Lov & Data

Nr. 152
Desember 2022

Nr. 4/2022










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

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

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

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

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

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

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

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

Trykk og layout: Aksell AS

Leder

Jarle Roar Sæbø

I dag vil jeg gjerne rope hurra for Datatilsynet. I det siste har vi igjen sett eksempler på at aktører med særinteresser innenfor et bestemt område, krever datainnsamling på en måte som tilsidesetter borgernes personvern på en urimelig måte. SSB krevde at dagligvarekjedene NorgesGruppen, Rema 1000, Coop og Bunnpris i sanntid skulle overføre kvitteringer til SSB. For 70 % av kundene ville Datatilsynet være i stand til å koble dataene til enkeltpersoner via betalingsinformasjonen, og Datatilsynet ville da få informasjon om hvem som har handlet hva samt tid og sted for handlene. Informasjonen ville komme inn til SSB i sanntid, slik at SSB visste hva du har handlet sekunder etter at handelen var gjennomført.

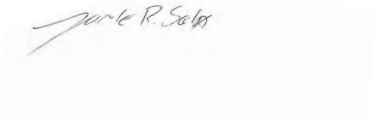
I sin egen Kost-nyttevurdering som ble overgitt til Datatilsynet, understreket SSB at de allerede behandlet personopplysninger av sensitiv art, herunder helseopplysninger. Her er det likevel en prinsipiell forskjell i at de aktuelle helseopplysningene allerede finnes i offentlige registre. Det nye tiltaket fra SSB ville derimot innebære tvungen overføring av personopplysninger fra

det private næringsliv og over i et offentlig register. Man kan kanskje innvende at dette er personopplysninger som allerede finnes, og som ligger i hendene til private aktører. Til dette vil jeg bemerke at summen av personopplysninger fra fire ulike dagligvarekjeder ville gi et enda mer intimt bilde av enkeltpersoners private anliggender enn de personopplysningene kjeden besitter hvor for seg.

Etter min vurdering har SSB feilet i avveiningen av de ulike interesser. SSB har sine helt legitime formål, og de har et viktig samfunnsoppdrag, men SSB burde likevel ha innsett at personvernhensyn ikke ville bli tilstrekkelig ivaretatt med dette forslaget. Når SSB feilet på denne måten, er det altså grunn til å rope hurra for Datatilsynets handlekraft, fordi Datatilsynet har varslet forbud mot tiltaket. Vi får håpe at SSB legger dette forslaget til side.

En statistikk jeg kunne tenke meg å se i denne sammenheng er som følger: Hvor stor andel av befolkningen bruker kontanter fordi de ikke er komfortable med dagens datainnsamling slik den allerede er, og hvor mye ville denne andelen vokse om de visste at SSB ville sitte med en komplett oversikt over alle deres innkjøp i dagligvarebutikker? Min personlige kontantbruk har iallfall gått opp bare ved å ha lest forslaget fra SSB. Når offentlige aktører tilsidesetter personvernet på denne måten, bør borgerne selv ta de grep man kan for å verne om sitt personvern.

Jarle Roar Sæbø



Lov om register over reelle rettighetshavere – kan allmennheten gis tilgang til registrerte opplysninger etter nylig avsagt dom i EU-domstolen?

Av Øystein Flagstad og Martha Krogli Brygfjeld

1. Innledning

Den norske loven om register over reelle rettighetshavere[1] har som formål å legge til rette for tilgang til opplysninger om hvilke fysiske personer som direkte eller indirekte kontrollerer en virksomhet. Loven inneholder bestemmelser om innhenting av opplysninger om reelle rettighetshavere, og bestemmer at opplysningene skal registreres i et offentlig register der allmennheten skal ha tilgang. Bestemmelsene om registrering har imidlertid ennå ikke trådt i kraft.

I en fersk avgjørelse fra EU-domstolen, avsagt i storkammer 22. november 2022, ble den tilsvarende direktivbestemmelsen om tilgang for allmennheten kjent ugyldig, i lys av EU-charterets bestemmelser om rett til respekt for privatlivet og beskyttelse av personopplysninger. Spørsmålet er hvilken betydning denne dommen får for de norske bestemmelsene om registrering av reelle rettighetshavere og særlig om allmennhetens tilgang til opplysningene.

2. Det norske registeret over reelle rettighetshavere

Formålet med loven er etter § 1 å «legge til rette for rapporteringspliktiges, myndighetenes og andres tilgang til opplysninger om reelle rettighetshavere». En slik åpenhet rundt eierskapet til og kontrollen av juridiske personer eller arrangementer omtales i forarbeidene som «et vesentlig tiltak for å motvirke misbruk av disse enhetene til hvitvasking, terrorfinansiering og annen kriminalitet»[2].

Øystein Flagstad

Martha Krogli Brygfjeld

Reelle rettighetshavere defineres som «de fysiske personene som anses å ha endelig eierskap til eller kontroll over juridiske personer eller juridiske arrangementer, slik som selskaper».[3]

Lov om register over reelle rettighetshavere ble kunngjort 1. mars 2019. Loven har delvis trådt i kraft, ved at virksomheter som omfattes av loven fra 1. november 2021 ble pålagt å innhente opplysninger over hvilke fysiske personer som er reelle rettighetshavere i den enkelte virksomhet, og på forespørsel å utlevere disse til offentlige myndigheter og rapporteringspliktige etter hvitvaskingsloven. Bestemmelsen i lovens kapittel 3 om registrering av opplysninger om reelle rettighetshavere i et offentlig register har ennå ikke trådt i kraft. Oppgaven med å føre register over reelle rettighetshavere er gitt til Brønnøysundregistrene, som foreløpig ikke har ferdigstilt de nødvendige tekniske løsningene for slik registrering. Det er imidlertid varslet at løsningene vil kunne være klare i løpet av 2023.

Hvitvaskingsutvalget foreslo opprinnelig at registeret som utgangspunkt kun skulle være tilgjengelig for offentlige myndigheter og andre med et legitimt behov for opplysningene, men dette ble på et senere tidspunkt i lovgivningsprosessen endret.[4] Slik bestemmelsen nå er utformet, skal «enhver» ha tilgang til de registrerte opplysningene, med unntak av opplysninger om fødselsnummer og D-nummer, som bare er tilgjengelig for offent-

1 LOV-2019-03-01-2

2 Innst. 143 L (2018–2019) side 1.

3 Innst. 143 L (2018–2019) side 1.

4 NOU 2016:27 side 248 og Prop. 109 L (2017–2018) side 26.

lige myndigheter og rapporteringspliktige, jf. forskriften[5] § 3-9(2).

Det følger videre av § 3-9(4) at registerfører etter søknad kan gjøre unntak fra tilgang til opplysninger dersom det foreligger «en konkret, ekstraordinær og uforholdsmessig risiko for at den fysiske personen søknaden gjelder, utsettes for bedrageri, utpressing, trakassering, vold eller trusler».

> Spørsmålet er hvilken betydning denne dommen får for de norske bestemmelsene om registrering av reelle rettighetshavere og særlig om allmennhetens tilgang til opplysningene.

3. Forente saker C-37/20 og C-601/20 LBR

Avgjørelsen i forente saker C-37/20 og C-601/20 *LBR* omhandler gyldigheten av endringsdirektiv 2018/843 (EUs femte hvitvaskingsdirektiv) artikkel 1 (15) bokstav c, som endret artikkel 30 (5) i direktiv 2015/849 (EUs fjerde hvitvaskingsdirektiv), i lys av retten til respekt for privatlivet og beskyttelse av personopplysninger, jf. EU-charteret artikkel 7 og 8. Endringen innebar at opplysningene i registeret over reelle rettighetshavere skulle være tilgjengelige for enhver – ikke bare de som kunne dokumentere en legitim interesse, slik direktivet ga anvisningen på før endringen.

Sakene gjaldt to prejudisielle foreleggelser fra en kretsdomstol i Luxembourg. På tidspunktet for søksmålene var rettstilstanden i Luxembourg at allmennheten kunne få tilgang til opplysninger om den reelle rettighetshavers navn, statsborgerskap, fødselsdato og bopelsland samt arten og omfanget av de aktuelle rettighetene. En registrert enhet eller reell rettighetshaver kunne i ekstraordinære situasjoner anmode at opplysningene skulle begrenses til nasjonale myndigheter.

Begge sakene gjaldt Luxembourg Business Registers' (LBR) nektelse av å forhindre at allmennheten fikk tilgang til informasjon om to selskapers reelle rettighetshavere. Kretsdomstolen i Luxembourg mente utleveringen av opplysninger om de reelle rettighetshaverne kunne innebære et uforholdsmessig inngrep i deres rettigheter etter EU-charteret, og stilte derfor en rekke spørsmål til EU-domstolen. Det første, og eneste, spørsmålet domstolen drøfter, er gyldigheten av bestemmelsen om allmennhetens tilgang til registeret over reelle rettighetshavere.

Som et utgangspunkt for vurderingen av gyldighetsspørsmålet legger domstolen raskt til grunn at allmennhetens tilgang til registeret utgjør et alvorlig inngrep i de grunnleggende rettighetene til respekt for privatlivet og beskyttelse av personopplysninger, nedfelt i henholdsvis artikkel 7 og 8 i EU-charteret. Dette begrunnes med at opplysningene gjør det mulig for et potensielt ubegrenset antall personer å finne ut av blant annet den finansielle situasjonen til rettighetshaveren. De mulige konsekvensene av misbruk av personopplysninger forsterkes videre av at opplysningene ikke bare kan konsulteres, men også beholdes og spres. Rettighetshavernes muligheter til å beskytte seg mot misbruk blir dermed vanskelig – «or even illusory».

Domstolen går så over til å vurdere om dette inngrepet i de grunnleggende rettighetene kan rettferdiggjøres, altså om det overholder legalitetsprinsippet, respekterer det vesentlige innhold i rettighetene, ivaretar en allmenn interesse og er egnet, nødvendig og forholdsmessig.

Domstolen kommer, uten særlig inngående drøftelser, til at inngrepet har hjemmel i nedskreven rett og respekterer det vesentlige innholdet i rettighetene som følger av charterets artikkel 7 og 8. Når det gjelder spørsmålet om inngrepet ivaretar en allmenn interesse, er domstolen klar i sin sak; målet om å forhindre hvitvasking og terrorfinansiering er av slik allmenn interesse at det kan rettferdiggjøre selv alvorlige inngrep i rettighetene til respekt for privatliv og beskyttelse av personopplysninger.

> Endringen innebar at opplysningene i registeret over reelle rettighetshavere skulle være tilgjengelige for enhver – ikke bare de som kunne dokumentere en legitim interesse.

Det som gjenstår for domstolen å vurdere er dermed om inngrepet er egnet, nødvendig og forholdsmessig. Domstolen ser først på kravet til egnethet, og kommer til at allmennhetens tilgang informasjon om reelle rettighetshavere er egnet til å forebygge hvitvasking og terrorfinansiering. Dette begrunnes i at slik tilgang for allmennheten vil bidra til å skape et miljø som i mindre grad kan anvendes til slike formål.

Domstolen går deretter over til å vurdere om inngrepet er strengt nødvendig for å oppnå det angitte formålet. I denne forbindelse hadde Rådet og Kommisjonen anført at fraværet av en ensartet definisjon av begrepet «legitim interesse», som tidligere var et vilkår for å få tilgang til registeret, hadde medført praktiske vanskeligheter og at dette var bakgrunnen for endringen. Dette kunne ikke løses ved å foreslå en ensartet definisjon av begrepet, et-

5 FOR-2021-06-21-2056 § 3-9 fjerde ledd.

tersom begrepet vanskelig kunne defineres juridisk.

Dette er ikke EU-domstolen enig i. Etter domstolens syn kan ikke vanskeligheter ved å oppstille presise betingelser for tilgang til registeret begrunne at offentligheten får tilgang til dette. Domstolen viser deretter til tilfeller hvor det vil foreligge en slik legitim interesse og konkluderer med at inngrepet i charterets artikkel 7 og 8 ikke er begrenset til det strengt nødvendige.

Ikke nok med det, inngrepet var heller ikke forholdsmessig. Domstolen viser her til at formålet med inngrepet riktignok kan begrunne selv alvorlige inngrep i de grunnleggende rettigheter, men at bekjempelse av hvitvasking og terrorfinansiering hovedsakelig påhviler det offentlige, samt enheter som kredittinstitusjoner og finansieringsinstitutter. En regel som gir enhver tilgang til opplysningene, utgjør et mer alvorlig inngrep enn hva de oppnådde fordeler kan rettferdiggjøre.

Domstolen konkluderer etter dette med at direktivbestemmelsen om at registeret skulle være tilgjengelig for allmennheten, er ugyldig.

> En regel som gir enhver tilgang til opplysningene, utgjør et mer alvorlig inngrep enn hva de oppnådde fordeler kan rettferdiggjøre.

4. Konsekvenser av avgjørelsen under norsk rett

Saken vil antakelig få konsekvenser for den norske loven om register over reelle rettighetshavere, som gjennomfører deler av direktiv 2015/849. Bestemmelsen i lovens § 11 om at enhver skal ha tilgang til registrerte opplysninger tilsvarer langt på vei regelen som ble ansett som ugyldig av EU-domstolen. Selv om EU-charteret ikke er en del av EØS-avtalen, kan de grunnleggende rettighetene som ugyldigheten begrunnes i uansett gjenfinnes i norsk rett, både i Grunnlovens kapittel E og Norges internasjonale forpliktelser etter menneskerettsloven, særlig EMK artikkel 8 om retten til respekt for privatliv og familieliv.

> Vi ser ikke bort fra at departementet ville vurdert spørsmålet annerledes etter avklaringen i den nye dommen fra EU-domstolen.

Dessuten kan man spørre, slik EU-domstolen kort er inne på, om regelen også er i strid med GDPR. EU-domstolen viser til at GDPR kommer til anvendelse for behandling av personopplysninger som skjer under hvitvaskingsdirektivet. Kretsdomstolen i Luxembourg stilte bl.a. spørsmål om offentlig tilgang til personopplysningene er i samsvar med grunnprinsippene for behandling av personopplysninger i GDPR artikkel 5, nærmere bestemt bestemmelsene om formålsbegrensning i bokstav b, bestemmelsen om dataminimering i bokstav c, bestemmelsen om integritet og konfidensialitet i bokstav f, og om slik tilgang oppfyller bestemmelsen om personvern som standardinnstilling i artikkel 25(2). EU-domstolen besvarte ikke dette spørsmålet direkte, ut over å slå fast at GDPR kommer til anvendelse.

I lovgivningsprosessen foretok departementet en vurdering av lovligheten av en generell bestemmelse om tilgang til registeret i lys av EMK og personvernforordningen.[6] Departementet konkluderte med at verken EMK eller forordningen innebar skranker for nasjonale myndigheters valg om å gi en slik generell tilgang, og la her vekt på at en slik tolkning «synes dessuten vanskelig å forene med EUs egen regulering på dette området, herunder i revidert fjerde hvitvaskingsdirektiv». Vi ser ikke bort fra at departementet ville vurdert spørsmålet annerledes etter avklaringen i den nye dommen fra EU-domstolen. *LBR*-avgjørelsen foranlediger uansett en ny vurdering av dette spørsmålet.

Basert på dette er det altså grunn til å tro at den norske bestemmelsen om allmennhetens tilgang til opplysninger om reelle rettighetshavere må endres som følge av avgjørelsen fra EU-domstolen, og at tilgangen til opplysninger om reelle rettighetshavere derfor må begrenses til mottakere som har et dokumentert behov for tilgang. Dette vil typisk være offentlige myndigheter og virksomheter som er underlagt hvitvaskingsloven og som har plikt til å innhente opplysninger om reelle rettighetshavere i forbindelse med gjennomføring av kundetiltak.

Øystein Flagstad er advokat og partner i GjessingReimers.

Martha Krogli Brygfjeld er advokatfullmektig i GjessingReimers.

6 Prop. 109 L (2017–2018) side 26 flg.

NIS2-direktivet

Av Kristina Jonsson, Johan Grenefalk og Carl Gleisner

Kristina Jonsson

Johan Grenefalk

Carl Gleisner

Direktivet om åtgärder för en hög gemensam nivå av säkerhet i nätverks- och informationssystem i unionen (NIS) har nyligen ersattas av ett uppdaterat direktiv om åtgärder för en hög gemensam nivå av cybersäkerhet i unionen (NIS2).[1] Det nya direktivet omfattar fler aktörer och ställer högre krav på åtgärder än sin föregångare.

Medlemsstaterna har 21 månader på sig från och med att direktivet även antas av rådet att genomföra direktivet i sin nationella lagstiftning. De nationella lagarna kan därför väntas träda i kraft i slutet av 2024. I den här artikeln sammanfattar vi de mest väsentliga nyheterna i det nya direktivet.[2]

Beroendet av it har blivit synbart

Det är svårt att överdriva vårt samhälles beroende av digital teknik. Som en del i arbetet med att möta hoten som detta medför har EU antagit NIS2. Bakgrunden till regleringen är framför allt tilltagande cyberangrepp mot samhällsviktiga aktörer de senaste åren. Även det försämrade säkerhetspolitiska läget har implikationer för dessa aktörers cybersäkerhet. Vårt beroende av it har blivit synligt för alla.

De mest väsentliga ändringarna

NIS2 kommer att införa ett flertal väsentliga ändringar i det existerande regelverket. Ändringarna syftar till att höja nivån av säkerhet samt att åtgärda problem som identifierats under implementeringen och tillämpningen av NIS. Det finns mycket att säga om NIS2 men följande punkter är de mest väsentliga att känna till.

- **Fler aktörer och verksamheter omfattas.** Det utökade tillämpningsområdet medför att t.ex. telekom, leverantörer av betrodda tjänster, sociala medier och offentlig förvaltning omfattas. I första hand tillämpas direktivet av stora och medelstora aktörer som bedriver verksamhet i vissa utpekade sektorer.[3] Utöver dessa kommer även vissa andra aktörer, oberoende av storlek, att omfattas eftersom deras verksamhet anses ha stor betydelse för samhället. Medlemsstaterna kommer inte längre kunna skräddarsy kraven vilket kommer medföra en mer enhetlig tillämpning inom unionen. Den tidigare uppdelningen mellan samhällsviktiga tjänster och digitala tjänster överges.
- **Mer konsekvent tillämpning.** NIS2 väntas leda till mer konsekvent tillämpning i fråga om vilka aktörer som ska omfattas, säkerhetsåtgärder, rapportering av incidenter, tillsyn, sanktioner och medlemsstaternas kompetens.
- **Högre krav på säkerhetsåtgärder.** Direktivet ställer högre krav på aktörernas säkerhetsåtgärder. I det nuvarande regelverket anges det i korta ordalag att ändamålsenliga och proportionerliga tek-

1 Det nuvarande regelverket infördes genom Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS). Direktivet har genomförts genom lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

2 Artikeln är baserad på den text som antagits av Europaparlamentet (P9_TA(2022)0383). Direktivet publiceras i EU:s officiella tidning först efter att texten även antagits av rådet.

3 Gränsvärdena som ska tillämpas följer av Kommissionens rekommendation (2003/361/EG) om definitionen av mikroföretag samt små och medelstora företag.

niska och organisatoriska åtgärder ska vidtas. I NIS2 ställs däremot krav på att vissa konkreta åtgärder ska vidtas. Åtgärderna avser bl.a. hantering av incidenter, säkerhet i leverantörskedjan, säkerhet vid inköp, utveckling och underhåll samt offentliggörande av sårbarheter.

- **Strömlinjeformad incidentrapportering.** Medlemsstaterna ges mindre utrymme att bestämma hur kravet på rapportering av incidenter ska utformas. Rapporteringen av incidenter ska ske i två steg. En initial rapport ska lämnas 24 timmar efter att aktören fått kännedom om en incident. En slutlig rapport ska lämnas senast efter en månad.
- **Striktare sanktioner.** Direktivet föreskriver en minimilista av sanktioner mot bristande efterlevnad. Sanktionerna omfattar bl.a. bindande instruktioner, föreläggganden att implementera rekommendationer till följd av en oberoende revision och förelägganden att tillse tillräckliga säkerhetsåtgärder för att efterleva kraven i direktivet. Administrativa sanktionsavgifter på upp till det högsta av 10 miljoner euro eller 2 % av aktörens totala globala omsättning kan också dömas ut.
- **Ledningen får ökat ansvar.** Aktörens ledning ska godkänna ledningssystemet, övervaka dess tillämpning, genomgå regelbunden utbildning och kunna hållas personligt ansvariga för bristande efterlevnad.

Fler verksamheter omfattas, en ny indelning

Den tidigare uppdelningen mellan leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster överges. Aktörer kommer i stället klassificeras som antingen essentiella eller viktiga.[4]

Klassificeringen som essentiell eller viktig ska reflektera hur kritisk sektorn är samt aktörens storlek.[5] Kraven på säkerhetsåtgärder och rapportering av incidenter är desamma för såväl essentiella som viktiga aktörer. Reglerna om tillsyn och sanktioner är däremot striktare för de essentiella aktörerna än för de viktiga.

- **Essentiella aktörer.** Det är i första hand aktörer inom de angivna sektorerna vilka även överskrider gränserna för medelstora företag som utgör essentiella aktörer. Vidare omfattas kvalificerade leverantörer av betrodda tjänster, re-

4 Artiklarna 2 och 3.
5 Skäl 15.

gistrarer för toppdomäner och leverantörer av DNS-tjänster oberoende av dessas storlek. Utöver dessa omfattas även offentlig förvaltning med vissa undantag. Slutligen utgör även aktörer som identifierats efter en nationell riskbaserad bedömning, kritiska entiteter enligt direktivet om kritiska entiteters motståndskraft samt tidigare identifierade leverantörer av samhällsviktiga tjänster essentiella aktörer.

- Viktiga aktörer. Aktörer med verksamhet inom de angivna sektorerna men som inte uppfyller kriterierna för att klassificeras som essentiella aktörer utgör viktiga aktörer.

De aktuella sektorerna listas i bilagor till direktivet. Följande övergripande sektorer anges vara **högst kritiska** (bilaga 1).

1. Energi
2. Transport
3. Bank
4. Infrastruktur för finansiella marknaden
5. Hälso- och sjukvård
6. Dricksvatten
7. Vattenrening
8. Digital infrastruktur
9. Offentlig förvaltning
10. Rymd

Andra kritiska sektorer (bilaga 2).

1. Post- och kurirtjänster
2. Avfallshantering
3. Tillverkning och distribution av kemikalier
4. Livsmedelsföretag
5. Producenter av vissa tekniska produkter
6. Leverantörer av vissa digitala tjänster
7. Forskningsorganisationer

Sektorerna i förteckningarna är i sin tur indelade i undersektorer med angivelse av vissa typer av verksamheter.

> NIS2 kommer att införa ett flertal väsentliga ändringar i det existerande regelverket. Ändringarna syftar till att höja nivån av säkerhet samt att åtgärda problem som identifierats under implementeringen och tillämpningen av NIS.

Högre krav på säkerhetsåtgärder

NIS2 kommer att ställa högre krav på säkerhetsåtgärder jämfört med kraven i det nuvarande NIS-regelverket som är allmänt hållna. Enligt det nuvarande regelverket ska aktörerna vidta ”ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder”. Genom NIS2 införs i stället en katalog med konkreta säkerhetsåtgärder.[6]

- Riskanalys och policyer
- Incidenthantering
- Kontinuitet
- Säkerhet i leverantörskedjan
- Säkerhet vid inköp, utveckling och underhåll
- Bedömning av ledningssystemets verkan
- Grundläggande cyberhygien
- Hantering av kryptografi och kryptering
- Personalsäkerhet och kontroll av åtkomst
- Inventering av tillgångar
- Flerfaktorsautentisering
- Säkra verktyg för kommunikation (även vid kris)

Medlemsstaterna ska uppmuntra aktörer att efterleva internationellt eller europeiskt godkända standarder inom området för informationssäkerhet.

6 Artikel 21.

Även aktörer som inte omfattas av det nya regelverket kommer att påverkas i den mån dessa är leverantörer till aktörer som omfattas av den nya regleringen, eftersom deras informationssäkerhet då kommer att bli föremål för granskning.

En mer strömlinjeformad incidentrapportering

Vid utvärderingen av det nuvarande regelverket konstaterades det att medlemsstaterna implementerat kravet på rapportering av incidenter på väsentligt olika sätt. För aktörer som är verksamma i mer än en medlemsstat har skillnaderna i lagstiftningen skapat en extra börda.[7] I NIS2 ges medlemsstaterna därför mindre utrymme att bestämma hur kravet på rapportering av incidenter ska utformas.

Rapporteringen av incidenter ska ske i två steg. En första rapport ska lämnas 24 timmar efter att aktören varseblivit om en incident. En slutlig rapport ska lämnas senast en månad efter samma tidpunkt. Utöver detta specificeras åtskilliga andra detaljer kring förfarandet.[8] Den ökade enhetligheten kommer sannolikt att vara välkommen bland de aktörer som bedriver verksamhet i flera medlemsstater och behöver rapportera incidenter.

> Även aktörer som inte omfattas av det nya regelverket kommer att påverkas i den mån dessa är leverantörer till aktörer som omfattas av den nya regleringen, eftersom deras informationssäkerhet då kommer att bli föremål för granskning.

7 The NIS2 Directive, European Parliamentary Research Service Briefing, PE 689.333, June 2022.

8 Artikel 23.

Ledningen får ökat ansvar

En väsentlig förändring i NIS2 är att ledningarna för de omfattade aktörerna får ett klart större ansvar. De åläggs att godkänna säkerhetsåtgärderna som krävs enligt regelverket samt att övervaka implementeringen av dessa. Vidare ska de kunna hållas personligen ansvariga för aktörens bristande efterlevnad.[9] Direktivet harmoniserar inte formen för ansvaret. Det är därför upp till medlemsstaterna att välja huruvida sanktionen är straffrättslig eller administrativ.[10]

Förändringen avseende just ledningens ansvar är sannolikt av stor betydelse för informationssäkerheten inom unionen. Det kan givetvis diskuteras huruvida ”piskan eller moroten” är det lämpligaste verktyget för att uppnå ”egentlig” säkerhet och inte enbart formell efterlevnad. Oavsett hur det förhåller sig med det kan reglerna om ansvar förväntas att åtminstone föra frågan om informationssäkerhet ännu högre upp på agendan.

Ledningen har en särskilt betydelsefull roll när det gäller informationssäkerhet. Ingen organisation kan komma vidare i sina ansträng-

> ”Direktivet harmoniserar inte formen för ansvaret. Det är därför upp till medlemsstaterna att välja huruvida sanktionen är straffrättslig eller administrativ.

ningar utan att ledningen ger den sitt stöd. Samtidigt gäller givetvis det omvända. Ett engagemang från ledningen kan dock ofta frigöra drivkrafter inom organisationer som vill bidra till ett mer försvarbart förhållningssätt till det som hotar informationssäkerheten.

Beslut om en organisations aptit och tolerans för risker när det gäller informationssäkerhet är självklart en fråga för ledningen, inte enbart för it-avdelningen. Den omständigheten att ledningar i många organisationer engagerar sig först sedan de själva har en insats i leken kanske är av mindre betydelse så länge arbetet påbörjas över huvud taget.

Medskick

Förändringarna i direktivet förväntas kunna implementeras i nationell lagstiftning **i slutet av 2024**. Den som tror sig kunna omfattas av det nya regelverket får med sig följande medskick.

- **Omfattas vi?** Kontrollera i första hand huruvida er organisation bedriver verksamhet inom någon av de angivna sektorerna. Bedöm även om er organisations överskrider gränsvärdena för medelstora företag. Kom dock ihåg att vissa aktörer omfattas oberoende av storlek. Ta hjälp om ni är osäkra.
- Vad behöver vi göra? Om ni omfattas, börja planera tidigt för att lyckas uppnå efterlevnad till en försvarbar kostnad.
  - Inled samtal i ledningen för att föra frågan på agendan så tidigt som möjligt.
  - Avsätt tid och resurser för att planera arbetet och identifiera behov av resurser.
  - Planera budget för att ta höjd för implementering av åtgärder och en eventuell ny organisation.
  - Påbörja rekrytering av kompetenta medarbetare och konsulter.
  - Utvärdera risker och åtgärder löpande.

Kristina Jonsson, advokat och delägare, Johan Grenefalk, advokat och delägare samt Carl Gleisner, biträdande jurist, är verksamma vid Wesslau Söderqvist Advokatbyrå i Stockholm

9 Artikel 20.1 och artikel 32.6.
10 Skäl 131-132.

Åpne algoritmer

Av Thale Cecilia Gautier Gjerdsbakk

Dette er den andre i en serie på tre artikler om kunstig intelligens og hvordan det utfordrer rettferdighets- og åpenhetsprinsippet i personvernforordningen (pvf.) art. 5 nr. 1 (a).[1] Den første artikkelen ble publisert i Lov & Datas 3. utgave 2022 og den neste publiseres i 1. utgave 2023.

Dagens teknologi gjør det mulig å samle inn, dele og sammenstille store mengder personopplysninger og andre data.[2] Denne muligheten har gitt grobunn for utviklingen av kunstig intelligens (KI) på et nytt nivå. KI har et vidt anvendelsesområde; det kan bidra til alt fra å effektivisere byråkratiske prosesser til å hjelpe leger med å forutsi faren for hjertesvikt. KI har åpenbare fordeler, og brukes stadig mer.[3] For eksempel blir KI stadig oftere benyttet til beslutningsstøtte, nettopp av effektiviseringshensyn. Med beslutningsstøtte mener jeg tilfeller der KI brukes som ledd i å fatte en beslutning, men ikke helautomatiserte

Thale Cecilia Gautier Gjerdsbakk

avgjørelser etter pvf. art. 22 nr. 1. Det er KI brukt som beslutningsstøtte artikkelserien tar for seg.

Bruken av KI innebærer imidlertid utfordringer for personvernet. Manglende transparens (åpenhet) og urettferdighet trekkes gjennomgående frem som problematiske forhold ved KI. Denne artikkelen fokuserer på åpenhetsprinsippet i pvf. art. 5 nr. 1 (a) og problemstillinger knyttet til overholdelsen av åpenhetsprinsippet ved bruk av KI som beslutningsstøtte.[4]

1. Åpenhetsprinsippets formål

Et av de overordnede målene med personvernforordningen er å gi enkeltpersoner kontroll over egne opplysninger. En forutsetning for kontroll er at man vet hva som skjer med egne opplysninger – det vil si åpenhet. Det er derfor på sin plass at åpenhetsprinsippet er plassert i artikkelen som gjerne kalles for personvernets grunnlov: personvernforordningens grunnleggende prinsipper i art. 5. Etter art. 5 nr. 1 (a) skal personopplysninger «behandles på en (…) åpen måte». Åpenhet er en forutsetning for at den registrerte skal kunne vurdere om behandlingen tilfredsstiller personvernforordningens krav og er avgjørende for å skape tillit til behandlingsprosessen.

2. Retten til åpen behandling av personopplysninger

Åpenhetsprinsippet er utdypet med mer konkrete krav til informasjonen som skal gis til de registrerte i pvf. art. 12-15. Kravet til åpenhet er todelt. For det første forutsetter åpenhet at behandlingsansvarlige gir en bestemt *type informasjon* om behandlingen av personopplysninger, jf. pvf. art 13, 14 og 15 (innholdskrav).[5] For det andre må informasjonen være *forståelig* for den registrerte, jf. pvf. art. 12 (formkrav).[6] Det er den behandlingsansvarliges ansvar at informasjonen er forståelig og tilgjengelig for den registrerte, jf. pvf. art. 5 nr. 2.

Kravene i art. 12-15 er minimumskrav. Det grunnleggende kravet om åpenhet i art. 5 nr. 1 (a) kan nemlig innebære at behandlingsansvarliges plikt til å sikre åpenhet går lenger enn kun oppfyllelse av art. 12-15. Sett sammen med ansvarlighetsprinsippet i art. 5 nr. 2, innebærer åpenhetsprinsippet at behandlingsansvarlig må vurdere hvilke åpenhetstiltak som er nødvendige og forholdsmessige for at den registrerte skal ha mulighet til å ivareta egne rettigheter og interesser. Også Datatilsynet forstår åpenhetsprinsippet slik.[7] Eksempelvis kan åpen-

1 Europaparlamentets og Rådets forordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF [personvernforordningen/pvf.].

2 Personvernforordnongens fortalepunkt 6.

3 NOU 2020:11 Den tredje statsmakt – Domstolene i endring, s. 254.

4 Personvernforordningen art. 5 nr. 1 (a).

5 Personvernforordningen art. 13 og 14.

6 Personvernforordningen art. 12 nr. 1.

7 Rapport AVT, februar 2022, s. 16, Datatilsynets sak 20/03087, saksdokument 14, 07.08.2020.

> Sett sammen med ansvarlighetsprinsippet i art. 5 nr. 2, innebærer åpenhetsprinsippet at behandlingsansvarlig må vurdere hvilke åpenhetstiltak som er nødvendige og forholdsmessige for at den registrerte skal ha mulighet til å ivareta egne rettigheter og interesser.

hetsprinsippet tilsi at behandlingsansvarlig må gi mer utdypende informasjon enn det art. 13-15 krever.

Ettersom personvernforordningen er teknologinøytral, omfatter kravene i forordningen også behandling av personopplysninger ved hjelp av ny teknologi, slik som KI. Ved bruk av KI som beslutningsstøtte må den behandlingsansvarlige altså tilfredsstille både form- og innholdskravet som åpenhetsprinsippet innebærer. I personvernforordningen fortalepunkt 58 understrekes det at teknologisk kompleksitet gjør åpenhet ekstra viktig.

Som med de fleste kravene i personvernforordningen, er det ikke mulig å lage en standardisert liste med oppfyllelseskriterier som gjelder for alle behandlingstilfeller. Det samme gjelder når åpenhetsprinsippet skal forstås ved bruk av KI som beslutningsstøtte. Likevel er det mulig å identifisere noen retningslinjer og problematiske områder man må være ekstra oppmerksom på i forsøket på å være åpen rundt bruken av KI.

3. Krav til forståelighet

Etter pvf. art. 12 nr. 1 skal behandlingsansvarlige sørge for at informasjonen er forståelig for den registrerte gjennom et klart og enkelt språk, slik at det blir åpenhet rundt behandlingen. Etter art. 12 nr. 2 skal behandlingsansvarlige, gjennom slik åpenhet, legge til rette for at de registrerte kan utøve de rettighetene de har etter personvernforordningen.

For å oppfylle kravene i art. 12 nr. 1 og 2 er formidlingen av informasjon fra behandlingsansvarlig til den registrerte særlig viktig. Det hjelper ikke å ha gitt informasjon, dersom de registrerte ikke har forstått innholdet. Dette samsvarer med formålet for åpenhetsprinsippet, nemlig å gi de registrerte kontroll og valgfrihet når det kommer til behandling av deres personopplysninger.

Skal den behandlingsansvarlige sikre at de registrerte forstår informasjonen, forutsetter det at behandlingsansvarlig har kunnskap om de registrerte, og kan tilpasse informasjonen etter mottakernes kunnskapsnivå. Personvernrådets forgjenger, Artikkel 29-gruppen, sin rettesnor var at den gjennomsnittlige registrerte må forstå informasjonen.[8] Ved bruk av KI kan mottakernes kunnskapsnivå generelt antas å være relativt lavt, gitt KIs tekniske kompleksitet og at det for de fleste personer er ny teknologi. Dette skaper utfordringer for muligheten til å forklare bruken av personopplysninger enkelt og forståelig. Behandlingsansvarlige må i det minste unngå å bruke for tekniske og ukjente termer, som det er mange av når man snakker om KI.

Pvf. fortalepunkt 60 og 71 presiserer at særlige omstendigheter rundt og sammenhengen behandlingen skjer i skal tas hensyn til ved informasjon til den registrerte. For eksempel er det naturlig å stille strengere krav jo større personverninngrep behandlingen utgjør, desto skjevere maktforholdet mellom registrert og behandlingsansvarlig er og jo vanskeligere det er å forstå behandlingsmetoden. En særlig omstendighet ved bruk av KI er teknologien er såpass nå at behandlingsmetoden er lite kjent. Behandlingsansvarlige må derfor vurdere å gi grunnleggende informasjon om KI som behandlingsverktøy for å øke forståeligheten for den registrerte.

Maskinlæring åpner for å kunne gi forklaringer av den underliggende logikken basert på avanserte matematiske og statistiske modeller. Selv om slik informasjon egner seg til å gi helt korrekt og presis informasjon, vil ikke matematiske forklaringer tilfredsstille forståelighetskravet i pvf. art. 12 nr. 1 når selv programvareutviklere kan ha problemer med å forstå disse. Behandlingsansvarlige må derfor balansere retten til presis informasjon mot muligheten til å forstå informasjonen.

4. Innholdskravet

Pvf. art. 13 og 14 lister opp konkret informasjon som den registrerte har krav på ved innsamling av personopplysninger. Pvf. art. 15 gir den registrerte rett til innsyn i egne opplysninger. Art. 13-15 innebærer at den registrerte blant annet har krav på å vite kategorier av personopplysninger som samles inn, formålet ved behandlingen og hvordan behandlingsansvarlige kan kontaktes.

I min forrige artikkel påpekte jeg at KI ofte er så komplekst sammensatt at mennesker ikke klarer å forstå hvilke sammenhenger og tilpasninger algoritmen gjør.[9] Ugjennomtrengeligheten gjør det umulig selv for utviklerne av KI-systemene å forklare hvorfor systemene løser oppgavene som de gjør.[10] Vektingen og justeringen algoritmen gjør i sine skjulte lag medfører at beslutningsprosessen til KI-en er like ugjennomsiktig som en sort boks. Dette kalles det 'sorte boks' problem', og

8 Artikkel 29-gruppen *Guidelines on transparency under Regulation 2016/679*, avsnitt 9. Personvernrådet (EDPB) revidert og tilsluttet Artikkel 29-gruppens anbefalinger 11.04.2018.

9 NOU 2020:11 s. 254.

10 Datatilsynet (2018), s. 12.

kan gjøre det utfordrende å oppfylle personvernforordningens krav til åpenhet.

Men er det egentlig nødvendig å kunne forklare den underliggende logikken til KI-en for å tilfredsstille kravet til åpenhet?

Ved utelukkende automatiserte avgjørelser, herunder profilering, som har rettsvirkning for eller på tilsvarende måte betydelig påvirker vedkommende etter pvf. art. 22 nr. 1 og 4, stilles det krav om forklarbarhet i pvf. art. 13 nr. 2 (f), 14 nr. 2 (g) og 15 nr. 1 (h). Ordlyden i de tre artiklene er lik: Behandlingsansvarlig må gi «relevant informasjon om den underliggende logikken samt om betydningen og de forventede konsekvensene av en slik behandling for den registrerte». I tilfeller der KI benyttes som beslutnings*støtte*, vil ikke de registrerte være gjenstand for en helautomatisert avgjørelse, etter art. 22 nr. 1 og 4. Dette er fordi resultatet KI-en presenterer kun vil være ett av flere elementer i en vurdering som gjøres av et menneske.

Kravet til forklarbarhet i art. 13-15 gjelder «i det minste» tilfeller etter art. 22 nr. 1 og 4. Det vil si at det også kan stilles krav til forklarbarhet i andre tilfeller. Hvorvidt kravet til åpenhet også innebærer et krav om forklarbarhet, må derfor vurderes i hvert konkrete tilfelle. Vurderingen må ses sammen med behandlingsansvarliges ansvar for å vurdere hvilke åpenhetstiltak som er nødvendige og forholdsmessige for at de registrerte skal kunne ivareta egne rettigheter og interesser. Ved spørsmålet om det kan stilles krav til forklarbarhet er det spesielt interessant å se om forklarbarhet er nødvendig for å sikre en rettferdig og åpen behandling.[11]

Spørsmålet om åpenhet innebar forklarbarhet ble drøftet i de tre første prosjektene i Datatilsynets sandkasse for KI. Secure Practice, som ønsket å benytte KI for profilering av arbeidstakere i forbindelse med sikkerhetsopplæring, konkluderte med at det ikke var et forklarbarhetskrav. Likevel anbefalte sandkassen å gi informasjon om hvordan verktøyet fungerte, fordi det kunne bidra til å skape tillitt. Hverken NAV, som ønsket å bruke KI som beslutningsstøtte når saksbehandlere skal vurdere om de skal innkalle sykemeldte til et dialogmøte, eller AVT, som ønsket å bruke KI som læringsstøtte i skolen konkluderer på om det i deres tilfeller er et rettslig krav til å forklare den underliggende logikken til KI-en. Likevel presenterer både AVT og NAV flere argumenter for hvorfor de likevel burde forklare modellens underliggende logikk. Argumenter som tillit til KI-en, asymmetriske maktforhold, krav til ansvarlighet og ønske om etisk og ansvarlig KI er trukket frem. Uten at rapportene har noen stor rettskildemessig vekt, tyder de på at det praktiseres en relativt høy terskel for når åpenhetskravet tilsier et krav om forklarbarhet utenfor pvf. art. 22 nr. 1-tilfellene, og at det er andre hensyn og faktorer enn rettslige krav som tilsier at prosjektene burde sikre forklarbarhet. Med så lite avklarte, og tilsynelatende snevert praktiserte juridiske krav til forklarbarhet, overlates et større etisk ansvar for å ivareta de registrertes interesser og rettigheter til den behandlingsansvarlige.

> Hvorvidt kravet til åpenhet også innebærer et krav om forklarbarhet, må derfor vurderes i hvert konkrete tilfelle.

5. Den sorte boks' problem

Betyr et snevert rettslig krav til forklarbarhet at den sorte boks' problem i de fleste tilfeller ikke er et problem for oppfyllelsen av åpenhetsprinsippet i personvernforordningen, så lenge man bruker KI kun som beslutningsstøtte? Selv om reguleringen i personvernforordningen kan tyde på dette, er det flere problematiske forhold ved den sorte boksen som tilsier at det burde kreves en viss grad av forklarbarhet også for KI benyttet til beslutnings*støtte*.

Personvernforordningens metode er å la det være opp til hver enkelt behandler av personopplysninger å vurdere om bruken av KI tilfredsstiller forordningens krav. Når behandlingsansvarlige skal vurdere om åpenhetsprinsippet innebærer et krav til forklarbarhet kan det fort bli fristende å konkludere med at det ikke er et krav til å forklare KI-ens underliggende logikk og vekting, ettersom det kan være svært vanskelig å forklare.

I IB-saken hadde fraværet av forklaring uheldige konsekvenser. International Baccalaureate Organization (IBO) anvendte i denne saken en «modell» for å fastsette elevenes standpunktkarakterer på grunn av manglende eksamensavvikling som følge av Covid-19 pandemien. Flere elever fikk store og uventede avvik mellom antatt og endelig karakter. IBO opplyste hverken i forkant av karaktersettingen eller etter anmodning fra Datatilsynet om hvordan de ulike faktorene var vektet eller de endelige karakterene ble regnet ut.[12] I sitt varslede vedtak konkluderer Datatilsynet med at IBO ikke overholdt åpenhetsprinsippet, da logikken bak modellen og vektingen modellen foretok hverken var forklart for elevene eller offentliggjort slik

11 Art. 13 nr. 2 første setning.

12 Det fremstår derfor også noe uklart om elevene var utsatt for en helautomatisert avgjørelse. Datatilsynet nevner ikke art. 22 nr. 1 og 4 og kravene til forklarbarhet i art. 13-15, men konkluderer på bakgrunn av åpenhetsprinsippet i art. 5 nr. 1 (a). Saken er derfor egnet til å si noe om Datatilsynets praktisering og tolkning av når åpenhetsprinsippets innebærer et krav til forklarbarhet.

at den kunne etterprøves og utfordres.[13]

Det er usikkert om manglende evne til å forklare modellen var bakgrunnen for manglende forklaring fra IBO. Saken viser uansett at det er uheldig om behandlingsansvarlig ikke må informere om den underliggende logikken og vektingen. Med uklare juridiske krav til forklarbarhet blir samfunnet i større grad avhengig av årvåkne registrerte med ressurser til å håndheve sine rettigheter for å sikre overholdelse av personvernforordningens prinsipper. Dette kommer spesielt på spissen der KI benyttes på eller går spesielt ut over en ressurssvak gruppe. Jo mer åpen behandlingsansvarlig er, desto enklere blir det for offentligheten å kontrollere KI-en og overholdelsen av personvernprinsippene og de registrertes rettigheter og interesser. Da er man heller ikke så avhengig av at de registrerte reagerer på åpenbart urettferdige resultater for å avdekke eventuelle skjevheter, som i IB-saken.

Dessuten kan urettferdige resultater være skjult i den forstand at de ikke er mulig å oppdage i enkeltsaker. Man er da avhengig av å kunne se KI-ens underliggende logikk og vekting for å oppdage systematiske feil. La oss se på eksempelet fra forrige artikkel. Der ble KI trent på historisk data for å hjelpe dommere med å avgjøre fengslingskjennelser. KI-en kom frem til at brillebruk, ektefellerelasjon og arbeidsledighet spilte inn på om man burde fengsles eller ikke. Brillebruk er en irrelevant faktor i spørsmålet om du burde fengsles eller ikke. Det er åpenbart urettferdig at manglende brillebruk skal tippe vektskålen i retning fengsling. Med mindre du får fremlagt hvilke faktorer KI-en har vektlagt, ville du neppe avdekket at KI-en vektla manglende brillebruk. Uten forklaring blir det vanskelig for de registrerte å avdekke og reagere på skjevheter. Manglende forklaring og åpenhet kan altså medføre at man ikke får avdekket brudd på andre prinsipper, som rettferdighet. Dersom behandlingsansvarlig må forklare KI-ens underliggende logikk og vekting, kan urettferdigheter avverges før de har skjedd og registrerte kan vurdere om deres egne rettigheter og interesser er ivaretatt.

Som nevnt er åpenhet avgjørende for at den registrerte skal kunne ivareta sine rettigheter. Pvf. fortalepunkt 60 fremhever at de registrerte bør informeres om det skjer profilering og konsekvensene av dette. Av Artikkel 29-gruppens veiledning om automatiserte avgjørelser og profilering fremgår det at det er «good practice» å følge informasjonskravene i pvf. art. 13 nr. 2 (f) og 14 nr. 2 (g) ved all form for profilering.[14] De fleste typer KI som brukes på personopplysninger innebærer pro-

13 Sak 20/03087 (IB-saken), saksdokument 14, 07.08.2020. Datatilsynet fattet aldri endelig vedtak i saken på grunn av manglende jurisdiksjon, se *https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2021/lukker-ib-saken/*.

14 Artikkel 29-gruppen, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, s. 25. Personvernrådet (EDPB) revidert og tilsluttet Artikkel 29-gruppens anbefalinger 06.02.2018.

filering, og burde innrette seg etter veilederen og fortalen.

I lys av risikoen manglende forklaring innebærer for de registrerte, kan det stilles spørsmål ved om det er tilstrekkelig at forklaring av underliggende logikk og vekting ved bruk av KI som beslutningsstøtte er god praksis, og ikke et rettslig krav. Spesielt sett i lys av åpenhet som en forutsetning for ivaretakelsen av den registrertes rettigheter og øvrige grunnleggende prinsipper i art. 5 nr. 1 (a).

Tolker man åpenhetsprinsippet i art. 5 nr. 1 (a) i lys av risikoen for de registrertes interesser og rettigheter som skissert over, mener jeg at utgangspunktet burde være en plikt til forklaring av KI-ens underliggende logikk. Dette fordi en forklaring av underliggende logikk ofte er nødvendig for at de registrerte skal kunne ivareta egne rettigheter og interesser. Så kan det heller gjøres unntak for tilfeller der det ikke er forholdsmessig å pålegge behandlingsansvarlig forklaringsplikt, for eksempel der behandlingen vil ha liten innvirkning på den registrerte. Hvor grundig forklaring som kreves, må også tilpasses forholdsmessig etter risikoen det enkelte behandlingstilfellet innebærer.

6. Oppsummering/Konklusjon

Du vet nå at for å benytte KI til behandling av personopplysninger, må du være åpen om behandlingen. Dette innebærer at informasjonen må være forståelig, og at du må ta utgangspunkt i mottakergruppen når du vurderer om du oppfyller

> I lys av risikoen manglende forklaring innebærer for de registrerte, kan det stilles spørsmål ved om det er tilstrekkelig at forklaring av underliggende logikk og vekting ved bruk av KI som beslutningsstøtte er god praksis, og ikke et rettslig krav.

åpenhetsprinsippet. Når KI er en såpass ny og ukjent teknologi, skaper kravet generelt vanskeligheter, samtidig som det gjør åpenhet spesielt viktig.

Videre vet du at hver behandlingsansvarlig selv må vurdere for hvert konkrete tilfelle hvilke andre åpenhetstiltak enn de som følger av pvf. art. 12-15 som må iverksettes. Om behandlingsansvarlige ved bruk av KI som beslutningsstøtte må informere om underliggende logikk og vekting må derfor vurderes konkret for hvert tilfelle. Dersom terskelen for når forklarbarhet er et rettslig krav blir for høy, vil det ha uheldige konsekvenser for rettferdighetsprinsippet og registrertes adgang til å håndheve sine rettigheter. Ved spørsmål om åpenhetsprinsippet stiller krav til forklarbarhet, burde man hensynta risikoen den registrerte utsettes for ved å ikke gi forklaring. Risikoen for den registrertes rettigheter og interesser ved ikke å gi forklaring burde etter min mening tilsi at behandlingsansvarlig som utgangspunkt har plikt til å forklare KI-ens underliggende logikk og vekting. Eventuelle unntak må avgjøres ut ifra en forholdsmessighetsvurdering av de registrertes personvern og behandlingsansvarliges interesser.

> Risikoen for den registrertes rettigheter og interesser ved ikke å gi forklaring burde etter min mening tilsi at behandlingsansvarlig som utgangspunkt har plikt til å forklare KI-ens underliggende logikk og vekting.

En konsekvens av manglende forklaring av underliggende logikk og vekting er at det blir vanskelig å avdekke brudd på retten til rettferdig behandling av personopplysninger. Neste artikkel vil ta for seg rettferdighetsprinsippet og de utfordringene som oppstår når prinsippet skal anvendes på KI som beslutningsstøtte.

Thale Cecilia Gautier Gjerdsbakk er advokatfullmektig med spesialisering innen personvern, teknologi og KI i advokatfirmaet BULL. tcgg@bull.no

Innleide konsulenter – Når skal det inngås databehandleravtale?

Av Fride Hedin, Line Haukalid og Rune Opdahl

Fride Hedin

Line Haukalid

Rune Opdahl

I et konsulentoppdrag vil konsulenter kunne få tilgang til, eller for øvrig måtte behandle, personopplysninger. Da oppstår spørsmålet om hvilken personvernrettslig rolle konsulenten har.

I denne artikkelen vil vi se nærmere på konsulenters rolle under GDPR, med fokus på spørsmålet om konsulenten skal anses som databehandler.

Når foreligger det et databehandleroppdrag

Det foreligger et databehandleroppdrag når en behandlingsansvarlig engasjerer en databehandler til å behandle personopplysninger på den behandlingsansvarliges vegne. Spørsmålet om et konsulentoppdrag innebærer et databehandleroppdrag vil bero på konsulentoppdragets karakter. Nedenfor vil vi illustrere dette ved å se på tre typetilfeller.

Når vi i det følgende refererer til «konsulenten», siktes det til selskapet konsulenten opptrer på vegne av, enten dette er et enkeltpersonforetak eller et konsulentselskap.

Typetilfelle 1: Konsulenten arbeider «in-house» hos kunden

I noen konsulentoppdrag arbeider konsulenten tilnærmet likt som kundens egne ansatte. Konsulenten vil typisk få utdelt PC og en e-postadresse hos kunden, og arbeider utelukkende eller primært i kundens systemer (enten i kundens lokaler, via fjerntilgang, eller en kombinasjon). Konsulenten vil ved utførelse av oppdraget være underlagt kundens retningslinjer, prosedyrer og instruksjonsmyndighet.

> Spørsmålet om et konsulentoppdrag innebærer et databehandleroppdrag vil bero på konsulentoppdragets karakter.

EDPB har presisert at ansatte og andre personer som er underlagt den behandlingsansvarliges myndighet, enten de er faste eller midlertidige ansatte, ikke skal anses som databehandlere. Begrunnelsen er at de ikke er en separat enhet i relasjon til den behandlingsansvarlige, men i stedet behandler personopplysninger som en del av den behandlingsansvarliges virksomhet.[1] I henhold til GDPR artikkel 29 er personer «som handler for den behandlingsansvarlige» også bundet av den behandlingsansvarliges instruks når de behandler personopplysninger. Det er derfor verken nødvendig eller hensiktsmessig å inngå en databehandleravtale i tillegg til disse instruksene.

> EDPB har presisert at ansatte og andre personer som er underlagt den behandlingsansvarliges myndighet, enten de er faste eller midlertidige ansatte, ikke skal anses som databehandlere.

1 EDPB's Guidelines 07/2020, avsnitt 78 på side 26.

Om innleide konsulenter skal likestilles med kundens personale når det gjelder behandling av personopplysninger, må vurderes konkret fra sak til sak. Der konsulentoppdraget likner et ansettelsesforhold som beskrevet ovenfor, taler gode grunner for å anse konsulenten som en del av kundens virksomhet hva gjelder konsulentens behandling av personopplysninger. Dette gjelder uavhengig av om konsulenten er ansatt hos et annet selskap eller utfører oppdraget fra et enkeltpersonforetak.

Legger man en slik tilnærming til grunn, skal det ikke inngås en databehandleravtale mellom kunden og konsulenten. De typiske databehandlerforpliktelsene som oppstilles i en databehandleravtale vil heller ikke treffe på et slikt konsulentforhold. Eksempelvis vil det være lite treffende å pålegge konsulenten plikt til å implementere egnede tekniske og organisatoriske tiltak når kundens eksisterende tiltak allerede gjelder for konsulenten og utstyret konsulenten arbeider på

Det danske datatilsynet synes å ha en noe annen tilnærming. I sin veileder legger det danske datatilsynet til grunn at en konsulent i utgangspunktet ikke behandler personopplysninger som en del av den behandlingsansvarliges virksomhet, slik at spørsmålet blir om konsulenten opptrer som en databehandler.[2] Begrunnelsen som gis er at den behandlingsansvarlige ikke har samme rettigheter og plikter overfor en konsulent som overfor egne ansatte. For det danske datatilsynet er arbeidsrettslige betraktninger tilsynelatende utslagsgivende.

Vi mener at EDPBs tilnærming fremstår riktigere. De åpner for en bredere tilnærming, og en tilnærming som er mer forankret i reelle enn formelle omstendigheter.

Typetilfelle 2: Konsulenten har omfattende eller systematisk tilgang til kundens personopplysninger

Det foreligger et databehandleroppdrag i GDPRs forstand når et konsulentoppdrag helt eller delvis går ut på å behandle personopplysninger på vegne av kunden. Datatilsynet legger til grunn at dersom man gir en konsulent tilgang til personopplysninger i stor eller systematisk grad består oppdraget i det minste delvis i å behandle personopplysninger, selv om dette ikke nødvendigvis er hovedoppdraget.[3]

Datatilsynet nevner som eksempel at kunden engasjerer en konsulent for å yte generell support til ansatte i kundens IT-systemer. Behandling av personopplysninger er ikke hovedformålet med konsulentoppdraget, men konsulenten må ha kontinuerlig fjerntilgang til kundens systemer og personopplysninger som ligger der for å utføre oppdraget. Ifølge Datatilsynet foreligger det her trolig et databehandleroppdrag.

Det danske datatilsynet nevner som et annet eksempel at konsulenten skal gjennomgå kundens saksbehandling for å avdekke eventuelle saksbehandlingsfeil. Som en del av oppdraget, må konsulenten gjennomgå og søke i personopplysninger på vegne av kunden.[4] Ifølge det danske datatilsynet vil konsulenten her opptre som databehandler i relasjon til kunden.

Typetilfelle 3: Konsulenten skal i utgangspunktet ikke behandle personopplysninger

Hvis kunden ikke har instruert konsulenten om å behandle personopplysninger, verken helt eller delvis, foreligger det ikke et databehandleroppdrag. Et eksempel fra det danske datatilsynet er at konsulenten skal analysere kundens arbeidsstrømmer for å effektivisere kundens saksbehandling. Det inngår

2 Vejledende principper: Dataansvar for vikarer og konsulenter

3 Datatilsynets veileder; Behandlingsansvarlig og databehandler

4 Vejledende principper: Dataansvar for vikarer og konsulenter

ikke i oppdraget å behandle personopplysninger på vegne av kunden.[5]

Et annet eksempel fra det danske datatilsynet er at en IT-konsulent hyres inn for å søke etter og rette feil i kundens programvare. Retting skjer ved at konsulenten gjør endring i programvarens kildekode. Heller ikke i dette eksempelet er det en del av oppdraget å behandle personopplysninger.

I begge eksemplene vil konsulenten imidlertid kunne få utilsiktet tilgang til personopplysninger som finnes i kundens systemer, for eksempel i forbindelse med feilsøkingen. Spørsmålet er om konsulenten av den grunn likevel må anses som en databehandler. Det danske datatilsynet sier ikke noe om dette i sin veileder.

EDPBs veileder berører dette spørsmålet i et eksempel om en IT-konsulent som skal fikse en programvarefeil. Det forutsettes i eksempelet at konsulenten ikke er engasjert for å behandle personopplysninger, og at en eventuell tilgang til personopplysninger vil være utilsiktet og derfor svært begrenset i praksis. På denne bakgrunn legger EDPB til grunn at IT-konsulenten ikke er databehandler (og heller ikke behandlingsansvarlig) for personopplysningene konsulenten eventuelt får tilgang til. Fra dette eksempelet kan det utledes to vilkår for at slike konsulentoppdrag ikke utgjør et databehandleroppdrag i GDPRs forstand: i) formålet med tjenesten er ikke å behandle personopplysninger, og ii) en eventuell tilgang til personopplysninger er utilsiktet og svært begrenset i omfang.[6]

I lys av dette, må det vurderes konkret om konsulentens eventuelle tilgang til personopplysninger er av en slik karakter at det foreligger et databehandleroppdrag, eller kun et leverandøroppdrag. Uansett må kunden sørge for tilstrekkelig sikkerhet for personopplysningene i tråd med GDPR artikkel 32, herunder iverksette tiltak for å hindre uautorisert behandling av personopplysninger.[7]

> Vi mener at EDPBs tilnærming fremstår riktigere. De åpner for en bredere tilnærming, og en tilnærming som er mer forankret i reelle enn formelle omstendigheter.

Avtaleregulering der konsulenten ikke er databehandler

Selv om det ikke skal inngås databehandleravtale, er det viktig at kunden sørger for å ha kontroll på konsulentens potensielle befatning med personopplysninger i kundens systemer. Dette gjelder både der konsulenten anses som en del av kundens virksomhet (typetilfelle 1) og i tilfeller hvor konsulenten i utgangspunktet ikke skal behandle personopplysninger (typetilfelle 3). Eksempelvis bør kunden i oppdragsavtalen stille krav om god behandling av personopplysninger der dette er hensiktsmessig, innta passende taushetspliktsbestemmelser, samt kommunisere interne retningslinjer om behandling av personopplysninger i den grad det er relevant. For å sikre notoritet om vurderinger knyttet til partenes personvernrettslige roller og ansvar, kan det også være fornuftig å avtaleregulere at konsulenten ikke skal anses som databehandler i relasjon til kunden, med en kort begrunnelse.

Særlig om bruk av konsulenter i land utenfor EØS

GDPR stiller særskilte krav til overføring av personopplysninger til land utenfor EØS (tredjeland). Der man engasjerer en konsulent som skal behandle personopplysninger fra et tredjeland, må man derfor sørge for at behandlingen skjer i samsvar med kravene i GDPR kapittel 5. Dette inkluderer blant annet å få på plass gyldig overføringsgrunnlag (typisk EUs standardklausuler), samt gjennomføre og dokumentere tilleggsvurderingene som følger av Schrems II-avgjørelsen og EDPBs etterfølgende veiledere.

> Vi erfarer at mange uten nærmere overveielser har en oppfatning om at konsulenter er databehandlere og derfor inngår en databehandleravtale som ledd i oppdragsavtalen, eller at man gjør det for å være på «den sikre siden».

En forutsetning for at det foreligger en «overføring» i GDPRs forstand, er at mottaker opptrer som selvstendig behandlingsansvarlig eller databehandler.[8] Det betyr at hvis konsulenten befinner seg i et tredjeland når den behandler personopplysninger, men ikke gjør dette som en databehandler eller behandlingsansvarlig, vil det ikke foreligge en overføring i GDPRs forstand. I så fall utløses ikke overføringsreglene i GDPR kapittel 5.

5 Vejledende principper: Dataansvar for vikarer og konsulenter

6 EDPB's Guidelines 07/2020, avsnitt 83 på side 28.

7 EDPB's Guidelines 07/2020, avsnitt 83 på side 28.

8 EDPB Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.

Det forhold at det skjer en *de facto* overføring til et tredjeland, fordi konsulenten i tredjelandet får tilsendt personopplysninger eller får tilgang til personopplysninger, bør likevel hensyntas i etterlevelsen av de øvrige forpliktelsene i GDPR, herunder informasjonssikkerhetskravene i GDPR artikkel 32.

Oppsummering

Spørsmålet om konsulenter er databehandlere beror på en konkret vurdering. Det er ingen automatikk i at et konsulentoppdrag innebærer et databehandleroppdrag.

Vi erfarer at mange uten nærmere overveielser har en oppfatning om at konsulenter er databehandlere og derfor inngår en databehandleravtale som ledd i oppdragsavtalen, eller at man gjør det for å være på «den sikre siden». Det er imidlertid ikke gitt at det å inngå databehandleravtale med en leverandør som ikke er databehandler er å være på «den sikre siden». Vi mener partene bør tilstrebe å avklare de personvernrettslige rollene, og å sørge for at avtaleverket reflekterer disse rollene på en riktig måte.

Fride Hedin (Senior Associate), Line Haukalid (Managing Associate) og Rune Opdahl (partner), advokatfirmaet Wiersholm.

JUSNYTT

Halvor Manshaus

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

Høyesterett sa nei til bruk av lydopptak i dokumentarserie

Høyesterett har i en nylig avsagt kjennelse (HR-2022-2106-A, avsagt 2. november 2022) tatt stilling til spørsmål om bruk av lydopptak fra en avsluttet straffesak. I kjennelsen forkastes anken fra produksjonsselskapet Indie Film AS som ønsket å bruke opptaket i en dokumentarserie som vises på TV2. Den aktuelle serien har fått navnet «Direktøren», og handler om en mann som mener at han ble uriktig dømt i en straffesak som ble avsluttet i Borgarting lagmannsrett i 2016. Kjennelses ble avsagt under sterk dissens (3-2). Artikkelforfatteren representerte partshjelper i saken, Norsk Redaktørforening.

Det aktuelle lydopptaket kom fra en privatperson som hadde gjort opptak i skjul under hovedforhandling i straffesaken for lagmannsretten. Indie Film fikk først tilgang til opptaket senere i forbindelse med undersøkelser knyttet til dokumentaren. Opptaket stammet således ikke fra dokumentarteamet, men en privat tredjepart. Dette skillet har betydning, ettersom domstolloven § 131 a forbyr opptak gjort av media for etterfølgende offentliggjøring, mens det samme forbudet ikke får anvendelse på private opptak:

> «Under forhandlingene i straffesaker er fotografering, filmopptak og opptak for radio eller fjernsyn forbudt.»

Indie Film kunne således ikke selv ha gjort lydopptak til bruk i dokumentaren, og var heller ikke tilstede i retten under hovedforhandlingen. Dermed ble det avgjørende spørsmålet hvorvidt Indie Film kunne benytte det private opptaket, ettersom dette ikke var direkte omfattet av forbudet.

En forespørsel ble rettet fra Indie Film til lagmannsretten som hadde behandlet straffesaken. Det ble vist til at man ønsket å bruke opptak av forsvarerens innlegg, samt domfeltes egen forklaring. Begge disse hadde samtykket til den aktuelle bruken. Fornærmede var derimot bosatt i utlandet, og det hadde ikke latt seg gjøre å kontakte vedkommende. Bistandsadvokaten viste til at det derfor ikke var grunnlag for hverken å akseptere eller motsette seg den aktuelle bruken, men uttalte samtidig at han anså bruken av lydopptakene som «problematisk».

Lagmannsretten avslo begjæringen om bruk av lydopptakene. Det ble vist til at domstolloven § 131a ikke forbyr private opptak, slik at disse ikke trenger rettens tillatelse. Lagmannsretten la likevel til grunn at bestemmelsen innebar at offentliggjøring av slike opptak i utgangspunktet er forbudt og derfor krever eksplisitt samtykke fra retten. Etter en konkret vurdering kom lagmannsretten til at det i denne saken ikke skulle gis tillatelse til bruk av de aktuelle lydopptakene i dokumentaren.

Indie Film anket avgjørelsen til Høyesterett. Ettersom det ikke forelå noen reell motpart i saken, ble regjeringsadvokaten bedt om å prosedere for staten som konstruert motpart. Dette ble gjort for å sikre kontradiksjon i saken. Norsk Redaktørforening trådte inn som partshjelper for Indie Film. I saker som behandles i etter straffeprosessloven er det åpning for analogisk anvendelse av tvisteloven § 15-7, slik det fremgår av blant annet Rt-2010-1150. Domfelte i saken for lagmannsretten holdt også et innlegg for Høyesterett ved sin forsvarer.

Et spesielt trekk ved sakens utvikling er verdt å merke seg. De aktuelle lydopptakene var altså ønsket til bruk i den aktuelle dokumentarserien. Til tross for at Høyesterett gjorde en rask berammelse av saken, ble produksjonsselskapet nødt til å benytte skuespillere for å lese inn de aktuelle utdragene fra lydopptakene for å rekke premieredatoen som allerede var fastlagt av kanalen. Da saken sto i Høyesterett var med andre ord den aktuelle episoden av dokumentarserien allerede

vist på TV2, men med stemmer fra skuespillere som gjenga innholdet i opptakene fra domfelte og forsvareren. Det var enighet om at en slik ordrett gjengivelse av innholdet på opptakene ikke var i strid med forbudet mot offentliggjøring av pressens opptak i domstolloven § 131 a.

Det kunne også reises spørsmål ved om domstolloven § 131 a rammer selve opptaket som ble gjort av privatpersonen i nærværende sak, ettersom dette opptaket til slutt ble gjort tilgjengelig for Indie Film. Kjennelsen gir i avsnitt 42 klar anvisning på at et slikt privat opptak ikke rammes, selv om det på et etterfølgende tidspunkt kan komme opp spørsmål om å offentliggjøre innholdet. Dette betyr kun at selve opptakshandlingen i seg selv ikke var å anse som rettsstridig. Høyesterett går deretter videre til å vurdere om de konkrete opptakene kunne brukes i dokumentaren:

> «I en avgjørelse fra ankeutvalget i Rt-2012-380 avsnitt 15 er det lagt til grunn at domstolloven § 131a ikke rammer selve opptakshandlingen når det på opptakstidspunktet ikke forelå noen hensikt om å bruke opptaket i radio eller TV. Men spørsmålet nå er altså om § 131a må forstås slik at det likevel kreves tillatelse for å bruke lydopptak fra rettsforhandlingene dersom det senere blir aktuelt å bruke det «for radio eller fjernsyn».

Høyesteretts drøftelse av § 131 a tar utgangspunkt i det generelle prinsippet om offentlighet i rettspleien, jfr. Grunnloven § 95 første ledd og EMK (den europeiske menneskerettighetskonvensjon) artikkel 6 nr. 1. Dette har gitt seg utslag i flere spesialbestemmelser, som domstolloven § 124 som Høyesterett også omtaler i avsnitt 25:

> «Prinsippet om offentlig rettergang trygger rettsstaten ved å gjøre det mulig for allmennheten å øve kontroll med at det går rett og riktig for seg i den enkelte sak. Mer generelt bidrar prinsippet til å styrke så vel rettsstaten som ytringsfriheten og demokratiet ved å legge til rette for en offentlig debatt om rettsvesen og lovgivning. En konsekvens av prinsippet er dermed også retten til å gjengi offentlig fra rettsforhandlinger og rettsavgjørelser, jf. domstolloven § 124 første ledd.»

Fra dette generelle utgangspunktet vises det deretter til at det er gjort unntak fra prinsippet om offentlighet i rettspleien, blant annet under henvisning til retten til privatliv og personvernhensyn. Deretter vises det i avsnitt 28 til at ulike former for gjengivelse fra rettsforhandlinger kan gi ulik effekt eller opplevelse hos mottakeren.

> «Den tradisjonelle formen for gjengivelse har vært referat i etterkant av selve rettsmøtet. Bruk av lyd- og bildeopptak fra rettsmøtet virker gjerne sterkere – slik Indie Film er inne på i sin søknad til lagmannsretten. Bruk av slike opptak kan dermed lettere enn andre formidlingsformer komme i konflikt med personvernhensyn og andre legitime hensyn.»

Dette er et vanskelig område ved anvendelsen av regler om ytringsfrihet og offentlighet. I hvilken grad skal domstolene legge vekt på formidlingsform i en hypotetisk vurdering av noe som ennå ikke er offentliggjort? Det er i flere avgjørelser fra EMD (den europeiske menneskerettighetsdomstolen) lagt vekt på at media har en vid skjønnsmargin ved valg av publikasjonsform, jfr. saken Jersild (sak 15890/89 avsnitt 31):

> *"At the same time, the methods of objective and balanced reporting may vary considerably, depending among other things on the media in question. It is not for this Court, nor for the national courts for that matter, to substitute their own views for those of the press as to what technique of reporting should be adopted by journalists. In this context the Court recalls that Article 10 (art. 10) protects not only the substance of the ideas and information expressed, but also the form in which they are conveyed (see the Oberschlick v. Austria judgment of 23 May 1991, Series A no. 204, p. 25, para. 57).*»

Dette går delvis på domstolens retrospektive rolle, som får spesiell betydning på ytringsfrihetens område. Skal domstolen legge vekt på ytringens form før ytringen har funnet sted? Eller skal domstolen avvente begivenhetenes gang for så å gripe inn? EMK er generelt skeptiske til å legge avgjørende vekt utelukkende på ytringens form, der ytringen fremsettes av media. Meningen er nok å trekke en grense mellom de redaksjonelle vurderinger og domstolenes helhetsvurdering av den fremsatte ytring i den aktuelle kontekst. Et annet moment vil være at publikum i utgangpunktet har adgang til selv å møte opp og høre direkte det som blir uttalt i retten. Dette innebærer at en offentliggjøring av lydopptak ikke i seg selv vil medføre at publikum får tilgang til noe det rent prinsipielt allerede har etter reglene om offentlig rettergang. Det er altså flere ulike hensyn som kommer inn i det som må bli en totalvurdering med utgangspunkt i den konkrete foreliggende saken.

I kjennelsen går Høyesterett inn for at domstolloven § 131 a må forstås slik at det kreves tillatelse også for bruk av slike opptak som ikke er gjort umiddelbart av pressen selv. Det var med andre ord riktig av Indie Film å forelegge spørsmålet for lagmannsretten. Høyesterett viser i avsnittene 44-55 til flere momenter knyttet til personvernhensyn, samt behovet for at forhandlingene i

straffesaker ikke påvirkes ved at gjøres opptak. Det ble konkludert med at disse hensyn samlet sett taler for at det kreves tillatelse for senere offentliggjøring også for rent private opptak.

I vurderingen av om det i denne saken skulle tillates å bruke opptakene, viser førstvoterende innledningsvis til den forutgående drøftelsen knyttet til hvorvidt rettens tillatelse i det hele tatt var påkrevet. Videre ble det vist til behovet for å beskytte øvrige parter i saken mot belastningen ved at opptakene skulle spilles av, og at direkte opptak vil ha sterkere virkning enn andre former for gjengivelse. I denne forbindelse vises det til særskilte omstendigheter ved den underliggende straffesaken, som var av en alvorlig karakter.

Det gjøres med andre ord en helhetsvurdering der førstvoterende konkluderer med at det ikke forelå tilstrekkelig grunner til å fravike ordlyden i domstolloven § 131, som krever «særlige grunner» for å tillate offentliggjøring.

Annenvoterende har en annen inngang på drøftelsen av spørsmålet om tillatelse, og diskuterer i avsnitt 90 kravet til «særlig grunn» som fremgår av § 131. Her åpnes det for en mer åpen tilnærming, med utgangspunkt i EMK artikkel 10 om ytringsfrihet:

> «Selv om det etter lovens ordlyd er tillatelse, og ikke avslag, som krever «særlige grunner», mener jeg dette vilkåret i saken her må praktiseres relativt liberalt for best å ivareta de tungtveiende hensynene som EMK artikkel 10 er et utslag av. Jeg viser her til førstvoterendes redegjørelse for disse. Slik jeg oppfatter det, vil en slik tolking også være i overenstemmelse med foreliggende rettspraksis.»

Med en slik forståelse av lovens vurderingstema blir også den etterfølgende drøftelsen av selve spørsmålet om tillatelse vurdert mer åpent, og det legges i større grad vekt på samtykket fra de personene som det var aktuelt å benytte opptak fra.

Et viktig innspill fra annenvoterende er knyttet opp mot et punkt som er omtalt ovenfor, betydningen av ytringens form. Her trekkes det i avsnitt 94 opp en prinsipiell linje i rollefordelingen mellom media og domstoler:

> «Avgjørende for meg i denne saken er at domstolene bør være varsomme med å overprøve pressens faglige vurderinger. Slik jeg oppfatter lagmannsrettens begrunnelse i saken, nærmer domstolen seg her den redaksjonelle vurderingen som det er pressen selv som skal foreta. Det er pressens oppgave å sørge for en balansert fremstilling, å ivareta en eventuell tilsvarsrett mv., noe også Indie Film i sin søknad har redegjort for. Selv om også jeg har forståelse for at fornærmede og hennes ektefelle vil kunne oppfatte dokumentaren som belastende, mener jeg vilkårene for å gi tillatelse etter domstolloven § 131a andre ledd er oppfylt.»

Flertallet konkluderte i tråd med førstvoterende, slik at utfallet av saken ble at anken fra Indie Film ble forkastet.

Utgangspunktet etter denne avgjørelsen vil således være at eventuell offentliggjøring av private opptak fra straffesaker krever samtykke fra retten. Slik premissene er utformet vil dette ha betydning ikke bare for offentliggjøring fra pressen, men kan også være aktuelt for andre former for offentliggjøring.

Når domstolen skal gjøre den konkrete vurderingen etter domstolloven § 131 a vil det være nødvendig å gjøre en helhetsvurdering med utgangspunkt i det generelle prinsippet om offentlig rettergang, men der det også sees hen til de momenter som er fremhevet i kjennelsen, herunder behovet for personvern og hensynet til at selve rettergangen ikke påvirkes negativt av at det gjøres opptak for etterfølgende offentliggjøring.

Det skal nevnes at Domstolsadministrasjonen har hatt et prøveprosjekt med lydopptak som gjøres ved utvalgte domstoler. I første omgang har dette skjedd ved Nord-Troms tingrett og Hålogaland lagmannsrett, før også Jæren tingrett og Gulating lagmannsrett ble medtatt i prosjektet. Meningen har vært at det skulle implementeres lydopptak ved samtlige domstoler i løpet av et par år, men budsjettet for dette prosjektet har blitt endret. I skrivende stund er det ikke lagt opp til et budsjett som gjør dette mulig å gjennomføre med det første. Slike opptak vil imidlertid ikke være allment tilgjengelig, og regelverket er lagt opp rundt en sterk grad av fortrolighet knyttet til selve opptakene. Lydopptakene er ment delvis å erstatte forklaringer avgitt i første instans der det er uenighet om konkrete bevisspørsmål, og for eksempel ved vurdering av om en anke skal tillates fremmet.


Delphi

Rebecka Harding og Emilia Nordström

Senaste nyheterna inom svenskt dataskyddsområde

PTS inleder tillsyn av NIS-leverantörer

Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (”NIS-lagen”) trädde i kraft den 1 augusti 2018. NIS-lagen, vilken implementerar NIS-direktivet, syftar till att uppnå en hög nivå på säkerhet i nätverk och informationssystem hos leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster. Av NIS-lagen följer att leverantörer av samhällsviktiga och digitala tjänster ska bedriva systematiskt och riskbaserat arbete.

Post- och telestyrelsen (”PTS”) har tillsynsansvar för samhällsviktiga tjänster inom sektorn digital infrastruktur samt för digitala tjänster i Sverige och har även meddelat föreskrifter och allmänna råd (PTSFS 2021:3) om säkerhetsåtgärder för dessa leverantörer. PTS har nu inlett en tillsyn som avser att granska vissa leverantörers arbete med riskanalyser och riskbedömningar. Tillsynen är en planlagd tillsyn och således inte föranledd av en specifik händelse eller incident. Den aktuella tillsynen omfattar tre leverantörer av samhällsviktiga tjänster inom sektorn digital infrastruktur som tillhandahåller DNS-tjänster och registreringsenheter för toppdomäner.

IMY ger tillstånd för hantering av uppgifter om lagöverträdelser

Privata företag måste söka tillstånd från Integritetskyddsmyndigheten (”IMY”) för att få behandla personuppgifter om lagöverträdelser om det inte finns ett rättsligt stöd för behandlingen i lag eller förordning.

IMY har nu beslutat att två företag, ett säkerhetsföretag och en bank, får sådana tillstånd. IMY anser att företagen har berättigade intressen att behandla personuppgifterna enligt artikel 6.1 f i GDPR. Säkerhetsföretaget erbjuder en tjänst som innefattar bland annat bakgrundskontroller av arbetssökande, i syfte att inte sätta människor i en arbetsroll där de kan begå liknande brott igen. Banken utför kontroller av individer som anmälts för penningtvätt eller finansiering av terrorism som alla i koncernen har tillgång till, för att se till att de individerna inte kan vända sig till en annan filial och ha fortsatt tillgång till banken. I båda fallen anser IMY att det berättigade intresset väger tyngre än den registrerades integritetsintresse, och ger tillstånd att hantera personuppgifterna om lagöverträdelser.

IMY utfärdar reprimand avseende uppgifter om hälsa

IMY inledde granskning av en nyhetsbyrå efter att ha tagit emot klagomål mot nyhetsbyråns söktjänst för bland annat bakgrundskontroller. Söktjänsten gör det möjligt för användare att vid sökning på personer kunna ta del av uppgift om att den eftersökta personen varit föremål för tvångsvård på grund av psykisk ohälsa eller missbruk. Nyhetsbyrån har ett så kallat utgivningsbevis enligt yttrandefrihetsgrundlagen. Det innebär att söktjänsten omfattas av ett särskilt grundlagsskydd, som normalt innebär att GDPR inte är tillämplig. Till följd av en grundlagsändring 2019 kan GDPR ändå vara tillämplig i vissa fall om det rör en särskilt integritetskänslig uppgiftssamling.

IMY kom fram till att GDPR är tillämplig på nyhetsbyråns söktjänst, samt att det saknas rättslig grund för behandlingen av de känsliga personuppgifterna. IMY ansåg däremot att det skulle vara oproportionerligt att påföra nyhetsbyrån en sanktionsavgift för överträdelserna. Detta eftersom att det varit fråga om tolkningen av ett undantag från det grundlagsskydd utgivningsbevis ger samt att undantaget inte tidigare tillämpats av IMY eller någon domstol. IMY utfärdar dock en reprimand samt förelägger nyhetsbyrån att vidta åtgärder så att det inte längre ska vara möjligt att efter sökning på personer kunna ta del av uppgift om att de varit föremål för tvångsvård.

Rebecka Harding är senior associate/advokat och Emilia Nordström är thesis trainee vid Advokatfirman Delphi, Stockholm.

Gorrissen Federspiel

Tue Goldschmieding

Justitsministeriet udsteder foreløbige retningslinjer for statslige myndigheders opbevaring af SMS-beskeder

I kølvandet på den danske Mink-kommissions beretninger udsendte det danske Justitsministerium den 7. juli 2022 foreløbige retningslinjer for statslige myndigheders opbevaring af SMS-beskeder. Formålet med retningslinjerne er at sikre en ensartet praksis for statslige myndigheders opbevaring af SMS-beskeder, der ikke skal journaliseres.

Af hensyn til tidshorisonten for afdækning af tekniske muligheder for en central og brugeruafhængig opbevaring af SMS-beskeder, har Justitsministeriet i sine foreløbige retningslinjer anbefalet, at (i) medarbejdere og ministre instrueres i ikke at slette arbejdsrelaterede SMS-beskeder på deres tjenestetelefon, (ii) der løbende tages en lokal kopi af ministres, særlige rådgiveres og departementschefers arbejdsrelaterede SMS-beskeder og (iii) ministres, særlige rådgiveres, departementschefers og andre ansatte i chefstillingers arbejdsrelaterede SMS-beskeder fortsat opbevares efter telefonskift eller fratrædelse.

Læs nyheden her: *https://www.justitsministeriet.dk/pressemeddelelse/foreloebige-retningslinjer-for-statslige-myndigheders-opbevaring-af-sms-beskeder/*

Læs de foreløbige retningslinjer her: *https://www.justitsministeriet.dk/wp-content/uploads/2022/07/Foreloebige-retningslinjer-for-statslige-myndigheders-opbevaring-af-SMS-beskeder-mv..pdf*

Rigspolitiet pålægger teleudbydere at foretage målrettet logning

Fra den 28. juni 2022 pålagde det danske Rigspoliti teleudbydere at foretage målrettet geografisk logning af trafikdata.

Pålægget om målrettet logning af trafikdata opstod som følge af EU-Domstolens afgørelse af 5. april 2022 i *Commissioner of An Garda Síochána m.fl.* (sag C-140/20). Dommen medførte en afskæring af nationale retshåndhævende myndigheders adgang til i forbindelse med efterforskningen af grov kriminalitet at indhente trafikdata, som er logget generelt og udifferentieret af teleudbydere. Rigspolitiets pålæg er dermed en nødvendig foranstaltning for at genetablere politiets og den danske Anklagemyndigheds muligheder for at bekæmpe grov kriminalitet ved hjælp af teledata.

Pålægget indebærer, at teleudbydere skal foretage målrettet geografisk logning af trafikdata på områder, hvor der er et højt antal anmeldelser af grov kriminalitet, og på visse sikringskritiske områder. Disse trafikdata skal opbevares af teleudbyderne i et år fra registreringstidspunktet.

Muligheden for at iværksætte geografisk logning og målrettet logning af trafikdata rettet mod bestemte personer følger af de nye logningsregler, der trådte i kraft den 30. marts 2022. Den ovenfor nævnte afgørelse fra EU-Domstolen af 5. april 2022 bekræfter tillige, at en sådan målrettet logning er forenelig med EU-retten, når den foretages i tilknytning til grov kriminalitet.

Ud over konkret iværksatte pålæg om målrettet geografisk logning, er teleudbyderne fortsat forpligtet til at logge trafikdata generelt og udifferentieret for at beskytte den nationale sikkerhed, idet betingelsen om, at der skal foreligge en konkret og aktuel trussel mod den nationale sikkerhed i Danmark, fortsat anses for opfyldt.

Læs nyheden her: *https://www.justitsministeriet.dk/pressemeddelelse/nu-ivaerksaettes-maalrettet-logning/*

Datatilsynet udtaler alvorlig kritik af Sports Connection for manglende behandlingssikkerhed

Den 4. juli 2022 traf det danske Datatilsyn afgørelse i en sag med journalnummer 2021-441-10210 om Sports Connection ApS (»Sports Connection«), hvori de udtalte alvorlig kritik, på baggrund af et hackerangreb mod virksomhedens webshop, der kompromitterede kundebetalingsoplysninger.

Forud for hackerangrebet havde Sports Connection forsømt at sikkerhedspatche sit e-handelssystem (webshop) til seneste version, hvilket Datatilsynet fandt ville have fjernet generelle sårbarheder ved programmet.

Datatilsynet fandt herefter, at selskabet som dataansvarlig ikke havde truffet de tilstrækkelige tekniske og organisatoriske foranstaltninger til at beskytte de registreredes personoplysninger, grundet en manglende effektiv risikovurdering og løbende opdatering af deres platform. Datatilsynet henviste til, at det var en kendt risiko, at e-handelsplatforme forsøges kompromit-

teret gennem deres indbyggede svagheder. Der var således tale om en overtrædelse af Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«) artikel 32, stk. 1 om passende behandlingssikkerhed.

Endvidere konstaterede Datatilsynet, at GDPR artikel 24, stk. 1, jf. artikel 32, stk. 1, om den dataansvarliges ansvar var overtrådt, da Sports Connection ikke kunne fremlægge fornøden dokumentation for sin behandlingssikkerhed i form af logfil over løbende opdateringer af det kompromitterede system. Virksomheden var derfor ikke i stand til at påvise, at behandlingen var udført i overensstemmelse med GDPR. Det forhold, at Sports Connection havde anvendt en ekstern partner til udvikling af deres e-handelsplatform, var uden betydning for vurderingen.

Læs afgørelsen her: *https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/jul/alvorlig-kritik-af-sports-connection-for-manglende-behandlingssikkerhed*

Datatilsynet indleder undersøgelse om overvågning af medarbejdere i Aalborg Kommune

Det danske Datatilsyn udsendte den 7. juli 2022 nyhed om, at de har indledt en undersøgelse af Aalborg Kommune, efter de igennem medieomtale er blevet bekendt med, at medarbejdere efter eget udsagn er blevet overvåget gennem video og lyd.

Formålet med undersøgelsen er ifølge Datatilsynet at afklare, om overvågningen har fundet sted, og i så fald, om det er sket i overensstemmelse med databeskyttelsesreglerne. Det indebærer særligt et krav om hjemmel og sagligt formål, samt at de grundlæggende principper om lovlighed, rimelighed og gennemsigtighed er opfyldt. Derudover har medarbejderne også krav på at blive informeret om, at de bliver overvåget.

Læs pressemeddelelsen her: *https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/jul/datatilsynet-undersoeger-sag-om-overvaagning-af-medarbejdere*

Datatilsynet udtaler kritik og giver to påbud til EG Digital Welfare ApS på baggrund af IT-systemet Mediconnect

Det danske Datatilsyn offentliggjorde den 7. juli 2022 afgørelse i en sag med journalnummer 2021-431-0144 vedrørende IT-systemet Mediconnect, som udbydes af EG Digital Welfare ApS (»EG«).

EG er databehandler for IT-systemet, Mediconnect, i forbindelse med kommuner, regioner og forsikringsselskabers brug af systemet til håndteringen af følsomme og fortrolige personoplysninger. Sagen opstod på baggrund af en henvendelse, hvoraf det blandt andet fremgik, at konti blev brugt som fælleskonti af flere læger og klinikker, at systemet ikke indeholder to-faktor login, at der ikke foretages logning af hvilke medarbejdere, der tilgår hvilke oplysninger i systemet og at adgangskoderne er tilgængelige i klartekst i databaserne.

Datatilsynet udtalte kritik af, at EG som databehandler for Mediconnect, behandler personoplysninger i strid med GDPR artikel 32, stk. 1, ved ikke at have truffet passende organisatoriske og tekniske sikkerhedsforanstaltninger. Datatilsynet meddelte samtidig EG påbud om (i) at anvende en anerkendt algoritme til irreversibel kryptering af alle kodeord, så disse hverken opbevares eller gøres tilgængelige i klartekst, og (ii) at indføre en loginløsning for alle brugere af IT-systemet med adgang til oplysninger af særlige kategorier, der vil gøre det umuligt at få adgang til disse oplysninger alene ved brug af brugernavn og kodeord.

Læs afgørelsen her: *https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/jul/datatilsynet-udtaler-kritik-og-giver-to-paabud-til-eg-digital-welfare-aps*

Datatilsynet gennemfører skriftligt tilsyn med Region Syddanmarks brug af personoplysninger til forskning

Det danske Datatilsyn gennemførte den 20. juli 2022 et skriftligt tilsyn med Region Syddanmark, journalnummer 2020-422-0026, med fokus på behandling af personoplysninger til forskningsbrug.

Datatilsynet havde, som genstand for undersøgelsen, udvalgt tre forskningsprojekter inden for emnerne »behandlingsgrundlag« og »ansvar og roller«.

Datatilsynet fandt ikke anledning til at kritisere Region Syddanmarks vurdering af retsgrundlaget for behandlingen af personoplysninger i de tre projekter, nemlig GDPR artikel 9, stk. 2, litra j om behandling af særlige kategorier af personoplysninger til videnskabelige forskningsformål, GDPR artikel 6, stk. 1, litra e om behandling nødvendig af hensyn til udførelse af en opgave i samfundets interesse, mm., samt lov nr. 502 af 23. maj 2018 (»den danske databeskyttelseslov«) § 10, stk. 1 om behandling af oplysninger i forbindelse med videnskabelige undersøgelser.

For så vidt angik projekt nr. 1 og 3 fandt Datatilsynet imidlertid anledning til at udtale kritik af, at Region Syddanmark ikke havde påvist, at der var taget stilling til tilsynsniveauet.

Datatilsynet fremhævede, at en dataansvarlig skal føre tilsyn med sikkerheden hos sine underdatabehandlerne, da den dataansvarlige selv skal overholde ansvarlighedskravet i GDPR artikel 5 og dermed kunne dokumentere, at behandlingen af personoplysninger er i overensstemmelse med GDPR. Region Syddanmark havde som dataansvarlig ikke opfyldt ovennævnte krav ved blot at indgå en aftale med databehandlerne.

Læs afgørelsen her: *https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/jul/tilsyn-med-region-syddanmarks-brug-af-personoplysninger-til-forskning*

Tv-overvågning af medarbejdere var i overensstemmelse med reglerne i GDPR

Det danske Datatilsyn traf den 8. august 2022 afgørelse i en sag med journalnummer 2020-431-0115 vedrørende træningscenteret Fitness World A/S' (»FW«) tv-overvågning af medarbejdere.

Sagen, som Datatilsynet indledte af egen drift, handlede om, hvorvidt FW overholder databeskyttelsesreglerne i forbindelse med overvågning af ansatte i træningscentrene.

En arbejdsgiver må kun iværksætte overvågning af arbejdspladsen, hvis der er en saglig grund til dette, og overvågningen begrænses til, hvad der skønnes nødvendigt. Derudover er det vigtigt, at medarbejdere informeres om tv-overvågningen samt formålet med overvågningen. Bruges overvågningen til at føre kontrol med medarbejderens arbejde, er der skærpede krav til at informere ansatte om dette.

I sagen kom Datatilsynet frem til, at FW's tv-overvågning skete med henblik på at forebygge kriminalitet i fitnesscentrene. Datatilsynet lagde i sagen til grund, at medarbejderne i forbindelse med ansættelse var blevet informeret om tv-overvågningen, og at overvågningen ville kunne blive brugt for at gøre et muligt retskrav gældende mod medarbejderen. På den baggrund fandt Datatilsynet, at FW's behandling var i overensstemmelse med GDPR artikel 6, stk. 1, litra f, om legitim interesse og artikel 14 om oplysningspligten.

Datatilsynet tog også stilling til, hvorvidt behandlingssikkerheden i centrene var i overensstemmelse med GDPR artikel 32, stk. 1. FW opbevarede i den forbindelse følsomme oplysninger om en række medarbejdere, herunder lægeerklæringer, opsigelser, kontrakter og skriftlige advarsler samt tv-overvågningsbilleder på en fælles computer. Oplysningerne var endvidere gemt på et forkert drev, og var følgelig tilgængelige for andre medarbejdere end ledelsen.

Datatilsynet udtalte alvorlig kritik på baggrund heraf, da opbevaringen udgjorde en nærliggende risiko for medarbejdernes databeskyttelsesretlige rettigheder. FW valgte efterfølgende at udlevere personlige computere med tilhørende personligt login til centrenes ledere samt at videreuddanne medarbejdere, særligt ved målrettet uddannelse til de lokale ledere.

Læs hele afgørelsen her: *https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/aug/tv-overvaagning-af-medarbejdere-levede-op-til-gdpr*

Datatilsynet udtaler alvorlig kritik af KMD A/S efter utilsigtet adgang til oplysninger om børn

Det danske Datatilsyn traf den 25. august 2022 afgørelse i en sag med journalnummer 2021-431-0126 om KMD A/S (»KMD«), der ved implementeringen af en ny funktion i sit system, ikke havde testet systemet tilstrækkeligt, hvilket førte til, at plejeforældre fik uberettiget adgang til oplysninger om plejebørnene via folkeskolernes kommunikationsplatform, AULA. Datatilsynet fandt ikke, at KMD's behandling af oplysninger var i overensstemmelse med GDPR artikel 32 om behandlingssikkerhed, og udtalte følgelig alvorlig kritik.

Datatilsynet fik kendskab til bruddet på baggrund af anmeldelser fra seks kommuner i perioden fra den 19. januar 2021 til den 21. januar 2021. Anmeldelserne gik på, at en systemfejl i januar 2021 hos de pågældende kommuners databehandler, KMD, havde medført, at plejeforældre uberettiget havde haft adgang til AULA.

Datatilsynet vurderede, at KMD, ved ikke at have udført passende tests af den nye funktion, herunder hvordan funktionaliteten fungerede sammen med AULA, ikke havde truffet passende organisatoriske og tekniske foranstaltninger for derigennem at sikre et sikkerhedsniveau, der passer til de risici, der er forbundet med KMD's behandling af personoplysninger. Det blev endvidere tillagt vægt, som en skærpende omstændighed, at Datatilsynet tidligere i november 2020 havde behandlet en hændelse vedrørende de samme systemer, som leverer data til AULA, omend hændelsen ikke var identisk med den foreliggende.

Læs hele afgørelsen her: *https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/aug/alvorlig-kritik-utilsigtet-adgang-til-oplysninger-om-boern*

Datatilsynet udtaler alvorlig kritik af Familieretshusets utilsigtede videregivelser af beskyttede navne- og adresseoplysninger

Det danske Datatilsyn har den 6. september 2022 truffet afgørelse i en sag med journalnummer 2021-432-0063 om det danske Familieretshus og fandt på baggrund af sagen anledning til at udtale alvorlig kritik samt påbud om fornyet risikovurdering, i henhold til GDPR artikel 32, stk. 1, og artikel 58, stk. 2, litra d.

I efteråret 2021 indledte Datatilsynet af egen drift en undersøgelse af Familieretshusets utilsigtede videregivelse af bl.a. beskyttede navne- og adresseoplysninger til uvedkommende.

Personoplysningerne var bl.a. videregivet ved aktindsigtsanmodninger, fremsendelser af afgørelser, orienteringsskrivelser og partshøringer. De utilsigtede videregivelser skyldes hovedsageligt menneskelige fejl. Herudover er videregivelserne i vidt omfang sket til modparter, som de registrerede havde navne- og adressebeskyttelse for at beskytte sig mod.

Datatilsynet har tidligere, den 4. marts 2021, i en sag med journalnummer 2020-432-0037, truffet af-

gørelse i en lignende sag om Familieretshusets uberettigede videregivelse af personoplysninger. Hertil kommer, at Datatilsynet i perioden op til og mens sagen blev oplyst, fra 27. maj 2021 til 16. august 2022, modtog 37 anmeldelser om brud på persondatasikkerheden, som alle omhandlede Familieretshusets uberettigede videregivelse af den ene parts beskyttede adresse.

Datatilsynet har kunnet konstatere, at Familieretshuset har foretaget betydelige organisatoriske foranstaltninger for at undgå yderligere utilsigtede videregivelser, siden afgørelsen af 4. marts 2021. Alligevel fandt Datatilsynet, at de gentagne konstateringer af ligeartede brud på persondatasikkerheden burde have givet Familieretshuset anledning til at reflektere over de allerede foretagne risikovurderinger, idet gentagne episoder antyder behov for yderligere kontrolforanstaltninger og/eller opdateret teknisk understøttelse af eksisterende foranstaltninger.

Familieretshuset havde derfor, ved ikke at træffe passende organisatoriske og tekniske foranstaltninger for at sikre et sikkerhedsniveau, forsømt at iagttage sin pligt til at etablere passende behandlingssikkerhed i henhold til GDPR artikel 32, stk. 1.

Af betydning for denne vurdering er der særligt lagt vægt på, at Familieretshuset ikke i tilstrækkeligt omfang havde haft de fornødne procedurer for regelmæssig efterprøvning, vurdering og evaluering af effektiviteten af de allerede etablerede foranstaltninger.

Datatilsynet har ved valg af reaktion lagt særlig vægt på, at det kan være forbundet med store konsekvenser for de registrerede, når deres beskyttede adresse eller opholdssted utilsigtet videregives til den person, de forsøger at skjule sig for.

Læs afgørelsen her: *https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/sep/alvorlig-kritik-af-familieretshuset*

Datatilsynet fandt, at det Konservative Folkeparti havde lovligt grundlag for advokatundersøgelse

Det danske Datatilsyn har den 6. september 2022 truffet afgørelse i en sag med journalnummer 2021-31-5542, hvor klager klagede over behandlingen af oplysninger i en advokatundersøgelse.

Undersøgelsen blev, på vegne af det danske Konservative Folkeparti (»Konservative Folkeparti«), indledt af advokatfirmaet Plesner Advokatpartnerselskab (»Plesner«) med henblik på en faktuel undersøgelse af de i dagspressen, mod klager, fremsatte beskyldninger om seksuelle krænkelser og overgreb.

Datatilsynet fandt, at behandlingen af oplysninger, herunder oplysninger om mulige strafbare handlinger og seksuelle forhold, var inden for rammerne af GDPR artikel 6, stk. 1, litra f om legitim interesse, artikel 9, stk. 2, litra d om behandling af særlige kategorier af personoplysninger i en politisk organisation samt den danske databeskyttelseslov § 8, stk. 3, 2.pkt. om behandling af oplysninger om strafbare forhold, hvis det er nødvendigt til varetagelse af en berettiget interesse.

Datatilsynet fandt imidlertid anledning til at udtale kritik af det Konservative Folkeparti samt Plesner, for ikke at have givet klager tilstrækkelige oplysninger om behandlingen, og dermed forsøgt at iagttage oplysningspligten i henhold til GDPR artikel 14.

Læs afgørelsen her: *https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/sep/det-konservative-folkeparti-havde-et-lovligt-grundlag-for-at-gennemfoere-advokatundersoegelse*

Chromebooks: Datatilsynet suspenderer forbud mod Helsingør Kommunes brug af Google Workspace og giver påbud om lovliggørelse

Den 8. september 2022 offentliggjorde det danske Datatilsyn sin fjerde afgørelse under journalnummer 2020-431-0061 i sagen angående Helsingør Kommunes behandling af personoplysninger i folkeskolen ved brug af Chromebooks og Google Workspace.

Tilbage i september 2021 udtalte Datatilsynet alvorlig kritik samt påbud om udarbejdelse af en risikovurdering i sin første afgørelse under samme journalnummer. I den konkrete sag havde Helsingør Kommune undladt at foretage de fornødne vurderinger af risikoen for de registreredes rettigheder ved brugeroprettelsen til Chromebook og brugen af Google G-suite for Education (nu Google Workspace), som er en pakke af værktøjer til cloudcomputing, produktivitet og samarbejde. Kommunen havde endvidere undladt at foretage tilstrækkelig sikring mod uautoriseret brug af computerne.

Den 14. juli 2022, fandt Datatilsynet igen anledning til at udtale alvorlig kritik af Helsingør Kommunes behandling af personoplysninger i folkeskolen ved brug af Google Workspace i den næste Chromebook-sag under samme journalnummer. Afgørelsen gav herudover Datatilsynet anledning til at nedlægge forbud mod Helsingør Kommunes behandling af personoplysninger ved brug af Google Chromebooks og Google Workspace, indtil brugen blev bragt i overensstemmelse med GDPR. I tillæg til ovenstående, suspenderede Datatilsynet også enhver overførsel af personoplysninger til USA, som Helsingør Kommune havde instrueret Google Cloud EMEA Limited i at foretage, som databehandler for kommunen, indtil Helsingør Kommune kunne påvise iagttagelse af reglerne i GDPR kap. V.

Datatilsynet fandt, at Helsingør Kommunes risikovurdering var mangelfuld, fordi nogle helt konkrete risici i forhold til databehandlerkonstruktionen ikke var tilstrækkeligt afdækket. Det fremgik desuden af databehandleraftalen, at der kun-

ne overføres oplysninger til tredjelande i supportsituationer uden det fornødne sikkerhedsniveau.

Den 18. august 2022 meddelte Datatilsynet i den tredje sag under samme journalnummer, at man fastholdt forbuddet udstedt i juli, idet Datatilsynet vurderede, at Helsingør Kommune ikke kunne nedbringe risikoen til et acceptabelt niveau uden ændringer i kontraktgrundlaget og teknologien.

Den 8. september 2022 suspenderede Datatilsynet imidlertid dette forbud. I stedet meddelte Datatilsynet Helsingør Kommune et påbud om lovliggørelse, i sin fjerde sag under samme journalnummer. Helsingør Kommune måtte således genoptage brugen af Google Workspace, men på betingelse af at bringe aftalen med Google som databehandler i overensstemmelse med GDPR senest den 5. november 2022. Herudover skulle Helsingør Kommune også udarbejde en opdateret konsekvensanalyse baseret på alle de risici, som kommunen under dokumentationsprocessen har identificeret, såfremt det måtte være relevant.

Kommunernes Landsforening har orienteret Datatilsynet om, at de forventer at fremsende lignende henvendelser om lovliggørelse af brugen af Google Workspace i andre kommuner. Datatilsynet har meldt ud, at de forventer at stille de samme krav til andre kommuner, der foretager lignende behandlinger.

Læs Datatilsynets afgørelse af 8. september 2022 her: *https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/sep/chromebooks-datatilsynet-suspenderer-forbud-og-giver-paabud-om-lovliggoerelse*

Læs Datatilsynets afgørelse af 18. august 2022 her: *https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/aug/datatilsynet-fastholder-forbud-i-chromebook-sag*

Læs Datatilsynets afgørelse af 14. juli 2022 her: *https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/jul/datatilsynet-nedlaegger-behandlingsforbud-i-chromebook-sag-*

Læs Datatilsynets afgørelse af 10. september 2021 her: *https://admin.datatilsynet.dk/afgoerelser/afgoerelser/2021/sep/afgoerelse-vedroerende-brud-paa-persondatasikkerheden*

Datatilsynet meddeler Aarhus Kommune påbud om ændring af databehandleraftale indgået med Google Workspace

Det danske Datatilsyn meddelte den 8. september 2022 Aarhus Kommune et påbud om at ændre den indgåede aftale med databehandleren, Google Workspace, på en sådan måde, at den bringes i overensstemmelse med GDPR.

Datatilsynet henviste i sin afgørelse til den tilsvarende sag vedrørende Helsingør Kommunes brug af Google Chromebooks og Workspace (gengivet ovenfor). Datatilsynet fandt, at Aarhus Kommune, på samme måde som Helsingør Kommune, skal opdatere sin databehandleraftale med Google Workspace, herunder f.eks. ved at tydeliggøre, hvornår databehandleren agerer som selvstændig dataansvarlig, samt til hvilke formål, de supportsituationer, som Aarhus Kommune ikke benytter længere, og sikre, at alle tilsigtede overførsler til usikre tredjelande overholder GDPR, samt udarbejde fornøden dokumentation herfor.

Ydermere blev Aarhus Kommune påbudt at beskrive de datastrømme, der finder sted, og identificere de personoplysninger, der videregives til leverandøren, og at tydeliggøre, hvornår leverandøren agerer som selvstændig eller fællesdataansvarlig.

Læs afgørelsen her: *https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/sep/vedroerende-aarhus-kommunes-behandling-af-personoplysninger*

Datatilsynet konkluderer, at Google Analytics ikke kan anvendes lovligt uden videre. Lovlighed forudsætter implementering af supplerende foranstaltninger udover de indstillinger, Google stiller til rådighed

Det danske Datatilsyn har den 21. september 2022, efter nærmere gennemgang af værktøjet Google Analytics, konkluderet, at Google Analytics, på baggrund af dets indstillinger og vilkår, ikke uden videre kan bruges lovligt.

Værktøjet Google Analytics anvendes til indsamling af data om besøgende på hjemmesider og apps, for derigennem at udarbejde statistiske rapporter, som hjemmesideindehaverne kan bruge til f.eks. at optimere design, funktioner, webshop, mm. Datatilsynet har på baggrund af en fælleseuropæisk analyse vurderet, at værktøjet, der medfører overførsel af personoplysninger til USA, ikke er foreneligt med GDPR, idet de amerikanske regler ikke yder samme beskyttelse som databeskyttelsesreglerne.

Virksomhederne står herefter med et valg om enten at træffe effektive supplerende foranstaltninger, såsom pseudonymisering, for derigennem at overholde databeskyttelsesreglerne eller helt ophøre med deres brug af værktøjet og finde alternativer herfor.

Datatilsynet har i tilknytning til de mange spørgsmål, som der er opstået i kølvandet på diverse afgørelser fra europæiske datatilsyn, oprettet en FAQ, hvor de besvarer en række af de mest stillede spørgsmål vedrørende Google Analytics.

Læs pressemeddelelsen her: *https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/sep/brug-af-google-analytics-til-webstatistik*

Læs Datatilsynets FAQ om Google Analytics her: *https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/internet-medier-og-apps-/google-analytics*

Datatilsynet nedsætter nyt specialudvalg

Den 28. september 2022 nedsatte det danske Datatilsyn et specialudvalg med fokus på behandling af personoplysninger i forbindelse med forskning.

Datatilsynet lancerede i 2020 et nyt strategisk grundlag med ny vision, mission og værdigrundlag, hvorefter tilsynet ønsker et øget fokus på konkret vejledning, information, tilgængelige afgørelser og et målrettet tilsyn. Datatilsynet har arbejdet med at skabe en endnu tættere dialog med omverdenen og sigtet på en bred interesseinddragelse, for at sikre efterlevelse af GDPR, med et særligt fokus på at skabe mere klarhed omkring omfanget og betydningen af databeskyttelsesreglerne, hos de dataansvarlige.

Interesseinddragelsen indebærer bl.a., at specialudvalget er nedsat ved en bred invitation til både relevante interesseorganisationer, ministerier og styrelser. Planen er, at specialudvalget skal mødes to gange årligt, hvoraf det første møde blev afholdt den 29. september 2022. Her vil medlemmerne blive orienteret om Datatilsynets aktuelle arbejde på forskningsområdet, herunder det internationale område, ligesom de vil have anledning til at komme med input.

Læs nyheden her: *https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/sep/specialudvalg-om-forskning*

Datatilsynet udgiver ny vejledning om valgkampagner

Det danske Datatilsyn udgav den 4. oktober 2022 en ny vejledning om databeskyttelsesreglerne i forbindelse med valgkampagner.

Valgkampagner føres ikke længere kun på plakater og med valgbrochurer, men er også rykket ind på sociale medier og andre digitale platforme. Kampagnerne kan ved hjælp af dataindsamling og algoritmebaseret teknologi målrettes specifikke befolkningsgrupper. Det er i den forbindelse vigtigt, at databeskyttelsesreglerne fortsat overholdes, særligt når kampagnerne ofte behandler oplysninger om personers politiske overbevisning, der kategoriseres som en følsom personoplysning i GDPR artikel 9.

Vejledningen er opdelt i fire punkter. Indledningsvist behandles spørgsmålet om GDPR's anvendelsesområde, med særligt fokus på undtagelsen med hensyn til ytrings- og informationsfrihed. Datatilsynet er af den opfattelse, at undtagelsen omfatter meningsdannere og politiske partier i de tilfælde, hvor der udbredes information, meninger eller idéer til offentligheden. Undtagelsen skal fortolkes bredt, og gælder også, selvom der er tale om informationer, der kan opfattes som chokerende eller forstyrrende. Herudover kan formidling af et politisk budskab, der indeholder personoplysninger, også være omfattet af undtagelsen.

Undtagelsen omfatter som udgangspunkt ikke rent private oplysninger. Hvad der udgør »rent private oplysninger«, varierer dog afhængigt af den konkrete person og kontekst, f.eks. skal der differentieres mellem tilfælde, hvor der er tale om en privatperson eller et folketingsmedlem. Behandling forud for spredning af politisk budskab, f.eks. via profilering på sociale medier, kan ligeledes ikke undtages. Det omfatter for eksempel den situation, hvor et politisk parti ønsker at sende sit partiprogram ud via SMS, og derfor indhenter telefonnumre via offentligt tilgængelige kilder.

Det næste punkt i vejledningen handler om ansvarsfordelingen i valgkampagner. Begreberne »dataansvarlig«, »databehandler« og »fælles dataansvarlig« introduceres, med henblik på at udpege, hvem der har ansvaret for iagttagelse af databeskyttelsesreglerne, bevisbyrden for, at reglerne er overholdt, samt hvilke forpligtelser der alene påhviler databehandleren. Der gives flere tænkte eksempler på, hvordan rollerne fordeler sig i forbindelse med valgkampagner, da fordelingen afhængig af det politiske partis opbygning kan være meget forskellig.

De fleste politiske partier og organisationer vil være dataansvarlige i forskellige situationer, enten alene eller sammen med andre. Som dataansvarlig påhviler det partiet eller organisationen at sikre, at databeskyttelsesreglerne overholdes, også af den anvendte databehandler.

EU-domstolen har flere gange fastslået, at kommercielt brug af sociale medieplatforme giver et fælles dataansvar med det sociale medie, også selvom det sociale medie tilbyder en standardiseret ydelse. Vejledningen fremhæver, at der i en sådan situation skal etableres en »fælles ordning«, hvorefter det politiske parti og det sociale medie på en gennemsigtig måde fastlægger, hvordan de påtænker at iagttage deres respektive ansvar.

Vejledningen indeholder afslutningsvist en tjekliste, der i otte punkter opridser, hvad man som politisk aktør skal huske under en valgkampagne i forbindelse med GDPR.

Læs hele vejledningen her: *https://www.datatilsynet.dk/Media/638004710562663269/Databeskyttelsesreglerne i forbindelse med valgkampagner.pdf*

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

Gorrissen Federspiel

Tue Goldschmieding

Ændring af udlandsbekendtgørelsen medfører nye regler for vederlagsmodellen til udøvende kunstnere og fonogramproducenter fra tredjelande

Det danske Kulturministerium har den 1. juli 2022 sendt et udkast til ændring af bekendtgørelse nr. 218 af 9. marts 2010 om anvendelse af ophavsretsloven i forhold til andre lande (»den danske udlandsbekendtgørelse«) i offentlig høring. Udkastet indebærer en ophævelse af udlandsbekendtgørelsens § 14 og § 16, stk. 2, således at kunstnere og fonogramproducenter har krav på betaling, når deres musik anvendes i tilfælde af offentlige fremførelse, uanset om danske rettighedshavere ikke har samme krav på betaling i det pågældende tredjeland.

I dag sker betaling til udøvende kunstnere og fotogramproducenter fra tredjelande ud fra reglerne i udlandsbekendtgørelsen. Betalingen sker ud fra et gensidighedsprincip, der indebærer, at betaling ydes til kunstnere og fotogramproducenter fra tredjelande, såfremt danske rettighedshavere tilsvarende modtager betaling fra tredjelandet, når deres indhold udnyttes i tredjelandet.

EU-Domstolen har imidlertid fastslået i sin praksis i *RAAP mod PPI* (sag C-265/19), at alene EU-lovgiver kan fastsætte et sådant gensidighedsprincip. Afgørelsen fastslår, at vederlagsretten gælder for alle udøvende kunstnere og producenter, desuagtet nationalitet, så længe EU-lovgiver ikke udtrykkeligt bestemmer, at noget andet skal gælde. Kulturministeriet måtte følgelig ændre bekendtgørelsen for at bringe den i overensstemmelse med EU-Domstolens praksis.

Høringsfristen udløb den 19. august 2022.

Læs høringen her: *https://hoeringsportalen.dk/Hearing/Details/66564*

Forbrugerombudsmanden udsteder ny kvikguide om reglerne for udbetaling af værdien af elektroniske gavekort

Den danske Forbrugerombudsmand har den 21. september 2022 offentliggjort en ny kvikguide, der har til formål at hjælpe virksomheder med at overholde betalingslovens regler for udbetaling af værdien af elektroniske gavekort.

Kvikguiden, der hovedsageligt bygger på lovbekendtgørelse nr. 2710 af 7. december 2021 (»den danske betalingslov«) § 96 om udstedelse og indløsning af elektroniske penge, opstiller tre betingelser, der skal være opfyldt, før indehaveren af gavekortet har krav på at få det udbetalt. Betingelserne er, at (i) gavekortet skal være elektronisk, (ii) det skal være udstedt mod betaling og (iii) må ikke være en billet eller kvittering for betaling.

Kvikguiden følger herefter op med at besvare nogle af de af virksomhederne og forbrugerne almindeligt stillede spørgsmål, herunder bl.a. om, hvornår virksomheden er forpligtet til at udbetale værdien af gavekortet, eller om virksomheden må kræve et gebyr for at udbetale værdien.

Læs pressemeddelelsen her: *https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2022/ny-kvikguide-skal-hjaelpe-virksomheder-med-at-efterleve-reglerne-for-udbetaling-af-elektroniske-gavekort/*

Læs guiden her: *https://www.forbrugerombudsmanden.dk/media/56764/kvikguide-til-udbetaling-af-elektroniske-gavekort.pdf*

Østre Landsret hjemviser sag vedrørende Orklas varemærkeregistrering af det tredimensionale mærke, der viser KiMs Snack Chips.

Østre Landsret afsagde den 11. juli 2022 dom i sag BS-196068/2020-OLR anlagt af Orkla Confectionery & Snacks Danmark A/S (»Orkla«) mod Estrella ApS, Intersnack Knabber-Gebäck GmbH & Co. KG (»Intersnack«) og det danske Ankenævn for Patenter og Varemærker (»Ankenævnet«).

Sagen angik Sø- og Handelsrettens prøvelse af Ankenævnets kendelse, som stadfæstede Patent- og Varemærkestyrelsens afgørelse om ophævelse af varemærkeregistrering af Orklas tredimensionelle mærke gengivet i form af et billede af en chip, som blev markedsført under navnet, »KiMs Snack Chips«. Ankenævnet fastslog at mærkets væsentligste kendetegn var den rillede overflade, hvilket udgjorde en teknisk funktion i forhold til produktets tekstur og sprødhed, hvorfor varemærkeregistrering var udelukket i henhold til undtagelsesbestemmelsen i lovbekendtgørelse af nr. 88 af 29. januar 2019 (»den danske varemærkelovs«) § 14, stk. 1, nr. 1 om absolutte hindringer for registrering.

Østre Landsret fandt derimod, at mærkets væsentlige kendetegn ikke

alene bestod af den rillede overflade, men tillige mærkets firkantede form. Rillerne fandtes forsat at være af teknisk funktion, ligesom Landsretten ikke fandt fornødent grundlag for at tilsidesætte Ankenævnets vurdering, hvorefter den firkantede form ikke havde nogen teknisk funktion.

Med afsæt heri, ændrede Østre Landsret Sø- og Handelsrettens dom, hvor Ankenævnet blev frifundet, ved at hjemvise sagen til fornyet behandling ved Ankenævnet. Hjemvisningen var begrundet i, at Ankenævnet og Patent- og Varemærkestyrelsen i den administrative sag hverken havde taget stilling til, om den firkantede form fulgte af varens egen karakter eller til indsigelserne fra Intersnack om manglende særpræg.

Læs dommen her: *https://www.domstol.dk/media/vncjnltz/dom-af-11-juli-2022-i-bs-19068-2020.pdf*

LegalTech Denmark og en række binavne var i strid med LEGALTECHS rettigheder til sit selskabsnavn efter selskabsloven

Sø- og Handelsretten afsagde den 15. august 2022 dom i sagen BS-37430/2021-SHR mellem LEGALTECH ApS (»LEGALTECH«) som sagsøger og LegalTech Denmark ApS (»LegalTech Denmark«) som sagsøgte. LEGALTECH er et selskab, der har til formål at eje immaterielle rettigheder og udøve virksomhed med handel og service samt aktiviteter i tilknytning hertil. LegalTech Denmark har derimod til formål at drive virksomhed med ydelser inden for informationsteknologi og dermed forbundet virksomhed.

Sagen omhandlede, hvorvidt LegalTech Denmark benyttelse af navnene Legal Tech ApS, LegalTech Denmark ApS, og Copenhagen Legal Tech ApS som selskabsnavn samt LEGALTECH DENMARK som forretningskendetegn er i strid med LEGALTECHs rettigheder efter lovbekendtgørelse nr. 88 af 29. januar 2019 (»den danske varemærkelov«), lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«) og lovbekendtgørelse nr. 1952 af 11. oktober 2021 (»den danske selskabslov«).

Retten fandt, at selskabsnavnene Legal Tech ApS, LegalTech Denmark ApS, Legal Tech Denmark ApS og Copenhagen Legal Tech ApS reelt er identiske med LEGALTECHs selskabsnavn, og at der er en nærliggende risiko for forveksling mellem virksomhederne. Hverken kapitaliseringen af bogstaverne, orddelingen samt tilføjelse af stedbetegnelse i de forskellige selskabsnavne, førte til en anden vurdering. Selskabsnavnene måtte derfor opgives i henhold til selskabslovens § 2, stk. 2, hvorefter et kapitalselskabs navn tydeligt skal adskille sig fra navnet på andre virksomheder.

Vedrørende påstanden om, at LEGALTECH DENMARK som forretningskendetegn er i strid med LEGALTECHs rettigheder efter markedsføringsloven, fandt retten det ikke godtgjort, at LEGALTECH er erhvervsaktiv, eller at der i øvrigt er konkrete og aktuelle planer om erhvervsmæssig aktivitet. LEGALTECH kunne følgelig ikke påberåbe sig rettigheder efter markedsføringsloven.

Sagen er den 12. september 2022 anket til Østre Landsret.

Læs dommen her: *https://domstol.fe1.tangora.com/media/-300011/files/BS-37430-2021-SHR_Dom.pdf*

Sangen »Nede Mette« var en bearbejdelse af det originale værk

Sø- og Handelsretten afsagde den 16. august 2022 dom i sagen BS 27932/2019-SHR mellem personerne A og B, som begge havde været med til at stifte pladeselskabet Flex Music.

Tvisten handlede om rettighederne til musiknummeret »Nede Mette«, der efter udgivelsen opnåede stor succes, og var det mest downloadede og streamede nummer i Danmark i 2016.

Musikværket blev skabt i en oprindelig version af produceren A og forsangeren C i 2012, men først udgivet fire år senere af B, hvorfor A mente, at han var berettiget til minimum 33,33 % af ophavsrettighederne og KODA-indtægterne til musikværket.

Retten kom indledningsvist frem til, at den oprindelige version af sangen fra 2012 var ophavsretligt beskyttet, idet der var tale om et gennemarbejdet værk, der både melodisk og tekstligt havde opnået værkshøjde. Den nye version fra 2016 var således en bearbejdning af det oprindelige musikværk efter § 4 i lovbekendtgørelse nr. 1144 af den 23. oktober 2014 om ophavsret (»den danske ophavsretslov«). Ved vurderingen blev der lagt særlig vægt på skønsmandens udtalelse, hvorefter det var hævet over enhver tænkelig tvivl, at 2016-versionen ikke kunne være skabt uden et indgående kendskab til 2012-udgaven.

Da A ikke havde samtykket til bearbejdelsen, var der tale om en krænkelse af A's ophavsret til 2012-versionen af musikværket. På den baggrund måtte A som udgangspunkt have et økonomisk krav mod B. Der var dog ikke nedlagt særskilt påstand om erstatning, hvorfor retten alene skulle tage stilling til ophavsretskrænkelsen.

Ophavsretskrænkelsen kunne imidlertid ikke føre til, at A's påstande, der, som de forelå, tilsigtede at fastslå en procentuel andel af ophavsrettighederne og KODA-indtægterne for A til 2016-udgaven af »Nede Mette«, kunne tages til følge.

Læs hele dommen her: *https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-27932-2019-SHR.pdf*

Nordtronic A/S har handlet i strid med markedsføringsloven ved at sælge visse af deres produkter under betegnelsen »Patented«

Sø- og Handelsretten afgjorde ved kendelse den 16. august 2022 i sag BS-13969/2022-SHR, at mærkningen af produkter som »Patented« var i strid med § 3 om god markedsføringsskik og § 20 om vildledende handelspraksis i lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«).

Genstanden for søgsmålet, Nordtronic A/S' (»Nordtronic«) lamper, havde tidligere været patenteret, og var i forbindelse hermed blevet fysisk mærket med »Patented«. Lamperne havde dog ikke været beskyttet som patent eller som brugsmodel siden den 14. september 2021.

Retten fandt, at en mærkning med betegnelsen »Patented«, uden at produktet var egentligt patenteret, udgjorde uberettiget anvendelse af betegnelsen, hvorfor det var egnet til at vildlede forbrugeren og skade Nordtronics konkurrenter. Dette var henset til, at betegnelsen kunne give det indtryk, at produkterne nød særlig beskyttelse, og på baggrund heraf foretrækkes frem for lignende produkter.

Betegnelsen var således vildledende og i strid med god markedsføringsskik, hvorfor der af retten blev udstedt påbud om tilbagekaldelse af alle lamper med mærkningen, såvel som et forbud mod at producere, markedsføre, sælge, importere og eksportere de omtvistede produkter.

Læs kendelsen her: *https://domstol.fe1.tangora.com/media/-300011/files/BS-13969-2022-SHR_-_Kendelse.pdf*

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


Bird & Bird

Nathalie Lindes Sjölander, Associate,
och Nicole Lundström, Trainee

Vissa frågor relaterade till upphovsrättsintrång och beräkning av skälig ersättning, PMT 13244-21

Patent- och marknadsöverdomstolen (PMÖD) avgjorde den 10 juni 2022 ett mål avseende upphovsrättsligt skyddade verk och olovlig spridning. Frågan i målet gällde vidare ersättning för sådant nyttjande som skett av verken. Domstolen prövade även om tillgängliggörandet av verken på internet inneburit en kränkning av upphovsmannens respekträtt.

Käranden instämde i Patent- och marknadsdomstolen (PMD) att domstolen skulle förplikta Stockholms stad att betala ersättning för nyttjandet av hans två dokumentärfilmer. Filmerna hade under perioden 2009 – 1 februari 2016 tillgängliggjorts på Stockholms stadsmuseums webbplats. Käranden menade även att filmerna spridits till tredje part och att hans anseende skadats genom att filmerna tillgängliggjorts på ett annat sätt och till en betydligt bredare krets än vad som varit den ursprungliga avsikten.

PMD började med att diskutera huruvida filmerna utgjorde verk så som det kommer till uttryck i 1 § lag (1960:729) om upphovsrätt till litterära och konstnärliga verk (upphovsrättslagen) och om de i sådana fall var upphovsrättsligt skyddade. Domstolen konstaterade att filmerna utgjorde verk och således åtnjöt ett upphovsrättsligt skydd och att Stockholms stads nyttjande därmed inneburit intrång i upphovsmannens upphovsrätt till filmerna. Vid beräkning av den skäliga ersättningen för utnyttjandet (54 § upphovsrättslagen) ansåg PMD att den skulle sättas till 15 000 kr per film vilket var betydligt lägre än vad käranden i första hand yrkat. PMD ansåg inte att det skett ett intrång i den ideella rätten.

Käranden överklagade domen och yrkade att hans talan avseende skälig ersättning och skadestånd skulle bifallas i dess helhet, eller i andra hand det belopp som domstolen fann skäligt. Stockholms stad motsatte sig ändring av PMD:s dom. Det var i PMÖD inte längre tvistigt att filmerna utgjorde upphovsrättsligt skyddade verk. Frågan som domstolen istället skulle bedöma var påståenden om ytterligare ett fall av spridning och fråga om upphovsmannen var berättigad ytterligare ersättning för nyttjandet. Även frågan om skadestånd på grund av kränkning av respekträtten bedömdes.

PMÖD fastslog att bedömningen av vad som utgör skälig ersättning ska utgå från principer som fastslagits av Högsta domstolen i NJA 2019 s. 3. Däri framgår att beräkningen ska utgå från en så kallad ”*hypotetisk licensavgift*” som innebär att ersättningen fastställs som om det på förhand hade träffats ett avtal om ersättning för en upplåtelse av rätten att förfoga över verket på det sätt som faktiskt har skett. Eftersom det råder fri prissättning på licensmarkanden för dokumentärfilmer åberopade käranden dels vittnen till stöd för sitt yrkande, dels en prisguide. PMÖD fann att den åberopade bevisningen gav stöd för att avgiftsprinciperna var etablerade i branschen och att en tillämpning av dessa skulle innebära ett överstigande av yrkandena i målet. Domstolen biföll därför kärandens yrkande och beslutade om ersättning fullt ut. PMÖD gjorde samma bedömning som PMD i fråga om intrång i den ideella rätten.

Se avgörandet i dess helhet här: *https://www.domstol.se/patent--och-marknadsoverdomstolen/patent--och-marknadsoverdomstolens-avgoranden/2022/115244/*

Bedömningen av skälig ersättning vid varumärkesintrång, PMT 13188-30

Målet vid Patent- och marknadsöverdomstolen (PMÖD) gällde ett varumärkesintrång avseende ett figurvarumärke för sport- och idrottsaktiviteter i klass 41. Käranden, som tidigare varit ägare av svarandebolaget, är personlig innehavare av det figurvarumärke som dels kärande själv använt under tiden denna ägde svarandebolaget, dels använts av svarandebolaget efter att kärande sålt sina aktier i bolaget. Kärande begärde ersättning för vad kärande menade var ett varumärkesintrång för tiden efter att kärande sålt sina aktier i svarandebolaget.

Vid Patent- och marknadsdomstolen (PMD) hade fastslagits att svarandebolaget var ersättningsskyldig för varumärkesintrång gentemot kärande. Frågorna vid PMÖD efter överklagande av PMDs dom var för vilken tidsperiod som ersättningen skulle utgå samt till vilket belopp den skäliga ersättningen ska bestämmas.

Vad gäller tiden så hade redan vid PMD kostanterats att svarandebolaget hade en tyst licens att nyttja varumärket i vart fall tills kärande inte längre var ägare av bolaget. En

sådan licens måste sägas upp för att en fortsatt användning ska innebära ett intrång i ensamrätten till varumärket. I likhet med PMD fann PMÖD att ersättning endast kan utgå för den tid som löpt efter det att kärande formellt informerat svarande om att användandet av varumärket inte längre är tillåten.

Vad gäller frågan om skälig ersättning så uttalade PMÖD att ersättningen får bestämmas utifrån en samlad värdering av den utredning som förelåg i målet. PMÖD framhöll att mot bakgrund av svarandebolagets egna uppgifter om att figurvarumärket var den mest värdefulla tillgången i rörelsen så framstår den skäliga ersättning som fastställts av PMD som alltför låg. Eftersom varumärket använts under tävlingsarrangemang lät PMÖD antalet deltagare och den startavgift som varje deltagare erlagt vara styrande för bedömningen – om än med viss försiktighet. PMÖD fastställde den skäliga ersättningen för varumärkesintrånget till 45 000 kr, något som kan jämföras med att PMD fastställde att skälig ersättning uppgick till 18 568 kr.

Se avgörandet i dess helhet här: https://www.domstol.se/patent--och-marknadsoverdomstolen/patent--och-marknadsoverdomstolens-avgoranden/2022/115756/

Avslag på ansökan om tilläggsskydd med anledning av att villkoret avseende försäljningsgodkännande i tilläggsskyddsförordningen inte anses uppfyllt, PMÖÄ 12516-21

Klagande hade vid Patent- och marknadsöverdomstolen (PMÖD) överklagat Patent- och registreringsverkets (PRV) avslag av klagandes ansökan om tilläggsskydd för ett visst läkemedel. PRV hade som grund för sitt avslag menat att ansökan inte uppfyllde villkoret i artikel 3.b i Europaparlamentets och rådets förordning (EG) nr 469/2009 av den 6 maj 2009 om tilläggsskydd för läkemedel (tilläggsskyddsförordningen), d.v.s. villkoret avseende försäljningsgodkännande, något även Patent- och marknadsdomstolen (PMD) höll med om.

PMÖD fann i likhet med PMD att handlingarna som legat till grund för ansökan inte ger att det försäljningsgodkännande som finns avser den kombinationsprodukt som det är fråga om i målet. PMÖD ställde sig också frågan huruvida annat underlag än det som legat till grund för ansökan om försäljningsgodkännandet kan tas hänsyn till vid bedömningen. Utifrån rådande praxis, med hänvisning till avgöranden från EU-domstolen, konstaterade PMÖD att det inte finns stöd för att ta hänsyn till annan dokumentation än den som legat till grund för försäljningsgodkännandet för att avgöra vad som utgör produkten enligt försäljningsgodkännandet. Därav fann PMÖD att artikel 3.b i tilläggsskyddsförordningen inte var uppfyllt, varför överklagandet avslogs.

PMÖD har tillåtit överklagande av beslutet. Detta motiveras av att beslutet enligt PMÖD innehåller frågor där det är av vikt för ledning av rättstillämpningen att ett överklagande prövas av Högsta domstolen.

Se avgörandet i dess helhet här: https://www.domstol.se/patent--och-marknadsoverdomstolen/patent--och-marknadsoverdomstolens-avgoranden/2022/118867/


SELMER

Kine Emilie Helgeneseth og Maren Tveten Aalbu

Heving av IT-kontrakt – en redegjørelse av Borgarting lagmannsretts dom i tvisten mellom Statens vegvesen og IBM (Grindgut-saken)

14. oktober i år avsa Borgarting lagmannsrett dom i den såkalte «Grindgut-saken»(LB-2020-82571[1]). Saken gjaldt kunden, Statens vegvesen (SVV), sin rett til å heve IT-kontrakt inngått med leverandøren, International Business Machines AS (IBM). I de fleste komplekse IT-prosjekter oppstår det en eller annen form for uenighet mellom partene. Slike tvister løses vanligvis gjennom forhandlinger eller konfidensiell voldgift, og ender derfor sjeldent opp i alminnelige domstoler. Grindgut-saken er likevel den andre tvisten om heving av IT-kontrakt som de ordinære domstolene har behandlet i løpet av forholdsvis kort tid.

Den første av de to dommene, den såkalte Felleskjøpet-saken, ble avgjort av Eidsivating lagmannsrett 13. juli 2021 (LE-2018-76187-3[2]). Lagmannsretten reverserte tingrettens avgjørelse fullstendig, og konkluderte med at Felleskjøpets heving var urettmessig, herunder at Felleskjøpet hadde hevet for sent. I Grindgut-saken konkluderer Borgarting lagmannsrett blant annet med at SVV hadde hevet for tidlig, og at hevingen derfor ikke var rettmessig. IBM ble tilkjent over 174 MNOK i erstatning med tillegg av sakskostnader.

I skrivende stund er lagmannsrettens dom i Grindgut-saken enda ikke rettskraftig. Dommen er uansett av stor betydning, og reiser spørsmål om hvilke muligheter kunden egentlig har til å heve en IT-kontrakt når det oppstår problemer i prosjektet. I det følgende skal vi se nærmere på denne avgjørelsen.

Sakens bakgrunn

SVV og IBM inngikk den 20. desember 2013 avtale om levering av en IKT-løsning for innkreving av bompenger i Norge («Leveranseavtalen»). Partene inngikk samtidig tre andre avtaler: én om drift og forvaltning, én om videreutvikling og konsulentbistand og én om finansiering («Finansieringsavtalen»). Prosjektet fikk navnet «AutoPASS Grindgut». Leveranseavtalen var basert på IT-kontraktstandarden PS2000, mens drift- og forvaltningsavtalen og videreutviklings- og konsulentbistandsavtalen var basert på statens standardavtaler (SSA-D, SSA-F, SSA-U og SSA-B).

IBMs løsning for AutoPASS Grindgut var basert på en løsning som allerede var tatt i bruk i tre andre byer. Grindgut-prosjektet var imidlertid mer komplisert enn de tidligere bompengeprosjektene. I tilbudet til SVV estimerte IBM likevel å bruke langt færre timer på Grindgut enn på det mest sammenliknbare prosjektet. Prosjektet ble organisert med opptil fem leveransesteder og en offshoreandel på over 70 prosent. I dommen viser lagmannsretten blant annet til utta-

1 Lovdata: *https://lovdata.no/dokument/LBSIV/avgjorelse/lb-2020-82571*

2 Lovdata: *https://lovdata.no/dokument/LESIV/avgjorelse/le-2018-76187-3*

lelser fra sakkyndige vitner om at de aldri hadde kommet over et prosjekt med «*så mange kommunikasjonsledd*» og «*så kompleks organisering*», og at IBM hadde satt opp prosjektet på en slik måte at det «*nærmest ville være umulig å lykkes*».

I Leveranseavtalen var prosjektet delt inn i fire hovedfaser: behovsfase, løsningsbeskrivelsesfase, konstruksjonsfase og godkjenningsfase. Hver hovedfase skulle avsluttes ved en hovedmilepæl (HMP). Hovedmilepælene for løsningsbeskrivelsesfasen (HMP1), konstruksjonsfasen (HMP2) og godkjenningsfasen (HMP3) var satt til henholdsvis 13. februar 2014, 14. oktober 2014 og 19. mars 2015. Fremdriftsplanene inneholdt også tidspunkter for øvrige milepæler i de enkelte fasene, og konstruksjonsfasen inneholdt den første dagbotsanksjonerte milepælen (HMP2.2), som var satt til 8. januar 2015.

Allerede i løsningsbeskrivelsesfasen oppsto det forsinkelser. Løsningsbeskrivelsesfasen tok dobbelt så lang tid som planlagt. Partene ble derfor enige om å endre fristene for HMP2 og HMP3 til 28. april og 13. november 2015, og den første dagbotsanksjonerte milepælen HMP2.2 til 4. september 2015.

Etter at løsningsbeskrivelsen ble godkjent, gikk prosjektet over i konstruksjonsfasen. I denne fasen skulle leveransen utvikles gjennom tre iterasjoner, som alle skulle evalueres av SVV i hvert sitt kontrollpunkt (KP1, KP2 og KP3). Allerede i konstruksjonsfasen hadde IBM problemer med å få opp produktiviteten på ønsket nivå, og når leveransene i den første iterasjonen ble kontrollert (KP1), viste det seg at IBM bare hadde levert halvparten av det som var planlagt. KP1 ble aldri formelt godkjent av SVV.

Heller ikke KP2 ble godkjent av SVV. Begrunnelsen var at testrapporten hadde mangler, IBM hadde levert mindre enn avtalt av løsningen og at fremdriftsplanen var urealistisk. IBM bestred denne underkjenningen, og viste blant annet til at IBM ville prioritere å levere resterende innhold til et nytt kontrollpunkt, kalt 2.5.

Tvisten om YTvunderkjenningen av KP2 ledet til at SVV den 22. juni 2015 fremsatte hevingsvwarsel. Det ble gjort gjeldende at Leveranseavtalen kunne heves med grunnlag i både inntrådt vesentlig mislighold og antesipert vesentlig forsinkelse. SVV hevet Leveranseavtalen og tilhørende avtaler den 27. juli 2015. IBM mente at hevingen var uberettiget, og dermed utgjorde et vesentlig mislighold. IBM valgte derfor selv å heve Leveranseavtalen og de øvrige avtalene.

Staten v/Samferdselsdepartementet (SVV) reiste den 29. mars 2016 søksmål mot IBM med krav om erstatning. IBM tok til motmæle og krevde vederlag fra staten. Oslo tingrett avsa dom 31. januar 2020 (TOSLO-2016-51424), og konkluderte med at SVVs heving var urettmessig.

Staten anket dommen til Borgarting lagmannsrett, som i likhet med tingretten konkluderte med at SVV

ikke hadde rett til å heve, verken på grunnlag av inntrådt vesentlig mislighold eller antesipert vesentlig forsinkelse. Lagmannsretten tilkjente også IBM vederlag og erstatning.

SVV kunne ikke heve på grunnlag av vesentlig mislighold

1. Hevingsvarselet som ramme

Lagmannsretten starter sin vurdering av om SVV kunne heve på grunnlag av inntrådt vesentlig mislighold med å se på hvilke rammer hevingsvarselet satte for de forhold SVV kunne påberope som hevingsgrunn.

Etter en gjennomgang av Leveranseavtalens ordlyd og øvrige rettskilder, legger lagmannsretten til grunn at hevingsvarselet må «*identifisere og konkretisere alle forholdene som påberopes som hevingsgrunn slik at adgangen til retting blir reell*», og at det som et alminnelig kontraktsrettslig prinsipp «*ikke er adgang til å påberope andre forhold som hevingsgrunn enn de som er påberopt i hevingsvarselet*».

Lagmannsretten er imidlertid av den oppfatning at dette kan stille seg annerledes hvis partene «*har en felles forståelse av hvilke konkrete feil som foreligger*», eller hvis det er «*tale om presisering av samme forhold eller hvis de nye forholdene påberopes innen rimelig tid*». Lagmannsretten er derfor enig med staten i at det er relevant å se hen til hva SVV skrev til IBM kort tid før og etter at hevingsvarselet ble gitt.

Lagmannsretten går så over til å vurdere hva som fremgår av SVVs hevingsvarsel, og konkluderer med at varselet var «*meget generelt formulert*». Etter en gjennomgang av kommunikasjonen mellom partene fra en måned før til to måneder etter at hevingsvarselet ble gitt, legger imidlertid lagmannsretten til grunn at de forholdene som var påberopt i hevingsvarselet hadde blitt presisert, og at ytterligere forhold hadde blitt tilstrekkelig identifisert og konkretisert til at de kunne påberopes som grunnlag for heving.

De forholdene som kunne påberopes, og som ble påberopt av SVV, var etter dette (i) realistisk gjennomføringsplan, (ii) rapportering om fremdrift og leveranseomfang, (iii) verktøybruk, herunder for konfigurasjonsstyring og kravssporing, (iv) bemanning og organisering, (v) estimering, (vi) innsyn i arkitekturbeslutninger, (vii) helhetlig logisk datamodell, (viii) flytting av innhold, (ix) stans i arbeidet og (x) endringsanmodninger.

2. Terskelen for heving, herunder sondringen mellom hoved- og biforpliktelser

Lagmannsretten vurderer det slik at alle forholdene SVV kunne påberope som hevingsgrunn hadde med IBMs prosjektstyring å gjøre. Lagmannsretten er videre enig med IBM i at prosjektstyringen måtte anses som en biforpliktelse, til tross for at kontrakten var en samspillskontrakt. Det var resultatforpliktelsen som var IBMs hovedforpliktelse etter kontrakten.

I vurderingen av hvilken betydning dette ville ha for SVVs hevingsrett, viser lagmannsretten til at hevingsretten i kontrakten i første rekke var knyttet til resultatforpliktelsen. Lagmannsretten legger likevel til grunn at også brudd på biforpliktelser kan gi hevingsrett, men at det skal en del til for at slike brudd utgjør et vesentlig mislighold. Etter rettens syn er «*prosjektets størrelse*» og «*mengden nedlagte ressurser*» fra leverandørens side momenter som taler for en høy terskel for heving ved brudd på biforpliktelser før levering. Dette gjør seg særlig gjeldende hvis misligholdet av biforpliktelsen «*ikke er til hinder for at resultatforpliktelsen kan oppfylles i tide*».

Lagmannsretten legger videre til grunn at dersom brudd på biforpliktelser ikke kan anses som vesentlige, kan bruddene være relevante ved vurderingen av om det foreligger hevingsrett på annet grunnlag, i dette tilfellet antesipert vesentlig forsinkelse.

Lagmannsretten går så over til å vurdere om de forholdene SVV kunne påberope som hevingsgrunn utgjorde mislighold av kontrakten, og i tilfelle om misligholdet var vesentlig.

3. De påberopte forholdene utgjorde ikke et vesentlig mislighold

Etter en inngående gjennomgang av hvert enkelt forhold som kunne påberopes, konkluderer lagmannsretten med at det kun var IBMs fremdriftsrapportering som utgjorde et mislighold av kontrakten. Fremdriftsrapporteringen var ikke i tråd med bransjestandard, og viste ikke reell fremdrift. Lagmannsretten anser likevel ikke dette som et vesentlig mislighold isolert sett. Misligholdet var bare knyttet til en biforpliktelse, og var ikke til hinder for at IBM kunne oppfylle resultatforpliktelsen i tide.

Lagmannsretten konkluderer derfor med at SVV ikke kunne heve på grunnlag av inntrådt vesentlig mislighold.

En av hovedgrunnene til at lagmannsretten kommer til denne konklusjonen, er at de vurderer de påberopte forholdene ut fra situasjonen på hevingstidspunktet. Lagmannsretten var riktig nok enig med SVV i at IBM ikke hadde oppfylt alle sine forpliktelser, herunder fremsatt en realistisk gjennomføringsplan og bemannet prosjektet riktig. Etter lagmannsrettens syn hadde imidlertid IBM rettet opp i disse forholdene før hevingstidspunktet, eller i hvert fall rettet tilstrekkelig til at IBM kunne oppfylt hovedforpliktelsen i tide.

Lagmannsretten går så over til å begrunne hvorfor SVV heller ikke kunne heve på grunn av antesipert vesentlig forsinkelse.

SVV kunne ikke heve på grunnlag av antesipert vesentlig forsinkelse

1. Terskelen for heving

Lagmannsretten starter sin begrunnelse med å se på beviskravet for antesipert forsinkelse.

Retten viser til PS2000 punkt 6.3.2, som gir en part rett til å heve hvis det er «*klart*» at det vil inntre kontraktsbrudd som vil gi denne parten hevingsrett. Kunden gis videre hevingsrett «*når dagbotperioden har utløpt*», her 100 kalenderdager etter en dagbotsanksjonert milepæl.

Lagmannsretten legger derfor til grunn at SVV bare kunne heve på grunnlag av antesipert vesentlig forsinkelse dersom det ut fra informasjonen på hevingstidspunktet var «*klart*» at IBM ville overskride en dagbotsanksjonert milepæl med mer enn 100 dager.

Etter lagmannsrettens syn tilsier uttrykket «klart» at det kreves mer enn alminnelig sannsynlighetsovervekt. Lagmannsretten viser også til veilederen til PS2000, hvor det angis at det må være «*overveiende sannsynlig*» at en part vil misligholde sine forpliktelser.

Lagmannsretten ser også hen til tilsvarende kontraktstandarder, andre lovregler og alminnelige kontraktsrettslige prinsipper, og konkluderer etter en samlet vurdering med at det kreves «*noe nær visshet for antesipert misligholdt eller at det er noe nær sikkert at et slikt misligholdt vil inntre*».

Dette beviskravet kan, slik retten ser det, oppfylles på to måter: enten ved at leverandøren gir «*et utvetydig tilkjennegivende*» om at det ikke fins noen mulighet for å levere i tide, eller ved en vurdering av informasjonen om planer, aktuell fremdrift og tilgjengelige ressurser på hevingstidpunktet.

Lagmannsretten vurderer det også slik at det eneste som må være «*klart*» er at en dagbotsanksjonert milepæl ville blitt overskredet med mer enn 100 dager. IBM fikk derfor ikke medhold i at hvert trinn i utviklingen frem mot levering måtte vurderes. Lagmannsretten mener likevel at en slik trinnvis tilnærming vil gi en god struktur på totalvurderingen av om IBM ville greid å levere i tide.

Videre legger lagmannsretten til grunn at det kan være et støtteargument i vurderingen av antesipert vesentlig forsinkelse om kunden kommer i en bedre situasjon ved å heve. Dette ble imidlertid ikke ansett for å være tilfellet for SVV. Erstatningskravet ville nemlig ikke ha dekket kostnadene ved en alternativ løsning, og en alternativ løsning ville også tatt lengre tid enn en videreføring av avtalen med IBM.

2. IBM hadde ikke gitt en utvetydig tilkjennegivelse for antesipert forsinkelse

Lagmannsretten går så over til å vurdere statens anførsel om at beviskravet for antesipert forsinkelse var oppfylt ved at IBM hadde gitt et «*utvetydig tilkjennegivende*». I et møte den 8. juni 2015 presenterte IBM to planskisser som viste at HMP2 ville bli flere hundre dager forsinket. Ifølge SVV innebar disse skissene en utvetydig tilkjennegivelse for antesipert vesentlig forsinkelse.

Lagmannsretten er i ikke enig i dette. Retten viser til at det verken av skissene eller referatet fra møtet gikk frem at det «*ikke fantes noen mulighet for å unngå misligholdt*». Planskissene var videre merket med «*draft*», og ble presentert etter oppfordring fra SVV om å redegjøre for hvilke tiltak IBM ville iverksette for å sikre at prosjektet kunne bli realisert. Lagmannsretten så derfor planskissene som et forsøk fra IBMs side på å komme SVV i møte etter at SVV hadde underkjent tidligere planer som urealistiske. Etter rettens syn er det rom for å presentere skisser som forhandlingsutspill uten at dette er en utvetydig tilkjennegivelse for antesipert forsinkelse.

Lagmannsretten konkluderer derfor med at IBM ikke hadde gitt en utvetydig tilkjennegivelse, og at beviskravet for antesipert misligholdt ikke var oppfylt på dette grunnlaget.

3. Det var heller ikke «klart» på hevingstidspunktet at det ville inntre vesentlig forsinkelse

Lagmannsretten går derfor over til å vurdere om det ut fra øvrig informasjon på hevingstidspunktet var «*klart*» at IBM ville overskride en dagbotsanksjonert milepæl med mer enn 100 dager.

Det første lagmannsretten tar stilling til er hvilke milepælsdatoer som må legges til grunn for vurderingen.

Etter de opprinnelige milepælene skulle HMP2 vært nådd 28. april 2015. Den første dagbotsanksjonerte milepælen var HMP2.2, som skulle vært nådd 4. september 2015. Tillagt 100 kalenderdager hadde hevingsfristene blitt henholdsvis 6. august 2015 og 13. desember 2015.

IBM anførte imidlertid at de hadde krav på fristforlengelse og flytting av disse milepælene på grunn av SVVs ferier og påberopte endringsordre, herunder økt kompleksitet (EA053), mer krevende arbeidsform (EA054), IBMs deltakelse i en ekstern arkitekturvurdering bestilt av SVV (EA067) og flytting av personell fra Kina som følge av nye sikkerhetskrav fra SVV (EA078). IBM hadde også fremsatt ytterligere tre endringsanmodninger (EA108, 113 og 117) som forutsatte at SVV urettmessig hadde underkjent kontrollpunkt 2 (KP2).

Lagmannsretten går svært detaljert inn i hver påberopte endringsordre for å vurdere om de gir grunnlag for fristforlengelse og flytting av milepæler. Vurderingene er tett knyttet opp til faktum i saken.

Det er likevel verdt å merke seg lagmannsrettens begrunnelse for hvorfor SVVs underkjennelse av KP2 var urettmessig. SVV begrunnet underkjenningen blant annet med at IBM hadde levert mindre av løsningen enn avtalt. Som vi har vært inne på tidligere, skulle leveransen utvikles og leveres gjennom

tre iterasjoner. IBM hadde imidlertid flyttet en betydelig andel av leveransene fra KP2 til iterasjon 3, og leveransene til KP2 omfattet derfor langt mindre enn det som var avtalt. Lagmannsretten mente imidlertid at SVV hadde blitt bundet ved passivitet til å akseptere denne endrede volumfordelingen. Etter rettens syn hadde nemlig SVV i omkring ett år fått informasjon om disse endringene uten å fremsette umiddelbare innsigelser.

IBM fikk medhold i de aller fleste forholdene som ble påberopt som grunnlag for fristforlengelse og flytting av milepæler, og hovedmilepælene skulle etter lagmannsrettens vurdering vært flyttet med i alt 250 dager. Hevingsfristene (milepælsdatoer med tillegg av 100 dager) ble derfor forskjøvet til 5. april 2016 med utgangspunkt i HMP2 (opprinnelig 6. august 2015) og 12. august 2016 med utgangspunkt i HMP 2.2 (opprinnelig 13. desember 2015). Lagmannsretten mener at det er disse fristene som må legges til grunn ved spørsmålet om antesipert vesentlig forsinkelse fra IBMs side.

Lagmannsretten går så over til å vurdere om det på hevingstidspunktet var «*klart*» at IBM ville overskredet de endrede hovedmilepælene med mer enn 100 dager, noe som ble besvart benektende.

Staten hadde innhentet to sakkyndigrapporter om fremdriften til HMP2. Den første rapporten konkluderte med at IBM ville endt med en forsinkelse på over 400 dager i forhold til den kontraktsfestede HMP2-datoen, uansett scenario, og 418 dager forsinket optimistisk sett. Den andre rapporten konkluderte med at IBM ville blitt 547 dager forsinket i forhold til den kontraktfestede HMP2-datoen. Dersom det tas utgangspunkt i de endrede hovedmilepælene som lagmannsretten la til grunn, ville IBM endt opp med en forsinkelse på 150 dager etter den første rapporten og 297 dager etter den andre rapporten. I begge tilfeller ville SVV hatt rett til å heve.

Lagmannsretten legger imidlertid ikke de sakkyndiges konklusjoner til grunn. Retten foretar i stedet sin egen vurdering med «*utgangspunkt i de sakkyndiges metode*» og i de samme «*trinnene som de sakkyndige*». Ettersom beviskravet for antesipert forsinkelse er strengt, ville ikke beviskravet, etter rettens vurdering, være oppfylt dersom «*IBM realistisk sett kunne ha nådd hevingsfristen*». Det avgjørende var om det kunne latt seg gjøre å nå hevingsfristen i praksis. Retten legger i denne sammenhengen vekt på at IBM i februar 2015 hadde fått en ny testleder, noe som hadde økt produktiviteten i prosjektet. Testlederen forklarte at testproduktiviteten kunne vært økt, ressurser kunne vært omdisponert og det var muligheter for overtids- og helgearbeid.

Med dette som utgangspunkt, mener lagmannsretten at HMP2 alt i alt realistisk sett kunne vært nådd i underkant av 4 måneder før SVV hadde rett til å heve. Lagmannsretten konkluderer derfor med at SVV ikke hadde grunnlag for å heve på grunn av antesipert forsinkelse.

IBM hadde krav på vederlag

Lagmannsretten er altså av den oppfatning at det verken forelå vesentlig mislighold eller antesipert vesentlig forsinkelse, og at SVVs heving av Leveranseavtalen og tilhørende avtaler var urettmessig. IBM hadde derfor rett til å heve avtalene, samt krav på vederlag og erstatning.

Etter en nærmere vurdering kommer lagmannsretten til at IBM hadde krav på vederlag og erstatning under Leveranseavtalen på til sammen MNOK 113, samt vederlag under Finanseringsavtalen på til sammen MNOK 61. IBM fikk imidlertid ikke medhold i sitt krav på avbestillingskompensasjon under avtalene om vedlikehold og drift.

SVV ble også pålagt å dekke IBMs sakskostnader for lagmannsretten tilsvarende MNOK 36 i tillegg til sakskostnadene for tingretten. Lagmannsretten påpeker at kravet var høyt, men at det hadde vært en omfattende og komplisert sak med behov for spesialkompetanse og et større advokatteam.

Det er verdt å merke seg at lagmannsretten er enig med IBM i at de hadde krav på betaling for programvare. Etter lagmannsrettens vurdering følger det av Leveranseavtalen at leverandøren kan velge mellom full betaling for alt som er levert eller å få tilbakelevert programvare mot tilbakebetaling. Ettersom IBM ikke hadde bedt om tilbakelevering av programvare, var SVV forpliktet til å betale.

Lagmannsretten er videre ikke enig med SVV i at IBMs krav på vederlag måtte begrenses til den andelen av løsningen som var utviklet på hevingstidspunket. Lagmannsretten mente at kontraktens ordlyd var klar, og at IBM hadde krav på vederlag for alt utført arbeid målt etter timeforbruket opp til avtalt målpristak.

Lagmannsretten kommer også med noen generelle uttalelser når det gjelder tolkningen av avtalt målpristak. Partene var nemlig uenige om hvordan dette skulle beregnes. Etter lagmannsrettens syn må det, i mangel av klare holdepunkter for en felles forståelse, foretas en objektiv tolkning av kontraktens regulering av målpristaket. Etter en objektiv tolkning var det fremdeles ikke klart og entydig hvordan målpristaket skulle forstås. Ifølge lagmannsretten må denne uklarheten gå utover SVV, som hadde forberedt anbudsgrunnlaget. Det høyeste målpristaket på 130 % ble derfor lagt til grunn.

Viktige «take aways» fra lagmannsrettens dom

Lagmannsrettens 211 sider lange dom illustrerer, i likhet med Felleskjøpet-saken, at det er ekstremt utfordrende for en kunde å heve en IT-kontrakt. Dommen baserer seg på et omfangsrikt faktum fra hele kontraktsperioden og et omfattende

rettskildegrunnlag. Kunden er derfor avhengig av å ha et godt faktisk og juridisk grunnlag før en hevingserklæring fremsettes. Dette er særlig krevende fordi kunden risikerer å miste hevingsretten om man venter for lenge med å heve.

Dommen bygger i stor grad på en tolkning av den konkrete avtalen mellom partene og en vurdering av sakens faktum. Lagmannsretten kommer likevel med interessante uttalelser som kan ha betydning for andre kontraktsforhold.

Dommen illustrerer blant annet at et hevingsvarsel må identifisere og konkretisere alle forhold som påberopes som hevingsgrunn, med mindre partene har en felles forståelse av hvilke konkrete feil som foreligger. Hovedregelen er at man ikke kan heve på grunn av andre forhold enn de som er påberopt i hevingsvarselet. Det er likevel rom for å presisere samme forhold eller påberope seg nye forhold innen rimelig tid etter hevingsvarselet. I denne saken ble som nevnt to måneder ansett som rimelig tid.

Dommen viser også at det kan ha betydning om det påberopte misligholdet relaterer seg til leverandørens hovedforpliktelse eller biforpliktelse. Resultatforpliktelsen ble ansett som leverandørens hovedforpliktelse, mens prosjektstyringen ble ansett som en biforpliktelse. Biforpliktelser kan gi hevingsrett, men det skal en del til. Prosjektets størrelse og mengden nedlagte ressurser fra leverandørens side taler for en høy terskel for heving. Dette gjør seg særlig gjeldende hvis misligholdet av biforpliktelser ikke er til hinder for at resultatforpliktelsen kan oppfylles i tide. Brudd på biforpliktelser som ikke er å anse som vesentlige, kan imidlertid være relevante ved vurderingen av om det foreligger hevingsrett grunnet antesipert vesentlig forsinkelse.

Videre viser dommen betydningen av prosjektets utvikling. Hevingsretten vurderes ut fra situasjonen på hevingstidspunktet. Tidligere problemer og utfordringer er bare relevante dersom de fortsatt gjør seg gjeldende på hevingstidspunktet. Kritikkverdige forhold er altså ikke av betydning dersom de har blitt rettet, og heller ikke dersom de har blitt rettet i en slik grad at leverandøren kunne ha oppfylt hovedforpliktelsen i tide.

Når det gjelder adgangen til å heve som følge av antesipert vesentlig forsinkelse, oppstiller lagmannsretten et særlig strengt beviskrav. Det kreves noe nær visshet for antesipert mislighold eller at det er noe nært sikkert at et slikt mislighold vil inntre. Dersom det ikke kan «*utelukkes*» at leveransen kunne vært ferdig på et tidligere tidspunkt, eller dersom det «*realistisk sett*» kunne latt seg gjøre å rekke fristen, er det ikke grunnlag for å heve. Hvorvidt dette beviskravet er oppfylt, beror på en konkret vurdering av planer, aktuell fremdrift og tilgjengelige ressurser på hevingstidspunktet. Det er også relevant å se hen til om det forelå forseringsmuligheter. Videre vil det være et støtteargument i retning av antesipert vesentlig forsinkelse dersom kunden kommer i en bedre situasjon ved å heve.

Beviskravet kan også oppfylles ved at leverandøren gir en utvetydig tilkjennegivelse av at det ikke finnes noen muligheter for å levere i tide. Lagmannsretten legger imidlertid en høy terskel til grunn for at leverandøren kan anses for å ha gitt en slik tilkjennegivelse. En presentasjon fra leverandørens side av mulige scenarioer er ikke tilstrekkelig.

Til sist illustrerer dommen betydningen av at endringsanmodninger og -ordre er riktig vurdert før kontrakten heves. Leverandøren kan nemlig få medhold i krav på fristforlengelse og flytting av milepæler, noe som igjen resulterer i at tidspunktet for når det vil være tale om en vesentlig forsinkelse vil kunne bli forskjøvet. Dersom en leverandør har fremsatt en rekke endringsanmodninger med tilhørende forskyvning av milepæler, bør altså kunden ta dette i betraktning i vurderingen av om det er tale om en antesipert vesentlig forsinkelse.

Det blir spennende å følge en eventuell ankebehandling av Grindgut-saken, og om Høyesterett vil bidra til rettsavklaring når det gjelder kundens adgang til å heve en IT-kontrakt.

Skrevet av Kine Emilie Helgeneseth, advokat i avdelingen HITEK i Advokatfirmaet Selmer, Oslo og Maren Tveten Aalbu, advokatfullmektig i samme avdeling.
Takk til praktikant Øystein Kolstad Kvalø for gode bidrag.

Gorrissen Federspiel

Tue Goldschmieding

Kommissionen fremsætter forslag til forordning om cyberrobusthed for at give sikrere hardware- og softwareprodukter

EU-Kommissionen fremsatte den 15. september 2022 et forslag til en ny forordning om cyberrobusthed, der har til formål at beskytte forbrugere og virksomheder mod produkter med utilstrækkelige sikkerhedselementer. Baggrunden for forslaget er det stigende antal af cyberangreb, der har vist, hvor vigtigt det er, at infrastrukturen beskyttes for at fremtidssikre EU's økonomi og samfund.

Forordningen, der er den første af sin art, indfører obligatoriske cybersikkerhedskrav for produkter med digitale elementer i hele deres livscyklus. Derudover vil forordningen øge fabrikanternes ansvar ved at forpligte dem til at understøtte deres produkters sikkerhed og levere softwareopdateringer for at afhjælpe konstaterede sårbarheder. Forordningen sikrer også, at forbrugerne nu får tilstrækkelige oplysninger om cybersikkerheden i deres produkter.

Den foreslåede forordning skal finde bred anvendelse, og vil gælde for alle produkter, der enten direkte eller indirekte er forbundet med en anden enhed eller et netværk. Dog undtages de produkter, der allerede er underlagt cybersikkerhedskrav i henhold til allerede eksisterende EU-regler, f.eks. inden for medicinsk udstyr, luftfart og biler.

Europa-Parlamentet og medlemsstaterne skal nu drøfte forslaget efter den almindelige lovgivningsprocedure, inden det endeligt kan vedtages.

Læs pressemeddelelsen her: *https://ec.europa.eu/commission/presscorner/detail/da/ip_22_5374*

Læs forslaget til forordningen her: *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0454*

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

Gorrissen Federspiel

Tue Goldschmieding

Nyt krav om mærkning af retoucherede reklamebilleder kan være på vej

Det danske Erhvervsministerium sendte den 5. juli 2022 et lovforslag om ændring af lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«) i høring.

Efter gældende ret begrænses brugen af retoucherede reklamebilleder udelukkende af markedsføringslovens bestemmelser om god skik og vildledning.

I et forsøg på at skærpe reglerne, foreslås at følgende bestemmelse indsættes i markedsføringsloven:

§ 11 c. En erhvervsdrivende, der i sin handelspraksis anvender retoucherede reklamebilleder, hvor kroppens facon, størrelse eller hud er ændret, skal mærke billederne, jf. stk. 2.

Stk. 2. Erhvervsministeren fastsætter nærmere regler om, hvordan reklamebilleder skal mærkes, herunder eventuelle undtagelser til mærkningspligten.

Hvis lovforslaget vedtages, stilles der således i fremtiden krav om, at annoncører skal gøre forbrugeren opmærksom på, at der anvendes retoucherede/redigerede billeder i deres reklamer. Det vil være den danske Forbrugerombudsmand, der foretager vurderingen af, hvorvidt en reklame er retoucheret og dermed omfattet af den nye mærkningsordning.

Mærkningsordningen skal skabe gennemsigtighed omkring anvendelsen af retoucherede billeder, og reducere børn og unges eksponering for urealistiske kropsidealer. Mærkningspligten skal dog ikke begrænses til reklamer rettet mod børn og unge.

Erhvervsministeren forventer, at lovændringen træder i kraft den 1. juli 2023.

Læs lovforslaget her: *https://prodstoragehoeringspo.blob.core.windows.net/822325f1-6a07-42ee-859e-ec633894bb09/Lattergas-%20og%20markedsf%C3%B8ringslov%20-%20h%C3%B8ring%20juli%202022.pdf*

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

Ønsker alle

God jul og godt nytt år!

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