Lov & Data

Nr. 154
Juni 2023
Nr. 2/2023

Innhold










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.lod.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 2023
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

EU-Domstolen gør op med, hvornår pseudonymiserede data skal betragtes som personoplysninger

Tue Goldschmieding

I en nylig afgørelse har Retten kastet lys over et centralt spørgsmål inden for databeskyttelse - hvornår skal pseudonymiserede data anses for at være personoplysninger?

Rettens afgørelse af 26. april 2023, i sag T-557/20 mellem SRB og EDPS, fastslår at, hvis en datamodtager ikke har midlerne til at genidentificere den registrerede person, vil pseudonymiserede data ikke blive betragtet som personoplysninger. Retten præciserede også, at personlige synspunkter og meninger ikke automatisk kan anses for at være personoplysninger; der kræves en konkret vurdering i hver enkelt sag.

Sagen opstod som følge af en aktionærundersøgelse, hvor Single

Resolution Board (SRB) via en elektronisk formular indsamlede synspunkter og meningstilkendegivelser, som blev delt med et konsulentfirma. SRB havde, for at beskytte respondenternes identitet, erstattet navnene ved hjælp af alfanumeriske koder. Afkodningsnøglen, der kunne knytte koderne til individuelle respondenter, blev ikke delt med konsulentfirmaet.

Efter en række klager fra respondenter i undersøgelsen vurderede Den Europæiske Tilsynsførende for Databeskyttelse (EDPS), at SRB havde delt pseudonymiserede personoplysninger uden at informere de berørte personer om denne deling. SRB appellerede afgørelsen til Retten og argumenterede for, at de delte data ikke opfyldte betingelserne for at være personoplysninger i henhold til GDPR. For at kvalificere sig som personoplysninger efter GDPR skal data "relatere" sig til en fysisk person, og denne person skal være "identificeret eller identificerbar". SRB appellerede til Retten og afviste EDPS' afgørelse om, at de delte undersøgelsesdata opfyldte disse kumulative betingelser.

Retten præciserede, i tråd med Breyer-sagen (C-582/14), at vurderingen af, om data er pseudonymiserede eller anonymiserede, skal tage højde for omstændighederne hos den part, der er i besiddelse af dataene.

Retten fandt, at hvis datamodtageren ikke har yderligere afkodningsoplysninger, der gør det muligt at genidentificere de registrerede personer, og ikke har nogen retlige midler til at få adgang til sådanne oplysninger, kan de delte data betragtes som anonymiserede og derfor ikke som persondata. Det faktum, at dataafsenderen har midler til at genidentificere de registrerede personer, er irrelevant og betyder ikke, at de delte data automatisk også er persondata for modtageren. Retten fastlog, at selvom personlige synspunkter og meninger kan udgøre personoplysninger, kan de ikke per automatik formodes at indeholde personoplysninger. En konkret vurdering fra sag til sag er nødvendig for at afgøre, om et synspunkt eller en udtalelse faktisk er knyttet til en identificerbar person.

Denne afgørelse fra Retten er et opgør med den hidtidige praksis under både databeskyttelsesdirektivet og -forordningen, og giver en række perspektiver på, hvordan vi skal forstå sikkerhedsforanstaltninger, som både pseudonymisering, anonymisering og kryptering. Det er samtidig vigtigt at have for øje, at vi står ved begyndelsen af en spændende rejse, hvor teknologien hastigt udvikler sig, og nye metoder til genidentifikation kan opstå. Afgørelsen skaber et spændende grundlag for at følge, hvordan den teknologiske udvikling kan forme databeskyttelseslovgivningen og vores forståelse af pseudonymisering. Hvad der i dag anses for at være tilstrækkeligt pseudonymiserede data, kan i fremtiden måske nemt genidentificeres.

Tue Goldschmieding

Retten til å protestere mot behandling av personopplysninger etter personvernforordningen artikkel 21 (1)

Av Melissa Tveit

1. Innledning

Den teknologiske utviklingen gjør det mulig for både private og offentlige aktører å benytte seg av personopplysninger i sitt arbeid i større grad enn tidligere. Teknologien har endret det økonomiske og sosiale liv, noe som krever en sterk og mer sammenhengende ramme for vern av personopplysninger. Den økende kapitaliseringen av personopplysninger har aktualisert et behov for å tydeliggjøre hvilke rettigheter de registrerte kan gjøre gjeldende overfor virksomheter som behandler personopplysningene deres. Personvernforordningen inneholder derfor en rekke rettigheter som den registrerte kan vise til overfor den behandlingsansvarlige. En av disse rettighetene er retten til å protestere mot behandling etter artikkel 21 (1). Bestemmelsen lyder slik:

«Den registrerte skal til enhver tid, av grunner knyttet til vedkommendes særlige situasjon, ha rett til å protestere mot behandling av personopplysninger om vedkommende, og som har grunnlag i artikkel 6 nr. 1 bokstav e) eller f) … Den behandlingsansvarlige skal ikke lenger behandle personopplysningene, med mindre vedkommende kan påvise at det foreligger tvingende berettigede grunner for behandlingen som går foran den registrertes interesser, rettigheter og friheter, eller for å fastsette, gjøre gjeldende eller forsvare rettskrav».

Retten til å protestere mot en behandling er en mekanisme den registrerte kan bruke til å rette opp i skjevhet i interesser som har oppstått under behandlingen. Den har derfor har en viktig rolle i å sikre at

Melissa Tveit

de grunnleggende prinsippene i GDPR overholdes. I denne artikkelen skal jeg se nærmere på hva som er forutsetningene for og konsekvensene av at en registrert fremsetter en protest til en behandlingsansvarlig.

2. Prosessuelle forutsetninger for å protestere

Det oppstilles ingen formkrav i personvernforordningen til selve protesten. Ordlyden tilsier derfor at protesten kan fremsettes både skriftlig og muntlig. Begjæringen trenger ikke å tituleres «innsigelse», «protest» e.l., så lenge den registrerte gjør det klart for den behandlingsansvarlige at man ønsker å bringe behandlingen til opphør.

Personvernforordningen stiller ikke krav om hvor eller hvordan den registrerte kan fremsette en protestbegjæring. Protesten kan derfor fremsettes til hvilken som helst del av organisasjonen.[1] Protesten må likevel aktivt fremsettes – det er ingen automatikk i at en behandling opphører fordi det har gått lang tid.

Behandlingen må imidlertid ha startet for at den registrerte skal kunne protestere. Det er ikke mulig å protestere i forveien og anføre at den behandlingsansvarlige ikke skal behandle personopplysninger i fremtiden.[2] Når behandlingen har startet, indikerer ordlyden at protestretten kan benyttes for så lenge som behandlingen fortsatt finner sted.

> Personvernforordningen stiller ikke krav om hvor eller hvordan den registrerte kan fremsette en protestbegjæring. Protesten kan derfor fremsettes til hvilken som helst del av organisasjonen. Protesten må likevel aktivt fremsettes – det er ingen automatikk i at en behandling opphører fordi det har gått lang tid.

Den registrerte vil i praksis ikke ha muligheten til å protestere om vedkommende ikke kjenner til protestretten. En nødvendig betingelse for at protestretten skal være reell, er derfor at den registrerte blir informert den.[3] Den behandlings-

1 ICO (2019) s. 113.

2 Öman (2021) s. 379.

3 C-201/14 avsnitt 33.

ansvarlige har derfor en plikt etter personvernforordningens artikkel 13 og 14 til å fremlegge informasjon om en rekke av forordningens rettigheter, blant annet om retten til å protestere.

GDPR oppstiller også krav til hvordan informasjon om protestretten skal gis den registrerte. Etter artikkel 12 (1) skal den behandlingsansvarlige «treffe egnede tiltak for å framlegge for den registrerte informasjonen nevnt i artikkel 13 og 14». Bestemmelsen spesifiserer at informasjonen skal gis på en «kortfattet, åpen, forståelig og lett tilgjengelig måte og på et klart og enkelt språk». Den behandlingsansvarlige skal unngå generelle og abstrakte formuleringer som «may», «might», «some», «often» og «possible».[4] Etter artikkel 21 (4) følger det at informasjonen skal fremlegges «atskilt fra annen informasjon». Dette kan eksempelvis gjøres ved å ha lagvise personvernerklæringer, hvor det første laget inneholder den informasjonen som har størst betydning for den registrerte og som kan overraske dem.[5]

Etter personvernforordningens artikkel 12 (2) skal den behandlingsansvarlige også «legge til rette» for at den registrerte kan utøve en rekke rettigheter, herunder retten til å protestere. Andre bestemmelser i forordningen stiller krav til konkrete tiltak. Artikkel 21 (5) bestemmer at den registrerte kan protestere «ved hjelp av automatiserte midler ved bruk av tekniske spesifikasjoner» i forbindelse med bruk av «informasjonstjenester». Dette kan for eksempel gjøres ved å ha en «opt-out»-lenke i en direkte markedsføringsepost.

3. Materielle vilkår for å protestere

For at den registrerte skal kunne protestere, må vedkommende for det første protestere på bakgrunn av grunner knyttet til vedkommendes «særlige situasjon», jf. GDPR artikkel 21 (1). Videre må behandlingen ha rettslig grunnlag i artikkel 6 (1) (e) eller (f).

Ordlyden av «nødvendig» gir anvisning på at noe må være uunnværlig, og at formålet ikke kan nås på en annen måte. Hensynet til dataminimering etter artikkel 5 (1) (c) må også tas i betraktning; ikke bare må databehandlingen i seg selv være nødvendig, men omfanget av data som behandles må være i tråd med formålet med behandlingen.[6] Metoden den behandlingsansvarlige velger må derfor være formålstjenlig, effektiv og proporsjonal, samt ikke medføre et unødvendig inngrep i den enkeltes privatliv.[7]

Som nevnt er det bare behandling etter artikkel 6 (1) (e) og (f) den registrerte kan protestere på. Behandling etter artikkel 6 (1) (e) kan skje hvor det er «nødvendig for å utføre en oppgave i allmennhetens interesse» eller for å «utøve offentlig myndighet som den behandlingsansvarlige er pålagt».

At behandlingen må være «pålagt» den behandlingsansvarlige, gir anvisning på at det må foreligge en rettslig forpliktelse til å foreta behandlingen. Det er ikke klart etter den norske språkversjonen hvilken del av bestemmelsen «pålagt» retter seg mot. Det må derfor avklares om «pålagt» både retter seg mot de tilfeller hvor det utføres en oppgave i «allmennhetens interesse» og de tilfellene hvor man «utøve[r] offentlig myndighet».

Konsultasjon av andre språkversjonene av GDPR gir heller ikke et entydig svar på spørsmålet. Den engelske og den franske språkversjonen tilsier at «pålagt» bare retter seg mot offentlig myndighetsutøvelse, mens den danske språkversjonen tyder på det motsatte.

Litteraturen er sprikende, men systemhensyn tilsier at «pålagt» kun retter seg mot offentlig myndighetsutøvelse. Det følger av artikkel 6 (3) at grunnlaget for behandling etter bokstav (e) skal fastsettes av unionsretten eller medlemsstatenes lov. Det er derfor ikke tilstrekkelig at vilkårene i 6 (1) er oppfylt - behandlingen må også ha hjemmel i nasjonal rett eller i EU-retten. Det foreligger derved allerede to sikkerhetsmekanismer – den behandlingsansvarlige må ha hjemmel, og det må være nødvendig å benytte seg av behandlingsgrunnlaget.

At «pålagt» rettet seg mot oppgaver som utføres i «allmennhetens interesse» ville også gjøre nødvendighetskriteriet overflødig. Dersom behandlingen både må være pålagt, samtidig som det skal foretas en nødvendighetsvurdering, risikerer den behandlingsansvarlige å måtte bryte med pålegget dersom man kommer frem til at behandlingen ikke er nødvendig. Et pålegg kan derfor sees på som at lovgiver selv har foretatt og vurdert tilfeller hvor behandling av personopplysninger er nødvendig. Dette tilsier at «pålagt» ikke retter seg mot oppgaver som utføres i «allmennhetens interesse». De fleste forhold taler for at dette er den riktige løsningen.

Hva en behandling i «allmennhetens interesse» er, defineres ikke i GDPR. Ordlyden tilsier imidlertid at behandlingen må være begrunnet i en større samfunnsinteresse. En minoritet av befolkningen kan utgjøre «allmennhetens interesse» dersom det er en ubestemt krets av personer.[8] Det er antatt at interessen skal være «regulert i nasjonale regler som kan håndheves offentligrettslig, og ikke utelukkende være underlagt privatrettslig håndheving.»[9] Interessen kan imidlertid ikke komme fra et tredjeland – det er eksempelvis ikke tilstrekkelig at personopplysningene blir etterspurt av myndighetene i et tredjeland for en etterforskning som

4 WP29 (2018) s. 9.
5 Jarbekk (2021) note 2 til artikkel 12.
6 Krzysztofek (2021) s. 92.
7 Öman (2021) s. 175.
8 Schartum (2020) s. 131.
9 Skullerud (2019) s. 182.

tjener en offentlig interesse som indirekte også eksisterer i lovgivningen til et medlemsland.[10]

Dersom det er i allmennhetens interesse, kan rettssubjektet også være underlagt regler som håndheves privatrettslig.[11] Behandlingen kan i de tilfellene utføres av private aktører. Dette er tilfellet ved eksempelvis forskning, som gjennomføres av både av offentligrettslige og privatrettslige aktører.

Artikkel 6 (1) (e) er også anvendelig for behandling som er «nødvendig for å utøve offentlig myndighet». Ettersom det bare er de tilfellene hvor utøvelsen av offentlig myndighet er «pålagt», betyr det at oppgaver som følger av kontraktsrettslige forpliktelser, selv i den offentlige interesse, faller utenfor.[12] Behandlingsgrunnlaget er også anvendelig hvor private rettssubjekter har fått kompetanse til å utøve offentlig myndighet og derfor treffer enkeltvedtak på vegne av det offentlige.[13]

Etter artikkel 6 (1) (f) er behandlingen lovlig dersom den er «nødvendig for formål» knyttet til de «berettigede interessene» som forfølges av den behandlingsansvarlige eller en tredjepart med mindre den registrertes «interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn».

Forordningen definerer ikke hva som utgjør en «berettiget interesse». Det er imidlertid ikke noe krav om at den må være tvingende.[14] Både behandlingsansvarliges og tredjepersoners interesser omfattes, noe som betyr at man kan ta i betraktning mer generelle samfunnshensyn. Vurderingen kan oppsummeres i tre krav: Interessen må være lovlig, tilstrekkelig klart formulert slik at interessen kan veies mot den registrertes interesser og grunnleggende rettigheter, og den må representere en reell og nåværende interesse.[15]

EU-domstolen har i sin praksis trukket frem utlevering av personopplysninger i forbindelse med erstatningssaker, beskyttelse av eiendom og sunnhet og liv som legitime interesser.[16] Andre normsystemer må tas i betraktning ved vurderingen, og bestemmelsen skal blant annet tolkes og anvendes i lys av de grunnleggende menneskerettighetene.[17]

Et særskilt spørsmål er om rene økonomiske interesser kan utgjøre en «berettiget interesse». WP29-gruppen anla en lav terskel for at noe skal anses som en «berettiget interesse» etter DPD artikkel 7 (1) (f), og rene kommersielle interesser ble anerkjent etter direktivet. Ettersom det tilsynelatende ikke er noen materielle endringer ved videreføringen av denne delen av bestemmelsen, tilsier det at det samme gjelder etter GDPR.

Systemhensyn tilsier at kommersielle interesser kan utgjøre en legitim interesse, ettersom en balansetest vil sikre at usaklige interesser må vike. De berettigede interessene utgjør derfor et startpunkt, heller enn en kvalitativ grense, for hvilke interesser som inngår i balansevurderingen.[18] Man unngår på denne måten at vurderingen av «berettigede interesser» foregriper balansevurderingen.

Utgangspunktet er at dersom det foreligger en «berettiget interesse», er behandlingen lovlig. Dette gjelder imidlertid bare «med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger» jf. artikkel 21 (1) annet punktum.

Ordlyden av «interesser» tilsier at alt med tilknytning til den registrerte kan tas i betraktning. Det fremgår av fortalens punkt 47 at det kan tas hensyn til de «registrertes rimelige forventninger på grunnlag av forholdet mellom den og den behandlingsansvarlige». Domstolen har i forbindelse med forgjengerbestemmelsen i DPD uttalt at «anvendelse av artikkel 7 (f) nødvendiggjør en avveining av de motstridende rettighetene og interessene som er berørt, og i denne sammenheng må det tas hensyn til betydningen av den registrertes rettigheter som følger av artikkel 7 og 8 i Charteret».[19] Det er imidlertid mer enn selve personopplysningsvernet som omfattes av den registrertes «fundamentale rettigheter», som for eksempel negative effekter for ytringsfrihet, religionsfrihet og bevegelsesfrihet.[20] Også den registrertes subjektive opplevelser og forventninger til behandlingen kan vurderes.[21]

Dersom «den registrertes interesser eller grunnleggende rettigheter» tilsier at behandling ikke skal finne sted, må disse avveies mot den behandlingsansvarliges og tredjeparters «berettigede interesse[r]». Det skal foretas en forholdsmessighetsvurdering av interessene i saken, og avveiningen skal ta utgangspunkt i omstendighetene i den konkrete sak.[22] Balanseringen må være genuin, og den skal verken veie til fordel for den registrerte eller behandlingsansvarlige.[23]

Det neste vilkåret for å protestere mot behandling av personlig data er at protesten knytter seg til den registrertes «særlige situasjon». Ordlyden tilsier at det må foreligge individuelle forhold knyttet til den enkelte registrerte som begrunner protestbegjæringen. I vurderingen

10 Krzysztofek (2021) s. 90.
11 Skullerud (2022) note til artikkel 6.
12 Kotschy (2020) s. 335.
13 Skullerud (2019) s. 182.
14 WP29 (2014) s. 30.
15 WP29 (2014) s. 25.
16 C-13/16, C-92/09 og C-212/13.
17 C-131/1 avsnitt 68.
18 WP29 (2014) s. 25.
19 Se C-131/12 avsnitt 74.
20 Schartum (2020) s. 133.
21 Schartum (2020) s. 133.
22 C-13/16 Rīgas satiksme.
23 WP29 (2014) s. 3.

Illustrasjon: Colourbox.com

kan man ta hensyn til alle spesifikke omstendigheter i den registrertes situasjon.[24] Situasjonen må verken være tungtveiende, viktig eller ekstraordinær.[25] Det stilles ikke krav om at den registrerte har fått ny kunnskap – det er tilstrekkelig at den registrerte bedømmer saksforholdet på en annen måte enn tidligere.[26] Det må imidlertid gis en individuell begrunnelse for protesten, og generelle betraktninger som at noe er skadelig, galt eller umoralsk kan ikke føre frem.[27]

Ettersom det er den registrertes oppfatning av situasjonen som er utgangspunktet for protest, tilsier dette at den registrertes «særlige situasjon» ikke må kunne dokumenteres eller sannsynliggjøres. Vekten av den registrertes «særlige situasjon» vil uansett avhenge av vurderingen av de «tvingende berettigede grunner» som tilsier at behandlingen skal fortsette.[28] Hensynet til dataminimering i artikkel 5 (1) (c) tilsier imidlertid at man ikke bør avdekke unødvendig informasjon om personlige forhold for å begrunne situasjonen.

4. Konsekvenser av at den registrerte har protestert

Utgangspunktet etter artikkel 21 (1) annet punktum er at «den behandlingsansvarlige ikke *lenger skal behandle personopplysningene*» dersom den registrerte har protestert og den behandlingsansvarlige ikke kan godtgjøre at det foreligger tvingende berettigede grunner som går foran den registrertes interesser, rettigheter og friheter. Den registrerte kan også kreve behandlingen begrenset etter artikkel 18 (1) (d) før protesten er vurdert.

Dersom den registrerte protester og vilkårene for videre behandling ikke er oppfylt, må behandlingen avbrytes dersom den allerede er igangsatt.[29] Utgangspunktet er derfor at den registrerte *skal* gis medhold med mindre grunnlag for videre behandling foreligger.[30]

Det følger imidlertid av artikkel 21 (1) at behandling likevel kan fortsette eller igangsettes igjen hvor den behandlingsansvarlige kan «påvise at det foreligger tvingende berettigende grunner» for behandlingen og disse går foran den registrertes «interesser, rettigheter og friheter». For det andre kan den behandlingsansvarlige fortsette behandlingen for å «fastsette, gjøre gjeldende eller forsvare et rettskrav».

Den legitime interessen må være «overwhelming and override the data subject's interests in a strong, significant way.»[31] Vilkåret nødvendiggjør en individuell vurdering av hvor betydelige interessene, rettighetene og frihetene til den registrerte er og i hvilken grad de krenkes dersom behandlingen fortsetter.[32]

Det fremgår ikke av 21 (1) annet punktum *hvordan* vurderingen skal

24 C-398/15 avsnitt 47
25 Skullerud (2020) s. 263.
26 Schartum (2020) s. 198
27 Schartum (2020) s. 198
28 Schartum (2020) s. 198.
29 Skullerud (2019) s. 159.
30 Skullerud (2019) s. 263.
31 Zanfir-Fortuna (2020), s. 517.
32 Krzysztofek (2021) s. 184.

foretas, men det slås fast at den behandlingsansvarlige kan nekte å imøtekomme protesten dersom et av unntaksvilkårene foreligger. Ettersom vurderingen i artikkel 21 (1) annet ledd er modellert på artikkel 6 (1) (f), kan det tenkes at man kan se hen til WP29 sin veileder knyttet til DPD artikkel 7 for å få en idé om hvordan vurderingen bør foretas.[33] Begge bestemmelser gir anvisning på en balanseringsøvelse, og vurderingstemaet er som utgangspunkt sammenfallende.

Legitime hensyn etter veilederen er b.la. interessenes aktverdighet, virkningen for den registrerte, en generell avveining av hensynene i saken og hvilke sikkerhetstiltak som iverksettes for behandlingen. Ettersom protestretten er nært knyttet til menneskerettighetene i Charterets artikkel 7 og 8, er det også naturlig at man kan la seg veilede av vurderingen til EMD og EU-domstolen knyttet til disse bestemmelsene.[34] Balanseringen må imidlertid gjøres på sak-til-sak basis.[35]

Det må likevel tas hensyn til de særlige hensyn som gjør seg gjeldende for artikkel 21 (1). Balanseringen i artikkel 21 har et større fokus på den konkrete konteksten i den registrertes situasjon sammenliknet med artikkel 6 (1) (f).[36] Også bestemmelsenes ulike formål må tas i betraktning. Behandling etter artikkel 6 (1) (f) har til hensikt å forhindre urettferdig databehandling og foretas før behandlingen har startet. Balanseringen i artikkel 21 (1) skal avhjelpe ubalanse som har oppstått under behandlingsaktiviteten.[37]

Det er den behandlingsansvarlige som må påvise at det foreligger «tvingende berettigede grunner» som går foran den registrertes interesser eller grunnleggende rettigheter og friheter.[38] Den behandlingsansvarlige må derfor fremføre argumenter for at interessene som taler for videre behandling veier tyngst i forholdsmessighetsvurderingen. Dette er en materiell endring fra bestemmelsens forgjenger i DPD. Etter DPD artikkel 14 (1) kunne den registrerte protestere «dersom innsigelsen er berettiget». Etter personvernforordningen er utgangspunktet det motsatte – behandlingen opphører, med mindre den behandlingsansvarlige fremfører «tvingende berettigede grunner» for behandlingen. Bevisbyrden er i så måte endret fra å påhvile den registrerte til å nå påhvile den behandlingsansvarlige, noe som kan gjøre det lettere for den registrerte å få medhold i protesten.

Det må foretas en forholdsmessighetsvurdering mellom den de «tvingende berettigede grunner» og den registrertes «interesser, rettigheter og friheter» ved protest både hvor behandlingen bygger på artikkel (6) (e) og (f). Hvor behandlingen bygger på artikkel 6 (1) (f), har den behandlingsansvarlige allerede foretatt en forholdsmessighetsvurdering mellom den registrertes og den behandlingsansvarliges interesser. Ordlyden av «tvingende berettigede grunner» i artikkel 21 (1) annet punktum tilsier at terskelen er høyere for at den behandlingsansvarlige kan fortsette behandlingen etter en protest sammenliknet med iverksetting av behandling. Den behandlingsansvarlige må derfor foreta en ny balanseøvelse, og kan ikke nøye seg med å vise til vurderingen etter 6 (1) (f). Balansetesten etter artikkel 21 (1) annet punktum tar hensyn til den registrertes subjektive forestillinger og til de spesielle argumentene den registrerte har fremsatt, heller enn generelle vurderinger slik som er tilfellet etter artikkel 6 (1) (f).

En ekstra vurdering er viktig ettersom protesten kan fremsettes på et mye senere tidspunkt enn behandlingens startpunkt. Både den behandlingsansvarliges interesser og den registrertes interesser kan derfor ha utviklet seg siden første vurdering. Behandlingen kan eksempelvis ha innvirket på den registrertes personvern på en måte som ikke var forventet da behandlingen startet eller nødvendigheten av behandlingen kan ha endret seg.

Behandlingen kan også fortsette for å «fastsette, gjøre gjeldende eller forsvare et rettskrav». Ordlyden sier ikke noe om hvem som må inneha rettskravet eller hvem som er rettighetssubjekt. Dette virker å være et bevisst valg, ettersom det følger av fortalepunkt 10 at «[n]år det gjelder behandling av personopplysninger for å oppfylle en rettslig forpliktelse (…) bør medlemsstatene kunne opprettholde eller innføre nasjonale bestemmelser for nærmere å presisere anvendelsen av reglene i denne forordning». Det er derfor den nasjonale retten som bestemmer når vilkåret er oppfylt. Etter fortalens punkt 52 gjelder dette uansett om det skjer innenfor rammen av rettergang eller en administrativ eller utenrettslig prosedyre.

> Oppsummeringsvis kan det sies at konsekvensene av protesten avhenger av den behandlingsansvarliges konklusjon.

En potensiell konsekvens er at personopplysningene må slettes. I behandlingsbegrepet inngår også lagring av data.[39] Hvor den registrerte får medhold i en protest som gjelder lagring, vil det vil da være nødvendig å slette personopplysningene. Etter forordningens artikkel 17 (1) (c) har også behandlingsansvarlig en «plikt til å slette person-

33 Det siktes her til WP29 (2014).
34 Ausloos (2020) s. 285.
35 Ausloos (2016)
36 Ausloos (2020) s. 296.
37 Ausloos (2020) s. 295
38 Fortalepunkt 69.
39 Se artikkel 4 nr. 2.

opplysninger uten ugrunnet opphold» dersom registrerte protesterer mot behandlingen i henhold til artikkel 21 nr. 1 og det «ikke finnes mer tungtveiende berettigede grunner til behandlingen».

Personvernforordningen definerer ikke hva sletting innebærer, men ordlyden tilsier en permanent fjerning av personopplysningene. Dette vil også være resultatet hvor den registrerte protesterer på lagring etter artikkel 21 (1). I de tilfellene hvor den registrerte får medhold i en protest knyttet til behandlingsoperasjoner som ikke er lagring, er det ingen automatikk i at personopplysningene slettes.

Oppsummeringsvis kan det sies at konsekvensene av protesten avhenger av den behandlingsansvarliges konklusjon. Dersom den behandlingsansvarlige gis medhold i sin protest, skal behandlingen straks opphøre. Dersom den registrerte ikke gis medhold, må den behandlingsansvarlige enten kunne «påvise at det foreligger tvingende berettigede grunner for behandlingen som går foran den registrertes interesser, rettigheter og friheter» eller for å «fastsette, gjøre gjeldende eller forsvare rettskrav» for å fortsette behandlingen.

Litteraturliste

Litteratur

Bøker

Ausloos (2020) — Ausloos, Jef. *The Right to Erasure in EU Data Protection Law*. Oxford, Oxford University Press, 2020. Conditions of the Right to Erasure | The Right to Erasure in EU Data Protection Law | Oxford Academic (uio.no)

Kotschy (2020) — Kotschy, Waltraut. *«Article 6 Lawfulness of processing» I The EU General Data Protection Regulation (GDPR): A Commentary Oxford: Oxford University Press USA 2020*

Krzysztofek (2021) — Krzysztofek, Marius. *GDPR: Personal Data Protection in the European Union,* Vol. 114, European Monographs Series Set. Alphen Aan Den Rijn: Wolters Kluwer, 2021

Öman (2021) — Öman, Sören. *Dataskyddsförordningen (GDPR) m.m.* (2. utgave). Stockholm, Norstedts Juridik, 2021.

Schartum (2020) — Schartum, Dag Wiese. *Personvernforordningen – en lærebok*. Bergen: Fagbokforlaget, 2020.

Skullerud (2019) — Skullerud, Åste Marie Bergseng, Cecilie Rønnevik, Jørgen Skorstad og Marius Engh Pellerud. *Personopplysningsloven og personvernforordningen (GDPR): Kommentarutgave.* (1. utg.), Oslo: Universitetsforlaget, 2019.

Zanfir-Fortuna (2020) — Zanfir-Fortuna, Gabriela. "Article 21. Right to object". I *The EU General Data Protection Regulation (GDPR): A Commentary* Oxford: Oxford University Press USA 2020

Artikler og lovkommentarer

Ausloos (2016) — Ausloos, Jef. *The Interaction between the Rights to Object and to Erasure in the GDPR,* 2016 The Interaction between the Rights to Object and to Erasure in the GDPR - CITIP blog (kuleuven.be)

Jarbekk (2021) — Jarbekk, Eva. «*Karnov lovkommentar til personopplysningsloven*.» (2021), [Lest i Lovdata Pro] hentet 16.11.2022.

Skullerud (2022) — Skullerud, Åste Marie Bergseng, Cecilie Rønnevik, Jørgen Skorstad og Marius Engh Pellerud. «Personopplysningsloven og personvernforordningen (GDPR): Kommentarutgave.», (2022) [Lest på Juridika.no] hentet 22.11.22

Traktater

Personverndirektivet	Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger [Personverndirektivet].

Avgjørelser fra EU-domstolen

Joined cases C-92/09 and C-93/09 Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen	ECLI:EU:C:2010:662
Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González	ECLI:EU:C:2014:317
Case C-212/13 František Ryneš v Úřad pro ochranu osobních údajů	ECLI:EU:C:2014:2428
Case C-201/14 Smaranda Bara and Others v Casa Națională de Asigurări de Sănătate and Others	ECLI:EU:C:2015:638
C-13/16 Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde mod Rīgas pašvaldības SIA «Rīgas satiksme»	ECLI:EU:C:2017:336

Retningslinjer og rapporter

WP29 (2014)	Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf
WP29 (2018)	Article 29 Working Party Guidelines on transparency under Regulation 2016/679 https://ec.europa.eu/newsroom/article29/items/62222
ICO (2019)	Information Commissioner's Office, Guide to Data Protection, 2019 https://ico.org.uk/media/for- organisations/guide-to-data-protection-1-1.pdf (sist sjekket 16.11.2022)

Melissa Jacobsen Tveit, Vit.ass. ved Nordisk Institutt for Sjørett.

Nytt förslag om långsiktig reglering av forskningsdatabaser

Av Katarina Fast Lappalainen

Projekt som bygger på analys av stora datamängder (big data) spelar idag en framträdande roll inom medicinsk forskning. Sverige är väl positionerat genom de medicinska register och befolkningsregister som byggts upp under lång tid. Forskningen har bidragit till att förbättra människors hälsa och till att rädda liv.

Frågan är emellertid hur dessa tillgångar kan och bör tillvaratas på ett mer effektivt och hållbart sätt samt hur en forskningsinfrastruktur för framtiden bör byggas. Det finns flera utmaningar, såsom en fragmenterad hälso- och sjukvård, något som till stor del är en konsekvens av decentralisering och privatisering. Forskningsdatabaserna med sina enorma uppgiftssamlingar innebär samtidigt ett potentiellt hot mot den personliga integriteten och säkerhetsriskerna kan vara stora.

Den svenska lagstiftaren har länge brottats med regleringen av området. En särskild utmaning har varit förutsättningarna för prospektiva forskningsdatabaser, d.v.s. databaser där underlag samlas in för framtida forskning. Påtagliga brister uppdagades i samband med det s.k. ”LifeGene-fallet” som utspelade sig i början av 2010-talet och som blev upprinnelsen till flera utredningar och ny lagstiftning.

För närvarande gäller den tidsbegränsade lagen (2013:794) om vissa register för forskning av vad arv och miljö betyder för människors hälsa, den s.k. *LifeGene-lagen*.[1] Lagen har förlängts vid flera tillfällen och gäller för närvarande fram till 2024-01-01.

1 Prop. 2012/13:163.

Katarina Fast Lappalainen

Sedan lagen infördes har två offentliga utredningar genomförts – Registerforskningsutredningen (SOU 2014:45) och Forskningsdatautredningen (SOU 2018:36) – utan att någon ny lagstiftning kommit till stånd. I slutet av 2022 presenterades ett nytt förslag i en departementspromemoria (Dnr. U2022/04089). Förslaget bygger på de två tidigare utredningarna.

Inledningsvis ges en bakgrund till LifeGene-lagen, följt av en sammanfattning av det nya förslaget. Avslutningsvis lämnas ett antal kritiska synpunkter på förslaget.

Bakgrunden till LifeGene-lagen

LifeGene är ett pågående nationellt projekt som leds och koordineras av Karolinska Institutet (KI). Syftet är samla in data som ska ligga till grund för kommande forskningsprojekt om arv, miljö och hälsa. Denna databas är ämnad att bidra till ökad kunskap om de vanligaste folksjukdomarna, såsom hjärt- och kärlsjukdomar och cancer samt hälsoproblem, t.ex. allergier och infektioner. Detta antas leda till förbättrad diagnostik, behandling och sjukdomsförebyggande rekommendationer i framtiden. I LifeGene-projektet har sedan 2009 uppgifter samlats in från totalt över 52 000 deltagare, av vilka blod, serum och urin från 29 500 deltagare finns lagrade i KI:s biobank.[2]

I samband med starten sökte KI ett etikgodkännande för projektet. Ansökan godkändes – med undantag för blodprov på barn under 6 år – av en regional etikprövningsnämnd. Karolinska överklagade beslutet till den centrala etikprövningsnämnden (CEPN).

> En särskild utmaning har varit förutsättningarna för prospektiva forskningsdatabaser, d.v.s. databaser där underlag samlas in för framtida forskning.

CEPN kom i ett beslut 2011 fram till att LifeGene inte omfattades av etikprövningslagen och att ett godkännande därför inte kunde lämnas. Skälet till detta var att det inte var fråga om ett konkret forskningsprojekt utan om en uppbyggnad av forskningsinfrastruktur för framtida forskning.[3]

Integritetsskyddsmyndigheten (IMY) fick upp ögonen för projektet och inledde tillsyn. IMY fann att ändamålet inte var tillräckligt precist

2 Se hemsidan för LifeGene: *https://lifegene.se* (hämtad i maj 2023).

3 Centrala etikprövningsnämnden, beslut 2011-03-04, dnr Ö 28-2010.

enligt den då gällande personuppgiftslagen och förelade LifeGene att upphöra med insamlingen av personuppgifter. IMY konstaterade också att insamling för framtida forskning borde bli föremål för särskild reglering.[4] Lagstiftaren grep därefter in och införde *LifeGene-lagen*.[5]

Nytt förslag om en forskningsdatabaslag

Enligt förslaget ska vissa forskningsdatabaser regleras genom en ny ramlag som kompletterar den allmänna dataskyddsförordningen (GDPR).[6] Omfattas gör sådana databaser som byggs upp med de registrerades samtycke och som främst består av personuppgifter vilka samlats in från de registrerade eller med deras aktiva medverkan.[7] Vidare ska databasen vara av karaktäriseras att den är eller har potential att bli en ”central forskningsdatabas”, d.v.s. antas vara av särskilt värde för forskningen i ett långsiktigt perspektiv.[8] Det innebär att den inte endast ska vara till för de projekt som forskningshuvudmannen ansvarar för utan rikta sig till andra forskningsprojekt, såväl nationella som internationella.[9]

Utveckling och förvaltning av forskningsdatabaser ska endast vara möjligt inom universitet och högskolor vid vilka forskning bedrivs och som har rätt att utfärda examen på forskarnivå, vilka bedöms ha den kapacitet som krävs för att kunna bedriva sådan verksamhet.[10]

Personuppgiftsbehandlingen anses ske för vetenskapliga forskningsändamål och den rättsliga grunden för denna är utförande av uppgift av allmänt intresse. Samtycke från de registrerade utgör därmed inte en rättslig grund utan en skyddsåtgärd enligt art. 9 GDPR.[11]

Lagen är som nämnts konstruerad som en ramlag. Vilka forskningsdatabaser som omfattas får bestämmas av regeringen i förordning. Ett lärosäte som vill skapa en ny forskningsdatabas måste därför ”väcka” frågan om reglering hos Regeringskansliet. Regeringen bör vid behov inhämta synpunkter från berörda myndigheter, såsom Vetenskapsrådet och IMY.[12]

Lagen ska vidare innehålla generella bestämmelser om vilka uppgifter som får ingå i en forskningsdatabas. Det är emellertid regeringen som i förordning ska bestämma vilka personuppgifter som får behandlas i det enskilda fallet. Genetiska uppgifter och uppgifter om lagöverträdelser får endast behandlas om regeringen tillåter detta. Regeringen får även begränsa vilka personuppgifter som får ingå i övrigt.[13]

De ändamål för vilka personuppgifter får behandlas i en databas ska enligt förslaget uttömmande regleras i lagen. Tillåtna primära ändamål är 1) att skapa underlag för framtida forskningsprojekt inom för forskningsdatabasen angivna forskningsområden och 2) att lämna ut uppgifter för sådana forskningsprojekt. Möjligheten att använda en forskningsdatabas för sekundära ändamål är begränsade till vissa specifika situationer, t.ex. för utredning om eventuell oredlighet i forskning eller för att fullgöra uppgiftsskyldighet enligt lag eller förordning.[14]

Lagen tillåter utlämnande från databasen till forskning som har fått etikgodkännande. Detta gäller även forskning som ska utföras i ett annat land, så länge som denna har granskats och godkänts enligt ett motsvarande förfarande som det svenska.[15] Även i denna fråga kan regeringen föreskriva begränsningar av vad som får lämnas ut.[16] Vid utlämning ska personuppgifter som huvudregel vara pseudonymiserade eller skyddade på något annat likvärdigt sätt.[17]

Den föreslagna lagen ställer också krav på att forskningshuvudmannen ska säkerställa integritetsskyddet. Det är fråga om krav på att t. ex. dokumentera elektronisk åtkomst och kontrollera att obehörig åtkomst inte har skett.[18]

Ett centralt fokus i lagen är den registrerades insyn och kontroll beträffande sina uppgifter i forskningsdatabasen. Ett viktigt inslag i detta är att den registrerade ska få utförlig information innan ett samtycke till medverkan i forskningsdatabasen lämnas. Den registrerade ska även löpande informeras om det efter registreringen sker en kompletterande insamling från andra källor, något som den registrerade även ska kunna motsätta sig. Möjligheterna till s.k. *opt-out* är betydande och det ska vara möjligt för den enskilde att när som helst få sina uppgifter raderade. Registrerade som var underåriga vid tidpunkten för registrering, ska när de uppnår myndighetsåldern om 18 år ska informeras om registreringen.[19]

Det finns redan särskilda sekretessbestämmelser i 24 kap. offentlighets- och sekretesslagen, den s.k. *LifeGene-sekretessen*, vilka ska anpassas och utvidgas enligt det nya förslaget. Fråga är om absolut sekretess, d.v.s. ingen skade- eller menprövning görs. Däremot ska det vara möjligt att bryta sekretessen vid allvarliga brott.[20]

4 Datainspektionens beslut (numera IMY) 2011-12-16, dnr 766-2011.
5 Prop. 2012/13:163.
6 En långsiktig reglering av forskningsdatabaser, Promemoria 2022-12-23, Utbildningsdepartementet, Dnr. U2022/04089, s. 122 ff (härefter ”promemorian”).
7 Ibid. s. 114 f.
8 Ibid. s. 97.
9 Ibid. s. 197.
10 Ibid. s. 128 ff.
11 Ibid. s. 140, s. 169.
12 Ibid. s. 287.
13 Ibid. s. 225.
14 Ibid. s. 141 ff.
15 Ibid. s. 198.
16 Ibid., s. 197 ff.
17 Ibid., s. 211.
18 Ibid. s. 196 ff.
19 Ibid., s. 114 f., s. 164 ff.
20 Ibid. s. 245 ff.

En ändring i statistiksekretessen föreslås också för att göra det möjligt för forskningshuvudmännen att ansöka om befogade kompletteringar av databasen genom en rätt att få ut uppgifter från vissa myndigheters register.[21]

Förslaget innebär också att lagen om rättspsykiatriskt forskningsregister upphävs och därmed sammanhängande sekretessbestämmelser. Skälet till detta är att detta register inte har uppdaterats på mer än femton år och nyligen har avvecklats.[22]

Om förslaget genomförs kommer lagen att träda ikraft i januari 2024. Vidare föreslås en övergångsbestämmelse som innebär att samtycke från dem som redan är registrerade i en befintlig forskningsdatabas före lagens ikraftträdande, inte behöver hämtas in.[23]

Avslutningsvis lämnas ett förslag till förordning om vissa forskningsdatabaser, närmare bestämt LifeGene och Tvillingregistret.[24]

Lagtekniska synpunkter och grundlagsenlighet: hur mycket bör regeringen bestämma?

Utredningens förslag har fått viktiga synpunkter av flera remissinstanser. Ett kritiserat inslag i förslaget är att regeringen ges en betydande makt att i förordningsform besluta om vilka forskningsdatabaser som ska få utvecklas. Ett varningens finger för politisering har framförts.[25]

Det kan ifrågasättas hur detta ansökningsförfarande överensstämmer med principen om att föreskrifter ska vara generella, då dessa kommer att träffa enskilda databaser. Det framstår som oklart om det är fråga om ett normbeslut eller ett förvaltningsbeslut. Möjligheten att påverka beslut i enskilda fall rörande forskningsdatabaser, som kan innefatta såväl risk- som lämplighetsbedömningar, begränsas därmed påtagligt då beslut genom förordning inte kan överklagas. En lösning som diskuterades i utredningen och som lyfts fram i remissrundan, är att dessa beslut istället borde fattas av en expertmyndighet, vars beslut kan överklagas.[26]

Konstruktionen med en ramlag med generell reglering och mer specifik reglering avseende de aktuella forskningsdatabaserna i förordningsform framstår således inte som självklar. Risken är vidare att reglering genom förordning kan öka komplexiteten på ett redan komplext rättsområde, vilket i förlängningen kan leda till svårigheter att överblicka regleringen och de likabehandlingsproblem som kan bli följden av detta.

I förslaget anges vidare att 2 kap. 6 § regeringsformen (RF) som reglerar skyddet för den personliga integriteten och som säger att var och en gentemot det allmänna är skyddad mot betydande intrång i den personliga integriteten om det sker utan samtycke, inte skulle vara tillämplig på den aktuella lagen eftersom den kommer att kräva samtycke och medverkan från de enskilda om att ingå forskningsdatabasen.

Denna tolkning kan problematiseras, då ett stort antal äldre personuppgifter som redan finns i de aktuella databaserna enligt de övergångsbestämmelser som föreslås inte omfattas av kraven på information och samtycke. Detta kan framstå som praktiskt lämpligt för förvaltarna av forskningsdatabaser, men med tanke på att betydande mängder uppgifter kan ha samlats in under lång tid, så framstår det inte som en rimlig tolkning av 2 kap. 6 § RF att databaser som innehåller sådana uppgifter bör regleras i förordningsform. Flera databaser kan ha inlett sin insamling av personuppgifter för länge sedan och kan innehålla data hänförligt till ett mycket stort antal personer. En forskningsdatabas som enligt förslaget ska regleras i förordning, det s.k. Tvillingregistret inrättades redan på 1960-talet.[27] En reglering enligt lag framstår härvid som nödvändig om skyddet för den personliga integriteten ska upprätthållas på ett tillfredsställande sätt, då samtycke från dessa individer kanske inte erhållits från första början och det inte heller är rimligt från en praktisk synvinkel att kräva att samtycke samlas in och löpande information om kompletteringar lämnas beträffande dessa.

Problematisering kring kretsen av de registrerade med anledning av EU-domstolens praxis

Samtycke och medverkan från de registrerade är centrala inslag i den föreslagna regleringen. I det här sammanhanget finns det skäl att med anledning av EU-domstolens praxis diskutera hur stor kretsen av de registrerade ska vara. Av EU-domstolens storkammardom från 2022 i mål C-184/20, *OT, Vyriausioji tarnybinės etikos komisija,* framgår att även indirekta personuppgifter kan utgöra särskilda kategorier av personuppgifter enligt art. 9 GDPR. I den meningen skulle den enskilde kunna vara indirekt registrerad i en forskningsdatabas.

I det aktuella fallet kan databaser innehålla genetisk information som omfattas av detta stadgande i GDPR, vilket innebär att även andra än den registrerade skulle kunna anses vara indirekt registrerade om de delar gener med den registrerade, t.ex. barn till denne. Innebär denna dom att samtycke och samverkan behöver ska även i förhållande till dessa personer? Denna dom behöver därför analyseras i det här avseendet och frågan är givetvis hur långt det i så fall är rimligt eller möjligt att föra detta krav på indirekt

21 Ibid. s. 263 ff.
22 Ibid. s. 239 ff.
23 Ibid. s. 275 ff.
24 Ibid. s. 227 f.
25 Remissvar av den 2022-12-28 från Göteborgs universitet, dnr. GU 2022/3947.
26 Promemorian s. 226.
27 Ibid. s. 97.

skydd. Härvid måste en bedömning göras i förhållande till såväl proportionalitetsprincipen som principen om uppgiftsminimering i artikel 5 i GDPR. Kan det innebära att särskilda skyddsåtgärder måste företas?

Hur ska ändamålet med en forskningsdatabas bestämmas?

Att genomföra en lämplig ändamålsbestämning för forskningsdatabaser framstår som en utmaning. Icke desto mindre torde det faktum att ett godkännande av Etikprövningsmyndigheten krävs innebära att en praxis i det här avseendet kommer att utvecklas. Det förutsätter att myndigheten får de resurser som krävs för att kunna fatta skyndsamma beslut som kan hålla hög kvalitet. I annat fall kan detta hämma forskning och utveckling. Uppföljning och kontroll av att ändamålet för forskningsdatabaser följs, är även en fråga för IMY som också kommer att kunna bidra med både praxis och vägledning på sikt.

> I det aktuella fallet kan databaser innehålla genetisk information som omfattas av detta stadgande i GDPR, vilket innebär att även andra än den registrerade skulle kunna anses vara indirekt registrerade om de delar gener med den registrerade, t.ex. barn till denne.

Ansvaret för forskningsdatabaser

Ansvaret för forskningdatabaser bör enligt förslaget vila på lärosätena som anses både besitta den kompetens som finns och ha siktet inställt på den långsiktighet som krävs. Av förslaget framgår inte närmare vad det innebär om en forskningsdatabas utvecklas av ett lärosäte eller ett privat forskningsföretag.

Det ställer vidare stora krav på att upprätthålla en hög informationssäkerhet. Läckor beträffande hälsodata och andra känsliga kategorier av data som skulle kunna inträffa om säkerheten inte i tillräckligt hög grad kan upprätthållas för forskningsdatabaserna, kan få förödande konsekvenser för enskilda och förtroendet för forskningen. Den s.k. Vaastamo-läckan i Finland 2020 är ett varnande exempel härpå. Med tanke på det rådande geopolitiska läget kan det även finnas ”*threat actors*” med skilda motiv. Det tarvar ytterligare analys. Till bilden hör att EU:s direktiv om åtgärder för en gemensam cybersäkerhetsnivå för hela unionen, det s.k. NIS2-direktivet, som ska ha implementerats i nationell rätt senast i oktober 2024, kan komma att omfatta universitet- och högskolor (se dir. 2023:30).

IMY har t.ex. tidigare kritiserat säkerheten beträffande LifeGene i ett beslut 2015, där bl.a. känsliga personuppgifter lämnades ut över öppet nät efter autenticering med endast användarnamn och lösenord.

I detta sammanhang finns det anledning att lyfta fram behovet av en tydlig lagstiftningsstrategi för forskningsinfrastruktur som driver på utbyggnaden av en säker sådan. Enligt utredningen om organisation, styrning och finansiering av forskningsinfrastruktur (SOU 2021:65) ansågs det lämpligt att samla det övergripande ansvaret för forskningsinfrastruktur av nationellt intresse i en myndighet, vilket är en idé som skulle kunna analyseras vidare i denna kontext.

Det europeiska hälsodataområdet

Ny lagstiftning inom EU är på gång som innebär att vidareutnyttjande av ”forskningsdata” och ”särskilda känsliga kategorier av data” ska kunna ske i allt större utsträckning, bl.a. i syfte att möjliggöra innovation som kan bidra till att förbättra människors hälsa. Den nya regleringen i dataförvaltningsakten (DFA), som trädde i kraft i juli 2022 och som ska tillämpas fr.o.m. september 2023, innehåller regler om sekundäranvändning. Forskningsorganisationer omfattas inte av denna, men DFA sätter upp en generell ram som ska stödja uppbyggnaden och utvecklingen av europeiska dataområden, varav hälsodataområdet är det första.

> Frågan är därför om den ordning som föreslås verkligen kommer att leda till att uppbyggnaden av nya och utvecklingen av befintliga prospektiva forskningsdatabaser och därmed möjliga framsteg inom den medicinska forskningen.

Ett förslag till förordning om ett europeiskt hälsodataområde lämnades av kommissionen våren 2022, vilken har en liknande struktur som DFA. I detta förslag är uppbyggnaden av offentlig vidareutnyttjandestruktur ett väsentligt inslag, i vilket det t.ex. ingår att bygga upp s.k. ”säkra behandlingsmiljöer” och gemensamma kontaktpunkter på nationell och EU-nivå (*one-stop-shop*). Av särskild relevans är möjlighet att utbyta och dela data för forskningsändamål samt upprättandet av ett förfarande för att möjliggöra s.k. dataaltruism. Hur förslaget om forskningsdatabaser står sig i förhållande till förslaget om ett europeiskt hälsodataområde bör analyseras närmare innan ett slutligt förslag

lämnas. Detta har inte analyserats i förslaget.

Slutord

Avslutningsvis, kan konstateras att förslaget är angeläget, men behäftat med vissa brister som kräver ytterligare utredning. Detta gäller i synnerhet regeringens makt över forskningsdatabaserna, vilket kan vara problematiskt både ur ett konstitutionellt och politiskt perspektiv. Det kan också diskuteras hur detta påverkar den akademiska friheten i Sverige.

Det ”ansökningsförfarande” som föreslås, d.v.s. att lärosätet måste väcka frågan om reglering av den databas som önskas planeras, framstår som komplext.

Frågan är därför om den ordning som föreslås verkligen kommer att leda till att uppbyggnaden av nya och utvecklingen av befintliga prospektiva forskningsdatabaser och därmed möjliga framsteg inom den medicinska forskningen.

Katarina Fast Lappalainen,*Universitetslektor i rättsinformatik, Institutet för rättsinformatik, Juridiska institutionen, Stockholms universitet*

Illustrasjon: Colourbox.com

Når vil kameraovervåking fange opp særlige kategorier av personopplysninger?

Av Ove A. Vanebo

Innledning

EUs personvernforordning 2016/679 av 27. april 2016 (heretter bare kalt «forordningen») regulerer bruk av personopplysninger også ved kameraovervåking. Et særlig spørsmål er når slik overvåking innebærer behandling av «særlige kategorier» av personopplysninger, som er opplysninger listet opp i forordningen artikkel 9 nr. 1. Særlige kategorier av personopplysninger nyter et særlig vern, og er i utgangspunktet forbudt å behandle med mindre det finnes et unntak for behandlingen.

Tradisjonelt sett har det vært lagt til grunn at filmopptak kun fanger opp særlige kategorier av personopplysninger dersom dette er *formålet* med behandlinger, jf. blant annet Personvernrådets retningslinjer.[1] I en interessant artikkel i Lov & Data nr. 1/23 problematiserer juristene Hanne Pernille Gulbrandsen, Steinar Østmoe og Ole-Martin Moe fra Deloitte Advokatfirma (i fellesskap omtalt som «Deloitte-juristene») denne tilnærmingen.[2]

Bakgrunnen er at EU-domstolens rettspraksis i sak C-184/20 av 1. august 2022 kan forstås som at kameraopptak må sies å inneholde «særlige kategorier» av personopplysninger også når dette *ikke* er *formålet* med filmingen. I den aktuelle

Ove A. Vanebo

saken gikk domstolen inn på om publisering av informasjon om offentlig ansattes ektefelle, samboer eller partner ville innebære behandling av særlige kategorier av personopplysninger. Hvis f.eks. en mannlig ansatt oppgis å ha en mannlig ektefelle, *kan* det uttrykke at han har en homofil legning, som omfattes av vernet i artikkel 9 nr. 1.

Deloitte-juristene fokuserer særlig på EU-domstolens avgjørelse, siden den «kan få betydning for vurderingen av når man fanger opp artikkel 9-opplysninger og som gjør at man kan stille spørsmål om [Personvernrådets] retningslinjer fremdeles gir uttrykk for gjeldende rett.» EU-domstolen påpekte at det må legges vekt på hva informasjon kan «reveal», dvs. avsløre, også selv om dette skjer mer indirekte og ikke uttrykkes eksplisitt.

Overført til situasjonen med kameraopptak, kan det tenkes at et kamera fanger opp informasjon om f.eks. religionstilhørighet, ved at det filmes personer med hijab eller jødisk kalott og tradisjonelle kinnkrøller. Den kontekstuelle tilnærmingen EU-domstolen anlegger, kan innebære at også slik informasjon vil utgjøre særlige kategorier av personopplysninger, selv om det altså ikke er formålet med opptaket.

Deloitte-juristenes artikkel har gjennomtenkte og tankevekkende resonnementer, som er godt underbygget. Jeg kan derfor ikke si at konklusjonen er gal. Mitt anliggende er imidlertid å tilby en annen metodisk tilnærming, som viser at erfarne jurister innenfor et fagfelt kan komme til noe ulike konklusjoner. Oppsummert er det nemlig min vurdering at jeg oppfatter at nettopp kameraopptak må vurderes noe annerledes, med forankring i forordningens formål og ordlyd. Dette kan også underbygges av mer praktiske hensyn.

> Den kontekstuelle tilnærmingen EU-domstolen anlegger, kan innebære at også slik informasjon vil utgjøre særlige kategorier av personopplysninger, selv om det altså ikke er formålet med opptaket.

1. Hva innebærer en kontekstuell forståelse av hva som utgjør «særlige kategorier» av personopplysninger?

Deloitte-juristene har åpenbart et poeng når de påpeker at det har vært en altfor ensidig vektlegging av den behandlingsansvarliges formål med behandlingen av personopplysninger – også i anerkjent teori.

1 Personvernrådet, *Guidelines 3/2019 on processing of personal data through video devices*.

2 Hanne Pernille Gulbrandsen, Steinar Østmoe og Ole-Martin Moe, *Kameraovervåking og særlige kategorier av personopplysninger*. I: Lov & Data nr. 1/2023 (Nr. 153), s. 19-25.

Samtidig stiller jeg meg tvilende til om avgjørelsen fra EU-domstolen tilsier at det fremover må legges opp til en klart lavere terskel for når kameraopptak behandler særlige kategorier av personopplysninger. Hvis det hadde vært tilfellet, er det naturlig å se for seg at de europeiske datatilsynene og Personvernrådet ville kommet på banen og uttrykt seg tydelig om rettstilstanden, slik det ble gjort med *Schrems II*-avgjørelsen. Selv om fravær av aktivitet bør tolkes med en klype salt, tenker jeg at en klarere omkalfatring av rettstilstanden ville påkalt mer oppmerksomhet.

Den formålsorienterte tilnærmingen til hva som utgjør «særlige kategorier» av personopplysninger, vil fokusere på den behandlingsansvarliges *intensjon* med behandlingen. Hovedspørsmålet vil ofte være om den behandlingsansvarlige ønsker å utlede særlige kategorier av personopplysninger ved behandlingen.[3] Utgangspunktet etter den kontekstuelle tilnærmingen, er at kategoriseringen av personopplysninger *primært* beror på en mer objektiv vurdering. Det er imidlertid ikke slik at den kontekstuelle tilnærmingen utelukker at flere subjektive forhold eller momenter vil være relevante i vurderingen. Tvert imot.

Jeg kan m.a.o. ikke se at en kontekstuell forståelse stenger for at fotografisk materiale (ofte) må behandles annerledes enn informasjon som fremkommer av f.eks. registre. At en vektlegging av formålet mer isolert er en for enkel tilnærming, betyr *neppe* at formålet er *irrelevant* i relasjon til kategorisering av fotografisk materiale. Det er tenkelig at forordningen krever svært konkret vurdering av hver enkelt informasjonstype og sammenheng. Dette er ikke et brudd med en kontekstuell fortolkning av materiale, men snarere en operasjonalisering av et slikt prinsipp. Man kan også si at en nedtoning av formålet i for stor grad vil innebære en *strengt objektiv* – og ikke en *kontekstuell* – forståelse av forordningens bestemmelser.

Med henvisning til sak C-184/20, påpeker Giacomo Delinavelli at EU-domstolen nettopp ikke klargjør hva en kontekstuell tilnærming innebærer: «The Court adopts a contextual approach, *without making explicit the specific criteria for the determination of potentially sensitive personal data*.»[4] [Min uthevning]

I annen juridisk teori er det vist til at en kontekstuell tilnærming kan fokusere på kontekst i *bred forstand*. Dette kan innebære å ta hensyn til bl.a. den behandlingsansvarliges og potensielle datamottakeres interesser, (for)målet med behandlingen, betingelsene for behandlingen, og dens mulige konsekvenser for de involverte personene.[5] En kontekstuell forståelse av hva særlige kategorier av personopplysninger er, kan altså fint ta hensyn til den behandlingsansvarliges intensjoner, siden dette får betydning for hvorvidt behandlingen kan innebære en risiko for de registrerte.

Jeg kan m.a.o. ikke se at en kontekstuell forståelse stenger for at fotografisk materiale (ofte) må behandles annerledes enn informasjon som fremkommer av f.eks. registre.

Et interessant eksempel på dette, er det svenske datatilsynets tilnærming til når informasjon fra kameraopptak utgjør personopplysninger om «religion». Integritetsskyddsmyndigheten (IMY) synes å ta utgangspunkt i en kontekstuell forståelse, der også formålet er et tungtveiende moment:[6]

> *«Allmänt gäller att endast en bild eller film på en person som bär en religiös symbol, klädsel eller andra kännetecken inte regelmässigt utgör en känslig personuppgift. Det som är avgörande är istället i vilket sammanhang som bilderna hämtas in, för vilket syfte och hur de används.»*

Selv om formålet ikke er utslagsgivende for kategoriseringen, kan det altså være relevant i vurderingen.

Mer spesifikt er det også argumentert for at C-184/20 legger til grunn en svært kontekstfokusert forståelse, der man må vurdere *mer konkret* hva som utgjør særlige kategorier av personopplysninger. Av den grunn antar Giacomo Delinavelli at: «[T]he Court does not provide a taxonomy of personal data, either concerning the same data subject or third parties, that combined among them would reveal sensitive information. The Court leaves this assessment on a case-by-case basis, and by doing this undermines legal certainty.»[7]

---

3 Personvernrådet, *Guidelines 3/2019 on processing of personal data through video devices*, s. 14.

4 Giacomo Delinavelli, *Comment to Case C-184/20 and the perils of a broad interpretation of Art. 9 GDPR*, datert 21. september 2022. Lest 21. mai 2023: *https://europeanlawblog.eu/2022/09/21/comment-to-case-c-184-20-and-the-perils-of-a-broad-interpretation-of-art-9-gdpr/*

5 Paul Quinn og Gianclaudio Malgieri, *The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework* Published online by Cambridge University Press: 19 January 2022. I: German Law Journal (2021), sidene 1583–1612.

6 Integritetsskyddsmyndigheten, *Kamerabevakning av religiösa byggnader och kyrkogårdar*. Lest 21. mai 2023: *https://www.imy.se/verksamhet/kamerabevakning/kamerabevakning-pa-olika-omraden/religiosa-byggnader-och-kyrkogardar/*

7 Giacomo Delinavelli, *Comment to Case C-184/20 and the perils of a broad interpretation of Art. 9 GDPR*, datert 21. september 2022. Lest 21. mai 2023: *https://europeanlawblog.eu/2022/09/21/comment-to-case-c-184-20-and-the-perils-of-a-broad-interpretation-of-art-9-gdpr/*

En kontekstuell forståelse kan derfor tilsi at fotografisk materiale må vurderes svært konkret, og normalt ikke anses å inneholde «særlige kategorier» av personopplysninger.

Tilsvarende behøver heller ikke en mer formålsorientert tolkningsstil å innebære at andre hensyn enn intensjon utelukkes. I sin bok om personvernforordningen synes Dag Wiese Schartum å mene at en formålsorientert tilnærming også kan vektlegge bl.a. konsekvenser og risiko. Han viser til at personopplysninger «trolig [vil] kunne anses for å komme inn under artikkel 9(1)» hvis det er «til formålet med behandling av personbilder knyttet behov for kunnskap om etnisitet» – og at det «samme gjelder dersom behandling av slike bildeopplysninger kan gi negative konsekvenser for personers rettigheter og friheter».[8] Dette kan overlappe med kontekstuell tolkningsstil, for som Schartum påpeker:

> «*Generelt er formålstolkning trolig det viktigste grepet for å løse slike spørsmål. Det betyr at en må vurdere betydningen personopplysningen har for vernet av «fysiske personers grunnleggende rettigheter og friheter, særlig deres rett til vern av personopplysninger», jf. artikkel 1(2). En kan da komme til at f.eks. personbilde som viser hudfarge og religiøse symboler, er uten betydning i noen sammenhenger, mens det i andre sammenhenger kan ha stor betydning.*»

En for svart-hvitt forståelse av ulike tolkningsstiler kan derfor fort overskygge nyansene; det er nemlig neppe vanntette skott mellom en kontekstuell og en formålsorientert tolkningsstil.

2. Hva kan utledes av forordningen hva gjelder fotografisk materiale og særlige kategorier av personopplysninger?

Det er også mulig å komme til at EU-domstolens sak C-184/20 ikke innebærer en klart annen forståelse av når særlige kategorier fanges opp av kameraopptak, med forankring i forordningen selv.

En klar indikasjon om at billedmateriale bør behandles annerledes enn f.eks. informasjon som utledes av et register, fremkommer av at artikkel 9 nr. 1 påpeker at særlige kategorier av personopplysninger omfatter «biometriske opplysninger med det formål å entydig identifisere en fysisk person». For slike opplysninger skal det altså vektlegges hva formålet med behandlingen er, og at det er et vilkår at det er for identifikasjon.

Deloitte-juristene er innom dette poenget, men viser til at: «Det foreligger imidlertid ingen eksplisitte unntak for opptak eller bilder i artikkel 9, og en slik tolkning har derfor mindre støtte i ordlyden.» Denne innvendingen overser imidlertid at det i forordningens fortalepunkt 51 er slått fast at:

> «*Behandling av fotografier bør ikke systematisk anses som behandling av særlige kategorier av personopplysninger, ettersom fotografier omfattes av definisjonen av biometriske opplysninger bare når de behandles ved hjelp av et særskilt teknisk middel som gjør det mulig entydig å identifisere eller autentisere en fysisk person.» [Min understrekning]*

Selv om biometriske personopplysninger nevnes i denne sammenhengen, synes første del av setningen å indikere at fotografier som hovedregel ikke skal anses å inneholde særlige kategorier av personopplysninger. Dette har også blitt lagt til grunn i juridisk teori.[9]

Det er også hensiktsmessig å vurdere forordningens regulering i lys av formålsbestemmelsen. Forordningen «fastsetter regler om vern av fysiske personer i forbindelse med behandling av personopplysninger samt regler om fri utveksling av personopplysninger», jf. artikkel 1 nr. 1. Personvernforordningen er derfor på mange måter et regelverk med et Janus-ansikt; det skal fremme gode, men til tider vanskelig forenlige, formål. Personvernet skal sikres, men også «fri flyt» er et viktig formål. Dette kommer også til uttrykk i artikkel 1 nr. 3: «Fri utveksling av personopplysninger i Unionen skal verken begrenses eller forbys av årsaker knyttet til vern av fysiske personer i forbindelse med behandling av personopplysninger.»

I Brendan van Alsenoys doktorgradavhandling vises det nettop til at harmonisering og fri flyt var et av de sentrale argumentene for et felleseuropeisk regelverk: «*The continued fragmentation of national approaches to data protection presented a clear risk to the European vision of further integration. The political push for greater harmonisation provided optimal conditions for further Community action.*»[10]

Noe av bakgrunnen for at det i det hele tatt ble utformet et felleseuropeisk regelverk, var at bilprodusenten Fiat fikk problemer med å sende personopplysninger mellom Italia og Frankrike.[11]

Også i rettspraksis har EU-domstolen fremhevet at for strenge vilkår, som bidrar til dårligere harmonisering i EU, kan være uakseptable selv om de sikrer et sterkere personvern. I EU-domstolens dom C-468/10, *Asociación National de Establecimientos Finansieros de Crédito* (ASNEF), av 24. november 2011, ble EU-domstolen forelagt et spørsmål av en spansk domstol om det var mulig å innføre tilleggsvilkår for å kunne benytte «berettigede

8 Dag Wiese Schartum, *Personvernforordningen - En lærebok*, 2020, s. 47.

9 Sören Öman, *Dataskyddsförordningen (GDPR) m.m.; En kommentar*, 2019, s. 228, og Dag Wiese Schartum, *Personvernforordningen - En lærebok*, 2020, s. 47.

10 Brendan Van Alsenoy, *Regulating data protection; The allocation of responsibility and risk among actors involved in personal data processing*, 2016, s. 213.

11 Jeanne Saliou, *1970-2021: Data protection spreads the world*, 2021. Lest. 18. mai 2023: *https://linc.cnil.fr/fr/1970-2021-data-protection-spreads-world*

interesser» som et rettslig grunnlag. En spansk lov hadde et vilkår utover at det må foreligge berettigede interesser, ved at personopplysningene også måtte fremkomme i et offentlig tilgjengelig register.

Med henvisning til det dagjeldende personverndirektivets formål om å sikre et enhetlig vernenivå i alle medlemsland, fastslo EU-domstolen i ASNEF-saken at direktivets artikkel 7 (som tilsvarer artikkel 6 i forordningen) oppstiller en uttømmende og fullstendig liste over tilfellene hvor behandling av personopplysninger kan anses som lovlig.[12] Medlemsstatene kunne derfor verken legge til nye prinsipper om for rettslige grunnlag eller fastsette tilleggskrav som endrer omfanget/innholdet av ett av de seks grunnlagene i artikkelen.[13]

Tilsvarende har den svenske regjeringen problematisert om informasjon om at noen har dratt fra regningen på bensinstasjoner vil være opplysninger om lovovertredelser i henhold til artikkel 10. Regjering har langt på vei avvist dette, under henvisning til å sikre flyt av personopplysninger i EU:[14]

> *«Ett av de huvudsakliga syftena med dataskyddsförordningen är att åstadkomma en ytterligare harmonisering av dataskyddsregleringen för att undanröja hindren för det fria flödet av personuppgifter inom EU (se t.ex. skäl 9 och 13). Det är därför angeläget att artikel 10 inte tolkas på ett mer extensivt sätt i Sverige än i andra medlemsstater.»*

Det er ingen tvil om at en forståelse av forordningen som innebærer at det er tilstrekkelig at informasjon mer objektivt sett inneholder særlige kategorier av personopplysninger, vil innebære at kamerabruk må begrenses sterkt. Videre vil det også være klart vanskeligere å formidle slik informasjon, f.eks. til samarbeidspartnere eller kunder.

Det er naturligvis også tenkelig at det er tilfeller hvor det er gode grunner for å mene at kategoriseringen av personopplysninger i et kameraopptak i mindre grad bør bero på formål – og være mer objektiv. Et mulig eksempel er hvis et bilde eller filmopptak viser røntgenbilder eller en sykejournal. Det samme kan være tilfellet dersom et kameraopptak filmer en politisk demonstrasjon eller religiøs utøvelse.[15]

Forordningens ordlyd og formål, samt andre kilder, synes imidlertid likevel å trekke i retning av at *formålet* bør tillegges betydelig vekt for så vidt gjelder fotografisk materiale.

For sammenhengens skyld nevner jeg at en slik forståelse samsvarer best med løsningen også i det nå opphevede personverndirektivet (95/46/EF)): Forløperen til dagens forordning var enda klarere på at en kontekstuell forståelse skulle legges til grunn når det ble vurdert om informasjon utgjør særlige kategorier av personopplysninger.[16] Likevel var det for det forrige direktivets del antatt at formålet med behandlingen i forbindelse med filming eller fotografering ofte ville være avgjørende.[17] Av den grunn ville avbildning av mer «hverdagslige» situasjoner *ikke* innebære behandling av særlige kategorier, f.eks. hvis bildet viste en kvinne i rullestol eller med mørk hud.[18]

> At det skal benyttes en kontekstuell tilnærming når personopplysninger skal kategoriseres, tilsier på ingen måte at formålet er irrelevant eller et «lett» moment.

3. Oppsummerende merknader

Det er ingen klare fasitsvar om det nå må legges til grunn en mer objektiv forståelse av når kameraopptak inneholder særlige kategorier av personopplysninger. Deloitte-juristenes bidrag er i så måte både viktig og interessant. Som jeg påviser over, er det imidlertid ikke åpenbart at EU-domstolens praksis tilsier en signifikant senket terskel for når fotografisk materiale inneholder opplysninger som er omfattet av forordningen artikkel 9 nr. 1. Selv antar jeg at den tidligere oppfatningen om vektlegging av formålet med behandlingen, i stor grad kan videreføres. At det skal benyttes en kontekstuell tilnærming når personopplysninger skal kategoriseres, tilsier på ingen måte at formålet er irrelevant eller et «lett» moment.

Ove A. Vanebo, advokat og assosiert partner i CMS Kluge Advokatfirma

12 Avsnittene 28 og 32.
13 Avsnitt 36.
14 Prop. 2017/18:105 s. 99.
15 Sören Öman, *Dataskyddsforordningen (GDPR) m.m.; En kommentar*, 2019, s. 228-229.
16 Personverndirektivet artikkel 8 inneholdt kun en formulering om hva informasjonen kunne «reveal», og hadde ikke holdepunkter knyttet til formål som i dagens forordning. Se også Artikel 29-gruppa, Advice Paper on Special Categories of Data («sensitive data»), (European Commission, Working Paper 444105, 2011), samt Quinn og Malgieri (2021) s. 1592-1593.
17 Prop. 56 LS (2017–2018) s. 129, med henvisning til Artikkel 29-gruppen, *Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance*, side 24. Sml. også Prop. 47 L (2011–2012) side 44.
18 Se blant annet den svenske utredningen SOU 1997:39 s. 358, samt Öman (2019) s. 228-229.

Artificiell intelligens i hälso- och sjukvården – vad händer med patientsäkerheten?

Av Matilda Larsson

Potentialen hos artificiell intelligens (AI) och dess möjliga inverkan på samhället har diskuterats länge men sällan har det varit så omdiskuterat som det är idag. Kanske på grund av att vi närmar oss allt fler tillämpningar som är påtagligt nära vår vardag. Ett område där AI anses ha stor potential är inom hälso- och sjukvården. Det pågår för närvarande praktiska studier på flera universitet och institut där användningen av AI avser bland annat granskningar av mammografibilder för att finna tumörer, bedömningar av röntgenbilder på kranskärl för att förutse risk för hjärtinfarkt och möjligheter att använda AI som ett diagnosverktyg.

Samtidigt som studierna förutspås leda till goda resultat och rädda liv så väcks frågan om hur användningen av AI förhåller till rättsliga krav på ”god vård” och att vård ska bedrivas i enlighet med ”vetenskap och beprövad erfarenhet”.[1] Är AI i praktiken ett diagnosverktyg som kan införas inom hälso- och sjukvården och vad innebär det för patientsäkerheten? Vart finner vi gränsdragningen mellan metoder som kan rättfärdigas genom en strävan att utveckla och förbättra hälso- och sjukvården och metoder som medför en oskäligt hög risk för patientsäkerheten? Nedan följer en analys av bestämmelserna om ”god vård” och ”vetenskap och beprövad erfarenhet” med syfte att utreda deras verkan i förhållande till AI.[2]

Matilda Larsson

Samtidigt som studierna förutspås leda till goda resultat och rädda liv så väcks frågan om hur användningen av AI förhåller till rättsliga krav på ”god vård” och att vård ska bedrivas i enlighet med ”vetenskap och beprövad erfarenhet”.

Rättsliga krav på vårdens kvalitet

Hälso- och sjukvårdslagstiftningen har utvecklats från att vara en praktik styrd av etik och allmänna instruktioner, till ett komplext rättsområde där praktisk verksamhet och juridik kombineras. Numera består hälso- och sjukvårdslagstiftningen av hundratals författningar. Materiellt sträcker sig författningarna över en mängd rättsområden, vad de har gemensamt är att de i varierande utsträckning syftar till att tillgodose och säkerställa en god och säker vård för den enskilde patienten. Två genomgående centrala komponenter inom hälso- och sjukvårdsjuridiken är bestämmelserna om ”god vård” och ”vetenskap och beprövad erfarenhet”. Bestämmelserna skiljer sig från varandra både i sin framställning och till sitt innehåll.

God vård som rättsligt begrepp har ett utpräglat materiellt innehåll och exempel på vad som bör innefattas återfinns både som exempel i lagtext, i propositioner och i myndighetsföreskrifter.[3] Att definiera ”vetenskap och beprövad erfarenhet” är inte lika enkelt från en materiell utgångspunkt. Bestämmelsen har sin historiska förankring i läkarinstruktionen som publicerades i slutet på 1800-talet.[4] Trots att hälso- och sjukvårdens omständigheter har förändrats sedan dess sedan dess används samma begrepp. Vad begreppet egentligen innefattar och vilka krav det ställer är inte helt

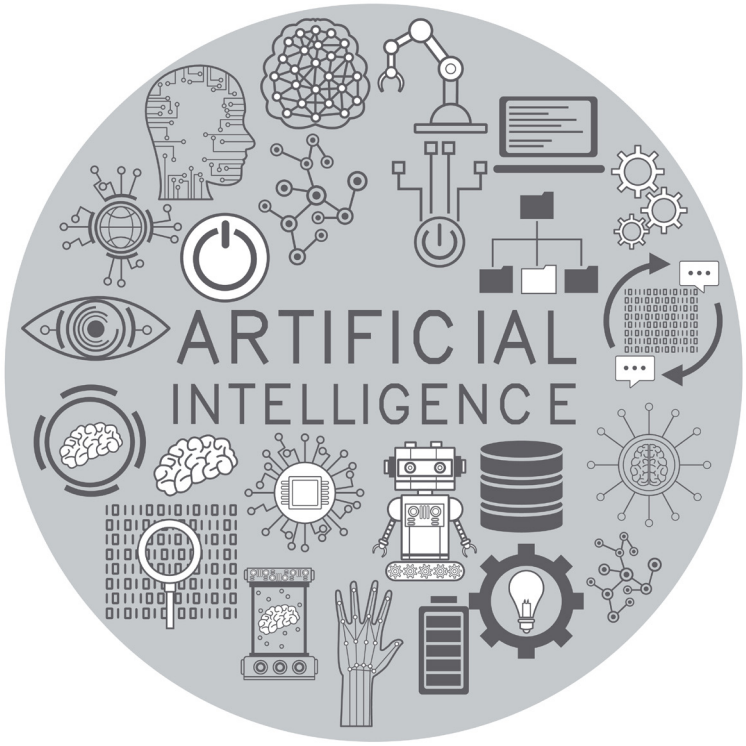
1 Se 5 kapitlet 1 § hälso- och sjukvårdslagen (2017:30) samt 6 kapitlet 1 § patientsäkerhetslagen (2010:659).

2 För fulltext se: Larsson, Matilda ”*Artificiell intelligens i hälso- och sjukvården – rättslig symbios eller juridisk huvudvärk? En undersökning om god vård och vetenskap och beprövad erfarenhet kan upprätthållas vid diagnosticering med artificiell intelligens*”, Stockholms universitet, 2023.

3 Se exempelvis 5 kapitlet 1 § hälso- och sjukvårdslagen, 1 kapitlet 7 § patientlag (2014:821), prop. 2016/17:43 s. 72, föreskrifter eller kunskapsstöd från Socialstyrelsen.

4 Se Pontin, David Magnus, *Författningar m.m. angående medicinalväsendet i Sverige, omfattande år 1890*. Stockholm, Kungliga Boktryckeriet P.A. Norstedt & Söner, 1891, s. 65.

klarlagt. Något förenklat kan det beskrivas som ett koncept som vuxit fram ur en starkt syftesreglerad bestämmelse där hälso- och sjukvårdens grundläggande mål att bota och lindra ska beaktas i varje led inom den praktiska verksamheten. Kombinationen av ovan nämnda bestämmelser uppställer unika krav och möjligheter för AI som diagnosverktyg utifrån vad vi i dagsläget vet om användningen av AI.



Illustrasjon: Colourbox.com

Juridik och teknik

Den juridiska komplexiteten på området är bland annat en konsekvens av de spänningsfält som finns mellan AI och juridik. En del av problematiken består av att AI är ett begrepp med flera funktioner och beroende på vilken bransch eller aktör som är aktuell kan definitionen av AI se olika ut. Det skapar en osäkerhet i hur eventuell kommande lagstiftning för att reglera AI borde definiera termen för att uppnå sitt ändamål och vad som kommer att innefattas.[5] En annan problematik som blir påtaglig när autonoma och självlärande system används är ”black-box problemet”. Något förenklat är problemet en illustration av att människor inte kan utläsa hur AI genererar sitt resultat.

Vid användning av AI inom hälso- och sjukvården finns det naturligtvis risker för patienten, till exempel att en diagnos som genereras är felaktig. Det kan vara något så simpelt som damm på en lins. Om maskinen inte har tränats för att identifiera sådana avvikelser är det möjligt att den genererar ett felaktigt resultat. Det skapar en risk för patienten, även om det är en risk som kan tränas bort. Ytterligare komplikationer kan uppstå i förhållande till ”mjuka värden”, med det avses användares tilltro till tekniken och därmed trygghet i att använda produkten. Brist på tilltro till tekniken får konsekvenser i förhållande till både god vård och vetenskap och beprövad erfarenhet.

God vård

God vård regleras i hälso- och sjukvårdslagen, vilken utgör en målinriktad ramlag. Det materiella innehållet har växt fram organiskt genom hälso- och sjukvårdens historia.[6] Socialstyrelsen har i en tolkning framställt att god vård handlar om att upprätthålla en god kvalitet, i lagtexten har begreppet delats upp i fem punkter som ska visas särskild hänsyn.[7] I en analys av regleringen om god vård i förhållande till användning av AI som diagnosverktyg är flera av punkterna i bestämmelsen intressanta. En av dem avser patientens behov av trygghet, kontinuitet och säkerhet. Bedömningen är subjektiv på så sätt att den upplevda säkerheten inte nödvändigtvis behöver grundas i om patientens hälsa riskerar att lida skada. Det kan likaväl avse den upplevda tryggheten hos medicinsk personal eller hos patienten, om det kan påverka patientens inställning till vården. Vilken trygghet en professionell vårdutövare känner i förhållande till tekniken kan således få inverkan på om denne kan använda AI i sin diagnosticering.

Vetenskap och beprövad erfarenhet

Vetenskap och beprövad erfarenhet utgör ett grundläggande kvalitetskrav, en måttstock inom hälso- och sjukvården som återfinns i patientsäkerhetslagen. Regleringen knyter an till att en hög patientsäkerhet och god kvalitet i hälso- och sjukvården måste beaktas genom hela vårdkedjan. Från praktiska uppgifter hos en enskild professionell vårdutövare till hur verksamheten organiseras. Det har i flera led diskuterats om regleringen verkligen avser att uppställa krav på vetenskap *och* beprövad erfarenhet, eller om det ena vid tillfälle kan väga upp för det andra.[8] I förhållande till AI uppkommer där definitionsfrågor, hur mycket underlag

5 Förslag på definition av AI lagts fram i ”AI-act”, definitionen är mycket bred och utgår från vad AI kan vara idag. Frågan om den definitionen kommer leda till en ändamålsenlig reglering som håller på lång sikt har diskuterats.

6 Till exempel infördes krav på hygienisk standard i lagtext när risk för antibiotikaresistens aktualiserades, se prop. 2005/06:50. Tidigare regleradesdes hygienisk standard i rekommendationer från Socialstyrelsen.

7 Se 5 kapitlet 1 § hälso- och sjukvårdslagen.

8 Se SOU 1989:60 s. 59.

krävs för att något ska uppnå ”beprövad erfarenhet” och hur ska ”vetenskap” definieras i förhållande till AI? Den gemensamma åsikten verkar vara att definitionsfrågorna avseende metoden är upp till den medicinskt skolade utövaren att avgöra utifrån sin kompetens.[9]

> Den aktuella frågan för juridiken idag är därmed inte om det går att införa AI inom hälso- och sjukvården utan hur juridiken ska hantera kommande utmaningar att upprätthålla patientsäkerheten och samtidigt främja visionen av en förbättrad hälso- och sjukvård genom tillämpning av AI.

För att kravet på vetenskap och beprövad erfarenhet ska uppfyllas, krävs inte bara en granskning av den valda åtgärden och den valda metoden, utan även en kontextuell bedömning i förhållande till det enskilda fallet. Att genomföra djupgående bedömning vid användning av AI kompliceras av black-box problemet eftersom utövaren inte kan få en fullständig bild av hur diagnosen fastställdes. Metoder har utvecklats för att ta del av vilka komponenter som var centrala i bedömningen men en fullständig bild uppnås inte.[10] Förarbetena talar dock för att det föreligger flexibilitet i förhållande till bestämmelsen.[11] Om en behandlingsmetod till exempel uppfyller bestämmelsens krav, men inte uppfyller hälso- och sjukvårdens övergripande syfte att bota och lindra, måste det överordnade syftet för hälso- och sjukvården dominera.

Medicinska gråzoner

Sammanfattat ska vetenskap och beprövad erfarenhet begränsas till den medicinska vetenskapen och i praktiken faller bedömningen för om en metod ska anses uppfylla vetenskap och beprövad erfarenhet på den professionella utövaren. För att upprätthålla en vetenskaplig standard som uppfyller regleringens syfte bör denne nyttja både ett reaktivt och ett proaktivt förhållningssätt till ny teknik, som innefattar att genomföra regelbundna utvärderingar och riskbedömningar. Det kan ifrågasättas om lagstiftningens syfte och de medicinska bedömningsgrunderna nödvändigtvis sammanfaller, eller om de differentieras nu eller i framtiden. Historiskt sett har gråzoner i restriktiv mån godkänts i praxis utan att det nödvändigtvis har ansetts stå i strid med regleringen. Går man tillbaka till läkarinstruktionen från vilket begreppet härrör, framgår det att vetenskap och beprövad erfarenhet ska följas ”så vidt möjligt”.[12] Om regleringen i nuvarande lagtext i vissa situationer är omöjlig att uppfylla i praktiken så finns det därmed utrymme att hävda att det enda ”rätta” är att tillåta avsteg från bestämmelsen. Det är emellertid av stor vikt för patientsäkerheten att syftet med hälso- och sjukvården inte försummas. Enligt vetenskap och beprövad erfarenhet borde en experimentell metod därmed inte tillåtas endast på grund av att det i framtiden kan främja utvecklingen av nya behandlingsmetoder. Det stödjs även av att en professionell måste upprätthålla en omsorgsfull och sakkunnig vård oavsett behandlingsmetod. Om AI brukas för att diagnosticera en patient krävs med andra ord att användaren anser att metoden är så pass säker att den uppfyller kriterierna i bestämmelsen om vetenskap och beprövad erfarenhet.

Tillåter lagens krav på patientsäkerhet att AI används som diagnosverktyg?

Det kan konstateras att varken bestämmelsen om god vård eller den om vetenskap och beprövad erfarenhet är så pass restriktiv att de kan antas hindra ett införande av AI som diagnosverktyg inom hälso- och sjukvården. Detta gäller under förutsättning att professionella användare kan förlita sig på den samt att den kan uppvisa vetenskaplig effektivitet och goda resultat. Detta sker på gott och ont för även om patientsäkerheten inom hälso- och sjukvården måste upprätthållas så bör även innovation som kan förbättra sjukvården och rädda liv främjas. Även om juridiken måste säkerställa ett säkerhetsnät för patienter är det också nödvändigt att den innefattar en viss flexibilitet för att kunna användas i praktiken. Mycket ansvar landar på lagstiftaren som måste bära med sig att när tekniken går framåt så måste även lagstiftningen göra det. Det handlar inte bara om att säkerställa dess effektivitet, utan även för att upprätthålla patientsäkerheten under nya och möjligen oväntade förhållanden. Den aktuella frågan för juridiken idag är därmed inte om det går att införa AI inom hälso- och sjukvården utan hur juridiken ska hantera kommande utmaningar att upprätthålla patientsäkerheten och samtidigt främja visionen av en förbättrad hälso- och sjukvård genom tillämpning av AI.

Matilda Larsson, arbetar som associate på KPMG i Stockholm.

9 Här avses att den professionelle ska bedöma om metoden uppfyller vetenskap och beprövad erfarenhet, tekniken i sig bedöms utifrån kriterier i annan lagstiftning.

10 Exempelvis LIME-metoden.

11 Jfr. SOU 1989:60 s. 61

12 Se Pontin, David Magnus, *Författningar m.m. angående medicinalväsendet i Sverige, omfattande år 1890*. Stockholm, Kungliga Boktryckeriet P.A. Norstedt & Söner, 1891, s. 65.

Hvem har varslet på meg? Om omvarsledes rett til innsyn i varslers identitet

Av Ole Martin Mo og Bjørn Ofstad

Varsling i arbeidslivet

Varsling om kritikkverdige forhold på arbeidsplassen er en grunnleggende forutsetning for et fungerende og seriøst arbeidsliv. De ansatte på arbeidsplassen står ofte nærmest til å avdekke kritikkverdige forhold, og vi er avhengige av å legge til rette for at man som ansatt skal kunne si ifra når dette skjer innenfor trygge rammer. Dette var også begrunnelsen for at generelle regler om arbeidstakeres rett til å varsle om kritikkverdige forhold ble inntatt i arbeidsmiljøloven i 2007. I 2016 oppnevnte regjeringen Varslingsutvalget for å gjøre en helhetlig gjennomgang av hvordan reglene hadde virket på området. Utvalgets arbeid resulterte i endringer i arbeidsmiljøloven i 2020 som ga ytterligere rammer for varsling, herunder en definisjon av «kritikkverdige forhold» og lovens formålsbestemmelse, § 1-1, ble utvidet til å omfatte hensynet til et godt ytringsklima.[1]

Det er også regulert i arbeidsmiljøloven at man har rett til å varsle anonymt. Avhengig av hva det er varslet om kan anonym varsling gjøre det vanskeligere for å arbeidsgiver å gjøre nærmere undersøkelser i saken, sammenlignet med saker der arbeidsgiver får mer identifiserende informasjon. Det har derfor en stor verdi at ansatte kan varsle med fullt navn innenfor trygge og forutsigbare rammer. Varslere har i likhet med alle andre ansatte rett til et fullt forsvarlig arbeidsmiljø.

1 Blekastad og Holte Hirst, s. 214.

Ole Martin Moe

Lovgiver har imidlertid ikke tatt stilling til et viktig spørsmål: hvilken rett har den omvarslede til å få vite varslerens identitet?

> Avhengig av hva det er varslet om kan anonym varsling gjøre det vanskeligere for å arbeidsgiver å gjøre nærmere undersøkelser i saken, sammenlignet med saker der arbeidsgiver får mer identifiserende informasjon.

I januar 2023 avsa EU-domstolen sin dom i sak C-154/21 Österreichische Post, som vi mener igjen aktualiserer spørsmålet om retten til innsyn etter personvernforordningen og viktigheten av at lovgiver tar stilling til dette spørsmålet i Norge. I denne artikkelen vil vi si noe om hvorfor.

Bjørn Ofstad

Rettslige rammer for informasjon om varslers identitet

Arbeidsmiljøloven

Arbeidsmiljølovens kapittel 2A regulerer varsling, men lovgiver har ikke tatt stilling til om arbeidsgiver kan holde varslers identitet hemmelig når den omvarslede ber om å få vite hvem dette er. I forarbeidene til loven uttaler departementet kun følgende om beskyttelse av identiteten:

> *Departementet slutter seg for øvrig til utvalgets generelle synspunkt om at det kan utledes av lovens krav om at varsleren skal ha et fullt forsvarlig arbeidsmiljø, at varslerens identitet ikke røpes i større grad enn nødvendig.*[2]

Det er imidlertid uklart når det er «nødvendig» å røpe varslers identitet, lovgiver har ikke regulert dette i arbeidsmiljøloven. Å dele varslerens identitet med den omvarslede utgjør imidlertid en behandling av person-

2 Prop. 74 L (2018-2019), pkt. 10.4.2.

opplysninger[3], og situasjonen omfattes dermed av personopplysningsloven med personvernforordningen GDPR.

Personvernforordningen (GDPR)

GDPR er et generelt regelverk som er ment å regulere *all* behandling av personopplysninger, og tar ikke høyde for de særlige hensynene som gjør seg gjeldende innenfor varsling i arbeidslivet. Forordningen skal gjennomføres slik den er vedtatt i EU, og i Norge er dette gjort gjennom inkorporasjon i personopplysningsloven (2018). Norge har et begrenset handlingsrom til å regulere personvern gjennom nasjonal lovgivning ettersom regelverket er en EU-forordning. Det tidligere personverndirektivet åpnet i større grad for nasjonal særlovgivning.

GDPR åpner likevel for at medlemslandene vedtar nasjonal særlovgivning innenfor noen bestemte områder, og ett av disse områdene er «i forbindelse med ansettelsesforhold» etter artikkel 88. Norge har imidlertid ikke benyttet seg av dette handlingsrommet for varslingssaker, og dette skaper stor uforutsigbarhet for de som er involvert i varslingssaker.[4] Konsekvensen av dette er at spørsmålet om hvorvidt omvarslede kan få innsyn i varslerens identitet er regulert av de generelle reglene i personvernforordningen. I denne sammenhengen er plikten til å gi informasjon etter artikkel 14 og retten til innsyn etter artikkel 15 relevante.

Rett til informasjon når personopplysninger ikke er samlet inn fra den registrerte

Etter personvernforordningen artikkel 14 nr. 2 bokstav f plikter arbeidsgiver å informere den registrerte om «fra hvilken kilde personopplysningene stammer fra». Datatilsynet skriver at de ikke har tatt stilling til om denne rettigheten omfatter informasjon om varslerens identitet.[5] Som vi vil komme tilbake til nedenfor mener vi imidlertid at C-154/21 Österreichische Post taler for at denne rettigheten omfatter informasjon om varslerens identitet.

> Datatilsynet skriver at de ikke har tatt stilling til om denne rettigheten omfatter informasjon om varslerens identitet.

Retten til innsyn i personopplysninger

Den som blir varslet om har ofte et ønske om å få vite hvem som har varslet for å kunne forsvare seg. Kontradiksjon er også et viktig hensyn å ivareta i varslingsprosessen.

Personvernforordningen artikkel 15 nr. 1 gir den registrerte, personen som personopplysninger handler om, rett til innsyn i personopplysninger. Innsynsretten innebærer at den registrerte har krav på en bekreftelse om at personopplysningene deres behandles eller ikke, samt en liste med informasjon som blant annet formålet med behandlingen, lagringstid, og mest interessant i denne sammenhengen – hvor opplysningene stammer fra:

> *«dersom personopplysningene ikke er samlet inn fra den registrerte, all tilgjengelig informasjon om hvor personopplysningene stammer fra»*

«All tilgjengelig informasjon» taler for at retten til innsyn gir rett til å få vite hvem varsleren er, såfremt arbeidsgiveren har informasjon om dette. Dersom varsleren har valgt å være anonym stiller dette seg annerledes.

Unntak fra retten til informasjon og innsyn

Retten til informasjon og til innsyn i egne personopplysninger er ikke absolutte, og personvernforordningen åpner for at den behandlingsansvarlige kan unnta opplysninger fra den registrerte. Unntakene finnes i personopplysningsloven § 16, samt personvernforordningen artikkel 15 nr. 4 og artikkel 14 nr. 5.

Felles for disse unntakene er at de er svært skjønnsmessige og at de skal vurderes konkret av arbeidsgiveren i hver enkelt sak. Personvernregelverket er som nevnt generelt, og unntakene tar ikke høyde for de særlige hensynene som gjør seg gjeldende i varslingssaker. I sin veileder om varsling skriver Datatilsynet at ulikhetene i saker gjør at det er en generell hovedregel om at arbeidsgiveren kan unnta opplysninger fra innsyn.

Vi mener at dagens rettstilstand skaper en uholdbar og uforutsigbar situasjon for menneskene som er involvert i varslingsprosesser på arbeidsplassen. Arbeidstilsynet skriver på sine nettsider:

> *Samfunnet er tjent med at alle, også arbeidstakere som sitter på verdifull kunnskap, har vid ytringsfrihet. Derfor har ytringer som bidrar til å rette opp i kritikkverdige forhold, stor betydning. Varslingsregelverket skal sikre denne ytringsfriheten og samtidig bidra til å beskytte arbeidstakere som sier fra om kritikkverdige forhold.*
>
> *For virksomheter er varsling en viktig del av helse-, miljø- og sikkerhetsarbeidet. Gjennom varsling kan virksomheten avdekke og forbedre kritikkverdige forhold. God håndtering av varsling kan styrke tilliten og omdømmet.*

Lovgiver er nødt til å gjøre dette mer forutsigbart for varslere og let-

3 Se personvernforordningen artikkel 4 nr. 1 bokstav a og b, og https://www.datatilsynet.no/personvern-pa-ulike-omrader/personvern-pa-arbeidsplassen/varsling/.

4 *https://www.datatilsynet.no/personvern-pa-ulike-omrader/personvern-pa-arbeidsplassen/varsling/* (sist besøkt 06.03.23)

5 *https://www.datatilsynet.no/personvern-pa-ulike-omrader/personvern-pa-arbeidsplassen/varsling/rett-til-informasjon-og-innsyn/* pkt. 4 (sist besøkt 10.03.23).

te byrden for arbeidsgivere som må gjøre disse vanskelige skjønnsmessige avveiningene i hver enkelt sak.

> Vi mener at dagens rettstilstand skaper en uholdbar og uforutsigbar situasjon for menneskene som er involvert i varslingsprosesser på arbeidsplassen.

C-154/21 Österreichische Post

Saken gjaldt GW, en person i Østerrike, som ba om innsyn etter personvernforordningen artikkel 15 hos det østeriske postvesenet, Österreichische Post, herunder hvorvidt postvesenet hadde utlevert personopplysningene hans til tredjeparter, og i så fall tilø hvem. Postvesenet besvarte innsynsbegjæringen med generell informasjon om hvilke kategorier av mottakere de hadde sendt eller skulle sende opplysningene hans til:

> *Österreichische Post merely stated that it uses data, to the extent permissible by law, in the course of its activities as a publisher of telephone directories and that it offers those personal data to trading partners for marketing purposes. It also referred to a website that set out more information and further data processing purposes. It did not disclose to RW the identity of the specific recipients of the data.*[6]

GW tok saken inn for domstolene i Østerrike, hvor landets høyesterett ba EU-domstolen om en «preliminary ruling» i saken. En slik avgjørelse er bindende for den nasjonale domstolen.

Spørsmålet i saken var hvorvidt GW, som registrert, hadde rett til informasjon om mottakerne av personopplysningers identitet, eller om postvesenet som behandlingsansvarlig kunne velge mellom å gi GW informasjon om mottakernes identitet eller nøye seg med å informere om kategoriene av mottakere.

Personvernforordningen artikkel 15 nr. 1 bokstav c sier at man har rett til følgende informasjon:

> *mottakerne eller kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til, særlig mottakere i tredjestater eller internasjonale organisasjoner*

EU-domstolen viser til fortalepunkt 39 og 63 i personvernforordningen og åpenhetsprinsippet i artikkel 5 nr. 1 bokstav a for å tolke ordlyden i artikkel 15. Domstolen viser til at bestemmelsen gir de registrerte en rettighet, i motsetning til artikkel 13 og 14 som pålegger den behandlingsansvarlige en forpliktelse. Det er derfor den registrerte som må få velge mellom informasjon om kategorier eller identiteten til mottakerne av personopplysningene deres, og ikke den behandlingsansvarlige. Dette sikrer også at hensynene bak retten til innsyn og åpenhetsprinsippet best ivaretas. Domstolen viser videre til at hensynet bak innsynsretten også er at den registrerte skal kunne utøve sine øvrige rettigheter etter regelverket, herunder retten til sletting, retting og begrensning av behandling. Å få informasjon om hvem som har mottatt opplysningene deres er avgjørende for dette. Domstolen viser også til personvernforordningen artikkel 19, som pålegger den behandlingsansvarlige å kommunisere retting eller sletting av personopplysninger til mottakerne av disse. På bakgrunn av disse kildene kommer domstolen til at den registrerte har rett til informasjon om identiteten til mottakerne av personopplysninger.

Sammenhengen mellom C-154/21 og retten til innsyn og retten til informasjon

Dommen fra EU-domstolen gjaldt artikkel 15 nr. 1 bokstav c, retten til informasjon om mottakerne av personopplysninger. Gode grunner taler for de vurderingene domstolen gjør i saken er relevante for retten til innsyn i hvor personopplysninger stammer fra og retten til informasjon om kilden til personopplysninger.

> Lovgiver må benytte seg av det handlingsrommet som finnes etter personvernforordningen og i dialog med partene i arbeidslivet skape forutsigbare rammer for hvordan varsleres identitet skal håndteres. Dette er avgjørende for at arbeidstakere skal tørre å varsle og for å sikre et fungerende varslingsinstitutt.

Det grunnleggende hensynet bak retten til innsyn er at man skal kunne kontrollere at den behandlingsansvarlige følger personvernforordningen og ikke behandler personopplysninger ulovlig.[7] Innsynretten spiller derfor en viktig rolle, fordi den både ansvarliggjør den behandlingsansvarlige i tråd med ansvarlighetsprinsippet i artikkel 5 nr. 2, og det gir den registrerte en grad av kontroll over egne personopplysninger i tråd med lovgivers intensjon bak personvernforordningen.[8] Retten til innsyn er derfor en av de viktigste rettighetene som oppfyller formålet bak hele regelverket.

Når EU-domstolen gjennomgår rettskildene for å vurdere rekkevidden av artikkel 15 nr. 1 bokstav c, er

6 C-154/21 Österreichische Post, avsnitt 18.

7 Fortalepunkt 63.

8 Fortalepunkt 7.

alle disse kildene relevante for retten til innsyn i hvor personopplysninger stammer fra og retten til informasjon om kilden til personopplysninger. Fortalepunkt 39 og 63, og hensynet til at den registrerte skal kunne utøve sine øvrige rettigheter etter forordningen bidrar også til å klargjøre innholdet i bokstav g.

Når EU-domstolen har gjort retten til innsyn enda klarere, blir det også klarere at lovgiver må ta stilling til hvordan dette påvirke varslere. Datatilsynet skriver dette om veien videre:

> *Desse vanskelege avvegingane blir forhåpentlegvis løyst i lovgivinga. Eit nytt direktiv om varsling av brot på EU-regelverk er vedtatt i EU (direktiv 2019/1937). Justis- og beredskapsdepartementet har sendt lovforslaget på høyring, og Datatilsynet ser fram til ein open debatt om kvar grensene skal gå for informasjon og innsyn i personopplysningar i samband med varsling.*[9]

Konklusjon

Varslingssaker er belastende for de involverte, og det er viktig at vi har et klart lovverk som letter byrdene for arbeidsgivere og arbeidstakere som står i varslingsprosesser. Lovgiver må benytte seg av det handlingsrommet som finnes etter personvernforordningen og i dialog med partene i arbeidslivet skape forutsigbare rammer for hvordan varsleres identitet skal håndteres. Dette er avgjørende for at arbeidstakere skal tørre å varsle og for å sikre et fungerende varslingsinstitutt.

Advokatfullmektig Ole Martin Moe og partner Bjørn Ofstad i Deloitte Legal.

9 *https://www.datatilsynet.no/personvern-pa-ulike-omrader/personvern-pa-arbeidsplassen/varsling/* (sist besøkt 01.06.23)

Illustrasjon: Colourbox.com

Brottsbekämpande myndigheter ges rätt till genomsökning på distans även utomlands

Av Christina Wikström og Anton Karlsson

I ett avgörande[1] från den 30 mars 2023 beslutade Högsta domstolen (HD) att genomsökning på distans får beslutas även om den eftersökta informationen kan vara lagrad utomlands. Genomsökning på distans utgör ett tvångsmedel som infördes i 28 kap. rättegångsbalken (1942:740) (RB) i juni 2022. Tvångsmedlet innebär att det under brottsutredningar under vissa förutsättningar är möjligt att besluta om att söka efter handlingar som kan ha betydelse som bevis och som finns lagrade i ett avläsningsbart informationssystem utanför den elektroniska kommunikationsutrustning som används för att utföra genomsökningen. Med ett avläsningsbart informationssystem avses exempelvis en molntjänst, och med en elektronisk kommunikationsutrustning avses exempelvis en dator eller en mobiltelefon.[2]

Innan tvångsmedlet tillkom var rättsläget oklart vad gäller huruvida brottsbekämpande myndigheter fick bereda sig tillgång till annan information än sådan som finns lokalt lagrad i den elektroniska kommunikationsutrustningen. Den dominerande uppfattningen har varit att så inte får göras, vilket innebär att brottsbekämpande myndigheter inte kunnat bereda sig tillgång till externt lagrade elektroniska handlingar. I det alltmer digitaliserade samhället ansågs dessa regler dåligt anpassade, varpå tvångsmedlet infördes i RB,

Christina Wikström

Anton Karlsson

vilket bland annat gör det möjligt för brottsbekämpande myndigheter att bereda sig tillgång till handlingar som finns lagrade i molntjänster.[3]

> Avgörandet möjliggör för brottsbekämpande myndigheter att i större utsträckning använda den digitala arenan för att samla in bevis, och däribland molntjänster vars användning ökat markant under senare år och där lagringen ofta sker i utlandet eller på okänd plats.

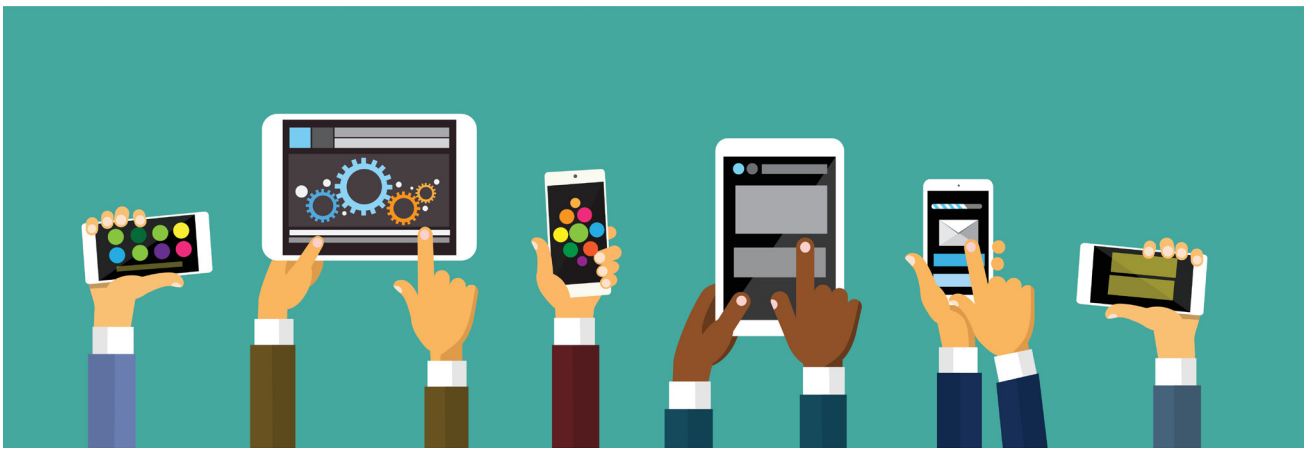
Enligt Europeiska kommissionen behövs i omkring 85 % av alla brottsutredningar tillgång till elektroniska bevis, och i två tredjedelar av dessa lagras informationen i en annan jurisdiktion.[4] Den fråga som HD prövade i avgörandet var huruvida förhållandet att elektroniska handlingar lagras i utlandet eller på okänd plats medför att det föreligger hinder mot eftersökning med stöd av tvångsmedlet. I förarbeten och doktrin i allmänhet har den dominerande uppfattningen varit att svenska myndigheter är förhindrade att bereda sig tillgång till elektronisk information under sådana omständigheter, bland annat med hänsyn till territorialitetsprincipen, detta även om informationens ägare finns i Sverige. Däremot på-

1 Mål nr Ö 5686–22, *Den okända lagringsplatsen*.

2 Prop. 2021/22:119, *Modernare regler för användningen av tvångsmedel*, s. 76–78.

3 Prop. 2021/22:119, *Modernare regler för användningen av tvångsmedel*, s. 75.

4 COM(2019) 70 final, *Rekommendation till rådets beslut om bemyndigande att inleda förhandlingar om ett avtal mellan Europeiska unionen och Förenta staterna om gränsöverskridande tillgång till elektroniska bevis för straffrättsligt samarbete*, s. 1.



Illustrasjon: Colourbox.com

talades i förarbeten till tvångsmedlet att det finns starka skäl för ett förändrat synsätt.

HD konstaterar i avgörandet att varken bestämmelserna i 28 kap. RB eller folkrätten sätter hinder för att svenska brottsbekämpande myndigheter bereder sig tillgång till elektronisk bevisning som finns lagrad i utlandet eller på okänd plats. Det saknar betydelse om det är känt i vilket land som informationen finns lagrad. Avgörandet möjliggör för brottsbekämpande myndigheter att i större utsträckning använda den digitala arenan för att samla in bevis, och däribland molntjänster vars användning ökat markant under senare år och där lagringen ofta sker i utlandet eller på okänd plats.

Christina Wikström, advokat och partner, och Anton Karlsson, biträdande jurist, verksamma vid Wikström & Partners Advokatbyrå i Stockholm och specialiserade på IT, IP och dataskydd.

Halvor Manshaus er leder IP/Media-gruppen i Advokatfirmaet Schjødt AS, Oslo og fast spaltist i Lov&Data.

Kaare M. Risung er partner i Schjødts faggruppe for TMT. Han har i en årrekke vært kursleder for JUC innen personvern.

Hvorvidt data utgjør personopplysinger – terskelen for identifiserbarhet

– på vei mot en pragmatisk fortolkning av gdpr

26. april avsa EU General Court 8. kammer dom i sak T-557/20 mellom Single Resolution Board, et EU-byrå for krisehåndtering innen bankindustrien, og European Data Protection Board. General Court er en selvstendig domstol i EU og er blant annet overinstans for Personalretten. I andre saker vil General Court være underinstans for EU-Domstolen. I saken som omtales nedenfor opptrer General Court som førsteinstans, og saken kan således ankes videre til EU-Domstolen. Avgjørelsen er med andre ord ikke rettskraftig i skrivende stund.

Mye har allerede vært skrevet om saken frem mot domsavsigelsen, og saken står sentralt i noe så grunnleggende som avklaring av selve begrepet personopplysning. Vi vil i denne artikkelen se spesielt på hvilken terskel som kan utledes av dommen for så vidt angår spørsmålet om identifiserbarhet. Dette har vært et omdiskutert tema, der det blant annet har vært uklart hvor lav terskel som kan legges til grunn for hva som utgjør identifisering og hvorvidt det må avgrenses mot rent teoretiske muligheter for identifisering. Etter avgjørelsen som nå foreligger i saken T-557/20, mener vi det er på tide å revurdere flere av spørsmålene i denne diskusjonen og samtidig legge til grunn en mer praktisk norm for vurderingen knyttet opp mot identifiserbarhet. Saken har betydning utover det konkrete tolkningsspørsmålet og kan på mange måte fremstå som en vekker for personvernmyndigheters tilnærming til tolkningsspørsmål generelt.

> Etter avgjørelsen som nå foreligger i saken T-557/20, mener vi det er på tide å revurdere flere av spørsmålene i denne diskusjonen og samtidig legge til grunn en mer praktisk norm for vurderingen knyttet opp mot identifiserbarhet.

Saksforholdet

Saken gjaldt i korte trekk at EU-byrået Single Resolution Board (SRB) gjennomførte en høring av mulige kompensasjon for aksjonærer og kreditorer etter tiltak for å redde den spanske banken Banco Popular Español SA som hadde havnet i økonomisk uføre og blitt overtatt av Banco Santander. SRB utgjør en viktig del av bankunionen innen EU, og har som overordnet formål å sørge for ordnet restrukturering av kriserammede bankvirksomheter. SRB samarbeider både med de enkelte medlemslandenes nasjonale banktilsyn, så vel som Europakommisjonen, den europeiske sentralbank og nasjonale myndigheter i konkret saker.

I den aktuelle saken ønsket SRB å gjennomføre høring kun av aksjonærer og kreditorer som faktisk ble påvirket av de aktuelle tiltakene. SRB implementerte tekniske løsninger med strenge krav til dokumentasjon av identitet og angivelse av nøyaktige økonomiske interesser knyttet til redningsaksjonen. I denne sammenheng ble det publisert en personvernerklæring som gjorde rede for hvordan SRB ville håndtere personopplysninger i forbindelse med høringen.

Høringen besto av 7 spørsmål i et elektronisk skjema og med begrenset plass for besvarelse. En begrenset gruppe innen SRB anonymiserte innspillene som var kommet inn fra 2855 respondenter. Dette ble gjort gjennom først å sjekke og bekrefte identitet, for deretter å allokere en 33-sifret alfanumerisk kode til den enkelte respondent. Det var kun denne gruppen

hos SRB som hadde tilgang til koden. Koden var altså et bindeledd som kunne koble besvarelsene som var inngitt til den enkelte respondentenes identitet.

SRB jobbet så med å finne fellesnevnere i de totalt 23822 kommentarene fra de omtalte 2855 respondentene for å lette det videre arbeidet med 15 temaer som SRB hadde identifisert. Enkelte av disse temaene dreide seg om verdsettelse av Banco Popular. SRB hadde engasjert Deloitte for å bistå i verdsettelsen og delte således 1104 kommentarer knyttet til verdsettelse med Deloitte. Kommentarene Deloitte mottok var kun identifisert gjennom den 33-sifrede koden.

Klagen og EDPBs behandling

5 av partene som hadde inngitt høringssvar klaget til European Data Protection Board (EDPD) som er EUs eget datatilsyn. Organet er opprettet direkte i personvernforordningen artikkel 68, og har en viktig oppsynsrolle innen persondata i EU. Klagen til EDPD viste til at SRB hadde delt respondentenes besvarelser med Deloitte og Banco Santander, uten at dette var opplyst i personvernerklæringen. Grunnlaget for klagen var forordning 2018/1725 artikkel 15(1)(d) om det offentliges behandling av personopplysninger. Bestemmelsen er identisk med personvernforordningen (General Data Protection Regulation, GDPR) artikkel 13(1)(e).

EDPD kom i første omgang til at delingen av personopplysninger med Deloitte var i strid med forordningen og uttalte *kritikk* i medhold av forordningen artikkel 58(1)(b). SRB klaget på dette vedtaket med begrunnelse i at dataene som var sendt til Deloitte var anonymisert og ikke lenger utgjorde personopplysninger. EDPB fattet da et nytt vedtak der de kom til at dataene var *pseudonymisert*. EDPB trakk på denne bakgrunn den formelle kritikken, men anbefalte at SRB i fremtidige saker skulle opplyse om alle delinger som ville bli foretatt. Å *pseudonymisere* innebærer at man endrer navn fra det opprinnelige ekte navnet til et fiktivt navn slik at identiteten ikke hefter ved opplysningen.

SRB opprettholdt sitt syn og brakte saken inn for EU-domstolen med sikte på å få EDPBs vedtak erklært ugyldig og opphevet.

Saken for EU-domstolen - avvisning

EDPB krevde prinsipalt saken avvist med grunnlag i at SRB manglet rettslig interesse i sakens utfall. Rent formelt var denne anførselen fremsatt som en påstand om inadmissability grunnet manglende rettslig virkning (legal effect) fra det siste vedtaket overfor SRB. Det ble vist til at EDPB hadde korrigert og langt på vei trukket den formelle kritikken av SRB. Denne anførselen fremstår som svakt fundert. EDPB hadde i det siste vedtaket konkludert angående det rettslige spørsmålet om det forelå en rettslig relevant overlevering av personopplysninger. Videre hadde EDPB fremmet en anbefaling på grunnlag av denne konklusjonen om hvordan saksbehandlingen hos SRB skulle foregå i fremtidige saker. Saken hadde også en direkte praktisk konsekvens ved at vedtaket fra EDPB medførte at det ville bli vanskeligere for SRB å innhente bistand til å behandle innspill ved slike høringsrunder. Anbefalingen om at alle delinger av personopplysningene må angis på forhånd setter også skranker for hvordan innsamlet materiale kan benyttes, også der man har tatt skritt for å sikre at identitet og opplysninger ikke uten videre kan sammenkobles. Når saken først var reist fremstår anførselen om manglende rettslig interesse som i overkant formalistisk. En mer pragmatisk tilnærming kunne ha vært å invitere domstolen til å gi en avklaring på et rettslig spørsmål som har praktisk betydning ikke bare for SRB, men også for en rekke andre virksomheter og organer som overleverer personopplysninger til tredjepart for behandling.

Domstolen gjengir endringene i det siste vedtaket fra EDPB i avgjørelsens avsnitt 32:

> *«1. The EDPS finds that the data the SRB shared with Deloitte were pseudonymous data, both because the comments in [the consultation phase] were personal data and because the SRB shared the alphanumeric code that allows linking the replies given in [the registration phase] with the ones given in [the consultation phase] – notwithstanding the fact that the data provided by the participants to identify themselves in [the registration phase] were not disclosed to Deloitte.*
>
> *2. The EDPS finds that Deloitte was a recipient of the complainants' personal data under Article 3(13) of [Regulation 2018/1725]. The fact that Deloitte was not mentioned in SRB's [privacy statement] as a potential recipient of the personal data collected and processed by the SRB as the controller in the context of the [right to be heard] process constitutes an infringement of the information obligations laid down in Article 15(1)(d) [of Regulation 2018/1725].*
>
> *3. In light of all the technical and organisational measures set up by the SRB to mitigate the risks for the individuals' right to data protection in the context of the [right to be heard] process, the EDPS decides not to exercise any of his corrective powers laid down in Article 58(2) of [Regulation 2018/1725].*
>
> *4. The EDPS nevertheless recommends the SRB to ensure that the data protection notice in future [right to be heard] processes covers the processing of personal data in both the registration phase and the consultation phase, and includes all potential recipients of the information collected, in order to fully comply with the obligation to inform data subjects in accordance with Article 15 [of Regulation 2018/1725].»*

Det er verdt å merke seg punkt 1 ovenfor, der bruken av pseudonyme data omtales. Ved at Deloitte ikke hadde fått tilgang til koblingen mellom kode og identitet mente Deloitte at dataene for *Deloitte* var å anse som anonymiserte. Lest som en helhet er det ikke vanskelig å forstå at SRB hadde et reelt behov for å få avklart grensene for bruk av slike data der respondentenes identitet rent faktisk ikke var gjort tilgjengelig.

EU-domstolen konkluderte med at SRB hadde rettslig interesse av en avgjørelse ettersom EDPB hadde fattet vedtak om at behandlingen var i strid med regelverket. Hvilken reaksjon EDPB hadde valgt i den konkrete saken var av underordnet betydning – SRB ville uansett blitt behandlet strengere i en senere sak dersom de hadde opprettholdt sin eksisterende praksis. Det ble også lagt vekt på at EDPB ved oversendelse av sitt andre vedtak hadde opplyst at saken kunne bringes inn for EU-domstolen. Selv om slike formuleringer er standardtekst i denne typen vedtak, gjenspeiler teksten nettopp det forhold at domstolen skal kunne vurdere og eventuelt overprøve vedtakets innhold.

Illustrasjon: Colourbox.com

Det materielle innhold

SRB påberopte seg to grunnlag for opphevelse av vedtaket - saksbehandlingsfeil ved brudd på god forvaltningsskikk og feil i vurderingen av hva som utgjør en personopplysning. Ettersom SRB fikk medhold i at dataene delt med Deloitte ikke var personopplysninger, var det ikke nødvendig for domstolen å ta stilling til spørsmålet om feil ved saksbehandlingen.

Det fremgår fra avgjørelsens avsnitt 14 følgende at behandlingen av opplysningene ble gjort på en måte som var strengt kontrollert og gjennomtenkt. En begrenset gruppe i SRB hadde tilgang til de opprinnelige høringsuttalelsene med kontaktdetaljer og informasjon om relasjonen til Banco Popular. En annen gruppe innen SRB hadde tilgang til alle besvarelser, men kun med den alfanumeriske 33-sifrede koden. Deloitte hadde tilgang kun til et sub-sett av dette datagrunnlaget. EDPB hadde i sitt vedtak ikke sondret klart mellom gruppene, og spesielt ikke mellom SDRB som avgiver og Deloitte som *mottaker*, slik definert i GDPR artikkel 4(9).

EU-domstolen tok naturlig nok utgangspunkt i forordningens definisjonen av personopplysning og viste til avgjørelsen i C-434/16 (Nowak). Her er det slått fast at det ved vurderingen av eventuell kobling mellom data og person må ses hen til både innhold, formål og effekt. Disse punktene må vurderes konkret opp i mot hvilken mottaker som vurderes. I den aktuelle saken var det Deloittes relasjon til dataene som var gjenstand for vurdering og det hadde ikke EDPD tatt tilstrekkelig høyde for. EU-domstolen oppsummerte dette i avsnitt 70 slik:

> *70: However, in the revised decision, the EDPS did not examine the content, the purpose or the effect of the information transmitted to Deloitte.*

Det følger av dette at en vurdering av hva som utgjør en personopplysning ikke er absolutt, men relativ. Dette skal vurderes konkret for den som behandler opplysningene. Dette poenget ble også gjentatt i dommen under avsnitt 97:

However, it is also apparent from the judgment of 19 October 2016, Breyer (C 582/14, EU:C:2016:779), that, in order to determine whether the information transmitted to Deloitte constituted personal data, it is necessary to put oneself in Deloitte's position in order to determine whether the information transmitted to it relates to 'identifiable persons'.

EDPB hadde angrepet saken feil ved å vurdere personopplysningene på avgivers hånd, i stedet for å foreta en relativisert vurdering utfra hva som faktisk var gjort tilgjengelig for mottakeren.

EU-domstolen gikk så over til å vurdere hva som ligger i vilkåret som omfatter enhver opplysning om en *«identifisert eller identifiserbar»* fysisk person. EDPB påpekte, og fikk støtte for, at det ikke oppstilles noe krav om at den den parts behandling som vurderes er den samme part som sitter på nøkkelen til å koble anonymiserte data og de opprinnelige personopplysningene. Det spiller altså ikke noen rolle om disse funksjonene er på én eller to hender.

EDPB hadde videre lagt til grunn at skillet mellom anonymiserte data og pseudonymiserte data går på hvorvidt det objektivt sett finnes informasjon som kan koble dataene til personopplysninger eller ikke. EU-domstolen angir EDPBs anførsel slik:

81 ... he stated that the difference between pseudonymous and anonymous data is that, in the case of anonymous data, there was no 'additional information' that could be used to attribute the data to a specific data subject, whereas, in the case of pseudonymous data, there is such additional information. Therefore, in order to assess whether data are anonymous or pseudonymous, it is necessary to consider whether there is any 'additional information' that can be used to attribute the data to specific data subjects.

Vurderingstemaet for EDPB hadde altså vært *om det fantes* en kobling mellom den alfanumeriske koden Deloitte hadde fått og de aktuelle personopplysningene. Det var ikke gjort noen form for vurdering av hva som i praksis skulle til for å etablere noen slik kobling. EU-domstolene hadde ikke grunnlag for å foreta en subsumpsjon slik saken var fremlagt, men avgjorde saken på det grunnlag at EDPBs vedtak var ugyldig fordi EDPB ikke hadde foretatt denne nødvendige og konkrete vurderingen.

For så vidt angår innholdet av testen for identifiserbarhet viser EU-domstolen til sin tidligere avgjørelse i C 582/1 (*Breyer*). Breyer dreide seg om potensiale for kobling mellom en brukers tildelte dynamisk IP-adresse og adressen på et nettsted. EU-domstolen kom i Breyer etter en konkret vurdering til at abonnenter var identifiserbare gjennom den tildelte dynamiske IP-dressen. Det er to sentrale punkter domstolen utleder fra Breyer og bruker i vår sak under avsnittene 92 og 93:

92: The Court of Justice nevertheless held that it must be determined whether the possibility to combine a dynamic IP address with the additional information held by the internet service provider constituted a means likely reasonably to be used to identify the data subject (judgment of 19 October 2016, Breyer, C582/14, EU:C:2016:779, paragraph 45).

93: The Court of Justice stated that that would not have been the case if the identification of the data subject had been prohibited by law or had been practically impossible on account of the fact that it would have required a disproportionate effort in terms of time, cost and man-power, so that the risk of identification would have appeared in reality to be insignificant (judgment of 19 October 2016, Breyer, C582/14, EU:C:2016:779, paragraph 46).

Det er verdt å merke at terskelen som beskrives i avsnitt 92 og 93 ikke er den samme. I avsnitt 92 er temaet hvorvidt muligheten for re-identifisering er *rimelig sannsynlig*. Terskelen er i avsnitt 93 gjengitt som at muligheten for re-identifisering i realiteten er ubetydelig. Domstolen avklarer forholdet mellom disse to tersklene i tilknytning til det foreliggende spørsmålet, og skriver i avsnitt 104:

104 It is apparent from paragraph 45 of the judgment of 19 October 2016, Breyer (C582/14, EU:C:2016:779), cited in paragraph 92 above, that it was for the EDPS to determine whether the possibility of combining the information that had been transmitted to Deloitte with the additional information held by the SRB constituted a means likely reasonably to be used by Deloitte to identify the authors of the comments.

Det er altså terskelen i avsnitt 92 som er relevant for denne vurderingen - *likely reasonably*. Begrepet *likely reasonable* kan oversettes til norsk med *rimelig sannsynlig*. Men, oversettelsen treffer ikke helt. Det vil være mer nærliggende å oppfatte dette som to-leddet: *likely* og *reasonable*. Dommen er ikke oversatt til svensk eller dansk, så det er ingen veiledning å hente fra disse språkene.. På tysk er følgende benyttet: *vernünftigerweise .. werden konnte*. På norsk kunne dette beskrives som *«med rimelighet kan forventes»*.

I forordning 2018/1725 fortalepunkt 16, som også EU-domstolen viser til i avsnitt 87, benyttes i relasjon til terskelen for identifisering *reasonably likely* – altså samme ord i motsatt rekkefølge. Denne teksten tilsvarer GDPRs fortalepunkt 26, tredje setning: «*To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.*». Offisiell norsk oversettelse

av samme punkt i GDPRs fortalepunkt 26 tredje setning er: «*Når det skal fastslås om en fysisk person er identifiserbar, bør det tas hensyn til alle midler som det med rimelighet kan tenkes at den behandlingsansvarlige eller en annen person kan ta i bruk for å identifisere vedkommende direkte eller indirekte, f.eks. utpeking.*». I den svenske versjonen brukes uttrykket «*med rimlig sannolikhet*».

> Men, i realiteten er poenget etter vår mening uansett at det må gjøres en konkret vurdering av faren for for at re-identifisering rimeligvis vil kunne skje.

Om «*med rimelighet kan tenkes*» er en god oversettelse av «*reasonably likely*» kan nok diskuteres. Men, i realiteten er poenget etter vår mening uansett at det må gjøres en konkret vurdering av faren for for at re-identifisering rimeligvis vil kunne skje. Den tyske oversettelsen viser klarere at man skal bruke sunn fornuft i vurderingen av hva mottaker med rimelighet kan tenkes å kunne gjøre for å re-identifisere. I vurderingen skal det legges vekt på flere elementer, f eks. tid, kostnader og innsats. I vurderingen vil det formodentlig være relevant også å se hen til også hvilket motiv den som besitter personopplysningene rimeligvis skulle ha for å ville re-identifisere. For øvrig har domstolen ikke uttrykkelig tatt stilling til hvilke krav som skal stilles for at opplysningene skal anses å være tilstrekkelig anonymisert.

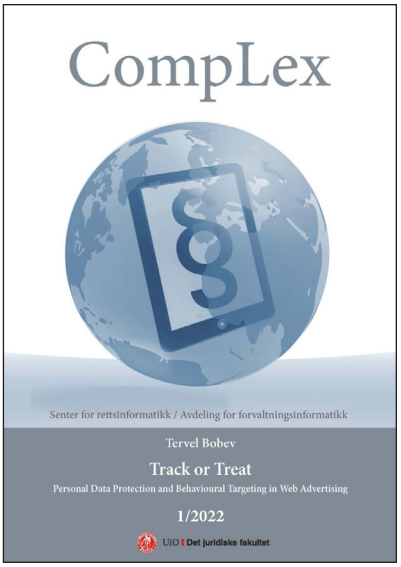
> Reglene fremstår i mange tilfelle som lite praktiske og like lite fleksible. Det er ikke uventet at denne saken fikk det utfallet den fikk.

Konklusjoner

Avgjørelsen i SRB-saken gir oss en viktig avklaring knyttet til overlevering av pseudonymiserte opplysninger. Denne måten å arbeide er svært utbredt, og avgjørelsen legger til rette for mer ryddige forhold på dette området. I avgjørelsen er det lagt til grunn en bred helhetsvurdering, der flere forhold inngår. SRB har for eksempel hatt en ryddig håndtering internt hos seg. Hver enkelt gruppe som har hatt befatning med opplysningene har kun hatt tilgang eller innsikt definert etter hvilket behov som foreligger. En slik tilnærming som er klart beskrevet og fulgt opp i praksis vil være et viktig element ved vurderingen. I dette ligger også at nøkler for å låse opp koblingen mellom opplysninger og identitet må oppbevares trygt og med tilgangsbegrensning. Da er det liten grunn til å tro – det kan ikke rimeligvis forventes – at nøklene kommer på avveie eller tilflyter den tredjeparten som har fått tilgang til opplysningene.

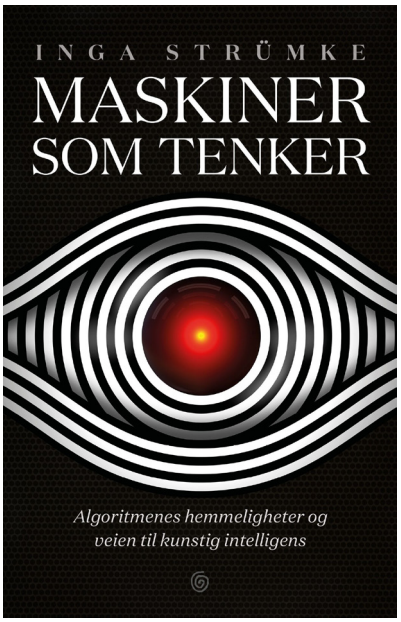
Videre vil det være et poeng å avtaleregulere og beskrive hvordan identiteten til avgiveren er beskyttet og samtidig slå fast at mottakeren ikke har rett til å forsøke re-identifisering av en eller flere personer. Ved at det da ikke er snakk om personopplysninger, kan man se for seg at det ikke vil være behov for en databehandleravtale. Tatt i betraktning at opplysningene opprinnelig har vært personopplysninger, og kun er for vanlige opplysninger å regne i den grad de er pseudonymiserte, kan det være et spørsmål om det er behov for en databehandleravtale eller ikke. Dette vil man måtte ta stilling til avhengig av hvordan den enkelte avtale og underliggende databehandling er tenkt utført.

I tillegg til det rene tolkningsspørsmålet, viser avgjørelsen en tilnærming fra EDPB som var snever og formalistisk uten å foreta de nødvendige konkrete vurderinger med en porsjon sunn fornuft.. Det er et gjennomgående problem i møtet med GDPR og personopplysninger at reglene kan medføre store utfordringer fra aktører som etter beste evne forsøker å innrette seg etter regelverket. Reglene fremstår i mange tilfelle som lite praktiske og like lite fleksible. Det er ikke uventet at denne saken fikk det utfallet den fikk. Kanskje mer overraskende er det at EDPB så lenge holdt fast på en lovforståelse som var så *unødvendig* sett opp mot formålet til GDPR. Slike feilvurderinger synes å bygge på en for stor avstand mellom skrivebordet hos EDPB og det virkelige liv, og er på sikt egnet til å svekke tilliten til både EDPB og GDPR.



Track or Treat. Personal Data Protection and Behavioural Targeting in Web Advertising.

By Tervel Bobev.
Oslo: Universitetet i Oslo, Juridisk fakultet 2022, 1/2022.
ISSN 2703-8777 Complex (online)
https://www.jus.uio.no/ifp/forskning/om/publikasjoner/complex/2022/2022-01.html



Maskiner som tenker. Algoritmenes hemmeligheter og veien til kunstig intelligens

Inga Strümke.
Maskiner som tenker. Algoritmenes hemmeligheter og veien til kunstig intelligens.
Oslo: Kagge forlag, 2023. 309 s.
ISBN: 9788248932505

«AI – teknologien som vil revolusjonere vår hverdag.»

Hvor raskt går utviklingen av kunstig intelligens? Og hvordan kommer AI (Artificial Intelligence) til å påvirke livet vårt i årene som kommer?

Når du ikke klarer å slutte å scrolle på sosiale medier er det databaserte algoritmer du kan takke for minuttene du aldri får tilbake. Sommeren 2022 varslet en Google-ingeniør om et dataprogram som hadde blitt bevisst, og få måneder senere sendte norske lærere bekymringsmelding til Stortinget på grunn av en intelligent chatbot. Alt dette – fra algoritmer som påvirker enkeltpersoner, til intelligente dataprogrammer i samfunnet – koker ned til ett spørsmål: Hvordan fungerer kunstig intelligens?

I Maskiner som tenker skriver Inga Strümke om hvordan vi mennesker prøver å lage kunstig intelligens, om vi endelig er i ferd med å lykkes, og om vi i det hele tatt kan fatte hva den nye teknologien vil innebære.

Omtalen er hentet fra Kagge.no: https://kagge.no/produkt/sakprosa/politikk-og-samfunn/maskiner-som-tenker/#tab-description

Podcast

Hard Fork – The New York Times

"Hard Fork" is a show about the future that's already here. Each week, journalists Kevin Roose and Casey Newton explore and make sense of the latest in the rapidly changing world of tech.

The future is already here: https://www.nytimes.com/2022/10/04/podcasts/hard-fork-technology.html

Delphi

Rebecka Harding og Petri Dahlström

Senaste nyheterna inom svenskt dataskyddsområde

IMY utfärdar reprimand för kamerabevakning på gymanläggningar

IMY bedömer efter granskning av ett gymföretag att företaget sedan februari 2019 har behandlat personuppgifter i strid med artikel 6.1 i GDPR genom att utan rättslig grund bedriva kamerabevakning av träningsytor och dörrar på ett antal av företagets träningsanläggningar. Företaget anser att övervakningen skett av säkerhetsskäl och att deras medlemmar har samtyckt till övervakningen genom att skriva under medlemsavtalet. IMY anser dock att övervakningen inte uppfyller det nödvändighetskriterium som krävs för att personuppgiftsbehandlingen ska vara laglig med stöd av artikel 6.1 f i GDPR, och att bevakningen inte heller kan stödja sig någon annan rättslig grund i artikel 6.1 i GDPR.

IMY bedömer vidare att gymföretaget inte har uppfyllt kravet på att informera de registrerade avseende kamerabevakningen enligt artikel 13 i GDPR. IMY utfärdar därför en reprimand avseende företagets överträdelser av både artikel 6.1 och 13 i GDPR.

IMY utfärdar reprimand för betungande verifieringsmetod gentemot rättighetsutövare

IMY bedömer att ett e-handelsföretag har behandlat personuppgifter i strid med artiklarna 5.1 c, 12.2 och 12.6 i GDPR genom att begära in ytterligare information av registrerade som begärt att få sina personuppgifter raderade. Företaget har bland annat krävt att de registrerade skulle tillhandahålla uppgifter om födelsedatum, folkbokföringsadress, betalningskortets fyra sista siffror och diverse andra referensnummer. IMY fastslår i sitt beslut att företagets begäran har inneburit en allt för betungande verifieringsmetod och att den inte har varit nödvändig för att bekräfta de registrerades identitet. Behandlingen har vidare inneburit att de registrerade inte har kunnat utöva sin rätt till radering enligt artikel 17 i GDPR.

Eftersom företaget redan innan tillsynsärendet hade vidtagit åtgärder och ändrat sina rutiner i syfte att efterleva kraven i GDPR anser IMY att det räcker med att utfärda en reprimand mot företaget med anledning av överträdelserna.

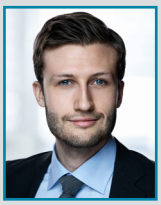
IMY påför sanktionsavgift mot region med anledning av bristfällig personuppgiftshantering

IMY inledde i november 2020 tillsyn mot en region efter att regionen inkommit med en anmälan om en personuppgiftsincident. Incidenten rörde en medarbetare som tappat bort ett okrypterat USB-minne innehållandes personnummer och känsliga personuppgifter om närmare 2 000 personer. USB-minnet hade av misstag glömts kvar i medarbetarens arbetskläder och sedan förvunnit när kläderna skickats till ett tvätteri.

IMY bedömer att regionen inte vidtagit tillräckliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå i förhållande till behandlingens risk. Vidare anser IMY att incidenten inneburit en hög risk för de registrerades fri- och rättigheter då innehållet på USB-minnet möjliggjort kopplingar mellan hälsouppgifter och ett stort antal patienter.

I sitt beslut understryker IMY att det är en försvårande omständighet att USB-minnet inte har lokaliserats och att det således är oklart vilken spridning personuppgifterna har fått. Myndighetens samlade bedömning är därför att regionen ska betala en administrativ sanktionsavgift på 200 000 kronor för överträdelsen.

Rebecka Harding är senior associate/advokat och Petri Dahlström är associate vid Advokatfirman Delphi, Stockholm.




Wiersholm

Av Carl Emil Bull-Berg og Line Helen Haukalid

Ny rettspraksis om definisjonen av personopplysninger

Den 26. april 2023 avsa EGC (European General Court, en underrettsinstans i EUs domstolshierarki), en avgjørelse som går i kjernen på en vanskelig sondring, nemlig forholdet mellom pseudonymisering og anonymisering.

Pseudonymiserte opplysninger er fortsatt personopplysninger, og er følgelig underlagt GDPR. Anonyme opplysninger er derimot ikke personopplysninger. Sondringen mellom disse to kategoriene er derfor svært viktig i praksis.

Sakens bakgrunn

Faktum i saken er – noe forenklet – at SRB (Single Resolution Board), som er et EU-byrå, innhentet synspunktet fra relevante parter (fysiske personer) i forbindelse med en sak de arbeidet med. De delte deretter synspunktene med konsulentfirmaet Deloitte. Før de delte opplysningene fjernet de navnet på personene som hadde kommet med innspill og erstattet navnet deres med et nummer. De fjernet også duplikater og irrelevante svar/synspunkter.

Personene som hadde kommet med sine innspill til SRB klaget saken inn til EDPS (som er datatilsynet til EU-byråer og organer). EDPS håndhever et regelverk som er tilnærmet likt som GDPR. Klagen handlet om at SRB ikke hadde informert om at personopplysninger ville bli utlevert til Deloitte.

Vilkårene for at det skal foreligge en personopplysning

Domstolen la til grunn at to kumulative vilkår må være oppfylt for at det skal foreligge personopplysninger som definert i GDPR:

For det første må det være snakk om en opplysning *om* en fysisk person (på engelsk: «related to»). Vilkåret er oppfylt dersom opplysningens innhold knytter seg til en person, men også dersom *formålet* knytter seg til en person eller dersom *resultatet* av bruken vil ha innvirkning på en person.

Det er interessant å merke seg at domstolen slo fast at noens meninger *kan* være personopplysninger, men at det ikke trenger å være det. Dette fordi det må vurderes konkret om innholdet, formålet eller effekten av meningene er linket til en fysisk person. Slik vurdering hadde ikke EDPS gjort.

For det andre, må de fysiske personene som opplysningene handler om være *identifiserte eller identifiserbare*.

I denne saken var det klart at Deloitte ikke kjente identiteten til personene bak synspunktene, og vurderingen var derfor om de var *identifiserbare*. SRB argumenterte med at for Deloitte var opplysningene anonymiserte, fordi de ikke med rimelighet kunne få tilgang tilleggsinformasjonen nødvendig for å identifisere personene bak synspunktene. EDPS, på sin side, synes å anføre at selve eksistensen av tilleggsopplysninger som kan re-identifisere de aktuelle personene, gjør at opplysningene er pseudonymiserte, selv hos en mottaker som ikke har disse tilleggsopplysningene.

Domstolen slo fast at vurderingen av om opplysningene er anonymiserte beror på om Deloitte kunne kombinere informasjonen de mottok med annen tilleggsinformasjon (som SRB besatt), og om dette var et virkemiddel som Deloitte med rimelighet kunne bruke. Ettersom EDPS ikke hadde foretatt en slik vurdering, kom domstolen til at EDPS ikke kunne konkludere med at opplysningene som Deloitte hadde mottatt var *person*opplysninger.

Relativt begrep

Avgjørelsen bekrefter at personopplysninger er et relativt begrep. Dette innebærer at hver aktør må gjøre sin egen vurdering. Selv om datasettet er pseudonymiserte opplysninger for avsenderen trenger det ikke være det for mottakeren, forutsatt mottakeren ikke med rimelighet kan re-identifisere personene. I så fall vil det ikke være nødvendig å gi informasjon om utleveringen i personvernerklæringen, og dette tilsier også at domstolen mener at det heller ikke er behov for behandlingsgrunnlag for utleveringen.

Det gjenstår å se om saken vil bli anket til CJEU. Dersom den blir anket vil EU sin øverste domstol forhåpentlig komme med viktige avklaringer rundt disse spørsmålene.

Line Helen Haukalid, Managing Associate i Advokatfirmaet Wiersholm.
Carl Emil Bull-Berg, Senior Associates i Advokatfirmaet Wiersholm.

Gorrissen Federspiel

Tue Goldschmieding

EU-Domstolen har afgjort spørgsmål om databeskyttelsesretlige reglers fortolkning og anvendelse inden for rammerne af national procesret

EU-Domstolen traf den 2. marts 2023 afgørelse i sag C-268/21. Sagen var en præjudiciel forelæggelse indgivet af den svenske højesteret.

Den svenske højesteret skulle træffe afgørelse i en national sag mellem to parter angående manglende betaling. I forbindelse med et processuelt spørgsmål om edition opstod tvivl om samspillet med de EU-retlige databeskyttelsesregler.

Tvivlen drejede sig om, hvorvidt Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«) artikel 6 stk. 3 og stk. 4 om lovlig behandling af personoplysninger fandt anvendelse i sagen. I bekræftende fald ønskede den svenske højesteret at vide, hvordan den nærmere skulle inddrage reglerne i vurderingen af, om der kunne træffes afgørelse om edition. I hidtidig retspraksis havde den svenske højesteret principielt ikke taget hensyn datasubjektets databeskyttelsesretlige rettigheder og interesser, når den skulle afgøre spørgsmål om edition. Den havde i stedet, som foreskrevet i den svenske retsplejelov, alene vægtet part og modparts bevismæssige interesser i editionsspørgsmålet.

EU-Domstolen kom frem til, at GDPR artikel 6, stk. 3 og stk. 4 skulle fortolkes således, at de fandt anvendelse ved behandling af personoplysninger inden for rammerne af den nationale civilretlige proces i en medlemsstat.

EU-Domstolen bemærkede herefter, at den konkrete vurdering af, om der skal ske edition, tilkommer den nationale retsinstans fra sag til sag. EU-Domstolen understregede samtidig, at vurderingen skal inddrage en vægtning af datasubjektets interesser over for hensynet til parternes interesse. Såfremt den nationale domstol kommer frem til, at der kan ske edition, vil den yderligere skulle sikre, at principperne for behandling af personoplysninger i GDPR artikel 5, stk. 1, herunder navnlig princippet om »dataminimering«, bliver overholdt. Dette kan bl.a. betyde, at den nationale retsinstans skal træffe supplerende foranstaltninger til beskyttelse af personoplysninger såsom pseudonymisering af de berørte personers navne eller begrænsning af offentlighedens adgang til sagsakterne. Anvendelsen af GDPR artikel 5 betyder også, at den nationale domstol, før den træffer afgørelse om edition, skal overveje, om bevisformålet kan forfølges på mindre databeskyttelsesretligt indgribende måder, herunder eksempelvis ved afhøring af vidner.

Afgørelsen fastslår således, at GDPR artikel 6, stk. 3 og stk. 4 finder anvendelse inden for rammerne af den nationale civilretlige proces. Dette betyder, at nationale domstole skal inddrage hensynet til datasubjekterne i hver enkelt sag og i den forbindelse sikre overholdelsen af principperne for databehandling i GDPR artikel 5, stk. 1.

Læs hele dommen her: *https://curia.europa.eu/juris/document/document.jsf?text=&docid=270823&pageIndex=0&doclang=da&mode=lst&dir=&occ=first&part=1&cid=943064*

National lovgivning må fastsætte strengere regler for afskedigelse af databeskyttelsesrådgivere

EU-Domstolen afsagde den 9. februar 2023 dom i sag C-453/21 mellem X-FAB Dresden GmbH & Co. KG (»X-FAB«) mod FC, som var ansat som databeskyttelsesrådgiver hos X-FAB. Sagen var indgivet som en præjudiciel forelæggelse af den tyske forbundsdomstol i arbejdsretlige sager.

Sagen vedrørte en fortolkning af GDPR artikel 38, stk. 3, 2. pkt. og artikel 38, stk. 6, der omhandler forbuddet mod afskedigelse af databeskyttelsesrådgiveren og dennes mulighed for at udføre andre opgaver og have andre pligter.

FC fik den 1. juni 2015 en stilling som databeskyttelsesrådgiver hos X-FAB. Samtidig havde han siden den 1. november 1993 varetaget hvervet som formand for samarbejdsudvalget i X-FAB og næstformand for det centrale samarbejdsudvalg, som er oprettet for tre virksomheder i den koncern, som X-FAB er en del af. X-FAB valgte den 1. december 2017 at afskedige FC fra stillingen som databeskyttelsesrådgiver, da man mente, at der var en risiko for interessekonflikt, hvis FC varetog hvervet som databeskyttelsesrådgiver samtidig med, at han var formand for samarbejdsudvalget. X-FAB mente, at de to stillinger var uforenelige.

FC indbragte herefter sagen for de tyske domstole, da en databeskyttelsesrådgiver ifølge GDPR artikel 38, stk. 3, 2. pkt., ikke må afske-

diges eller straffes af den dataansvarlige for at udføre sine opgaver.

Den tyske forbundsdomstol ønskede oplyst, hvorvidt tysk lovgivning kan stille strengere krav til afskedigelse af en databeskyttelsesrådgiver end dem, der er fastsat i GDPR. Ifølge tysk ret skal en databeskyttelsesrådgiver således fjernes fra sin stilling, hvis der er vægtige grunde til dette, selvom afskedigelsen ikke er forbundet med databeskyttelsesrådgiverens udførelse af sine opgaver. Yderligere ønskede forbundsdomstolen oplyst, om der eksisterede en interessekonflikt som omhandlet i GDPR artikel 38, stk. 6, 2. pkt., når en databeskyttelsesrådgiver samtidig varetog hvervet som formand for den dataansvarliges samarbejdsudvalg.

EU-Domstolen fandt, at reglen i GDPR artikel 38, stk. 3, har til formål at bevare databeskyttelsesrådgiverens funktionelle uafhængighed for at sikre effektiviteten af GDPR's bestemmelser. Hver medlemsstat kan frit fastsætte særlige beskyttelsesbestemmelser vedrørende afskedigelse af en databeskyttelsesrådgiver, så vidt lovgivningen ikke bringer formålet med GDPR i fare. Det vil eksempelvis være tilfældet, hvis den nationale regel forhindrer opsigelse af en databeskyttelsesrådgiver, som ikke er i stand til at udføre sine opgaver uafhængigt på grund af en interessekonflikt.

Det påhviler de nationale domstole at sikre sig, at dette ikke er tilfældet med den nationale lovgivning.

Endelig gentog Domstolen, at en databeskyttelsesrådgiver i henhold til GDPR artikel 38, stk. 6, har mulighed for at varetage andre opgaver i den virksomhed, de er ansat i, såfremt dette ikke medfører en risiko for interessekonflikt. Hvorvidt dette er tilfældet, skal afgøres fra sag til sag, og det var herefter op til den nationale domstol at bedømme, hvorvidt det var tilfældet i den foreliggende sag.

Læs hele dommen her: *https://curia.europa.eu/juris/document/document.jsf?text=&docid=270323&pageIndex=0&doclang=da&mode=lst&dir=&occ=first&part=1&cid=943064*

Den registreredes ret til indsigt i, hvem den dataansvarlige deler personoplysninger med

EU-Domstolen afsagde den 12. januar 2023 dom i en præjudiciel forelæggelse indgivet af den østrigske højesteret i sag C-154/21 om fortolkning af GDPR artikel 15, stk. 1, litra c, om den registreredes ret til at vide, hvem den dataansvarlige har videregivet personlysninger til.

Sagen blev indledt efter at en østrigsk borger anmodede en post- og logistikvirksomhed om indsigt i de personoplysninger, som virksomheden behandlede om vedkommende samt identiteten af eventuelle modtagere af disse oplysninger. Virksomheden, der var dataansvarlig, oplyste om behandlingsformål og modtagernes kategorier, men ikke om de specifikke handelspartnere, som havde modtaget personoplysningerne.

Borgeren sagsøgte virksomheden med krav om oplysning af handelspartnernes identitet. Ved første og anden instans fik den registrerede ikke medhold, da det blev anset som tilstrækkeligt at oplyse om kategorien af modtagere i overensstemmelse med GDPR artikel 15, stk. 1, litra c.

Sagen nåede den østrigske højesteret, som forelagde spørgsmålet om fortolkning af bestemmelsen for EU-Domstolen som et præjudicielt spørgsmål, da det var uklart, om der skal gives specifikke oplysninger om modtagerne, eller om det er tilstrækkeligt blot at oplyse om kategorien af modtagere.

EU-Domstolen fastslog indledningsvis, at ordlyden af artikel 15, stk. 1, litra c ikke entydigt angiver, om den registrerede har ret til at modtage specifikke oplysninger om modtagerne eller blot oplysninger om kategorien af modtagere. Derfor måtte spørgsmålet afgøres ved fortolkning af sammenhængen og formålet med bestemmelsen.

EU-Domstolen understregede, at for at sikre en effektiv udøvelse af de øvrige rettigheder i GDPR, såsom retten til sletning og retten til at gøre indsigelse mod behandlingen, er det afgørende, at den registrerede kender de konkrete modtagere af personoplysningerne. På den baggrund konkluderede EU-Domstolen, at den registrerede som udgangspunkt har ret til at få oplyst identiteten på hver modtager af sine personoplysninger.

Afslutningsvis kom EU-Domstolen frem til, at der kan afviges fra dette udgangspunkt, således at det under særlige omstændigheder kan være tilstrækkeligt at oplyse om kategorien af modtagere. For eksempel, hvis de konkrete modtagere er ukendte, eller hvis den registreredes anmodning er åbenbart grundløs eller overdreven, jf. GDPR artikel 12, stk. 5.

Læs hele dommen her: *https://curia.europa.eu/juris/document/document.jsf?docid=269146&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=DA&cid=149842*

EDPB iværksætter håndhævelsesaktion på tværs af EU med 26 nationale databeskyttelsesmyndigheder

Det Europæiske Databeskyttelsesråd (»EDPB«) har indledt en undersøgelse af rollen som databeskyttelsesrådgiver (»DPO«) under den koordinerede håndhævelsesramme for 2023, som omfatter 26 databeskyttelsesmyndigheder i EU/EØS, herunder EDPB.

Indsatsen fokuserer på DPO'ers udpegelse og stilling, idet de udgør en afgørende rolle i at sikre overholdelse af databeskyttelseslovgivningen og beskytte de registreredes rettigheder. En DPO er en integreret del af den dataansvarliges organisa-

tion i henhold til GDPR artikel 37-39, hvorfor vedkommende hverken er en del af databeskyttelsesmyndighederne eller fungerer som repræsentant herfor. Dog har en DPO en særlig stilling i forhold til myndighederne, da de samarbejder hermed og fungerer som kontaktled.

Databeskyttelsesmyndighederne vil anvende forskellige metoder til at vurdere, om DPO'er har den nødvendige stilling og de nødvendige ressourcer til at udføre deres opgaver efter GDPR. Dette vil omfatte udsendelse af spørgeskemaer til DPO'er, iværksættelse af formelle undersøgelser og opfølgning på igangværende undersøgelser. Resultaterne af initiativet vil efterfølgende blive analyseret og anvendt til at udvikle de nationale tilsyns- og håndhævelsesforanstaltninger samt til at opnå en dybere forståelse af DPO-rollen på EU-plan.

Dette er det andet initiativ under EDPB's koordinerede håndhævelsesramme, som har til formål at fremme samarbejdet og håndhævelse af GDPR blandt databeskyttelsesmyndighederne. Det første initiativ i 2022 fokuserede på den offentlige sektors brug af cloud-tjenester, og resultaterne blev offentliggjort i en rapport den 18. januar 2023. EDPB vil også offentliggøre en rapport om resultatet af den koordinerede håndhævelsesaktion om DPO'ers stilling i 2023, når denne er afsluttet.

Læs EDBP's pressemeddelelse om initiativet her: *https://edpb.europa.eu/news/news/2023/launch-coordinated-enforcement-role-data-protection-officers_en*

Læs om EDPB's koordinerede håndhævelsesramme (»CEF«) her: *https://edpb.europa.eu/our-work-tools/our-documents/other/edpb-document-coordinated-enforcement-framework-under-regulation_en*

Trods visse forbedringer, understreger EDPB en række bekymringer i udtalelse til EU-Kommissionens udkast til en tilstrækkelighedsafgørelse

I december 2022 offentliggjorde EU-Kommissionen et udkast til en tilstrækkelighedsafgørelse vedrørende beskyttelsesniveauet for personoplysninger, der overføres fra EU til USA under det nye EU-US Data Privacy Framework (»DPF«).

Udkastet blev efterfølgende sendt i høring til Europa-Parlamentet, de europæiske medlemsstater og til EDPB med henblik på disses bemærkninger.

EDPB offentliggjorde den 28. februar en udtalelse om Kommissionens udkast, to uger efter at Europa-Parlamentets Udvalg om Borgernes Rettigheder og Retlige anliggender (»LIBE«) opfordrede Kommissionen til ikke at vedtage dens udkast til tilstrækkelighedsafgørelse, men i stedet fortsætte forhandlingerne med den amerikanske regering.

I udtalelsen fremhæver EDPB, at der med Kommissionens udkast er sket en forbedring med indførelsen af principperne om nødvendighed og proportionalitet ved amerikanske efterretningstjenesters behandling af personoplysninger i forbindelse med signalefterretninger. Derudover mener EDPB, at klageadgangen for registrerede i EU også er blevet væsentligt forbedret med oprettelsen af en »Data Protection Review Court« sammenlignet med den tidligere ombudspersonsinstitution, der blev etableret under Privacy Shield-ordningen.

Trods forbedringerne har EDPB dog stadig en række bekymringer.

For så vidt angår de amerikanske myndigheders adgang til og brug af oplysninger, der er overført til USA, omhandler bekymringerne særligt den midlertidige masseindsamling af oplysninger og hvordan Data Protection Review Court kommer til at fungere i praksis.

Angående den kommercielle del relaterer bekymringerne sig til de registreredes rettigheder, herunder behovet for at præcisere, hvordan en registreret kan udøve sin ret til at få indsigt i sine oplysninger. EDPB mener også, at der er brug for specifikke regler i DPF vedrørende automatiske individuelle afgørelser, herunder profilering.

Derudover udtrykker EDPB bekymring over den del af udkastet, der omhandler videreoverførsel af personoplysninger fra den oprindelige modtager til andre tredjelande.

EDPB ønsker, at vedtagelsen såvel som ikrafttrædelsen bliver betinget af, at alle amerikanske efterretningstjenester implementerer de opdaterede politikker og procedurer til gennemførelsen af det præsidentielle dekret, som blev udstedt i oktober 2022 (executive order 14086).

EDPB opfordrer desuden Kommissionen til at foretage revision af tilstrækkelighedsafgørelsen hvert tredje år.

Læs udtalelsen fra EDPB her: *https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-52023-european-commission-draft-implementing_en*

EDPB har vedtaget tre nye retningslinjer

På plenarmødet den 14-15. februar 2023 vedtog EDPB tre retningslinjer.

De første retningslinjer vedrører forholdet mellem GDPR artikel 3 om GDPR's territoriale anvendelsesområde og bestemmelserne om internationale overførsler i kapitel 5. Formålet med disse retningslinjer er at bistå dataansvarlige og databehandlere med at identificere, om en databehandlingsaktivitet udgør en international overførsel samt at skabe en fælles forståelse af begrebet »internationale overførsler«. Efter den offentlige høring blev retningslinjerne revideret og suppleret med yderligere afklaringer. Særligt blev der tilføjet en præcisering af dataansvarliges ansvar, når dataeksportøren er en databehandler. Herudover

er der blevet indsat flere eksempler, for at belyse aspekter af direkte indsamling samt betydningen af, at dataimportøren er i et tredjeland.

Det andet sæt retningslinjer vedrører certificering som et overførselsværktøj. Det primære formål med retningslinjerne er at give yderligere afklaring på den praktiske anvendelse af dette overførselsværktøj. Retningslinjerne består af fire dele, der hver især fokuserer på specifikke aspekter vedrørende certificering som et værktøj til overførsler. Retningslinjerne supplerer EDPB's Retningslinjer 1/2018 om certificering, som giver mere generel vejledning om certificering.

Det tredje sæt retningslinjer vedrører vildledende designmønstre på sociale medieplatforme. Retningslinjerne giver praktiske anbefalinger til designere og brugere af sociale medieplatforme om, hvordan man vurderer og undgår vildledende designmønstre i sociale mediebrugerflader, som overtræder kravene efter GDPR. Retningslinjerne giver konkrete eksempler på typer af vildledende designmønstre og indeholder specifikke anbefalinger til designere af brugergrænseflader, der letter den effektive implementering af GDPR.

Læs hele pressemeddelelsen her: *https://www.datatilsynet.dk/internationalt/internationalt-nyt/2023/feb/edpb-vedtager-tre-vejledninger-og-arbejdsprogrammet-for-2023-2024*

EDPB vedtager rapport om offentlige myndigheders brug af cloud-baserede services

På plenarmødet den 17. januar 2023 vedtog EDPB en rapport vedrørende offentlige myndigheders brug af cloud-tjenester. Rapporten er udarbejdet som led i EDPB's koordinerede håndhævelsesramme (»Coordinated Enforcement Framework« (»CEF«)).

I 2022 gennemførte 22 af de europæiske, nationale tilsynsmyndigheder, herunder det danske Datatilsyn (»Datatilsynet«), en koordineret undersøgelse af offentlige myndigheders brug af cloud-tjenester for at opnå en harmoniseret tilgang til GDPR på dette område. Rapporten er baseret på de indledende, nationale tilsyn og de nationale tilsynsmyndigheders besvarelse af EDPB's spørgeskema herom. En række landes besvarelse af dette spørgeskema findes som bilag til rapporten. På baggrund af disse nationale tilsyn identificerer rapporten otte (hoved)udfordringer.

De identificerede udfordringer omfatter blandt andet manglende brug af risikovurderinger, manglende individuel og skræddersyet sammensætning af kontrakter indgået med leverandører af cloud-tjenester, samt udfordringer i forbindelse med overførelser af data til udlandet samt udenlandske offentlige myndigheders adgang til data lagret inden for EU/EØS.

På baggrund af udfordringerne, oplister rapporten en række fokuspunkter samt 13 konkrete anbefalinger til løsning, som sikrer overholdelsen af GDPR for de myndigheder der benytter cloud-tjenester.

De 13 konkrete anbefalinger vedrører blandt andet, at de nationale myndigheder bør foretage en Data Protection Impact Assessment (en konsekvensanalyse vedrørende databeskyttelse (»DPIA«)) og som minimum en risikovurdering, samt at der jævnligt foretages en fornyet gennemgang og analyse heraf. Derudover indebærer anbefalingerne, at de nationale myndigheder sikrer, at kontraktparternes roller er entydigt og tydeligt fastsat i de offentlige myndigheders kontrakter med leverandørerne og at leverandører af cloud-tjenester kun arbejder ud fra dokumenterede instruktioner fra den offentlige myndighed og altid overholder GDPR. EDPB anbefaler herudover, at der sker en styrkelse af samarbejdet de offentlige myndigheder imellem, når de forhandler med leverandørerne af cloud-tjenester, da dette giver en stærkere forhandlingsposition over for leverandørerne. Herudover anbefales det, at de offentlige myndigheder analyserer, hvorvidt et tredjelands lovgivning kan føre til, at disse lande kan tilgå en EU/EØS-leverandør af cloud-tjenesters datalagre, eller om der sker overførsel af data til tredjelande i forbindelse med leverandørernes levering af rutinemæssige tjenesteydelser eller i forbindelse med opfyldelse af leverandørens egne forretningsmål.

Læs den fulde rapport her: *https://edpb.europa.eu/our-work-tools/our-documents/other/coordinated-enforcement-action-use-cloud-based-services-public_en*

Læs Det Europæiske Databeskyttelsesråds pressemeddelelse her: *https://edpb.europa.eu/news/news/2023/edpb-determines-privacy-recommendations-use-cloud-services-public-sector-adopts_en*

DPC træffer afgørelse på baggrund af EDPBs bindende afgørelse over for mediet WhatsApp

Den irske databeskyttelsesmyndighed (»DPC«) har den 19. januar 2023 udstedt en bøde på € 5,5 mio. til WhatsApp Ireland Limited (»WhatsApp«) som følge af kommunikationsmediets overtrædelse af GDPR.

En tysk bruger klagede over WhatsApp-tjenesten den 25. maj 2018. Inden GDPR trådte i kraft, bad WhatsApp sine brugere om at acceptere nye servicevilkår for at fortsætte med at bruge tjenesten. WhatsApp mente, at accept af de opdaterede vilkår konstituerede en kontrakt mellem brugeren og WhatsApp, og at databehandlingen derfor var lovlig efter GDPR artikel 6, stk. 1, litra b. Klageren hævdede dog, at det reelt var et tvungent samtykke for brugerne, ved at gøre brugen af tjenesten betinget af accept af de nye vilkår, hvorfor dette var i strid med GDPR. Uenighed blandt DPC som ledende tilsynsmyndighed og de berørte tilsynsmyndigheder om dette retsgrundlag,

foranledigede tvistbilæggelsesproceduren hos EDPB efter GDPR artikel 65, stk. 1, litra a.

Den irske afgørelse om WhatsApp kom i forlængelse af de tre bindende afgørelser, som EDPB vedtog tilbage i december 2022. De vedrører alle moderselskabet Meta Platforms Ireland Limited (»Meta«) og dets behandling af personoplysninger på netværksplatformene Facebook, Instagram og WhatsApp. DPC's afgørelser for så vidt angår platformene Facebook og Instagram er behandlet i en forudgående udgave af Lov og Data, med udgivelsesnr. 150.

DPC's endelige afgørelse vedrørende WhatsApp, afspejler EDPB's bindende afgørelse. Følgelig fastsætter afgørelsen, at WhatsApp ikke kan benytte GDPR artikel 6, stk. 1, litra a som behandlingshjemmel i forbindelse med levering af serviceforbedringer og -sikkerhed (undtagen det, som EDPB i sin afgørelse betegnede som »IT-sikkerhed«) ved brug af WhatsApp-tjenesten. Virksomhedens forhenværende behandling af disse oplysninger i påstået tillid til dette aftalemæssige retsgrundlag, udgjorde herefter en overtrædelse af GDPR artikel 6, stk. 1. I forlængelse heraf pålagde DPC, at WhatsApp indordner sin databehandling i overensstemmelse med GDPR inden for en tidsfrist på seks måneder.

DPC's afgørelse om WhatsApp er endvidere interessant, da den rejser mulige spørgsmål om EDPB's kompetencer efter GDPR. Sideløbende med tolkningen af GDPR, påbød EDPB i sin bindende afgørelse DPC at foretage en fornyet og udvidet undersøgelse af WhatsApps behandling af personoplysninger. Dette har DPC dog udtalt, at man mener, overskrider EDPB's kompetencer over for de nationale tilsynsmyndigheder, hvorfor DPC har forbeholdt sig muligheden for at anfægte dette aspekt af den bindende afgørelse.

Læs EDPB's pressemeddelelse her: *https://edpb.europa.eu/news/news/2023/edpb-publishes-binding-decision-concerning-whatsapp_en*

Læs det irske datatilsyns pressemeddelelse her: *https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-inquiry-whatsapp*

EU-Kommissionen anmoder om input til ny GDPR-lovgivning om grænseoverskridende procedureregler

I oktober 2022 udarbejdede EDPB et brev til EU-Kommissionen, hvori EDPB præsenterede en liste over administrative procedureregler, som kan harmoniseres yderligere. I sit brev påpegede EDPB b.la., at det ikke er hensigtsmæssigt at revidere GDPR på daværende tidspunkt. I stedet appellerede rådet til at reducere forskellene i administrative procedurer og praksis på tværs af medlemslandene, da forskellige administrative procedurer kunne have negative konsekvenser for grænseoverskridende samarbejder.

EU-kommissionen har anerkendt det fremførte behov og har efterfølgende iværksat en høring og et kommende lovgivningsinitiativ, hvor det frem til den 24. marts var muligt at indgive input til den nye lovgivning om harmonisering af GDPR-procedureregler i grænseoverskridende samarbejder.

Læs hele pressemeddelelsen her: *https://www.datatilsynet.dk/internationalt/internationalt-nyt/2023/mar/eu-kommissionen-har-ivaerksat-hoering*

En række nationale parlamenter og internationale organisationer forbyder eller fraråder deres medarbejdere at bruge TikTok på deres arbejdstelefoner

EU-Kommissionen udstedte den 23. februar 2023 en pressemeddelelse, der forbød medarbejdere at bruge TikTok på arbejdstelefoner samt private telefoner, der havde Kommissionens IT-systemer integreret.

I slutningen af februar vedtog en række nationale parlamenter ligeledes, at deres medarbejdere skulle slette appen »TikTok«. Det danske Folketing udstedte i den forbindelse den 28. februar 2023 en pressemeddelelse om, at man fraråder medlemmer eller ansatte af Folketinget at bruge det populære medie på deres udleverede mobile enheder. Pressemeddelelsen blev udstedt på baggrund af en anbefaling fra det danske Center for Cybersikkerhed og har efterfølgende resulteret i, at det danske Medieråd har opfordret til, at børn og unge også bør genoverveje deres brug af TikTok.

Herudover har en lang række store virksomheder og internationale organisationer ligeledes meldt ud, at de forbyder deres medarbejdere at bruge mediet. I USA diskuteres det netop, om det er hensigtsmæssigt at indføre et generelt forbud mod brugen af appen.

Den styrkede opmærksomhed omkring appen skyldes, at der er risiko for, at TikTok kan få adgang til dine data. Det danske Center for Cybersikkerhed udtalte i den forbindelse, at der er risiko for spionage ved brugen af TikTok.

Læs Kommissionens pressemeddelelse her: *https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1161*

Læs Folketingets pressemeddelelse her: https://www.ft.dk/da/aktuelt/nyheder/2023/02/tiktok

Datatilsynet har offentliggjort en opdateret vejledning om databeskyttelse i ansættelsesforhold

Datatilsynet har offentliggjort en revideret udgave af Datatilsynets vejledning om databeskyttelse i ansættelsesforhold. Datatilsynet har på baggrund af de seneste års praksis revideret vejledningen, ligesom vejledningen har gennemgået en strukturel opdatering og indeholder en række præciseringer.

Tidligere har Datatilsynet i alle sammenhænge anbefalet at indhen-

te samtykke forud for indhentelse og afgivelse af en reference. Fremover kan et samtykke som udgangspunkt ikke længere danne grundlag for indhentelse og videregivelser af referencer. Det skyldes, at et samtykke i en ansættelsesproces ofte ikke lever op til kravet om frivillighed. Det rette grundlag for at indhente referenceoplysninger vil fremover kunne findes i interesseafvejningsreglen i GDPR artikel 6, stk. 1, litra f.

Særligt i forhold til straffeattester præciserer Datatilsynet, at det ikke er tilladt for en arbejdsgiver at have en generelt praksis for indhentning af straffeattester i forbindelse med rekrutteringsforløb. Arbejdsgiveren er fremover forpligtet til at foretage en konkret vurdering af den enkelte ansættelsessituation. Det fremgår af den reviderede vejledning, at en straffeattest med oplysninger om strafbare forhold fortsat kan behandles med hjemmel i lov nr. 502 af 23. maj 2018 (»den danske databeskyttelseslov«) § 8, stk. 3. Hvis straffeattesten derimod ikke indeholder oplysninger om strafbare forhold, vil grundlaget herefter udgøre interesseafvejningsreglen i GDPR artikel 6, stk. 1, litra f.

Datatilsynet har herudover også fundet anledning til at opdatere en række afsnit, herunder om arbejdsgiverens oplysningspligt og videregivelse af personoplysninger. Ifølge den opdaterede vejledning er det ikke tilladt for en arbejdsgiver at indhente kreditoplysninger om ansøgere fra Ribers Kredit Information, medmindre der er tale om ansættelse i en position, der anses for at være særligt betroet. Datatilsynet fremhæver, at bedømmelsen af, hvilke positioner der betragtes som betroede, vil afhænge af arbejdsretlige standarder. Dette kan omfatte ledende medarbejdere, eller andre stillinger, der indebærer en betydelig grad af ansvar og tillid.

Læs hele Datatilsynets pressemeddelelse her: *https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/mar/datatilsynets-vejledning-om-databeskyttelse-i-ansaettelsesforhold-er-revideret*

Læs hele Datatilsynets vejledning her: *https://www.datatilsynet.dk/Media/0/8/Vejledning%20om%20databeskyttelse%20i%20forbindelse%20med%20ans%C3%A6ttelsesforhold.pdf*

Datatilsynet lancerer ny database med statistik over brud på persondatasikkerhed

Datatilsynet lancerede den 23. marts 2023 en ny side på deres hjemmeside med statistik over brud på persondatasikkerheden. Statistikken udarbejdes ud fra de anmeldelser, som Datatilsynet modtager om brud på persondatasikkerheden efter GDPR. Statistikken opdateres derfor løbende.

På siden findes en detaljeret statistik for antallet af anmeldte brud til Datatilsynet, hvilke typer af brud der anmeldes, kategoriseret som hændelsestyper, samt hvilke sektorer der anmelder brud til Datatilsynet, kategoriseret under brancher.

Databasen gør det muligt for alle interesserede at få et detaljeret indblik i statistik over brud på persondatasikkerheden i forhold til f.eks. specifikke hændelsestyper eller inden for særligt udsatte områder, samt udviklingen over tid på området. Udstillingen af data skal være med til at forebygge lignende fremtidige brud på persondatasikkerheden og sikre databeskyttelsen.

Læs nyheden her: *https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/mar/ny-og-mere-detaljeret-statistik-over-brud*

Se databasen her: *https://www.datatilsynet.dk/sikkerhedsbrud/statistik-over-brud-paa-persondatasikkerheden*

Datatilsynet har truffet principielle afgørelser i sager om cookie walls og offentliggjort retningslinjer vedrørende brugen af cookie walls

Datatilsynet har i en pressemeddelelse den 20. februar 2023 oplyst, at de har truffet to principielle afgørelser vedrørende brugen af cookie walls. Afgørelserne er truffet i sager mod henholdsvis Gul og Gratis og Jysk Fynske Medier. Herudover har Datatilsynet også udstedt et sæt retningslinjer, der skal hjælpe dem, der driver hjemmesider med at overholde de databeskyttelsesretlige regler, når de vil benytte sig af cookie walls og alternativer hertil.

Offentliggørelsen af afgørelserne over for Gul og Gratis og Jysk Fynske Medier, er sket ved journalnummer 2021-31-4871 og 2021-31-5553.

En cookie wall er en funktion, der gør en adgang til en hjemmeside betinget af, at den besøgende samtykker til brug af cookies og eventuel underliggende behandling af sine personoplysninger, typisk til brug for markedsføringsformål. Brugen af cookie walls ses ofte på hjemmesider, der helt eller delvist finansieres af annonceindtægter. Indehaverne af sådanne hjemmesider supplerer sommetider brugen af en cookie wall med et alternativ, der kan give adgang til hjemmesiden, f.eks. ved at tilbyde en betalingsadgang. Brugen af såvel cookie walls som betalingsalternativer skal opfylde visse krav for at leve op til de databeskyttelsesretlige regler.

I Datatilsynets retningslinjer angående brugen af cookie walls er der opstillet 4 kriterier til at vurdere, om et samtykke kan anses for frivilligt og dermed gyldigt. For det første skal brugen af en cookie wall suppleres med et rimeligt alternativ. Her kan et betalingsalternativ til samtykket være legitimt, men det forudsætter, at tjenesten der tilbydes herigennem i vidt omfang svarer til den tjeneste, der følger med samtykket til behandling. Dernæst skal betalingsalternativet have en rimelig pris. Heri ligger, at betalingsalternativet ikke må være prissat så højt, at den hjemmesidebesøgende ikke reelt gives et frit valgt mellem adgang via samtykke og adgang via betaling. For det tredje skal den behandling af personoplysninger, der finder

sted efter samtykkeløsningen være begrænset til det nødvendige. Det betyder, at alle de formål, som virksomheden anmoder om samtykke til, er en nødvendig del af alternativet til betaling. For det fjerde skal behandlingen af personoplysninger for besøgende, der har benyttet sig af betalingsalternativet begrænses til det nødvendige. Dette medfører at kun personoplysninger, som er nødvendige for at levere den pågældende tjeneste må behandles. Det gælder eksempelvis, hvis det er nødvendigt at behandle visse personoplysninger til oprettelse og administration af en brugerprofil, såfremt denne profil følger med tjeneste, der er betalt for.

I sine afgørelser fastslår Datatilsynet, at hverken Gul og Gratis eller Jysk Fynske Medier levede op til samtykkekravet. Over for Jysk Fynske Medier fandt Datatilsynet, at den tjeneste der blev tilbudt mod samtykke til behandling af personoplysninger, ikke i vidt omfang svarede til den tjeneste, der blev tilbudt mod betaling. Dette skyldtes, at samtykket kun gav adgang til dele af indholdet på hjemmesiden, mens betalingsalternativet (abonnementstegning), gav adgang til alt indhold. Der forelå således reelt ikke et frit valg mellem de to løsninger, hvilket er et gyldighedskrav for samtykket i medfør af GDPR. I tillæg hertil fandt Datatilsynet, at Jysk Fynske Medier ikke havde påvist, at behandling af personoplysninger til statistiske formål var en nødvendig del af samtykkeløsningen. Jysk Fynske Mediers samtykkeløsning opfyldte således ikke GDPR artikel 6, stk. 1, litra a, og artikel 4, nr. 11, jf. GDPR artikel 5, stk. 2, jf. artikel 5, stk. 1, litra a.

Over for Gul og Gratis fandt Datatilsynet, at de to løsninger i vidt omfang svarede til hinanden, og der var således ikke et problem i relation til det frie valg mellem de to løsninger. Dog fandt Datatilsynet, ligesom i sagen mod Jysk Fynske Medier, at Gul og Gratis ikke havde påvist, at behandling af personoplysninger til statiske formål var en nødvendig del af samtykkeløsningen. Kravet til samtykkets frivillighed i medfør af GDPR var således heller ikke opfyldt.

Begge virksomheder blev i konsekvens heraf meddelt påbud om at påvise, at deres samtykkeløsninger opfylder de databeskyttelsesretlige krav om et frivilligt samtykke.

Læs hele pressemeddelelsen her: *https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/feb/brug-af-cookie-walls*

Læs mere om Datatilsynets retningslinjer her: *https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/cookies/cookie-walls*

Læs afgørelsen over for Gul og Gratis her: *https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/feb/gul-og-gratis-brug-af-cookie-walls*

Læs afgørelsen over for Jysk Fynske Medier her: *https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/feb/jysk-fynske-mediers-brug-af-cookie-walls*

Undersøgelse viser behov for øget fokus på sletning og konsekvensanalyse

Den 23. februar 2023 udsendte Datatilsynet en pressemeddelelse vedrørende et omfattende spørgeskema-baseret modenhedstilsyn af 50 kommuner og alle 5 regioner.

Modenhedstilsynet viste, at der generelt er behov for et øget fokus på sletning, rettighedsstyring og foranstaltninger ved fremsendelse af mails med personoplysninger. På baggrund af modenhedstilsynet har Datatilsynet udarbejdet en målrettet vejledning vedrørende nedslag i fem udvalgte tendenser.

For det første skal organisationer tage stilling til procedurer for sletning, herunder sikre sig, at de registrerede i et længere ikke kan identificeres i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles. For det andet skal organisationer reducere risikoen for, at personoplysninger sendes forkert. Datatilsynet anbefaler hertil, at en række forebyggende foranstaltninger implementeres, herunder scanning af alle udgående e-mails med henblik på at identificere personnumre og lignende. For det tredje anbefaler Datatilsynets at foretage en løbende kontrol af brugerens adfærd og sikre, at den dataansvarlige vurderer, om behandlingsaktiviteterne er nødvendige og står i rimeligt forhold til formålene. For at afbøde konsekvenserne ved et stort angreb eller nedbrud appellerer Datatilsynet til, at kommunerne løbende opdaterer og tester it-beredskabsplaner.

Som led i den nationale cyber- og informationssikkerhedsstrategi 2022-2024 har Datatilsynet endeligt inkorporeret 20 tekniske minimumskrav til it-sikkerhed. Kravene er obligatoriske for statslige IT-løsninger og skal sikre et ensartet højt sikkerhedsniveau i staten. Kravene relaterer sig til mailkommunikation, autentifikation, mobile enheder, logning, domæner og internetvendte tjenester. Alle minimumskrav skal være implementeret senest den 1. januar 2023.

Læs hele Datatilsynets pressemeddelelsen her: *https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/feb/modenhedstilsynet-i-2022-viser-behov-for-oeget-fokus-paa-bla-sletning-og-konsekvensanalyse*

Præcisering af regler for sletning af personoplysninger ved afslutning af forskningsprojekter

Datatilsynet udsendte d. 14. marts 2023 en pressemeddelelse vedrørende reglerne om personoplysninger ved afslutning af forskningsprojekter.

Fra den 1. januar 2023 er der sket en revision af bekendtgørelse nr. 1509 af 12. december 2019 (»den danske videregivelsesbekendtgørelse«), som fastsætter betingelserne for videregivelse af personoplysninger i forbindelse med statistiske el-

ler videnskabelige undersøgelser i henhold til den danske databeskyttelseslov § 10. Tidligere var det nødvendigt at slette, anonymisere eller tilbagelevere personoplysninger ved undersøgelsens afslutning, således at det ikke var muligt at identificere enkeltpersoner baseret på disse oplysninger alene eller i kombination med andre data. I lyset af, at den dataansvarlige kan være forpligtet til at opretholde dokumentationen i en periode efter undersøgelsens afslutning for at kunne bekræfte dens validitet, kan personoplysningerne fremover overføres til opbevaring i arkiv efter reglerne i den danske arkivlovgivning.

Ikke desto mindre bør den dataansvarlige altid overveje, om det er muligt at opnå formålet med behandlingen af personoplysninger efter undersøgelsens afslutning ved at behandle oplysningerne i en anden form, for eksempel ved at pseudonymisere eller anonymisere dem, i overensstemmelse med dataminimeringsprincippet.

Læs hele datatilsynet pressemeddelelsen her: *https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/feb/praecisering-af-regler-for-sletning-af-personoplysninger-ved-afslutning-af-forskningsprojekter*

Aalborg Universitet havde ikke foretaget tilstrækkelig kontrol eller tests med brugeradgange

Datatilsynet traf den 10. februar 2023 afgørelse i en sag med journalnummer 2022-442-19476 vedrørende Aalborg Universitets manglende test og utilstrækkelige kontrol af brugeradgange.

Sagen vedrørte et brud på persondatasikkerheden hos Aalborg Universitet, som universitetet selv anmeldte til Datatilsynet den 5. august 2022. I en ukendt periode frem til den 3. august 2022 var det muligt for alle brugere med en AAU-brugerprofil, herunder studerende, medarbejdere og gæstemedarbejdere, at logge på universitets IT-system, Webmanageren. Det var alene hensigten, at IT-medarbejdere skulle have adgang til oplysningerne som led i deres daglige arbejde. Webmanageren manglede derfor den nødvendige adgangsbegrænsning. I sagen blev det oplyst, at bruddet formentlig var et resultat af en teknisk eller menneskelig fejl i forbindelse med migrering til en ny server og omskrivning af kode i systemet i sommeren 2020. Der blev ikke efterfølgende foretaget testning af adgangskontrol i Webmanager-systemer og interne retningslinjer var ikke blevet fulgt.

Systemet indeholdte ikke-følsomme oplysninger om universitetets medarbejdere, hvoraf de fleste af oplysningerne i forvejen var offentliggjorte enten på universitetets hjemmeside eller internt i Outlook eller på intranettet, hvor alle medarbejdere har adgang.

Datatilsynet udtalte kritik af, at Aalborg Universitet ikke havde behandlet personoplysningerne i overensstemmelse med GDPR artikel 32, stk. 1.

Datatilsynet henviste i den forbindelse til, at dette normalt vil indebære, at ændringerne og opdateringer sker efter fastsatte procedurer, hvorved mulige konsekvenser og risici afdækkes. Yderligere skal der planlægges test, der kan verificere, at de fastsatte sikkerhedskrav, herunder adgangsbegrænsning, fortsat kan efterleves, når opdateringer gennemføres.

Endelig bemærkede Datatilsynet, at kravet i GDPR artikel 32 også indebærer, at den dataansvarlige løbende kontrollerer, at brugeradgange til et system med personoplysninger er begrænset til de brugere, der har et sagligt behov for adgang.

Læs hele afgørelsen her: *https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/feb/kritik-af-aalborg-universitet-for-manglende-test-og-utilstraekkelig-kontrol-af-brugeradgange*

Vækstfonden havde ikke indhentet gyldige samtykker og havde ikke opfyldt oplysningspligten ved brug af spy pixels i Vækstfondens nyhedsbreve

Datatilsynet traf den 20. december 2023 afgørelse i en sag med journalnummer 2022-432-0080. Sagen vedrørte Vækstfondens manglende indhentelse af gyldige samtykker samt manglende opfyldelse af oplysningspligten i forbindelse med behandling af personoplysninger indhentet ved brug af spy pixels i Vækstfondens nyhedsbreve.

I en konkret klagesag blev Datatilsynet gjort opmærksom på Vækstfondens anvendelse af spy pixels. Dette gav Datatilsynet anledning til af egen drift, den 17. januar 2022, at indlede en nærmere undersøgelse af Vækstfondens behandling af personoplysninger indhentet ved brug af spy pixels i nyhedsbreve.

Formålet for Vækstfonden med at benytte spy pixels i deres nyhedsbreve sendt ud til abonnenterne, var at analysere læsernes adfærd i forhold til nyhedsbrevet for at kunne tilrettelægge fremtidige nyhedsbreve herudfra samt at optimere selve udsendelsen af nyhedsbreve.

Vækstfonden bemærkede i sagen, at der alene var tale om behandling af almindelige personoplysninger og ikke følsomme eller fortrolige personoplysninger.

Vækstfonden blev opmærksom på problemet i maj 2021, hvorefter Vækstfondens indledte deres egen undersøgelse af sagen. Fonden oplyste i sagen, at de behandlede abonnenters data med samtykke som behandlingshjemmel, men at man grundet menneskelige fejl, ikke havde fået indhentet fornyede samtykker fra nyhedsbrevsmodtagerne i forhold til anvendelse af spy pixels, og fonden ophørte heller ikke med at anvende spy pixels i perioden september 2021 til januar 2022. Dette erkendte Vækstfonden.

Datatilsynet udtalte på den baggrund alvorlig kritik af, at Vækst-

fonden havde behandlet personoplysninger i strid med GDPR artikel 6, stk. 1, litra a og artikel 13.

Vækstfonden har senere oplyst, at de har skiftet leverandør til udsendelsen af nyhedsbreve samt opdateret deres privatlivspolitik, som der vil blive henvist til i samtykketeksten.

Læs hele afgørelsen her: *https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/dec/anvendelse-af-spy-pixels-i-forbindelse-med-udsendelse-af-nyhedsbrev*

Datatilsynet har offentliggjort sine fokusområder i 2023

Datatilsynet har i en pressemeddelelse den 2. februar 2023 oplyst, at der i 2023 vil være fokus på at finde en bedre balance mellem målrettede tilsynsaktiviteter og klagesagsbehandling, som del af Datatilsynets strategi for at styrke sin data- og risikobaserede tilsynsindsats: »Tilsyn med effekt: Datatilsynets data- og risikobaserede tilgang 2020-2023«.

Der har været en væsentlig stigning i tilsynsaktiviteterne de seneste år, men Datatilsynet vil nu foretage en justering af kursen, så der i færre tilfælde sker en tilbundsgående undersøgelse af klagesagerne - mens der tages flere generelle sager op af egen drift. Disse sager udvælges stadig ud fra bl.a. klager, brud på persondatasikkerheden, medieomtale og tips.

Datatilsynet vil også styrke indsatsen på de områder, hvor der er tale om mange borgeres personoplysninger, særligt beskyttelsesværdige personoplysninger eller personoplysninger med en høj risiko for borgerne.

Derudover har Datatilsynet offentliggjort en oversigt over de temaer, som vil være et særligt fokus for de målrettede tilsynsaktiviteter i 2023:

- Beskyttelsen af oplysninger om børn.
- Udpegning af databeskyttelsesrådgivere og deres rolle.
- Fremstillingsvirksomheder med særligt fokus på specialfremstillede produkter med levering direkte til borgerne.
- Folketinget og Folketingets institutioner.
- Behandling af personoplysninger om hjemmesidebesøgende.
- TV-overvågning, særligt parkeringsselskabers brug af tv-overvågning i forbindelse med udstedelse af parkeringsafgifter.
- Tilladelser til at videregive oplysninger fra forskning.
- Behandling af personoplysninger i fælleseuropæiske informationssystemer.
- Retshåndhævelsesloven.

Læs hele pressemeddelelsen her: *https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/feb/datatilsynets-fokusomraader-i-2023*

Se listen her: *https://www.datatilsynet.dk/afgoerelser/generelt-om-tilsyn/saerlige-fokusomraader-for-datatilsynets-tilsynsaktiviteter-i-2023*

Datatilsynet offentliggør vejledende tekst om påvisningskrav og dataminimering

Den 20. januar 2023 udsendte Datatilsynet en pressemeddelelse om, at de har udarbejdet en vejledende tekst om opbevaring af personoplysninger med henblik på dokumentation, nærmere bestemt opbevaring af personoplysninger med det formål at kunne påvise, at man som dataansvarlig overholder databeskyttelsesreglerne om samtykke.

Vejledningen bygger på, at GDPR artikel 7 indeholder en række betingelser, som skal være opfyldt, for at et samtykke kan anses for gyldigt. En af betingelserne er, at den dataansvarlige skal kunne påvise, at den registrerede har givet samtykke til behandling af sine personoplysninger. GDPR artikel 7 finder kun anvendelse, så længe behandlingen af personoplysningerne forløber. Personoplysninger, der behandles på baggrund af samtykke, skal derfor som udgangspunkt slettes i umiddelbar forlængelse af behandlingsaktivitetens ophør.

Forpligtelsen skal læses i sammenhæng med GDPR's øvrige regler og principper, blandt andet artikel 5, som stiller krav om f.eks. dataminimering og opbevaringsbegrænsning. Yderligere bestemmer GDPR artikel 24, at den dataansvarlige har ansvar for gennemførelsen af passende tekniske og organisatoriske foranstaltninger, der skal sikre og gøre den dataansvarlige i stand til at påvise, at behandling er sket i overensstemmelse med GDPR.

Påvisningskravene i artikel 5, stk. 2, og artikel 24 bør efter vejledningen opfyldes ved såkaldt systemdokumentation, der betegner dokumentation for procedurerne omkring indhentelsen af samtykket. Som eksempler herpå nævnes hvilke oplysninger den registrerede fik forelagt på tidspunktet for samtykkets afgivelse, og dokumentation for at fremgangsmåden opfyldte alle kriterier for et gyldigt samtykke.

Vejledningsteksten nævner, at en undtagelse til udgangspunktet om, at personoplysningerne skal slettes i umiddelbar forlængelse af behandlingsaktivitetens ophør er, hvis den fortsatte behandling af personoplysninger, herunder et afgivet samtykke, er nødvendig for, at et retskrav kan fastlægges, gøres gældende eller forsvares, jf. GDPR artikel 17, stk. 3, litra e. Der er imidlertid tale om en streng og konkret fortolkning af, hvad der kan anses for at være »nødvendigt«.

Den vejledende tekst har sit udspring i sagen om SmartResponse, hvor Datatilsynet blandt andet fastslog, at en opbevaringsperiode på fem år for at kunne dokumentere gyldigheden af et indhentet samtykke, ikke stemmer overens med princippet om opbevaringsbegrænsning i GDPR.

Sagen om SmartResponse er omtalt i Lov & Data 1. kvartal 2023, udgivelsesnr. 153.

Læs pressemeddelelsen her: *https://www.datatilsynet.dk/presse-og-nyhe-*

der/nyhedsarkiv/2023/jan/opbevaring-af-personoplysninger-med-henblik-paa-dokumentation

Læs vejledningsteksten her: *https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/samtykke/paavisningskrav-og-dataminimering*

Datatilsynet gør status efter et år med whistleblowerordningen

Datatilsynet fremlagde den 12. januar 2023 en beretning om det første år med whistleblowerordningen. Det fremgik af beretningen, at Datatilsynets eksterne whistleblowerordning nu har skiftet navn til »Den Nationale Whistleblowerordning«. Navneændringen skyldes, at man vil tydeliggøre, at ordningen kan anvendes til andre forhold end indberetninger vedrørende databeskyttelse, idet hele 66 % af de indberettede sager handlede om databeskyttelse.

Den danske whistleblowerordning i Datatilsynet trådte i kraft i december 2021. Ordningen er etableret i henhold til lov nr. 1436 af 29. juni 2021 om beskyttelse af whistleblowere (»den danske whistleblowerlov«, der gennemfører Europa-Parlamentets og Rådets direktiv (EU) 2019/1937 af 23. oktober 2019 om beskyttelse af personer, der indberetter overtrædelser af EU-retten (»whistleblowerdirektivet«).

Whistleblowerordningen er designet til at modtage og behandle anmeldelser vedrørende overtrædelser af EU-lovgivningen inden for områder som offentligt udbud, produktsikkerhed, miljøbeskyttelse, fødevaresikkerhed og lignende. Desuden vil ordningen også håndtere indberetninger om alvorlige lovovertrædelser og andre alvorlige forhold, herunder chikane.

I tillæg til den danske whistleblowerordning i Datatilsynet, stiller den danske whistleblowerlov bl.a. også krav om, at der skal etableres interne whistleblowerordninger på alle private og offentlige arbejdspladser med 50 eller flere ansatte.

I beretningen kan du læse nærmere om, hvor mange sager der er indberettet, hvem der blev indberettet om, og hvad udfaldet af indberetningerne blev.

Læs hele beretningen her: *https://whistleblower.dk/om-ordningen/whistleblowerordningen-i-tal*

Datatilsynet udtalte alvorlig kritik over for hjemmesides samtykkeløsning, som ikke levede op til kravene i GDPR

Datatilsynet udtalte den 23. december 2022 alvorlig kritik af virksomheden Leadwise A/S' (»Leadwise«) samtykkeløsning til placering af cookies på letfinans.dk, en hjemmeside til oprettelse og formidling af låneansøgninger. Sagen blev indledt på baggrund af en klage fra en registeret, som kunne konstatere, at cookies blev placeret på vedkommendes computer, allerede inden klager havde taget stilling til hjemmesidens samtykkeløsning. Samtykkeløsningen gav besøgende mulighed for en række afkrydsningsmuligheder samt mulighed for 'Accepter alle', 'Afvis alle' og 'Vis detaljer'.

Datatilsynet fandt at både den initiale placering af cookies inden interaktion med samtykkeløsningen og samtykkeløsningen i sig selv udgjorde overtrædelser af GDPR; navnlig artikel 6, stk. 1, litra a, og artikel 7.

Særligt vedrørende samtykkeløsningen udtalte Datatilsynet, at samtykket leveret herigennem var utilstrækkeligt informeret, bl.a. ved at hjemmesidebesøgende ikke blev informeret om retten til at trække samtykket tilbage.

Læs Datatilsynets pressemeddelelse her: *https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/feb/alvorlig-kritik-af-leadwises-samtykkeloesning-paa-letfinansdk*

Læs hele afgørelsen her: *https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/dec/alvorlig-kritik-af-leadwises-samtykkeloesning-paa-letfinansdk*

Datatilsynet strammer adgangen til personregistre på arbejdspladsen

Datatilsynet udsendte den 16. marts 2023 en pressemeddelelse vedrørende arbejdstageres adgang til at søge efter personoplysninger i registre.

Pressemeddelelsen blev udgivet som en reaktion på adskillige pressehistorier om sundhedspersonale, der uden saglig grund havde foretaget opslag i den elektroniske patientjournal.

Datatilsynet fremhæver, at man kun må behandle personoplysninger, herunder f.eks. lave journalopslag, kundekartoteker osv., hvis det er nødvendigt for at kunne udføre sit arbejde. *Datatilsynet understreger også, at arbejdsgiveren bærer ansvaret for eventuelle personopslag, som udføres af arbejdstagere. Det påhviler derfor arbejdsgiveren at sikre, at de ansatte er informeret om retningslinjerne for anvendelse af tilgængelige registre, samt at føre kontrol med arbejdstagernes opslag i disse. Desuden skal arbejdsgiveren sikre, at registrene er sat op og konfigureret på en tilstrækkelig sikker måde, som forhindrer uautoriseret adgang til registrene.*

Læs hele pressemeddelelsen her: *https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/mar/taenk-dig-om-foer-du-slaar-op*

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

Gorrissen Federspiel

Tue Goldschmieding

Ordmærket »Fucking Awesome« kunne ikke varemærkeregistreres på grund af manglende særpræg

Den Europæiske Unions Ret (»Retten«) afsagde den 15. marts 2023 dom i sag T-178/22, mellem FA World Entertainment Inc. (»FA World Entertainment«) og EUIPO.

Tvisten angik en anmodning om varemærkeregistrering af ordmærket »Fucking Awesome«. Varemærkeregisteringen vedrørte varer i Nice kvalifikationsklasse 9 om blandt andet briller og tilbehør, kvalifikationsklasse 18 om tasker, kvalifikationsklasse 25 om tøj og kvalifikationsklasse 28 om skateboards og udstyr hertil.

FA World Entertainment nedlagde påstand om annullation af EUIPO's afgørelse af 3. februar 2022 i sag R 1131/2021-5, hvor varemærket »Fucking Awesome« blev nægtet registrering, da det ikke fandtes at have et tilstrækkeligt særpræg efter Europa-Parlamentets og Rådets forordning (EU) 2017/1001 af 14. juni 2017 om EU-varemærker (»varemærkeforordningen«) artikel 7, stk. 1, litra b og f sammenholdt med varemærkeforordningens artikel 7, stk. 2.

FA World Entertainment bestred afgørelsen og gjorde modsat gældende, at ordmærket havde tilstrækkeligt særpræg. FA World Entertainment argumenterede, at begrebet »Fucking Awesome« ikke henviste til varernes egenskab eller kvalitet, men derimod at der var tale om et originalt ordspil, der henviste til varernes kommercielle oprindelse.

Retten fandt, at ordet »fucking« opfattes som en styrkemarkør mens ordet »awesome« opfattes som en beskrivelse af høj kvalitet. Retten fastslog på den baggrund, at ordmærket »Fucking Awesome« udsender et promoverende budskab og en beskrivelse af varernes kvalitet og karakteristika. Samtidig fastslog Retten, at ordmærket ikke var udtryk for den kommercielle oprindelse og det kunne ikke føre til anden konklusion, at ordmærket fremgik på etiketter, da placeringen af ordmærket ikke havde betydning.

Retten fandt herefter, at kombinationen af ordet »fucking«, omend ordet anses for vulgært, og »awesome«, ikke gør ordmærket originalt, da hvert ord har selvstændig betydning og der er dermed ikke tale om et ordspil. Retten henviste i den forbindelse til, at der er tale om et velkendt udtryk i det uformelle sprogbrug, som særligt den specifikke målgruppe forstår. På den baggrund fastslog Retten, at der ikke var tale om en sammensætning af ord, som krævede fortolkning eller igangsatte en kognitiv proces hos målgruppen.

Retten stadfæstede følgelig EUIPO's afgørelse om at afvise varemærkeregistreringen med henvisning til manglende distinktion efter varemærkeforordningens artikel 7, stk. 1, litra b og f sammenholdt med varemærkeforordningens artikel 7, stk. 2.

Læs hele dommen her: *https://curia.europa.eu/juris/document/document.jsf?text=&docid=271310&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=28352*

Undersiden af en cykelsadel var synlig under »normal brug« og kunne derfor designbeskyttes

Domstolen afsagde den 16. februar 2023 dom i en præjudiciel forelæggelse indgivet af den tyske højesteret i sag C-472/21 mellem Monz Handelsgesellschaft International mbH & Co. KG (»Monz«) og Büchel GmbH & Co. Fahrzeugtechnik KG (»Büchel«). Sagen vedrørte muligheden for designbeskyttelse af undersiden af en cykelsadel.

Tvisten i sagen angik, om en designregistrering i henhold til tysk lovgivning, der implementerer Europa-Parlamentets og Rådets direktiv 98/71/EF af 13. oktober 1998 om retlig beskyttelse af mønstre (»designdirektivet«), var gyldig. Büchel, en konkurrent til Monz, der ligeledes sælger cykelprodukter, påstod, at designregistreringen ikke var gyldig, da en del af et sammensat produkt kun kan beskyttes, hvis designet er synligt under normal brug af produktet. Dette følger af præambelbetragtning 12 til designdirektivet. Büchel mente ikke, at undersiden af en cykelsadel er synlig under normal brug, hvorfor designregistreringen ikke burde opretholdes.

Ved »normal brug« skal der i henhold til designdirektivets artikel 3, stk. 4, forstås den endelige brugers anvendelse, med udelukkelse af vedligeholdelse og reparation. Domstolen skulle derfor tage stilling til, om undersiden af cykelsadlen var synlig under den endelige brugers anvendelse af cyklen.

Domstolen kom frem til, at en sadel til en cykel skal betragtes som en komponent af et sammensat produkt efter designdirektivets artikel 3, stk. 3. Sadlen kan udskiftes, ligesom cyklen kan skilles ad og samles igen, og uden sadlen, ville cyklen ikke kunne bruges normalt. Ifølge Domstolen var det ikke et

krav, at designet i sin helhed var synligt ved enhver anvendelse af det sammensatte produkt. Yderligere skal synligheden for en udenforstående iagttager tages i betragtning ved vurderingen.

Vedrørende den »normale brug« af sadlen kom Domstolen frem til, at det ikke alene er hovedformålet med komponenten eller det sammensatte produkt, der skal tages i betragtning ved denne vurdering. Under den normale brug falder også de forskellige handlinger, der sker før og efter det primære formål med produktet. For en cykelsadel er det primære formål, at cyklisten kan sidde på denne og for cyklen som sammensat produkt, at man cykler på denne. Dertil udgør transport og opbevaring også normal brug, da disse handlinger udføres i forbindelse med den primære anvendelse.

Synligheden af undersiden af sadlen skulle derfor også vurderes i forbindelse med anden anvendelse end den primære brug, herunder transport og opbevaring. Undersiden af sadlen forekommer synlig i flere af disse situationer, f.eks. hvor cyklen løftes op og placeres på et cykelstativ. Det var således muligt, at designregistreringen af cykelsadlens underside kunne opretholdes, men det var op til den nationale ret at vurdere dette.

Dommen illustrerer, at der skal foretages en vid fortolkning af begrebet »normal brug« i tilknytning til designdirektivet. Dermed kan dele af et sammensat produkt også beskyttes, såfremt komponenterne er synlige i brugssituationer, der ikke kun udgør primær brug af produktet.

Læs hele dommen her: *https://curia.europa.eu/juris/document/document.jsf?text=&docid=270514&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=2619633*

Nyt Green Claims-direktiv tilføjer yderligere regler om miljømarkedsføring

Den 22. marts 2023 fremsatte EU-Kommissionen et forslag til et nyt direktiv med referencenr. 2023/166 (»Green Claims-direktivet«), der skal supplere reglerne om grøn markedsføring.

I dansk ret gælder et generelt forbud mod virksomheders vildledende handelspraksis over for forbrugerne, jf. lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«) § 5 og § 6. Yderligere gælder efter den danske markedsføringslovs § 13, at erhvervsdrivende skal kunne dokumentere rigtigheden af oplysninger om faktiske forhold. Reglerne udgør kernen i det nuværende forbud mod vildledende miljømarkedsføring.

Derudover har den danske Forbrugerombudsmand haft stort fokus på området og har udgivet en vejledning vedrørende brug af miljømæssige og etiske påstande samt en kvikguide til virksomheder om miljømarkedsføring.

Forslaget til Green Claims-direktivet indeholder blandt andet en bestemmelse om, at miljøanprisninger skal vurderes på en række minimumskriterier, der skal forhindre, at forbrugere bliver vildledt, jf. artikel 3. Det gælder blandt andet et kriterie om, at miljøanprisningen bygger på videnskabelig dokumentation, og at den påviser betydningen af virkninger, aspekter og ydeevne ud fra et livscyklusperspektiv.

I direktivforslagets artikel 4 foreslås det, at der anvendes ækvivalente oplysninger, når sammenlignelige produkters miljøpåvirkninger, aspekter eller ydeevne skal vurderes.

Kommissionen foreslår derudover regler om miljømærkningsordninger. Mærkninger baseret på egen certificering ønskes forbudte, og der skal være nærmere rammer for ordningerne. Herunder falder krav om gennemsigtighed og yderligere tilgængelighed af oplysninger om de bagvedliggende kriterier for opnåelse af certificeringen. Der foreslås derudover regler om tredjepartsverificering.

Tidshorisonten for eventuel ikrafttrædelse af forslaget er på nuværende tidspunkt ukendt, da forslaget efter den almindelige lovgivningsprocedure nu skal godkendes af Europa-Parlamentet og Rådet.

Læs hele direktivforslaget her: *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=-COM%3A2023%3A0166%3AFIN*

Højesteret tilkender Anne Black millionerstatning i sag om ophavsretlig krænkelse af keramikprodukter

Højesteret afsagde den 22. marts 2023 dom i sag BS-50856/2020-HJR mellem Anne Black ApS (»Anne Black«) og Salling Group A/S (»Salling Group«) samt Ronald A/S (»Ronald«). Sagen handlede om, hvorvidt dagligvarekæden Netto havde krænket Anne Blacks ophavsrettigheder ved at sælge eller markedsføre tre keramikprodukter.

I 2016 lancerede Netto en reklamekampagne, hvor en hængepotte, vase og lågkrukke blev annoncerede som såkaldte spotvarer i Nettos tilbudsavis og på sociale medier. Anne Black mente, at salget og markedsføringen af disse produkter krænkede ophavsretten til hendes produkter, som hun begyndte at sælge allerede i 2013.

Sø- og Handelsretten tog første gang i 2019 stilling til, hvorvidt Anne Blacks hængepotte, vase og lågkrukke var beskyttet efter § 1, stk. 1, i lovbekendtgørelse nr. 1144 af 23. oktober 2014 (»den danske ophavsretslov«). Sø- og Handelsretten kom frem til, at alle tre produkter var beskyttede, da de var udtryk for Anne Blacks egen kunstneriske frembringelse. Der var således tale om en krænkelse af Anne Blacks ophavsrettigheder. Retten konkluderede tillige, at Salling Group og Ronald havde handlet i strid med § 3 om god markedsføringsskik i lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«).

Østre Landsret kom ligeledes frem til, at alle tre produkter var beskyttede mod produktefterligninger

efter den danske markedsføringslov, da de fremstod med det fornødne særpræg og en kommerciel adskillelsesevne. Vedrørende spørgsmålet om den ophavsretlige beskyttelse konkluderede Østre Landsret dog, at det alene var hængepotten, der var beskyttet. Landsretten udtalte, at hængepotten havde et genkendeligt udtryk, der måtte være udtryk for Anne Blacks egen intellektuelle frembringelse, hvorfor den var beskyttet den danske ophavsretslov. Vasen og lågkrukken gjorde derimod brug af kendte designelementer, hvorfor der ikke var tale om Anne Blacks egne intellektuelle frembringelser.

Dette resulterede i, at Østre Landsret nedsatte erstatningssummen fra DKK 1,5 mio. til DKK 300.000.

Anne Black ankede sagen til Højesteret, der ikke alene skulle tage stilling til erstatningsudmålingen, men ligeledes skulle foretage en fornyet materiel bedømmelse af produkternes ophavsretlige beskyttelse, da Procesbevillingsnævnets anketilladelse ikke var begrænset. Højesteret traf kendelse om ankesagens indhold den 2. maj 2022 i kendelsen trykt i Ugeskrift for Retsvæsen 2022.2739 H.

Højesteret tiltrådte Østre Landsrets afgørelse vedrørende den ophavsretlige og markedsføringsretlige vurdering og kom ligeledes frem til, at Salling Group og Ronald ved salg og markedsføring af deres spotvarer krænkede Anne Blacks rettigheder.

Vedrørende erstatningsudmålingen vurderede Højesteret, at der efter karakteren og grovheden af Salling Group og Ronalds krænkelser var grundlag for at lempe kravene til bevisbyrden for tabets omfang.

På den baggrund fandt Højesteret det bevist, at en betydelig del af Anne Blacks omsætningsnedgang skyldtes markedsforstyrrelse foranlediget af krænkelsen. Erstatningen blev herefter forhøjet til DKK 1 mio.

Læs hele dommen her: *https://domstol.fe1.tangora.com/media/-300016/files/50856-50859_Dom_til_hjemmesiden.pdf*

Sø- og Handelsretten har frifundet Ankenævnet for Patenter og Varemærker i sag om prøvelse af nævnets afgørelser

Sø- og Handelsretten har den 17. marts 2023 afsagt dom i sag BS-29589/2021-SHR mellem Julius Sämann Ltd (»JSL«) og det danske Ankenævn for Patenter og Varemærker (»Ankenævnet for Patenter og Varemærker«).

Sagen drejede sig om, hvorvidt tre afgørelser truffet af Ankenævnet for Patenter og Varemærker var forkerte og skulle omgøres. Konkret handlede det om, hvorvidt Ankenævnet for Patenter og Varemærker i sine afgørelser korrekt havde fortolket og anvendt reglerne i lovbekendtgørelse nr. 88 af 29. januar 2019 (»den danske varemærkelov«) § 15, stk. 1 nr. 2 og § 15, stk. 3, nr. 1 i relation til registreringerne af en række varemærker. Bestemmelserne angiver indsigelsesgrunde, der kan hjemle afvisning eller bortfald af en anden aktørs varemærkeregistrering. JSL's varemærker bestod alle af et sort eller hvidt grantræ gengivet i naturtro form. De modstående varemærker indeholdt ligeledes et grantræ, som var gengivet på stiliseret vis med takker, og i hvid farve med sort omrids. I sagerne for Ankenævnet for Patenter og Varemærker havde JSL, grundet ligheden med grantræerne, fremsat indsigelser mod registrering af de modstående varemærker med støtte i de ovennævnte bestemmelser. Indsigelserne var alle blevet afvist af Ankenævnet for Patenter og Varemærker, hvorfor registrering af varemærkerne blev tilladt.

For Sø- og Handelsretten gjorde JSL gældende, at der både var forvekslighed mellem varemærkerne, jf. den danske varemærkelovs § 15, stk. 1, nr. 2, og »sammenhæng« mellem disse, jf. § 15, stk. 3, nr. 1, hvorfor registreringen burde have været nægtet af Ankenævnet for Patenter og Varemærker. Hertil gjorde JSL desuden gældende, at påvisningen af »sammenhæng« burde have medført en vurdering af de yderligere betingelser i den danske varemærkelovs § 15, stk. 3, nr. 1 om utilbørlig udnyttelse af JSL's varemærkers særpræg eller renommé, som Ankenævnet for Patenter og Varemærker, ifølge JSL, ikke havde taget stilling til. Efter JSL's opfattelse forelå der således en retlig fejl ved afgørelserne, som berettigede disses omgørelse.

I sin afgørelse bemærkede Sø- og Handelsretten indledningsvist, at dens prøvelse af Ankenævnet for Patenter og Varemærkers afgørelser fuldt ud omfattede sagernes faktuelle grundlag og retsanvendelsen, men at en tilsidesættelse af den skønsmæssige vurdering vedrørende forvekslelighed og »sammenhæng« forudsatte sikkert grundlag.

Sø- og Handelsretten fandt det herefter ikke godtgjort, at Ankenævnet for Patenter og Varemærker skulle have truffet sine afgørelser på forkert retligt grundlag og uden inddragelse af relevante og fornødne faktiske oplysninger. Sø- og Handelsretten fandt, ligesom Ankenævnet for Patenter og Varemærker havde gjort, at der var betydelige stilistiske og udtryksmæssige forskelligheder mellem varemærkerne, og at den omstændighed, at begge varemærker indeholdt et grantræ, ikke i sig selv var tilstrækkeligt til at statuere »sammenhæng« efter den danske varemærkelovs § 15, stk. 3, nr. 1. Der var herefter ikke det fornødne sikre grundlag for at tilsidesætte afgørelserne. Sø- og Handelsretten bemærkede afslutningsvist, at der heller ikke fandtes at være risiko for forveksling, jf. den danske varemærkelovs § 15, stk. 1, nr. 2, hvorfor der ej heller af den grund var grundlag for tilsidesættelse.

Ankenævnet for Patenter og Varemærker blev dermed frifundet, og

dets afgørelser om at tillade registrering af de omtvistede varemærker skulle således stå ved magt.

Læs hele dommen her: *https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-29589-2021-SHR.pdf*

Ordet »EtOH« for selskab, der sælger whisky, var af deskriptiv karakter og kunne ikke beskyttes

Sø- og Handelsretten afsagde den 9. februar 2023 kendelse i en sag med sagsnr. BS-37697/2022-SHR mellem EtOH Spirits ApS (»EtOH Spirits«) og Nordic Ethanol ApS (»Nordic Ethanol«).

Sagen vedrørte, om Nordic Ethanols brug af ordet »EtOH«, som varemærke og forretningskendetegn ved deres salg af alkoholiske drikke, var i strid med EtOH Spirits' rettigheder.

Sø- og Handelsretten undersøgte først, om Nordic Ethanol krænkede EtOH Spirits' registrerede EU-figurvaremærke, der indeholdt bogstaverne »EtOH« og var registreret i vareklasse 33, whisky. Ordelementet fandtes alene at være beskrivende for vareklassen, eftersom den almindelige forbruger vil opfatte figurmærket som en reference til alkohol, når det anvendes i forbindelse med alkoholiske drikke. EUIPO havde tidligere bekræftet dette synspunkt ved brev af 7. september 2021 vedrørende EtOH Spirits' anmodning om registrering af EU-figurvaremærket.

Der var derfor tale om en snæver beskyttelse. Yderligere markedsførte parterne ikke de samme alkoholiske produkter, henholdsvis whisky og gin, akvavit m.v., og de to figurvaremærker og parternes øvrige markedsføringsmateriale adskilte sig på andre punkter. Henset til dette, var der efter rettens vurdering ikke forvekslingsrisiko, jf. Europa-Parlamentets og Rådets forordning (EU) 2017/1001 af 14. juni 2017 om EU-varemærker (»varemærkeforordningen«) artikel 9, stk. 2, litra b.

Sø- og Handelsretten tog dernæst stilling til, om EtOH Spirits havde etableret en varemærkeret til ordet »EtOH«, jf. lovbekendtgørelse nr. 88 af 29. januar 2019 (»den danske varemærkelov«) § 3, stk. 1, nr. 3. Retten fandt i den forbindelse, at ordet »EtOH« måtte anses som deskriptivt for varer omfattet af vareklasse 33, alkoholiske drikke. Det manglede derfor særpræg, ligesom der ikke var tilstrækkelig intensiv indarbejdelse i markedet, til at der kunne anses at være etableret en varemærkeret til ordet »EtOH«.

Vedrørende potentiel overtrædelse af lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«) bemærkede retten, at der af tilsvarende grunde om manglende særpræg som ovenfor samt sparsomme oplysninger om EtOH Spirits' produkters markedsposition, måtte være tale om en ganske snæver beskyttelse. Produkterne fandtes herefter ikke at være beskyttede efter hverken den danske markedsføringslovs § 22 om forretningskendetegn eller § 3 om god markedsføringsskik.

Nordic Ethanol blev herefter frifundet for alle påstande.

Læs hele kendelsen her: *https://domstol.fe1.tangora.com/media/-300011/files/BS-37697-2022-SHR_Kendelse.pdf*

»Flyhjælp« var ikke af beskrivende karakter, og markedsføring kunne derfor forbydes

Sø- og Handelsretten afsagde den 31. januar 2023 dom i sag BS-5887/2022-SHR mellem Flyhjælp ApS (»Flyhjælp«) og Travelrefund ApS m.fl. (»Travelrefund«). Sagen angik spørgsmålet om krænkelse af Flyhjælps rettigheder til ordmærket »Flyhjælp«.

Flyhjælp og Travelrefund sælger begge tjenesteydelser til privatpersoner med hjælp til at opnå erstatning hos flyselskaber i forbindelse med flyforsinkelser, ombookninger og aflysninger. Flyhjælp er indehaver af varemærket »Flyhjælp«, og Flyhjælp sagsøgte på den baggrund Travelrefund for anvendelse af dette ordmærke i blandt andet deres markedsføring.

Sø- og Handelsretten fandt, at »Flyhjælp« ikke af den relevante omsætningskreds vil blive opfattet som beskrivende for de tjenesteydelser, som varemærket er registreret for, da »Flyhjælp« ikke angiver, at der er tale om hjælp til at opnå erstatning eller kompensation i tilfælde af flyforsinkelser eller aflysninger. Ordmærket »Flyhjælp« har derfor et iboende særpræg, og den relevante omsætningskreds vil ikke opfatte ordet »Flyhjælp« som beskrivende for de tjenesteydelser, som varemærket er registreret for.

Sø- og Handelsretten fandt således, at Travelrefunds markedsføring indebar en krænkelse af Flyhjælps rettigheder efter lovbekendtgørelse nr. 88 af 29. januar 2019 (»den danske varemærkelov«) § 4, stk. 2, nr. 1, idet »Flyhjælp« anvendtes for samme type tjenesteydelse, som dem for hvilke varemærket var beskyttet. Derudover indebar brugen af varemærket en overtrædelse af lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«) § 22 om forretningskendetegn.

Som følge heraf blev det forbudt Travelrefund at anvende ordet »Flyhjælp« i Danmark i forbindelse med udbud, markedsføring og salg af juridisk bistand vedrørende flypassagerers rettigheder.

Læs hele dommen her: *https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-5887-2022-SHR.pdf*

Erstatning i velkendt Bitz og Würtz-sag endelig opgjort

Sø- og Handelsretten afsagde den 30. januar 2023 dom i sag BS-1370/2016-SHR og BS-28315/2022-SHR mellem K. H. Würtz v/Kasper Heie Würtz (»Würtz«) og F & H A/S, Christian Bitz samt Bitz A/S (»Bitz«).

Sagen drejede sig navnlig om et økonomisk opgør mellem parterne på baggrund af Østre Landsrets

dom af 27. maj 2021. Det blev i dommen af 27. maj 2021 endeligt fastslået, at Bitz havde krænket Würtz' enerettigheder efter lovbekendtgørelse nr. 1144 af 23. oktober 2014 (»den danske ophavsretslov«) § 2 og lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«) § 3 om god markedsføringsskik. Spørgsmålet om udmåling af erstatning og vederlag var henvist til separat behandling i den pågældende sag efter det var statueret, at Bitz ved sit keramikstel krænkede Würtz' rettigheder for 15 Bitz-produkter.

Würtz nedlagde på baggrund af de konstaterede krænkelser påstande om vederlag, erstatning og godtgørelse på samlet lige under DKK 40 mio.

På den anden side nedlagde Bitz modpåstand om kompensation på DKK 3 mio.

Bitz mente, at Würtz havde overtrådt den danske markedsføringslovs § 20 om vildledende, aggressiv eller utilbørlig handelspraksis, den danske markedsføringslovs § 21 om sammenlignende reklame og/eller lovbekendtgørelse nr. 1360 af 28. september 2022 (»den danske straffelov«) § 267 om ærekrænkelse. Alt sammen som følge af karakteren af dele af mediedækningen af sagen og Würtz' andel i denne. Würtz havde angiveligt et medansvar for, at der i det danske tv-program, DR Kontant, var blevet fremvist produkter, som ikke havde relation til retssagen. Derudover mente Bitz, at Würtz var kommet med »faktuelt usande« udlægninger af sagen, idet han blandt andet havde udtalt, at »*Christian Bitz har taget vores håndværk, sendt det til Kina og kopieret det*«.

Sø- og Handelsretten kom frem til, at der efter den danske ophavsretslovs § 83, stk. 1, om erstatning og godtgørelse for ophavsretlig krænkelse, skulle tages udgangspunkt i, hvilket vederlag Würtz ville have haft krav på, hvis Bitz' udnyttelse af Würtz' værker var sket efter aftale. Vederlaget blev skønsmæssigt fastsat på baggrund af karakteren og omfanget af udnyttelsen til et rimeligt vederlag på DKK 4 mio. Sø- og Handelsretten fastsatte yderligere erstatning for markedsforstyrrelse til DKK 2,4 mio., så den samlede erstatning udgjorde DKK 6,4 mio.

Vedrørende Bitz' modpåstand om kompensation på DKK 3 mio., kom Sø- og Handelsretten frem til, at Würtz udtalelser ikke kunne danne grundlag for ærekrænkelse efter den danske straffelovs § 267. Set i lyset af sagen i øvrigt, var det yderligere ikke godtgjort, at Würtz havde overtrådt den danske markedsføringslov. Bitz' påstand blev herefter ikke taget til følge.

Læs hele dommen her: *https://domstol.fe1.tangora.com/media/-300011/files/BS-1370-2016-SHR_og_BS-28315-2022-SHR_Dom.pdf*

Læs Østre Landsrets dom af 27. maj 2021 her: *https://www.domstol.dk/media/pq1lof35/dom-wuertz.pdf*

Sortiment af børneprodukter udgjorde ikke krænkelse af den danske ophavsretslov eller den danske markedsføringslov

Sø- og Handelsretten afsagde den 18. januar 2023 dom i sag BS-24781/2021-SHR mellem Liewood A/S (»Liewood«) og nuuroo A/S (»nuuroo«).

Sagen vedrørte, hvorvidt nuuroo ved at sælge deres sortiment af børneprodukter og tilhørende emballage havde krænket Liewoods rettigheder efter lovbekendtgørelse nr. 1144 af 23. oktober 2014 (»den danske ophavsretslov«) og lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«). Yderligere skulle Sø- og Handelsretten tage stilling til, om Liewood havde handlet i strid med den danske markedsføringslov ved at udsende en meddelelse til deres forhandlere, hvori de blandt andet gjorde opmærksom på, at de mente nuuroos produkter var for tætte på deres egne.

Sø- og Handelsretten kom indledningsvis frem til, at Liewoods produkter ikke nød beskyttelse efter den danske ophavsretslov. Liewood havde ikke godtgjort, at deres arbejde var udtryk for en selvstændig designmæssig nyskabelse, der opfyldte kravet om originalitet i den danske ophavsretslovs § 1 og derfor kunne kvalificeres som værker af brugskunst. Udviklingen af produkterne var sket ved en tilpasning af design på eksisterende kendte elementer og former, som leveres af kinesiske leverandører. Tilsvarende nød Liewoods emballage heller ikke beskyttelse efter den danske ophavsretslov, da brunt pap med sort skrift anses for sædvanlig emballage, der anvendes til at signalere bæredygtighed.

Dernæst tog Sø- og Handelsretten stilling til, om Liewoods produkter nød beskyttelse efter den danske markedsføringslov, jf. § 3 om god markedsføringsskik. Sø- og Handelsretten fandt, at Liewoods produkter og emballage nød beskyttelse mod meget nærgående eller slaviske produktefterligninger, blandt andet henset til en række designmæssige valg og Liewoods kommercielle succes og markedsføring. Produkterne havde ikke sådanne fælles karakteristika, at de nød beskyttelse som en samlet produktserie.

Ved gennemgangen af de enkelte produkter fandt Sø- og Handelsretten, at der ikke for nogen af produkterne var tale om meget nærgående eller slaviske efterligninger. Tilsvarende udgjorde nuuroos emballage heller ikke en meget nærgående efterligning, blandt andet fordi der var forskel på skriften og udsmykningen på emballagen.

Sø- og Handelsretten frifandt derfor nuuroo.

Sø- og Handelsretten vendte dernæst sit fokus mod nuuroos selvstændige påstand om, at Liewood ved sin meddelelse til udvalgte forhandlere havde krænket den danske markedsføringslov. Sø- og Handels-

retten mente i den forbindelse ikke, at nuuroo havde løftet bevisbyrden for, at Liewood havde handlet ansvarspådragende eller i strid med den danske markedsføringslov. Det var ikke klart, hvor mange af Liewoods forhandlere der modtog meddelelsen, eller om beskeden var sendt som svar på konkrete henvendelser fra Liewoods forhandlere.

Læs hele dommen her: *https://domstol.fe1.tangora.com/media/-300011/files/BS-24781-2021-SHR_-_Dom.pdf*

Domænenavnet borgerlige.dk skulle overføres til Nye Borgerlige

Det danske Klagenævn for Domænenavne (»Klagenævnet for Domænenavne«) traf den 7. marts 2023 afgørelse i en sag med journalnr. 2023-0001 mellem klager Nye Borgerlige og indklagede 1st Class Internet Domain Names. Sagen vedrørte domænenavnet borgerlige.dk.

Nye Borgerlige er et dansk politisk parti, der har siddet i Folketingsgruppen siden 2019. Partiet er kendt for at være et borgerligt parti og er indehaver af internetdomænet nyeborgerlige.dk. I sit klageskrift indvendte partiet, at domænet, borgerlige.dk, er oprettet den 21. december 2022, hvorefter indklagede efterfølgende den 26. december 2022 og igen den 29. december 2022 har kontaktet partiet med tilbud om at købe domænet for henholdsvis 50.000 og 10.000 kr. Den 11. januar 2023 modtog Nye Borgerlige et yderligere tredje tilbud om at købe domænenavnet for 7.500 kr.

Nye Borgerlige mente derfor, at registranten åbenlyst og udelukkende havde anskaffet sig domænet med salg for øje.

Indklagede havde ikke svaret i sagen, hvorfor den blev afgjort på det foreliggende grundlag.

Klagenævnet for Domænenavne fandt, at sagen skulle afgøres efter lov nr. 164 af 26. februar 2014 om internetdomæner (»den danske domænelov«) § 25, stk. 2, der bestemmer, at registranter ikke må registrere og opretholde registreringer af domænenavne alene med videresalg eller udlejning for øje.

Eftersom indklagede uopfordret havde kontaktet Nye Borgerlige tre gange med tilbud om at købe domænenavnet, fandt Klagenævnet for Domænenavne, at der var en meget stærk formodning for, at formålet med indklagedes opretholdelse af registreringen af domænenavnet »borgerlige.dk« alene var at opnå en økonomisk gevinst.

Indklagede afkræftede ikke denne formodning, hvilket Klagenævnet for Domænenavne i henhold til sin forretningsorden kunne tillægge vægt i sin bevisbedømmelse.

Klagenævnet for Domænenavne fandt derfor, at registreringen af domænenavnet »borgerlige.dk« skulle overføres til Nye Borgerlige.

Læs hele afgørelsen: *https://www.domaeneklager.dk/sites/default/files/decision-pdf/2023-0001_borgerlige.dk_.pdf*

Forbrugerombudsmanden har politianmeldt diskotek for 51 ulovlige alkoholreklamer

Forbrugerombudsmanden oplyste i en pressemeddelelse den 21. marts 2023, at den har politianmeldt virksomheden SP ApS, der driver diskoteket Club Retro i Helsingør. Politianmeldelsen skyldes, at SP ApS skulle have overtrådt lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«) § 11, stk. 2 om forbud mod alkoholreklamer rettet mod unge under 18 år.

Diskoteket havde i alt 51 gange annonceret målrettet mod unge under 18 år for arrangementer med alkohol på Facebook ved at invitere unge fra 16 år og opefter til arrangementer med alkohol. I beskrivelsen til disse arrangementer, der ifølge hjemmesiden var »16+ arrangementer«, har der bl.a. været henvisninger til »bordpakker« og »happy hour«. Diskoteket havde således et strafansvar, uanset om de ikke faktisk udskænkede alkohol til mindreårige.

Efter skærpede sanktionsniveauer for overtrædelse af markedsføringsloven i 2022, er udgangspunktet en bøde på 10.000 kr. per opslag med omtale af alkohol, som er rettet mod unge under 18 år.

Læs pressemeddelelsen her: *https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2023/forbrugerombudsmanden-politianmelder-diskotek-for-51-ulovlige-alkoholreklamer/*

Visa, Mastercard og American Express indvilliger i at ændre betalingsvilkår

Den danske Forbrugerombudsmand oplyste i en pressemeddelelse af 19. januar 2023, at Visa, Mastercard og American Express har forpligtet sig til at ændre deres vilkår for at forebygge svindel med skjulte abonnementer.

Ændringerne er sket som led i et fælles EU-tiltag, som Forbrugerombudsmanden har taget initiativ til. Tiltaget skete på vegne af det europæiske CPC-samarbejde (Consumer Protection Cooperation) og med assistance fra EU-Kommissionen. Forbrugerombudsmanden har i forbindelse med tiltaget indskærpet overfor de tre kortselskaber, at deres vilkår skal sikre, at abonnementsbetalinger er i overensstemmelse med Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 af 25. november 2015 om betalingstjenester i det indre marked (»betalingstjenestedirektivet«) (PSD2) og Europa-Parlamentets og Rådets Direktiv 2005/29/EF af 11. maj 2005 (»UCP-direktivet«).

Der foreligger et skjult abonnement, når forbrugeren uberettiget får trukket betalinger via de betalingskortoplysninger, vedkommende har indtastet ved køb af eksempelvis en vare, uden at få oplyst, at forbrugeren også skal betale et abonnement.

Efter betalingstjenestedirektivets artikel 64 er en betalingstransaktion kun autoriseret, såfremt betaleren har samtykket til transaktionen. Der er ifølge Forbrugerombudsmanden

ikke givet det fornødne samtykke, hvis betaleren ikke får oplysninger om abonnementsbetalingerne, herunder beløbets størrelse og intervallet for betalingerne.

Kortselskaberne skal stille krav om, at virksomheder for at modtage betalinger med selskabernes betalingskort, understøtter samtykkeforpligtelsen efter betalingstjenestedirektivets artikel 64. Gør kortselskaberne ikke det, er det ifølge de forbrugerbeskyttende myndigheder i strid med UCP-direktivets artikel 5, der stadfæster forbuddet mod urimelig handelspraksis.

De tre kortselskaber ændrer således deres vilkår for at sikre, at forbrugerne får tydelige oplysninger om abonnentsbetalingers størrelse og hyppighed ved indtastning af betalingsoplysninger for dermed at modvirke forekomsten af skjulte abonnementer.

Læs hele pressemeddelelsen her: *https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2023/forbrugerombudsmandens-eu-samarbejde-star-bag-skaerpet-indsats-mod-skjulte-abonnementer/*

Forbrugerombudsmanden indskærper reglerne om vildledende markedsføring over for bilfirmaer og tankstationer

Den danske Forbrugerombudsmand indskærpede den 6. januar 2023 reglerne om vildledende markedsføring over for OK Benzin, Suzuki Bilimport og Toyota Danmark.

Indskærpelsen kom på baggrund af, at virksomhederne havde benyttet budskaber i deres markedsføring, der fik deres produkter til at fremstå bedre eller mindre skadelige for miljøet, end de faktisk var.

OK Benzin havde markedsført et dieselprodukt til erhvervskunder med udsagn om »Klimadiesel« og benyttet sig af et billede af en sennepsblomstermark på sine tankbiler. Suzuki Bilimport markedsførte »mild-hybridbiler« med betegnelsen »hybrid«. Endelig markedsførte Toyota Danmark en plugin-hybridbil med et udsagn om, at bilen henvendte sig til forbrugere, der vil have en miljørigtig bil, uden at være begrænset på rækkevidde, selvom bilen højst kunne køre 50 km uden at skulle genoplades.

I alle tilfælde vurderede Forbrugerombudsmanden, at der var tale om vildledende budskaber i strid med lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«) § 5 og § 6, om henholdsvis vildledende handlinger og udeladelser.

Forbrugerombudsmanden henviste herefter til sin kvikguide til virksomheder om miljømarkedsføring

Illustrasjon: Colourbox.com

fra 2021, som primært bygger på Forbrugerombudsmandens vejledning om brug af miljømæssige og etiske påstande m.v. fra 2014.

Læs hele pressemeddelelsen her: *https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2023/bilfirmaer-og-tankstationer-far-indskaerpet-reglerne-om-vildledning/*

Læs kvikguiden fra 2021 her: *https://www.forbrugerombudsmanden.dk/media/56731/kvikguide-om-miljoemarkedsfoering.pdf*

Læs vejledningen fra 2014 her: *https://www.forbrugerombudsmanden.dk/media/46475/2016-miljmssige-og-etiske-udsagn.pdf*

DSM-direktivets implementering i dansk ret

Den 10. marts 2023 sendte det danske Kulturministerium et lovforslag i offentlig høring. Lovforslaget har til formål at implementere Europa-Parlamentets og Rådets direktiv (EU) 2019/790 af 17. april 2019 om ophavsret og beslægtede rettigheder på det digitale indre marked (»DSM-direktivet«). Forslaget indeholder bestemmelser, som sigter mod at regulere og afklare retsstillingen for både rettighedshavere og brugere af ophavsretligt beskyttet indhold.

Lovforslaget omfatter flere forskellige bestemmelser, herunder blandt andet regler vedrørende forskningsinstitutioners adgang til at udføre tekst- og datamining af ophavsbeskyttet indhold. Tekst- og datamining er teknikker, som anvendes i forbindelse med træning af f.eks. kunstig intelligens samt software, der er designet til at finde mønstre eller sammenhænge i store datamængder. Med lovforslaget præsenteres to undtagelser til reglerne om rettighedshaverens eneret. Den første undtagelse tillader forsknings- og visse undervisningsinstitutioner at udføre tekst- og datamining uden rettighedshaverens samtykke, så længe det sker med henblik på offentlig forskning. Den anden undtagelse tillader anvendelse af tekst- og datamining til kommercielle formål, forudsat at rettighedshaverne ikke har forbeholdt sig brugen med passende midler.

Yderligere inkluderer lovforslaget bestemmelser, der sikrer, at undervisningsinstitutioner kan anvende beskyttede værker og materialer i deres undervisning, uden at opnå samtykke fra rettighedshaverne, hvis passende licenser ikke udstedes.

Endelig inkluderer lovforslaget nye bestemmelser, der sigter mod at regulere den retsstilling, som skabende og udøvende kunstnere har i forhold til producenter og andre aftaleparter. Reglerne er i stort omfang beskyttelsespræceptive til fordel for ophavsmanden og den udøvende kunstner. For det første indeholder lovforslaget et princip om, at kunstnerne skal modtage passende og forholdsmæssigt vederlag for deres arbejde. For det andet pålægger lovforslaget erhververe af rettighederne at give kunstnerne opdaterede og fyldestgørende oplysninger om, hvordan deres værker og frembringelser anvendes. For det tredje indebærer lovforslaget en aftalejusteringsmekanisme, der svarer til § 36 i lovbekendtgørelse nr. 193 af 2. marts 2016 (»den danske aftalelov«), men som specifikt er målrettet det vederlag, som kunstnerne modtager. For det fjerde udvides det danske Ophavsretslicensnævns kompetencer, så denne også omfatter konflikter, der vedrører gennemsigtighedsforpligtelser og aftalejusteringer. Endelig indeholder lovforslaget en ret for kunstnerne til at trække deres rettigheder tilbage fra erhververen, hvis rettighederne ikke udnyttes.

Lovforslaget blev fremsat for Folketinget den 3. maj 2023 og forventes at træde i kraft den 1. juli 2023.

Læs hele lovforslaget her: *https://www.ft.dk/samling/20222/lovforslag/L125/som_fremsat.htm*

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


simonsen vogtwiig

Hedda Baumann Heier og Henning Wahlberg

Oslo tingrett: ny dom om opphavsrett til undervisningsprogram

Den 31. mars 2023 avsa Oslo tingrett dom i en sak mellom Handelshøyskolen BI (heretter «BI») og tidligere professor ved BI, Paul Anders Moxnes. Tvisten dreide seg om rettighetene til undervisningsprogrammet «Samspill og ledelse», som Moxnes hadde fagansvar for i perioden 1992 til 2011 og som BI har fortsatt å tilby etter Moxnes gikk av med pensjon i 2011. Moxnes fremmet krav om vederlag for BIs bruk av undervisningsprogrammet samt krav om navngivelse.

Det første spørsmålet retten måtte ta stilling til var om undervisningsprogrammet er vernet som åndsverk, altså om programmet har verkshøyde etter åndsverkloven § 2. BI anførte at konsepter og metoder ikke kan ha vern som åndsverk. Moxnes på sin side hevdet vern for strukturen og opplegget i undervisningsprogrammet, og ikke faglige synspunkter eller vitenskapelige teorier. Retten fant at undervisningsprogrammets konkrete sammensetning av øvelser og forelesninger mv. var et resultat av frie og kreative valg, og at undervisningsprogrammet derfor var vernet som åndsverk.

Det neste spørsmålet var om programmet som BI har tilbudt de senere årene, er det samme som Moxnes utviklet. Opphavsrett er ikke til hinder for at noen utvikler nye og selvstendige verk. Retten fant etter en konkret vurdering at selv om programmet var blitt endret og pensum var byttet ut, kunne en likevel gjenfinne elementer som var vernet på Moxnes' hånd. Hovedtemaene og flere av modulene var fortsatt de samme. Retten mente at det kunne i høyden være tale om en bearbeidelse, men heller ikke bearbeidelser kan brukes i strid med opphavsretten til originalverket etter åndsverkloven § 6.

Videre fant retten at BI hadde gjort verket tilgjengelig for allmennheten ved å dele undervisningsprogrammet med noen tusen studenter. Det ble blant annet vektlagt at BI hadde handlet i kommersiell hensikt.

Retten fant altså at BIs bruk av undervisningsprogrammet krever enten samtykke eller rettighetsovergang fra Moxnes. Det var ikke avtalt noe uttrykkelig om rettighetsovergang mellom BI og Moxnes, og retten tok derfor utgangspunkt i Knophs maksime, som sier at «*prinsipalen vinner den rett over åndsverket som er nødvendig og rimelig, hvis arbeidsavtalen skal nå sitt formål, men heller ikke mer*».

Det har vært omdiskutert i hvilken grad en rettighetsovergang vil være rimelig og nødvendig for vitenskapelig ansatte i universitetssektoren, noe retten kommer inn på under henvisning til en innstilling fra Immaterialrettsutvalget fra 2003. Ifølge denne innstillingen viser praksis at Knophs maksime ikke uten videre gjelder i universitetssektoren. Samtidig konstateres det også at denne praksisen ikke er til hinder for at man også i universitetssektoren kan konstatere at det etter gjeldende rett skjer en rettighetsovergang i spesielle situasjoner med velbegrunnede behov.

Retten fant etter en konkret vurdering at det i denne saken hadde skjedd en rettighetsovergang, og la vekt på at Moxnes' primære arbeidsoppgave mens han var ansatt var å utvikle undervisningsprogrammet. Retten vektla også at saken ikke gjelder rettigheter til forskningsarbeider, et undervisningsprogram som tilbys som del av BIs kommersielle virksomhet. Dermed fant retten at BI hadde fått en ubegrenset og vederlagsfri rett til bruk av programmet i sin virksomhet.

Moxnes' navngivelsesrett etter åndsverkloven § 5 var imidlertid i behold, og BI ble dermed dømt til å navngi Moxnes ved bruk av undervisningsprogrammet.

Dommen er rettskraftig og har saksnummer 22-095448TVI-TOSL/04. Dommen er i skrivende stund ikke tilgjengelig i Lovdatas database.

Endringer i varemerkeloven

Den 1. mars trådte endringer i varemerkeloven i kraft. Endringene gjennomfører varemerkedirektivet (EU) 2015/2436, som ble vedtatt i EØS-komiteen 7. februar 2020. Endringene medfører også at Norge tiltrer Singaporetraktaten om varemerkerett, som forenkler formelle krav til varemerkeregistreringer. Noen av de mest sentrale endringene nevnes i korte trekk nedenfor.

Endringer i registreringsvilkårene.

Kravet om at et varemerke må bestå av tegn som kan «gjengis grafisk» erstattes nå med et teknologinøytralt krav om at merket må kunne gjengis «på en slik måte at myndighetene og allmennheten klart og

tydelig kan avgjøre gjenstanden for den beskyttelse merkehaveren gis.»

Endringen åpner for at nye merker kan registreres, så lenge det er tydelig hva som er omfattet av beskyttelsen. Dette åpner for at utradisjonelle merker så lenge beskyttelsesgjenstanden kan defineres klart, og kan i prinsippet åpne for merker som består av lukt, lyd eller videoer.

Registrering av merker i sort-hvitt.

Tidligere praksis har vært at merker registrert i sort-hvitt uten videre har fått vern i alle fargekombinasjoner. Etter lovendringen vil ikke dette lenger være tilfellet. Endringen vil ikke ha tilbakevirkende kraft, og gjelder for varemerker som har søknadsdag etter 1. mars 2023.

Absolutte registreringshindre

Videre er det gjort endringer i de absolutte registreringshindrene i varemerkeloven § 15. Bokstavene d-f er tilført etter endringen. Dette gjelder blant annet merker som inneholder visse opprinnelses- eller geografiske betegnelser eller betegnelser for vin, eller gjengir visse plantesortnavn eller gjelder en plantesort.

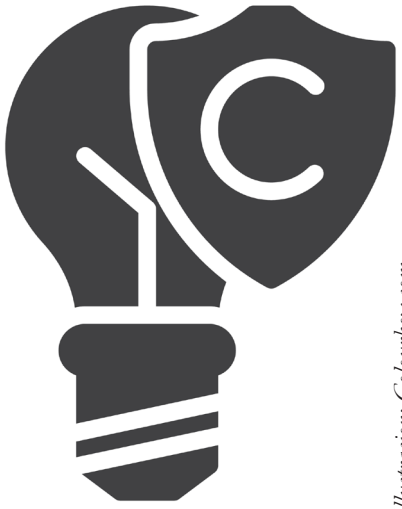
I tillegg krever direktivet at ond tro gjøres til en ubetinget *ugyldighetsgrunn*. Dette har blitt gjennomført som et absolutt registreringshinder i § 15 bokstav f. «Ond tro» har i denne konteksten ikke nødvendigvis det samme meningsinnholdet som fra den norske formueretten, men må tolkes som et selvstendig EU-rettslig begrep, jf. også sak C-320/12 *Malaysia Dairy*. De norske forarbeidene peker imidlertid på at ond tro-begrepet etter EU-domstolens praksis primært tar sikte på en vurdering av om søknaden utgjør en illojal handling i strid med god forretningsskikk, jf. sak C-529/07. Det blir interessant å se i hvilken grad praksis etter markedsføringslovens § 25, som ikke er EU-harmonisert, vil bli tillagt relevans i vurderinger etter varemerkelovens § 15 bokstav f.

Andre sentrale endringer

Den nye varemerkeloven § 29 og § 35 åpner for at et varemerke som har blitt registrert uten tilstrekkelig særpreg og klages inn, kan opprettholdes dersom det kan sies å ha innarbeidet særpreg i etterkant av søknaden.

Endringene åpner også for at manglende bruk kan anvendes som forsvar også i innsigelsessaker (§ 29 a). I tillegg kan registrerte varemerker og søknader særskilt pantsettes (§ 56 a).

Bidraget er skrevet av advokatfullmektig Henning Wahlberg og senioradvokat Hedda Baumann Heier i Advokatfirmaet Simonsen Vogt Wiig AS.



Illustrasjon: Colourbox.com

Wikström & PARTNERS

Gustaf Johnssén

Sekretessgenombrott vid utkontraktering II

I förra utgåvan av Lov & Data redogjordes för en lagrådsremiss med förslag till en sekretessbrytande bestämmelse, avsedd att underlätta myndigheters utkontraktering (outsourcing) av IT-tjänster.[1] Regeringen har den 23 mars 2023 lämnat en proposition till riksdagen med förslag till lagstiftning.[2] Förslaget till sekretessbrytande bestämmelse har utformats enligt Lagrådets förslag och lyder:

> Sekretess hindrar inte att en uppgift lämnas till en enskild eller till en annan myndighet som för den utlämnande myndighetens räkning har i uppdrag att endast tekniskt bearbeta eller tekniskt lagra uppgiften, om det med hänsyn till omständigheterna inte är olämpligt att uppgiften lämnas ut.

Frågan är nu vad denna nya bestämmelse konkret innebär för myndigheter som anlitar eller avser att anlita en extern leverantör för att behandla uppgifter.

För att förstå den föreslagna lagändringens praktiska betydelse för myndigheter och leverantörer är det klargörande att känna till den bredare bakgrunden. Förslaget utgör ett steg i en utveckling av de rättsliga förutsättningarna för myndigheters outsourcing som pågått i vart fall sedan 2014. JO granskade då några landstings utkontraktering av tjänster som avsåg bearbetning av patientuppgifter.[3] Förutsättningarna i det beslutet var på flera punkter speciella, men JO uttalade sig också generellt om de rättsliga förutsättningarna för under vilka omständigheter en myndighet kan överlåta behandling av sekretessreglerade uppgifter till en privat tjänsteleverantör. Enligt JO finns det två fall:

1. Oftast räcker det enligt JO med att man i avtal har ställt krav på tystnadsplikt för att det ska vara tillåtet att låta en extern leverantör behandla sekretessreglerade uppgifter. Detta är alltså enligt JO huvudfallet. Även om det inte berörs närmare får man anta att detta förutsätter att avtalet även ställer krav på relevanta säkerhetsåtgärder för att skydda uppgifterna.
2. När särskilt känsliga uppgifter hanteras, som i det aktuella fallet, är en avtalad tystnadsplikt inte tillräcklig. Det är då enligt JO inte tillåtet att överlåta behandlingen av uppgifterna till en extern leverantör med mindre än att leverantörens anställda omfattas av en lagstadgad och straffsanktionerad tystnadsplikt. Eftersom detta normalt inte är fallet, blir konsekvensen att det i praktiken är olagligt att utkontraktera behandlingen av sådana uppgifter.

I det första fallet behöver myndigheten göra en sekretessprövning innan uppgifterna lämnas ut. Om utfallet av sekretessprövningen blir att uppgifterna har ett sådant skydd hos leverantören att skaderekvisiten inte är uppfyllda, så är det tillåtet att lämna ut uppgifterna för behandling hos leverantören. Sakomständigheter att beakta i en sådan sekretessprövning är t.ex. vilka säkerhetsåtgärder som vidtas, om personalen har skrivit under sekretessförbindelser, under vilka omständigheter personalen har tillgång till uppgifterna som behandlas och flera andra omständigheter. När uppgifterna skyddas av sekretess utan skaderekvisit, s.k. absolut sekretess, är det alltså inte möjligt att outsourca behandlingen.

För att möjliggöra utkontraktering även i de fall då uppgifterna är särskilt känsliga infördes år 2020, genom lag

1 Se Lov&Data nr 153 1/2023, *Sekretessgenombrott vid teknisk bearbetning och lagring.*

2 Prop. 2022/23:97 *Sekretessgenombrott vid utlämnande för teknisk bearbetning eller teknisk lagring av uppgifter.*

3 Beslut 2014-09-09, dnr. 3032-2011, Allvarlig kritik mot vissa vårdgivare inom dels Västra Götalandsregionen, dels Stockholms läns landsting för att man har ingått avtal om journalföring med ett företag trots att detta inte varit förenligt med regelverket om sekretess inom hälso- och sjukvården.

(2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter, en ny tystnadsplikt för privata tjänsteleverantörer.[4] Lagen gäller vid teknisk bearbetning eller teknisk lagring av uppgifter som för en myndighets räkning utförs av en privat tjänsteleverantör. Därigenom skapades alltså den straffsanktionerade tystnadsplikt som tidigare saknats. Tystnadsplikten gäller för anställda och uppdragstagare som deltar i tjänsteleverantörens verksamhet. Myndigheten måste dock fortfarande göra en sekretessprövning innan behandlingen outsourcas. Den lagstadgade tystnadsplikten blev då en omständighet att beakta vid sekretessprövningen, tillsammans med övriga ovan nämnda omständigheter.

Det nu aktuella lagförslaget syftar till att ytterligare tydliggöra förutsättningarna för outsourcing av behandling av sekretessreglerade uppgifter. Innebörden av den nya bestämmelsen är att sekretess inte råder mellan en myndighet och en leverantör när behandlingen avser teknisk bearbetning eller teknisk lagring av uppgifter. I sådana fall får uppgifterna lämnas till leverantören utan föregående sekretessprövning. Detta gäller även när uppgifterna är särskilt känsliga eller omfattas av absolut sekretess. Det innebär dock inte att det alltid är fritt fram att lägga ut behandling av uppgifter på externa leverantörer. Enligt den föreslagna bestämmelsen får nämligen uppgifter bara lämnas ut om det inte är olämpligt. Regeringen ger ett antal exempel på omständigheter som kan vägas in i olämplighetsbedömningen, bl.a. uppgifternas art och vilka säkerhetsåtgärder som vidtas.

Den föreslagna bestämmelsen gäller, liksom tystnadsplikten, vid teknisk bearbetning och teknisk lagring. När det gäller området utanför teknisk bearbetning och teknisk lagring behöver myndigheten, på samma sätt som tidigare, göra en sekretessprövning för att avgöra om uppgifterna kan lämnas ut till leverantören.

Vad innebär då den föreslagna bestämmelsen för myndigheter som outsourcar eller avser outsourca behandling av sekretessreglerade uppgifter? Den nya bestämmelsen tydliggör ytterligare förutsättningarna för outsourcing av behandling av sekretessreglerade uppgifter. Det förändrade rättsläget kräver dock att myndigheterna gör bedömningar utifrån den nya lagstiftningen. Detta gäller både när nya avtal upphandlas, och för befintliga avtal och tjänster. För att kunna bedöma hur avtalskrav ska utformas behöver myndigheten veta exakt vilka regler som gäller. Liksom tidigare är grunden att myndigheten har en god kontroll på vilka uppgifter som hanteras och vilket skydd dessa behöver. Myndigheten behöver också analysera de tjänster man avser upphandla. Redan tidigare var det nödvändigt att analysera vilka säkerhetsåtgärder som vidtas och hur tjänsterna produceras. Enligt de nya bestämmelserna måste myndigheten också noga analysera i vilka delar tjänsten utgör teknisk bearbetning eller teknisk lagring, och i vilka delar tjänsten avser annan behandling. Detta är nödvändigt för att avgöra vilka bestämmelser som gäller, vilket i sin tur behöver vara tydligt för att kunna ställa ändamålsenliga avtalskrav och utforma avtal i övrigt. Regeringen anger ett antal exempel på behandlingar som man menar utgör teknisk bearbetning och teknisk lagring. Ytterst går dock bedömningen tillbaka på den reglering som finns i 2 kap. 13 § tryckfrihetsförordningen. De motiv som ligger till grund för den bestämmelsen har sitt ursprung i 1970-talet och det är inte självklart hur de ska tillämpas på samtida IT-tjänster.

Myndigheten behöver också göra en bedömning av om det är olämpligt att outsourca behandlingen. Det finns inga särskilda dokumentationskrav i lagtexten, men regeringen förordar i propositionen att de bedömningar som myndigheten gör dokumenteras. Denna bedömning kommer i praktiken förmodligen att i många delar likna den sekretessprövning som myndigheten tidigare har behövt göra. Även om regeringen ger en viss ledning genom att peka på omständigheter att beakta, är det långt ifrån tydligt hur bedömningen är tänkt att gå till i praktiken. Bedömningen förutsätter också, liksom bedömningen av vad som är teknisk bearbetning och teknisk lagring, en ingående förståelse för hur tjänsterna produceras hos leverantören. En kunskap som inte alltid finns i myndigheterna.

Dessa olika bedömningar, och dokumentationen av dem, behöver göras både när en ny tjänst ska upphandlas och för befintliga avtal. De senare kan behöva förändras eller kompletteras i ljuset av den nya bestämmelsen, t.ex. när det gäller gränsdragningen mellan teknisk bearbetning och teknisk lagring och andra behandlingar. Det är alltså ett digert arbete som ligger framför myndigheterna.

Även om naturligtvis varje myndighet ansvarar för att göra de bedömningar som behövs för att säkerställa att en utkontraktering är rättsenlig och säker. Men även leverantörer har all anledning att sätta sig in i de nya reglerna och analysera vilka konsekvenser de har. Exempelvis kan en leverantör förväntas ha en klar uppfattning om hur de egna tjänsterna ska bedömas när det gäller om de utgör teknisk bearbetning eller teknisk lagring, eller någon annan typ av behandling.

Sammantaget innebär den föreslagna bestämmelsen att ytterligare en sten läggs till det rättsliga systembygge som ska skydda känsliga uppgifter. Ändringen bidrar utan tvivel till att underlätta outsourcing. Men den innebär också att myndigheterna behöver göra ett arbete som inte är obetydligt för att säkerställa att lagens alla krav är uppfyllda och att den utkontraktering man gör är fullt ut rättsenlig.

Gustaf Johnssén, senior specialist med inriktning mot IT-rätt, dataskydd, outsourcing och annan samverkan mellan organisationer, Wikström & Partners advokatbyrå.

4 Prop. 2019/20:201, *Tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter.*



Kine Emilie Helgeneseth, Maren Tveten og Ståle L. Hagen

Kunders hevingsadgang i resultatansvarskontrakter etter «Grindgut» – og Felleskjøpet – Infor sakene

Den 29. mars 2023 besluttet Høyesteretts ankeutvalg at Statens vegvesens anke over Borgarting lagmannsretts dom av 14. oktober 2022 i den såkalte «Grindgut-saken» ikke skulle tillates fremmet (HR-2023-563-U[1]). Beslutningen innebærer at vi nå har to relativt nye rettskraftige avgjørelser fra de ordinære domstolene som gir leverandøren medhold i at kundens heving av en resultatansvarskontrakt var urettmessig.

Den første av de to avgjørelsene er den såkalte Felleskjøpet – Infor saken som ble avgjort av Eidsivating lagmannsrett 13. juli 2021 (LE-2018-76187-3[2]). Tvisten stod mellom kunden, Felleskjøpet Agri SA (FKA), og leverandøren, Infor (Steinhausen) II GMBH (Infor). Lagmannsretten kom til at FKAs heving av en avtale om levering av et ERP-system basert på statens standardavtale SSA-T var urettmessig, herunder slik at FKA hadde hevet *for sent*. Infor ble tilkjent erstatning for positiv kontraktsinteresse og sakskostnader.

Litt over ett år senere, den 14. oktober 2022, kom Borgarting lagmannsrett også til at kunden hadde hevet urettmessig i en annen sak omtalt som «Grindgut-saken» (LB-2020-82571-2[3]). Denne tvisten stod mellom kunden Statens vegvesen (SVV) og leverandøren International Business Machines AS (IBM), og gjaldt SVV's heving av en avtale om levering av IKT-løsning for innkreving av bompenger basert på kontraktstandarden PS2000. SVV's heving ble ansett for å være urettmessig blant annet fordi SVV hadde hevet *for tidlig*. IBM ble tilkjent erstatning for positiv kontraktsinteresse og sakskostnader.

I begge sakene var kontraktene basert på norske standardavtaler som jevnlig brukes i det norske markedet. Dommene bygger i stor grad på tolkning av de konkrete kontraktene mellom partene og en vurdering av sakenes omfattende og konkrete faktum, men fordi det er relativt sjelden vi får en rettslig prøving av IT-prosjekter av denne størrelsen er det likevel interessant å vurdere om det kan trekkes noe mer generelt ut av disse avgjørelsene. Både Borgarting lagmannsrett og Eidsivating lagmannsrett kommer med noen generelle uttalelser om adgangen til å heve, og avgjørelsene er derfor av betydning for alle som arbeider med IT-kontrakter. I det følgende skal vi se nærmere på noe av det som kan trekkes ut fra disse avgjørelsene.

For ordens skyld gjøres det oppmerksom på at Advokatfirmaet Selmer bistod Felleskjøpet i forbindelse med hevingsprosessen og rettssaken.

1. Fremgangsmåten ved heving

For det første illustrerer dommene at det stilles strenge krav til selve fremgangsmåten for heving.

1 Lovdata: https://lovdata.no/pro/#document/HRU/avgjorelse/hr-2023-563-u

2 Lovdata: https://lovdata.no/pro/#document/LESIV/avgjorelse/le-2018-76187-3?searchResultContext=1755&rowNumber=8&totalHits=203

3 Lovdata: https://lovdata.no/pro/#document/LBSIV/avgjorelse/lb-2020-82571-2

I begge avgjørelsene legger lagmannsretten til grunn at en betingelse for heving er at kunden først må varsle leverandøren om hva det vesentlige misligholdet består i, og gi leverandøren en frist til å rette opp i dette misligholdet. Kunden skal altså sende et hevingsvarsel. Dette er i tråd med alminnelige obligasjonsrettslige prinsipper, og oppstilles som vilkår for heving også i en rekke andre kontraktstandarder.

Når det gjelder krav til hevingsvarselets innhold, viser lagmannsretten i Felleskjøpet – Infor saken til at kunden må angi hva misligholdet består i, og hva som forventes for å avhjelpe dette. Tilsvarende legges til grunn i Grindgut-saken, herunder at hevingsvarselet må «*identifisere og konkretisere alle forhold som påberopes som hevingsgrunn*», med mindre kontraktspartene har en «*felles forståelse av hvilke konkrete feil som foreligger*».

Lagmannsrettene er også enige om at formålet med hevingsvarselet er å klargjøre hvilke forhold som må rettes for at heving skal avverges. I Felleskjøpet – Infor saken peker lagmannsretten på at «*formålet med kravet til forutgående varsel er at leverandøren ikke skal risikere hevning uten først å ha fått anledning til å rette på forholdet*», og at det «*normalt ikke*» vil «*være i noen av partenes interesse at hevning skjer i andre tilfeller av mislighold enn der hvor leverandøren ikke kan eller vil hjelpe*». I Grindgut-saken viser lagmannsretten til denne uttalelsen fra Felleskjøpet – Infor saken.

På denne bakgrunn uttaler begge lagmannsrettene at kunden som utgangspunkt ikke kan heve på grunnlag av andre forhold enn de som er påberopt i varselet. I Grindgut-saken uttaler lagmannsretten at de legger dette til grunn som et «*alminnelig kontraktsrettslig prinsipp*».

Basert på det samme grunnlaget skriver lagmannsretten i Felleskjøpet – Infor saken at kunden som utgangspunkt heller ikke kan skifte standpunkt eller påberope seg alternative eller supplerende hevingsgrunner. Dette utgangspunktet nyanseres noe i Grindgut-saken, som åpner opp for at det kan være rom for å i ettertid presisere allerede påberopte forhold, og at det også kan være adgang til å påberope nye forhold så fremt det gjøres *"innen rimelig tid»*. Lagmannsretten mente derfor at det var relevant å se på hva SVV skrev til IBM om hvilke forhold som kunne gi grunnlag for heving fra rundt en måned før til rundt to måneder etter at hevingsvarselet ble sendt.

Illustrasjon: Colourbox.com

Lagmannsrettene fokuserer imidlertid ikke bare på selve hevingsvarselets innhold. Særlig i Felleskjøpet – Infor saken er lagmannsretten også opptatt av prosessen etter at hevingsvarselet er sendt. Lagmannsretten uttaler i denne saken at kundens rett til å heve (naturligvis) faller bort dersom leverandøren har rettet opp i de forholdene som er påberopt i hevingsvarselet innen den fastsatte rettefristen. Dersom leverandøren innen utløpet av rettefristen ikke har bragt forholdet i orden, vil imidlertid heving kunne skje.

Ifølge lagmannsretten inntrer imidlertid ikke heving automatisk etter utløpet av rettefristen, og kunden kan dermed ikke i hevingsvarselet anføre at slik automatisk heving skal skje dersom leverandøren ikke har rettet opp misligholdet. Videre er det heller ikke adgang for kunden til å oppstille nærmere vilkår eller kriterier for å unngå heving. Kunden må vurdere om vilkårene for heving også foreligger etter at rettefristen er utløpt, altså en ny og konkret vurdering av om det på dette tidspunktet foreligger «vesentlig mislighold» av avtalen. I tillegg må kunden, etter å ha foretatt en slik reell vurdering, følge opp hevingsvarselet i form av en hevingserklæring. Lagmannsretten uttaler at «*fremsettes ikke hevingserklæring, er ikke avtalen hevet*».

Det er også verdt å merke seg at lagmannsretten i Felleskjøpet – Infor saken uttaler at etter en hevingserklæring er sendt, kan ikke kunden

trekke hevingen tilbake. Bakgrunnen for dette er at en hevingserklæring er å anse som et påbud som har rettsvirkning fra det øyeblikket det kommer frem til leverandøren.

Oppsummert legger domstolene til grunn at kunden må sende et hevingsvarsel som identifiserer og konkretiserer alle forhold som påberopes som hevingsgrunnlag, gi leverandøren en frist til å rette, foreta en reell vurdering av om det også ved utløpet av rettefristen foreligger «vesentlig mislighold», og følge opp hevingsvarselet med en hevingserklæring. I Grindgut-saken åpner lagmannsretten i større grad enn i Felleskjøpet – Infor saken opp for at hevingsvarselet kan suppleres med partenes felles forståelse og nye forhold som har oppstått i tiden før og etter hevingsvarselet. I Felleskjøpet – Infor saken har lagmannsretten en mer rigid tilnærming, og dommen kan leses som en advarsel mot å forhandle med leverandøren samtidig som hevingsvarselet fremsettes og rettefristen løper.

1. Tidspunktet for hevingsvurderingen

Dommene drøfter også at kundens vurdering av hvorvidt det er grunnlag for å heve kontrakten må vurderes ut fra situasjonen på hevingstidspunktet. Selv om dette er i tråd med alminnelig obligasjonsrettslige prinsipper, ser vi ofte at både kunder og leverandører lar tidligere problemer og utfordringer i prosjektet være en del av en senere beslutning om å heve.

Dette ble særlig trukket frem i Grindgut-saken, og var en av hovedgrunnene til at lagmannsretten kom til at SVV ikke kunne heve på grunnlag av inntrådt vesentlig mislighold. Lagmannsretten uttaler at tidligere problemer og utfordringer i prosjektet bare er relevante hvis de fortsatt gjør seg gjeldende på hevingstidspunktet. Flere av de forholdene som SVV hadde påberopt som hevingsgrunnlag var, ifølge lagmannsretten, rettet opp av IBM før hevingstidspunktet. Selv om IBM tidligere i prosjektet hadde misligholdt sine forpliktelser, ble ikke dette tillagt vekt i hevingsvurderingen.

Lagmannsretten går imidlertid lenger enn dette. Forhold som var rettet «*tilstrekkelig*» til at IBM, vurdert ut fra situasjonen på hevingstidspunktet, kunne oppfylt sin hovedforpliktelse i tide, ble heller ikke ansett for å utgjøre mislighold, og kunne derfor ikke begrunne heving.

Mislighold er altså ikke av betydning i hevingsvurderingen dersom de på hevingstidspunktet har blitt rettet, og heller ikke dersom de har blitt rettet i en slik grad at leverandøren kunne ha oppfylt kontrakten i tide. Dette illustrerer at kundens vurdering av egen hevingsrett er dynamisk. Selv om kunden har hatt rett til å heve på et tidspunkt, kan denne retten falle bort dersom leverandøren har klart å rette opp misligholdet i tilstrekkelig grad til at det ikke lenger er over hevingsterskelen. Selv om dette prinsippet kan fremstå som selvfølgelig, kan det være utfordrende for kunden å vurdere sin hevingsrett i komplekse kontraktsforhold der faktum stadig endrer seg. Gjentatte mislighold fra leverandøren kan til tross for at de blir rettet også medføre at kunden mister tillit til leverandøren, og gjøre det videre samarbeidet med leverandøren krevende.

2. Flytting av milepæler og fristforlengelse

I både Grindgut- og Felleskjøpet – Infor saken legger lagmannsretten til grunn andre milepæler og frister enn de kundene baserte sin hevingsrett på. Dette medførte at domstolen og kunden satte ulike datoer for når leverandørens forsinkelse oppstod, og dermed også ulike tidspunkter for når kunden hadde rett til å heve som følge av vesentlig forsinkelse.

I Felleskjøpet – Infor saken legger lagmannsretten, i motsetning til FKA (og tingretten), til grunn at partene var enige om å utsette leveringsdato for en av de dagbotbelagte milepælene (M3), og at partene heller ikke hadde fastsatt en ny leveringsfrist for denne milepælen. På denne bakgrunn legges det til grunn at det ikke lenger fantes en fastsatt leveringsfrist å oversitte, og at det dermed heller ikke forelå noen aktuell forsinkelse som ga FKA rett til å heve. Dette illustrerer at kunden må være varsom med å diskutere fristutsettelser eller forhandle med leverandøren om endringer i fremdriftsplanen, uten samtidig formelt å fastholde allerede kontraktsfestede datoer og eventuelle misligholdsbeføyelser.

Når det gjelder Grindgut-saken ville IBM vært betydelig forsinket dersom milepælene og fristene som fulgte av kontrakten og godkjente endringsordre hadde blitt lagt til grunn. Lagmannsretten ga imidlertid IBM medhold i krav på fristforlengelse og flytting av disse milepælene på grunnlag av påberopte, men ikke endelig godkjente, endringsordre. Dette resulterte i at de avtalte milepælene ble flyttet med i alt 250 dager. Fristen for når SVV hadde hatt rett til å heve som følge av antesipert forsinkelse (milepælsdatoer med tillegg av 100 dager) ble forskjøvet tilsvarende, og medførte at SVV ikke fikk medhold i sitt hevingskrav.

Kunden kan følgelig ikke uten videre legge til grunn de fristene og milepælene som fremgår av kontrakten og eventuelle godkjente endringsordre når de vurderer egen hevingsrett. Det må foretas en vurdering av alle faktiske forhold som kan medføre at leverandøren får medhold i fristforlengelse og flytting av milepæler, herunder endringsanmodninger og eventuell korrespondanse mellom partene om fristene.

3. Terskelen for heving

Dommene illustrerer også at terskelen for å heve en kontrakt er svært høy, både basert på aktuelt mislighold/forsinkelse og antesipert mis-

lighold/forsinkelse. Felleskjøpet – Infor saken gir veiledning når det gjelder terskelen for heving basert på aktuelt vesentlig mislighold, mens Grindgut-saken gir veiledning når det gjelder terskelen for heving basert på antesipert vesentlig forsinkelse.

a. Terskelen for heving basert på vesentlig aktuelt mislighold og forsinkelse

De aller fleste IT-kontrakter og kontrakter generelt, inkludert SSA-T som Felleskjøpet – Infor saken var basert på, gir kunden hevingsrett dersom det foreligger «vesentlig mislighold».

I Felleskjøpet – Infor saken ser lagmannsretten først hen til hva som ligger i dette vesentlighetskravet generelt, og viser til juridisk litteratur hvor det fremgår at det er en forutsetning at «*misligholdet er av en slik art og/eller omfang*» at det gir kunden «*rimelig grunn for å si seg løst fra kontrakten*», og at svaret etter rettspraksis beror på en «*nokså sammensatt helhetsvurdering*».

Lagmannsretten legger imidlertid til grunn en skjerpet hevingsterskel i Felleskjøpet – Infor saken. Bakgrunnen for dette er blant annet at (i) prosjektet gjaldt levering av et omfattende IT-system som skulle spesialtilpasses kundens virksomhet, (ii) det i slike leveranser ikke er uvanlig med forsinkelser, og at det også kan oppstå behov for re-planlegging underveis, og (iii) at leverandøren over lang tid hadde nedlagt en betydelig innsats i prosjektet.

I Grindgut-saken la retten til grunn at leverandørens mislighold var knyttet til brudd på en biforpliktelse (prosjektstyring), og ikke hovedforpliktelsen (resultatforpliktelsen). Lagmannsretten åpner for at brudd på en biforpliktelse kan gi hevingsrett, men likevel slik at «*det skal en del til*», særlig der mislighold av en biforpliktelse «*ikke er til hinder for at resultatforpliktelsen kan oppfylles i tide*».

b. Terskelen for heving basert på vesentlig antesipert forsinkelse

I begge sakene anførte kunden at kontrakten kunne heves på bakgrunn av antesipert vesentlig forsinkelse.

I Felleskjøpet – Infor saken går ikke lagmannsretten nærmere inn på dette spørsmålet. Ifølge lagmannsretten hadde FKA tidligere fastholdt kontrakten til tross for at de hadde fått informasjon om at prosjektet ville bli ytterligere 10-12 måneder forsinket. Selv om en forsinkelse av et slikt omfang isolert sett kunne gitt grunnlag for heving basert på antesipert forsinkelse, mente lagmannsretten at det ikke kunne ha kommet som noen overraskelse på FKA når Infor kort tid før hevingen igjen opplyste om at prosjektet ville bli 10 måneder forsinket. Den antesiperte forsinkelsen kunne derfor, etter lagmannsrettens syn, ikke gi grunnlag for heving. Dette kan leses som at lagmannsretten mente FKA hadde akseptert den varslede forsinkelsen på 10-12 måneder, og at de kun ville hatt hevingsrett dersom leverandøren ble forsinket utover denne allerede varslede forsinkelsen.

Grindgut-saken gir noe veiledning når det gjelder hva som skal til for å heve basert på antesipert vesentlig forsinkelse, og oppstiller et særlig strengt beviskrav. Lagmannsretten viser til at kontrakten mellom partene (PS2000) gir rett til å heve ved antesipert forsinkelse hvis det ut fra informasjonen på hevingstidspunktet er «*klart*» at leverandøren vil overskride en dagbotsanksjonert milepæl med mer enn 100 dager.

Etter lagmannsrettens syn tilsier uttrykket «*klart*» at det kreves mer enn alminnelig sannsynlighetsovervekt. Lagmannsretten uttaler at det kreves «*noe nær visshet*» for at det vil oppstå vesentlig 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 det «*realistisk sett*» kunne latt seg gjøre å rekke fristen, er det ikke grunnlag for å heve.

Dette beviskravet kan, ifølge lagmannsretten, oppfylles på to måter. Beviskravet er for det første oppfylt dersom det etter en konkret vurdering av planer, aktuell fremdrift og tilgjengelige ressurser på hevingstidspunktet er klart at det vil inntre vesentlig forsinkelse. Det er også relevant å se hen til om det forelå forseringsmuligheter. Beviskravet er for det andre oppfylt dersom leverandøren gir en «*utvetydig tilkjennegivelse*» om at det ikke finnes noen muligheter for å levere i tide. Det skal imidlertid mye til for at en leverandør anses for å ha gitt en slik tilkjennegivelse. I Grindgut-saken var selv ikke en presentasjon fra leverandøren om at prosjektet ville bli flere hundre dager forsinket tilstrekkelig, blant annet fordi lagmannsretten mente dette var et forslag til fremdrift og ikke absolutte sannheter.

4. Tap av hevingsrett ved «passivitet»

I begge dommene legger lagmannsretten vekt på det de mener er kundens passivitet når de mottar informasjon fra leverandøren.

I Felleskjøpet – Infor saken hevdet FKA at forsinkelsen løp fra 30. juni 2015. Lagmannsretten legger imidlertid til grunn at FKA mistet retten til å heve avtalen ved at FKA fastholdt avtalen, og lot Infor fortsette arbeidet i omtrent én og en halv måned etter utløpet av dagbotperioden, ca. 8. oktober 2015 og frem til 20. november 2015. Lagmannsretten legger også til grunn at FKA fikk opplysninger fra Infor 10. desember 2015 om at prosjekter var ti til tolv måneder forsinket. Da FKA til tross for dette ikke hevet kontrakten konkluderer lagmannsretten med at FKA heller ikke senere kunne heve på bakgrunn av at dette var en antesipert forsinkelse.

I Grindgut-saken får passivitetsbetraktninger betydning for hvilke

milepælsdatoer som legges til grunn for vurderingen. IBM anførte at de hadde krav på fristforlengelse som følge av tre endringsanmodninger. Dette forutsatte at SVV urettmessig hadde underkjent et kontrollpunkt. Lagmannsretten konkluderer med at SVVs underkjennelse av kontrollpunktet var urettmessig.

SVV begrunnet underkjenningen blant annet med at IBM hadde levert mindre av løsningen enn avtalt. IBM hadde flyttet en betydelig andel av leveransene fra det underkjente kontrollpunktet til en senere iterasjon, og leveransene til det underkjente kontrollpunktet omfattet derfor langt mindre enn det som var avtalt. Lagmannsretten mente at SVV ble 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 dermed medhold i fristforlengelse/flytting av milepæler som følge av endringsanmodningene.

Dommene viser at kunden må reagere raskt ved mottak av informasjon fra leverandøren som tilsier at det foreligger mangler eller forsinkelser. Samtidig kan ikke dette tolkes som at kunden ikke gis noe tid til å områ seg. Det er derfor viktig at kunden er transparent overfor leverandøren, herunder presiserer hva kunden aksepterer og ikke og fastholder eventuelle misligholdsbeføyelser. Det er en vanskelig balansegang mellom å forsøke å drive prosjektet videre og forhandle om løsninger, og samtidig fastholde hevingsretten dersom prosjektet likevel mislykkes.

5. Avsluttende bemerkninger

Begge dommene illustrerer at kunden må ha inngående kunnskap om alle deler av prosjektet ved vurderingen av egen hevingsrett. De viser også hvor vanskelig dette er i komplekse IT-prosjekter. I begge sakene fremstår det som om kunden har forsøkt å drive prosjektet fremover til tross for mangler og forsinkelser fra leverandøren. Lagmannsrettene tolket imidlertid langt på vei disse forsøkene som aksept av leverandørens mislighold og avkall på tilhørende misligholdsbeføyelser. Kunden må derfor være svært tydelig på forutsetningene som legges til grunn for kundens og leverandørens handlinger der prosjektet går dårlig.

Kundens hevingsrett står ikke sterkere enn tidligere i lys av disse dommene. Lagmannsretten viser stor sympati for at leverandørene har lagt ned mye arbeid i prosjektet og at dette arbeidet ikke skal være forgjeves, og kundene forventes å strekke seg langt i å videreføre prosjektene til tross for leverandørens mislighold og manglende tiltro til at leverandøren vil kunne levere i henhold til kontrakt.

Skrevet av Kine Emilie Helgeneseth, advokatfullmektig i avdelingen HITEK i Advokatfirmaet Selmer, Maren Tveten, fast advokat i samme avdeling og Ståle L. Hagen, partner i samme avdeling.

NORGE P. P.
posten

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

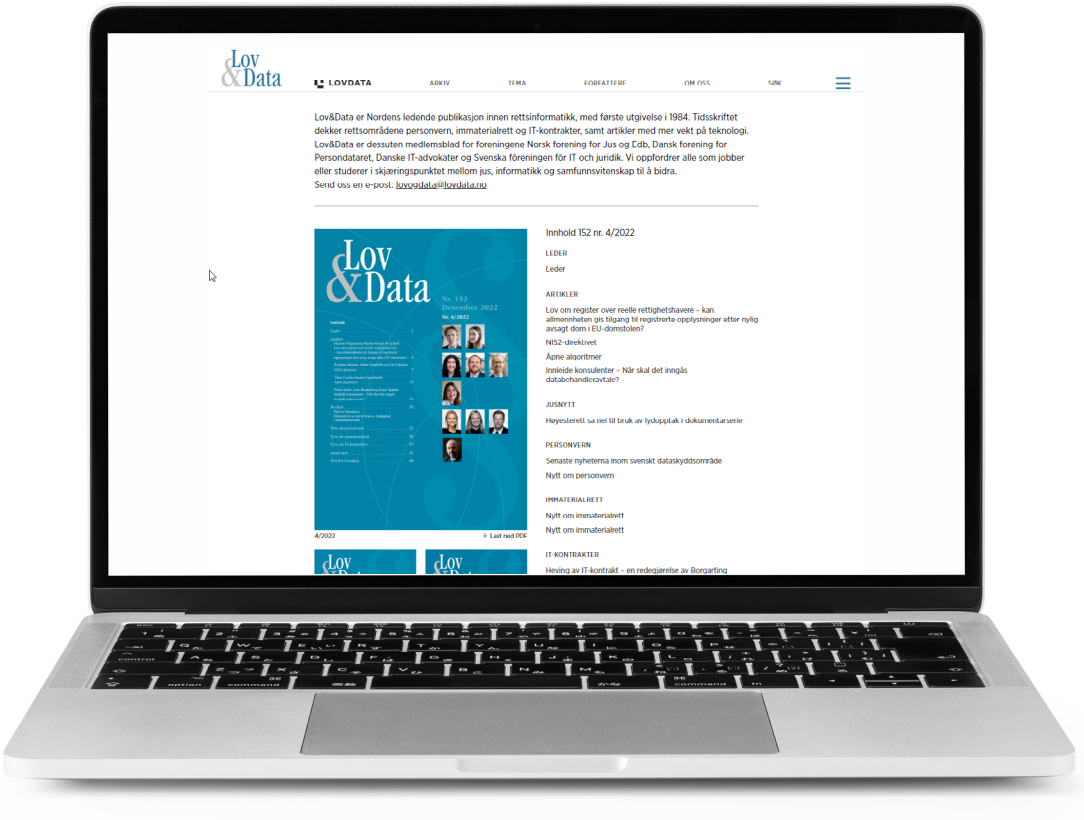
Nytt fra

LOVDATA

Tidsskriftet Lov&Data i digital utgave

Nå finner du tidsskriftet åpent og gratis tilgjengelig på lod.lovdata.no

Fra 2024 vil Lov&Data kun være tilgjengelig digitalt. Ønsker du å si opp papirutgaven send oss en e-post til marked@lovdata.no



Nettsiden er tilgjengelig på norsk, svensk og dansk – med integrasjon mot Lovdata Pro.

Vi ønsker deg god lesing!

Produksjon: Aksell AS