåtet att göra parodi på andras verk. Parodiundantaget har också fastställts och utvecklats i praxis (se bland annat NJA 1975 s. 679 och NJA 2005 s. 905). Vid bedömningen av om ett verk utgör en parodi tillämpades bestämmelsen i 4 § 2 st. upphovsrättslagen. Den föreskriver att om någon i fri anslutning till ett verk har åstadkommit ett nytt och självständigt verk, är hans upphovsrätt inte beroende av rätten till originalverket. Enligt praxis föreligger ett sådant fall när det nya verket visserligen har inspirerats av ett äldre verk, men samtidigt fått sin prägel av utförarens egen individualitet och har verkshöjd (se NJA 2017 s. 75 p. 12).

Upphovsrättslagen ska dock även tolkas i enlighet med Infosoc-direktivet. Direktivet innehåller en uttömmande lista över de inskränkningar från upphovsrätten som medlemsstaterna får införa i nationell rätt. Parodiundantaget återfinns i Infosoc-direktivets artikel 5.3(k). Till skillnad från det tidigare svenska synsättet regleras parodiundantaget inom EU-rätten som en inskränkning i upphovsmannens ensamrätt. Artikeln är visserligen fakultativ, men EU-domstolen har genom *Deckmyn*-avgörandet (mål C-201/13) uttalat att begreppet *parodi* utgör ett självständigt begrepp i unionsrätten och ska ges en autonom tolkning inom unionen.

2019 prövade Patent- och marknadsöverdomstolen parodiundantaget i förhållande till EU-rätten och *Deckmyn*-avgörandet (*Järnrörsmålet,* PMT 1473-18). Domstolen kom fram till att parodiundantaget i svensk rätt ska tolkas fördragskonformt. Det innebär att det är tillräckligt att parodin erinrar om men samtidigt skiljer sig från originalet. Dessutom ska parodin ha ett humoristiskt eller förlöjligande syfte. Däremot behöver inte parodin uppvisa egen originalitet. Genom avgörandet från 2019 får det numera anses

vara fastställt att en parodi inte längre behöver betraktas som ett nytt och självständigt verk.

Patent- och marknadsdomstolens avgörande

Aron Flam gjorde gällande att hans tigrar var egna självständiga verk och parodier enligt parodiundantaget som det formulerats i *Deckmyn* och *Järnrörsmålet*. Domstolen fann att Aron Flams illustrationer inte var egna självständiga verk trots att de förvisso uppvisade egen individualitet. Detta eftersom enligt domstolen Aron Flam samtidigt använt en tiger som behållit de väsentliga särdragen från Bertil Almqvists tiger.

Domstolen prövade därefter om Aron Flams illustrationer omfattades av det harmoniserade parodiundantaget. Domstolen konstaterade att Aron Flam förklarat att han "medelst parodins form har velat ifrågasätta tigerns symbolik och den censur- och tystnadskultur som enligt honom präglat samhälls- och kulturdebatten i Sverige under många års tid.". Mot bakgrund av Aron Flams berättelse fann domstolen att hans användning av en tiger utgjort ett parodiskt inslag i hans kommunikation, med udden riktad mot det som Almqvists tiger har kommit att bli symbol för och inte mot Almqvists tiger som sådan. Domstolen fann också att "Tigern satts i en ny kontext som märkbart skiljer sig från originalverket och den bär på ett tydligt och förlöjligande budskap". Med detta som utgångspunkt friade domstolen Aron Flam från ansvar för upphovsrättsintrång. På grund av friandet i skuldfrågan föll också yrkandet om förbud och skadestånd för påstått intrång i ekonomiska rättigheter.

Bertil Almqvists efterlevande och innehavare av de ideella rättigheterna till *En svensk tiger*, yrkade för egen del bland annat på ersättning för ideell skada under påstående att Aron Flam ändrat originalverket på ett sätt som var kränkande. Domstolen fann att någon kränkning av den ideella rätten inte kunde bli aktuellt eftersom parodin inte tog sikte på att kränka Bertil Almqvists konstnärliga anseende eller egenart utan genom ett parodiskt grepp ifrågasätta det budskap som Bertil Almqvists tiger med tiden kommit att representera. Därmed lämnades även detta yrkande utan bifall.

Aron Flam företräds av Advokat Monique Wadsted på Bird & Bird.

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


simonsen vogtwiig

Rune Ljostad og
Hedda Baumann Heier

Høyesterett med klargjøringer av reglene for erverv av rett til arbeidstakeroppfinnelser

Høyesterett avsa 22. oktober 2020 dom i saken mellom en tidligere stipendiat og Staten v/Universitetet i Oslo (UiO). Lagmannsrettsdommen i samme saksforhold er tidligere omtalt i *Nytt i immaterialretten*-spalten i Lov&Data nr. 141 1/2020.

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. Det viste seg imidlertid at hennes veiledere hadde bistått det svenske selskapet i forbindelse med utformingen av patentsøknadene.

Stipendiaten krevde bl.a. godtgjøring etter reglen i arbeidstakeroppfinnelsesloven § 7 som gir arbeidstaker rett til rimelig godtgjøring dersom arbeidsgiver erverver retten til en oppfinnelse som arbeidstaker har gjort. Ordlyden i § 7 åpner opp for at slikt erverv av rettigheter kan skje enten i medhold av de særlige prosedyrene beskrevet i arbeidstakeroppfinnelsesloven eller «*på annet grunnlag*». Spørsmålet Høyesterett tok stilling til var om oppfinnelsen i saken var blitt ervervet av UiO på annet grunnlag.

I avgjørelsen starter Høyesterett med å konstatere at en *avtale* mellom arbeidstaker og arbeidsgiver utvilsomt vil være et ervervsgrunnlag som kan gi krav på vederlag etter § 7. Høyesterett ville heller ikke utelukke at også andre ervervsgrunnlag kan være aktuelle, men presiserer at det må dreie seg om et grunnlag som gir arbeidsgiveren rett til selve oppfinnelsen. At arbeidsgiver disponerer over oppfinnelsen på egenhånd er etter Høyesteretts syn altså ikke tilstrekkelig hvis ikke også «*arbeidstakeren har akseptert eller godkjent arbeidgiverens erverv, det vil si gitt avkall på sin rett til oppfinnelsen*» (avsnitt 37). I mangel av en klar avtale blir det avgjørende altså om det foreligger disposisjoner eller adferd som viser at *begge* parter har bundet seg etter alminnelige avtalerettslige regler til å overføre rett til oppfinnelsen fra arbeidstaker til arbeidsgiver (avsnitt 39).

I den foreliggende saken var ikke stipendiaten kjent med veilederens samarbeid med det svenske selskapet om inngivelse av patentsøknad. Stipendiaten hadde derfor ikke – hverken uttrykkelig, stilltiende eller ved passivitet – bundet seg til å overføre rettigheter til UiO. Videre vektlegger Høyesterett også at veilederen ved universitetet ikke gjennom sine handlinger kunne binde universitetet da dette lå utenfor hans stillingsfullmakt som professor og seksjonsleder.

Resultatet ble i et enstemmig Høyesterett at UiO ikke hadde ervervet rettigheter til oppfinnelsen «på annet grunnlag».

Les dommen i Lovdatas database med saksnummer HR-2020-2017-A.

For ordens skyld gjøres det oppmerksom på at Advokatfirmaet Simonsen Vogt Wiig AS representerte det svenske firmaet som er eier av patentet på den omtvistede oppfinnelsen. Saken ble avvist for det svenske selskapets vedkommende på grunn av manglende norsk domsmyndighet, jf. LB-2016-135 328 jf. HR-2017-803-U.

Kulturdepartementet innhenter ekstern juridisk utredning av den norske kompensasjonsordningen for privat bruk

Etter åndsverkloven § 26 er det med visse unntak og begrensninger tillatt for den enkelte å fremstille eksemplar av offentliggjort åndsverk så lenge det er til privat bruk. Rettighetshavere kompenseres i dag for slik bruk gjennom en todelt ordning som består av en individuell del som forvaltes av Norwaco og en kollektiv del som forvaltes av Fond for lyd og bilde. Kulturdepartementet har tidligere varslet at det planla å se nærmere på kompensasjonsordningen for privat bruk av åndsverk. Som ledd i departementets arbeid med dette er det nå innhentet en juridisk utredning fra professor Ole-Andreas Rognstad ved Universitetet i Oslo.

Les utredningen og departementets pressemelding her: *https://www.regjeringen.no/no/aktuelt/kompensasjon-for-kopiering-til-privat-bruk--offentliggjoring-av-ekstern-juridisk-utredning/id2765352/*

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

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


SELMER
Vemund Sande og
Fredrik Lilleaas Ellingsen

Ny dom om forståelsen av avbestillingsklausulene i Statens standardavtaler

Oslo tingrett avsa 25. september 2020 dom i en prinsipiell sak om avtalefestet rett til kompensasjon ved avbestilling av Statens standardavtaler (SSA). Saken stod mellom det tyske softwareselskapet Softship GmbH («**Softship**») som saksøker og det norske shippingselskapet Wallenius Wilhelmsen Ocean AS («**WWO**») som saksøkt.

Softship skulle bistå WWO med implementering av et nytt ERP-system for WWOs samlede virksomhet, herunder forretningskritiske funksjoner som booking og håndtering av lasteoperasjoner for selskapets over 50 Roll-on Roll-off (RoRo) fartøy. Partene inngikk flere av SSAene for forskjellige deler av leveransen, herunder SSA-B og SSA-T (med visse endringer). WWO besluttet imidlertid å avbestille avtalene og ble senere saksøkt av Softship med krav om erstatning.

Spørsmålet for retten var blant annet hvordan avbestillingsklausulene i SSA skulle tolkes, og hvilke krav fra Softship som dermed var dekningsmessige under avtalene. Dette er første gang norske domstoler tar stilling til forståelsen av disse klausulene.

Både SSA-B og SSA-Ts standardtekst gir kunden en ubetinget rett til å avbestille tjenesten/leveransen med 30 dagers varsel. Ved slik avbestilling skal kunden dekke visse kostnader som påføres leverandøren, herunder leverandørens dokumenterte kostnader knyttet til omdisponering av personell. WWO anførte blant annet at Softship kun hadde krav på kostnadsdekning for lediggang hos konsulenter i avbestillingsperioden på 30 dager, mens Softship anførte å ha krav på kostnadsdekning utover denne perioden.

I dommen fikk WWO medhold på alle vesentlige punkter. Etter rettens syn var leverandøren kun berettiget til kostnadsdekning for lediggang hos konsulenter og arbeid i avbestillingsperioden på 30 dager under bistandsavtalen, beregnet etter leverandørens kostnad for interntid (ikke fulle timepriser). Retten tolket klausulen slik at Softship i avbestillingsperioden var forpliktet til å stille med én prosjektleder og fem konsulenter, slik partene hadde avtalt i april 2019. I den grad disse ressursene ikke kunne settes til annet inntektsbringende arbeid i den nevnte perioden, var dette en kostnad knyttet til omdisponering av personell som Softship kunne kreve dekket. Etter at avbestillingsperioden var over, tolket retten klausulen slik at partene var uforpliktet etter avtalen, og at Softship derfor ikke lenger hadde noen plikt til å reservere personell for WWO.

Softship fikk ikke medhold i sitt krav om dekning av kostnader for reservert utviklerkapasitet under utviklingsavtalen, ettersom det ikke forelå noen bestilte endringsordrer slik avbestillingsklausulen i den nevnte avtalen forutsatte (endret fra standardteksten). At Softship hadde rigget organisasjonen for å etterkomme kommende endringsordre, kunne etter rettens syn ikke føre til at klausulen måtte tolkes utvidende. Retten viste blant annet til at tjenesten kunne avbestilles med én ukes varsel (endret fra 30 dager i standardteksten) og at standardklausulen om kompensasjon ved avbestilling under spesifiseringsfasen ikke var inntatt i utviklingsavtalen som var inngått mellom partene. Avtalen la derfor opp til stor grad av fleksibilitet frem til endringsordre er avtalt.

Tingretten fant at WWO hadde vunnet saken i det vesentlige og selskapet ble tilkjent fulle saksomkostninger. Dommen er rettskraftig.

Etter vår mening er det grunn til å stille spørsmål ved rettens vurdering av spørsmålet under bistandsavtalen, herunder om det er mer treffende å tolke avbestillingsklausulen slik at avtalens generelle bestemmelser om kompensasjon gjelder i avbestillingsperioden, mens den nevnte klausulen gjelder utover dette, og at leverandøren derfor har krav på fulle timespriser i den nevnte perioden. En slik tolkning vil imidlertid ikke automatisk medføre at leverandøren har krav på kostnadsdekning for lediggang etter utløpet av avbestillingsperioden – dette må vurderes konkret. Den alminnelige tapsbegrensningsplikten vil kunne ha betydning for denne vurderingen.

Vemund Sande er advokatfullmektig og Fredrik Lilleaas Ellingsen er senioradvokat i avdelingen for HITEK i Advokatfirmaet Selmer, Oslo. Ellingsen var prosessfullmektig for WWO under tingrettssaken.

Gorrissen Federspiel

Tue Goldschmieding

K04 Standardkontrakt for IT-drift offentliggjort af Digitaliseringsstyrelsen

Den danske digitaliseringsstyrelse (»Digitaliseringsstyrelsen«) offentliggjorde den 25. august 2020 en ny statslig standardkontrakt for IT-drift udarbejdet i samarbejde med Advokatfirmaet Poul Schmith, Kammeradvokaten. Den nye standardkontrakt, K04, supplerer de eksisterende standardkontrakter, K01, K02 og K03, der vedrører IT-udviklingsydelser.

K04 består af en hovedaftale og i alt 45 bilag og følger den samme aftalestruktur som de øvrige K-standardkontrakter. K04 er tiltænkt anvendelig både som selvstændig driftskontrakt og som driftsbilag i forbindelse med IT-udvikling, hvor K02 eller K03 anvendes. K04 omfatter som udgangspunkt alle opgaver inden for IT-drift, men den kan som følge af dens modulære karakter tilpasses den konkrete driftsopgave.

K04 er ikke et *agreed document*, som K01 og K02 er, men det anføres, at Digitaliseringsstyrelsens hensigt med K04 var at udarbejde en afbalanceret kontrakt, der de facto vil blive en standardkontrakt for IT-drift, ligesom K02 blev for IT-udvikling.

Find nyheden fra Digitaliseringsstyrelsen her:
https://digst.dk/nyheder/nyhedsarkiv/2020/august/ny-standardkontrakt-for-it-drift/
Find kontrakten her:
https://digst.dk/styring/standardkontrakter/k04-standardkontrakt-for-it-drift/?Loginbox=true

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

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

Produksjon: 07 Media AS