

LOV & Data

Nr. 155
September 2023

Nr. 3/2023

Innhold

<i>Leder</i>	2
Daniel Westman Spiken i kistan for ifragsatt affarsmodell?	
<i>Artikler</i>	
Johanna Chamberlain Ideell skada enligt dataskyddsförordningen – en kommentar till EU-domstolens dom i mål C-300/21	4
Av Anna J.M. Tamuly Hvordan samspiller risikovurderingene i AI Act med risikovurderingene i GDPR?	7
Av Ove A. Vanebo og Ann-Helen Sveino Schøyen Er informasjon om fostre ansett som personopplysninger?	13
Av Line Helen Haukalid og Carl Emil Bull-Berg Overtredelsesgebyr for forsinket avviksmelding – når begynner fristen å løpe?	17
<i>JusNytt</i>	19
Halvor Manshaus: AI og åndsverk – fersk avgjørelse fra USA	
<i>Rettsinformatisk litteratur med mer</i>	23
<i>Aktuell i dag</i>	24
Stein Schjølberg om cyberkriminalitet	
<i>Nytt om personvern</i>	25
<i>Nytt om immaterialrett</i>	39
<i>Nytt om IT-kontrakter</i>	48
<i>Nytt fra Lovdata</i>	56



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 Gorrisen 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.

Lov&Data 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.

Abonnenter vil motta siste utgave i 2023 på papir. Fra 2024 vil Lov&Data kun være tilgjengelig på nett, lod.lovdata.no.

Lov
& Data

Trykk og layout: Aksell AS



Leeder

Spiken i kistan for ifrågasatt affærsmoedell?

Individanpassad annonsering base-rad på en omfattande insamling av användardata har varit en populär affærsmoedell på internet under de senast femton åren. Användarna har fått tillgång till innehållstjänster och sociala medier utan att direkt behöva betala för det. Uppgift om deras användning av tjänsterna har samlats in och använts för riktad annonsering. I många fall har insamling även skett på andra webbplatser och appar som samverkar med tjänsten.

Affærsmoedellen är dock alltmer ifrågasatt. Företagen som använder moedellen får en mycket ingående bild av användarna, t.ex. deras beteende, kontakter och preferenser. Sådan information kan användas för riktad ekonomisk eller politisk påverkan på ett sätt som är svårt för utomstående att granska. Vissa kommentatorer har därför valt att beskriva moedellen som en övervakningskapitalism. Risken finns också att informationen hamnar i orätta händer. Snowdens avslöjanden visade t.ex. att säkerhetsmyndigheter i olika länder hade ett stort interesse av att komma åt information i privata tjänster.

Det har länge stått klart att den omfattande och inte sällan integritetskänsliga hanteringen av personuppgifter kan ifrågasättas data-skyddsrettsligt. När dataskyddsförordningen (GDPR) antogs var vi många som trodde att grundläggande förändringar skulle bli nödvändiga, men många stora aktörer har varit duktiga på att ut-



Daniel Westman

nyttja de rettsliga gråzoner som fortfarande har funnits maximalt, något som har varit möjligt eftersom tillsynsbeslut och prejudicerande avgörande från EU-domstolen har dröjt. Rättsläget har emellertid steg för steg tydliggjorts, samtidigt som tillsynsbeslut med höga sanktionsavgifter har börjat dyka upp.

I centrum för den rettsliga bedömningen står frågan om rettslig grund för den aktuella behandlingen enligt artikel 6. Genom EU-domstolens praxis har de rettsliga och praktiska förutsättningarna för att tillämpa de tre rettsliga grunderna fullgörande av avtal, interesseavvägning/legitimt interesse och samtycke tydliggjorts, senast genom den principiellt viktiga domen den 4

juli 2023 i mål C-252/21, Meta Platforms m.fl.

När det gäller möjligheten att behandla personuppgifter utan samtycke slår domstolen fast att de rättsliga grunderna måste tolkas restriktivt (Meta Platforms m.fl., p. 93).

För att en behandling ska anses vara nödvändig för att fullgöra ett avtal krävs enligt domstolen att behandlingen måste vara ”objektivt oundgänglig för att uppnå ett ändamål som utgör en väsentlig beståndsdel av den tjänst som är avsedd för den registrerade”. Den personuppgiftsansvarige måste således kunna visa på vilket sätt avtalets huvudändamål inte skulle kunna uppnås utan den aktuella behandlingen (p. 99). Domstolens bedömning ligger i linje med Europeiska dataskyddsstyrelsens (EDPB) riktlinjer och myndighetens beslut i ärenden som rör gränsöverskridande behandling. Enligt EDPB innebär det förhållandet att leverantören i användarvillkoren har ålagt sig själv att utföra viss behandling av den registrerades personuppgifter, t.ex. för marknadsföringsändamål, inte per automatik innebär att avtalsundantaget blir tillämplig. Eftersom behandlingen av personuppgifter för marknadsföringsändamål sällan krävs för att en innehålls- eller kommunikationstjänst ska fungera blir denna rättsliga grund i praktiken svår att använda.

Dataskyddsmyndigheterna, t.ex. EDPB och Artikel 29-gruppen, har vidare sedan lång tid gjort bedömningen att omfattande och fördjupande behandling personuppgifter för marknadsföringsändamål normalt inte heller kan ske med stöd av intresseavvägningen/legitimt intresse. I Meta Platforms m.fl. har EU-domstolen bekräftat denna tolkning (p. 105–118). Enligt dom-

stolen kan användaren av ett digitalt socialt nätverk – trots att tjänsten är avgiftsfri – inte rimligen förvänta sig en omfattande behandling för att möjliggöra individanpassad reklam. Det gäller särskilt när behandlingen är synnerligen omfattande eftersom användaren då kan få känslan att hans eller hennes privatliv står under ständig övervakning, en formulering som känns igen från EU-domstolens praxis som rör datalagring. Bland annat av dessa skäl kommer intresseavvägningen typiskt sett att falla ut till de registrerades fördel.

Domstolens redovisade ställningstaganden gör att samtycke numer framstår som den enda realistiska rättsliga grunden för de flesta tillämpningar av den aktuella affärsmodellen. Men inte heller samtycke innebär någon en enkel väg framåt. I dataskyddsförordningen har den strikta definitionen av samtycke, som fanns redan i dataskyddsdirektivet, kompletterats med ytterligare krav i artikel 7, t.ex. beträffande vilka omständigheter som ska beaktas vid bedömningen av om ett samtycke har lämnats frivilligt.

I Meta Platforms m.fl. gällde prövningen Facebook, som ansågs ha en dominerande ställning på marknaden för sociala nätverk. EU-domstolen slog fast att den omständigheten inte i sig utesluter att användarna kan lämna ett frivilligt samtycke till personuppgiftsbehandling när de ansluter sig till tjänsten, men att det var en viktig omständighet som skulle beaktas till tillämpningen av de olika rekvisiten i samtyckesdefinitionen. Domstolen slog fast att användarna måste ha möjlighet att vägra att lämna sitt samtycke till bestämda åtgärder för behandling av personuppgifter, t.ex. insamling av uppgifter om användarens

beteende utanför Facebook, som inte är nödvändiga för fullgörandet av avtalet, utan att de är skyldiga att helt avstå från att använda Facebook. I praktiken innebär det enligt EU-domstolen att ”användarna ska erbjudas, i förekommande mot lämplig ersättning, ett likvärdigt alternativ” utan behandling för marknadsföringsändamål.

Även i övrigt är kraven för att ett giltigt samtycke ska föreligga stränga. Det är ingen överdrift att påstå att majoriteten av de dialoggruтор som vi idag ser i samband med användning av tjänster på nätet inte lever upp till dessa krav. Om användare ges genuint fria val att välja om de vill tillåta spårning och profilering av sina aktiviteter på nätet visar undersökningar att en majoritet väljer att avstå.

En möjlig lösning för att säkerställa att kravet på frivillighet uppfylls är som EU-domstolen antyder i sin dom att också erbjuda den aktuella tjänsten som en betalversion utan insamling av personuppgifter för marknadsföringsändamål. En viktig fråga är om leverantören i en sådan situation kan sätta vilket pris som helst på tjänsten. Domstolen talar om en ”lämplig” ersättning, vilket skulle kunna antyda att priset är en faktor som ska beaktas vid frivillighetsbedömningen.

Det är kanske för tidigt att tala om spiken i kistan för den här diskuterade affärsmodellen, men mycket tyder på att den har passerat sin höjdpunkt och nu är förenad med större risker. .

Daniel Westman



Ideell skada enligt dataskyddsförordningen – en kommentar till EU-domstolens dom i mål C-300/21

Av Johanna Chamberlain¹

Inledning och bakgrund

Äntligen lite praxis om artikel 82 dataskyddsförordningen (GDPR)!² Kanske till och med en chans att få det efterlängtrade tolkningsstödet kring vad de breda begreppen ”immateriell skada” och ”ersättning för uppkommen skada” egentligen betyder i det EU-rättsliga sammanhanget?³ Förväntningarna var höga bland alla intresserade när Europeiska unionens domstol (EUD) den 4 maj 2023 kom med sitt avgörande i målet UI mot Österreichische Post AB.⁴ Mål om artikel 82 GDPR, och innan dess om föregångaren artikel 23 i dataskyddsdirektivet,⁵ har nämligen lyst med sin frånvaro.

Bakgrunden till målet i EUD var att bolaget Österreichische Post AB sedan år 2017 hade samlat in upp-



Johanna Chamberlain

Foto: Tobias Björkgren

gifter om den österrikiska befolkningens politiska tillhörighet, i syfte att – med hjälp av algoritmer som förutspådde sannolikhet att rösta på ett visst parti – sälja adresslistor och således möjliggöra för organisationer att skicka ut riktad reklam. En av de registrerade, UI, kände sig förnärad över den politiska åskådning som tillskrevs honom mot bakgrund av de insamlade uppgifterna. Han väckte talan i nationell domstol och krävde dels att bolaget skulle förpliktas att upphöra med personuppgiftsbehandlingen, dels ersättning om 1 000 euro för ideell skada bestående i känslor av förlorad tillit, förargelse och förödmjukelse. Medan de nationella domstolarna biföll det förstnämnda yrkandet, begärde Österrikes högsta domstol förhandsavgörande gällande frågan om skadestånd. Följande tre viktiga och grundläggande frågor om ersättningsgill skada och ersättningsbestämning enligt artikel 82 ställdes till EUD:

1. Krävs det för att tillerkännas ersättning enligt artikel 82 i [dataskyddsförordningen], utöver en överträdelse av bestämmel-

” Äntligen lite praxis om artikel 82 dataskyddsförordningen (GDPR)! Kanske till och med en chans att få det efterlängtrade tolkningsstödet kring vad de breda begreppen ”immateriell skada” och ”ersättning för uppkommen skada” egentligen betyder i det EU-rättsliga sammanhanget?

serna i förordningen, även att klaganden har lidit skada, eller är överträdelsen av dataskyddsförordningen i sig tillräcklig för tillerkännande av ersättning?

2. Gäller vid beräkning av ersättningen ytterligare krav enligt unionsrätten utöver principerna om likvärdighet och effektivitet?
3. Är uppfattningen att det krävs en sådan följd eller verkan av en överträdelse som åtminstone är av viss allvarlighetsgrad och går utöver den förargelse som överträdelserna har orsakat för att [ersättning ska kunna beviljas för] ideell skada, förenlig med unionsrätten?

Domstolens dom och kommentarer till domen Den första tolkningsfrågan

Efter att ha utrett vissa invändningar om att ta upp den första och andra frågan till sakprövning, varvid man konstaterat att detta var möjligt, gav sig EUD in på prövningen i

1 Postdoktor i handelsrätt vid Företagsekonomiska institutionen, Uppsala universitet.
2 Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
3 Se på detta tema t. ex. Havu, ”Damages Liability for Non-material Harm in EU Case Law”, *European Law Review* 2019, Vol. 44 nr. 4, s. 492–514; Havu, ”Contemporary Member State Liability Case Law: On Causation and Harm”, *European Law Review* 2022, Vol. 47 nr. 6, s. 791–808.
4 ECLI:EU:C:2023:370.
5 Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.



Illustration: Colourbox.com

sak. Angående den första tolkningsfrågan resonerar domstolen enligt följande:

Begreppen i artikel 82 ska ges en självständig och enhetlig unionsrättslig tolkning, då hänvisningar till medlemsstaternas rättsordningar saknas.⁶ Artikel 82 ska tolkas så att enbart den omständigheten att GDPR överträtts inte är tillräckligt för att ge rätt till ersättning. För ersättning krävs alltså att överträdelser i fråga har orsakat någon form av skada. Denna slutsats når EUD med hjälp av en bokstavstolkning, där förekomsten av ordet ”skada” och kravet på orsakssamband i artikel 82 och skäl 75, 85 och 146 betonas.⁷ Vidare jämför EUD artikel 82 med artiklarna 83 och 84 i förordningen, vilka ”inte är beroende av förekomsten av en individuell skada”.⁸ Domstolen framhåller härvid att dessa artiklar har ett bestraffan-

de syfte, till skillnad från artikel 82, och att reglerna således kompletterar varandra.⁹

EUD:s resonemang i denna del innehåller inga egentliga nyheter eller överraskningar. För en skadeståndsrättare är det dock välkommet att få bekräftelse gällande den allmänna skadeståndsrättsliga principen att rätt till ersättning kräver en konstaterad skada. Det är också rimligt att skillnaden gentemot administrativa sanktionsavgifter enligt artikel 83 särskilt nämns – i det senare fallet räcker det alltså med en överträdelse. Denna skiljelinje mellan skadestånd och sanktionsavgift går tillbaka på de sedan länge etablerade funktionerna reparation och prevention eller bestraffning, vilket förstärker domstolens tolkning.¹⁰

9 Domen p. 40.

10 Se vidare Chamberlain & Reichel, ”The Relationship Between Damages and Administrative Fines in the EU General Data Protection Regulation”, *Mississippi Law Journal* 2020, Vol. 89 nr. 4, s. 667–696.



För en skadeståndsrättare är det dock välkommet att få bekräftelse gällande den allmänna skadeståndsrättsliga principen att rätt till ersättning kräver en konstaterad skada.

Den tredje tolkningsfrågan

Domstolen valde därefter att behandla den tredje tolkningsfrågan. Ställningstagandet blev här att artikel 82 utgör hinder för nationell lagstiftning eller praxis, enligt vilken en förutsättning för ersättning för ideell skada är att skadan ska vara av en viss allvarlighetsgrad.¹¹ Som stöd för tolkningen uttalar EUD att ”skada” inte definieras i förordningen, men att skäl 146 anger att begreppet ska tolkas brett.¹² Av skäl 10 framgår

11 Domen p. 51.

12 Domen p. 45–46.

6 Domen p. 29–30.

7 Domen p. 31–37.

8 Domen p. 40.

vidare att förordningen syftar till att skapa en hög och enhetlig skyddsnivå för personuppgifter inom unionen, något som skulle riskera att undergrävas om rätten till ersättning gjordes beroende av en allvarighetströskel som potentiellt kan variera domare emellan.¹³ Den registrerade måste emellertid fortfarande visa att det finns en ideell skada i den mening som avses i artikel 82.¹⁴

Tolkningen är delvis väntad. Ett huvudsyfte med GDPR är ökad harmonisering på dataskyddsområdet, och det skulle då vara märkligt om EUD öppet förespråkade trösklar för ersättning som kan komma att variera inom medlemsstaterna (även om dessa sedan gammalt har olika standarder för ideell skada som inte endast inbegriper ersättningsnivåer utan även ersättningsgilla skador¹⁵). Däremot hade EUD gärna fått säga betydligt mer om hur skadebegreppet, särskilt ”materiell skada”, ska förstås i den EU-rättsliga kontexten och dataskyddssammanhanget. De riktlinjer och den ökade klarhet som praktiker och potentiella parter i mål har önskat uteblir helt genom EUD:s rundgång om att någon (undre) tröskel för en ersättningsgill ideell skada inte får finnas, men att en ideell skada i linje med artikel 82 fortfarande måste visas. Detta får anses innebära att det tills vidare är upp till medlemsstaterna att tolka och fylla begreppet – vilket medför att bedömningen, tvärtemot EUD:s harmoniseringsönskemål, kommer att bli beroende av nationella standarder och nationella domare som uppställer just olika trösklar.¹⁶

Den andra tolkningsfrågan

Slutligen behandlade EUD den andra tolkningsfrågan, och kom till följande slutsats. Vid beräkningen av ersättning för ideell skada enligt artikel 82 ska de nationella domstolarna tillämpa medlemsstatens interna bestämmelser om den ekonomiska ersättningens omfattning – under förutsättning att principerna om likvärdighet och effektivitet iakttas.¹⁷ Domstolen hänvisar återigen till skäl 146 GDPR som anger att ”full och effektiv” ersättning ska utges, och menar att ersättningen är full och effektiv så länge den fullt ut möjliggör kompensation av den skada som vållats till följd av den aktuella överträdelsen (varvid skadestånd med bestraffande funktion inte anses nödvändigt för att full ersättning ska uppnås).¹⁸

” Detta får anses innebära att det tills vidare är upp till medlemsstaterna att tolka och fylla begreppet – vilket medför att bedömningen, tvärtemot EUD:s harmoniseringsönskemål, kommer att bli beroende av nationella standarder och nationella domare som uppställer just olika trösklar.

Härmed tydliggör domstolen att inga ytterligare faktorer behöver beaktas när ersättningsbestämningen hanteras i medlemsstaterna, vilket innebär att samma ordning som tidigare fortsätter gälla för utombliatoriskt skadestånd – nationell

processuell autonomi inskränkt av likvärdighets- och effektivitetsprinciperna. Uttalandet angående full och effektiv ersättning tillför måhända inte så mycket, men det kan noteras att skadeståndsrättens kompensatoriska syfte betonas (liksom gällande den första tolkningsfrågan) och att en skillnad åter görs gentemot så kallat punitivt skadestånd.

Slutord

Sammanfattningsvis levererar EUD:s första substantiella dom om ideell skada på dataskyddsområdet inte riktigt de klargöranden som varit efterfrågade. Däremot bekräftar i domen att skadestånd alltså är beroende av att en överträdelse av dataskyddsreglerna har orsakat en faktisk skada, att harmonisering är ett huvudsyfte med förordningen och att likvärdighets- och effektivitetsprinciperna ska iakttas i samband med begreppet ”full och effektiv” ersättning (liksom i övrigt när EU-rätten genomförs). Även om dessa hållpunkter var högst kända sedan innan, kan vi i vart fall känna oss trygga med att fortsätta tillämpa artikel 82 GDPR som hittills. I övrigt får vi sätta vårt hopp till de övriga mål om artikel 82 som lyckligtvis pågår och som kan komma att få större betydelse framöver.¹⁹

Jobanna Chamberlain är postdoktor i handelsrätt vid Företagsekonomiska institutionen, Uppsala universitet, där hon forskar om risk- och ansvarsfrågor kopplade till artificiell intelligens. Hon undervisar inom både offentlig rätt och civilrätt, med särskilt fokus på skadeståndsrätt och dataskydd.

13 Domen p. 48–49.

14 Domen p. 50.

15 Se t. ex. Wagner, ”Liability Rules for the Digital Age”, *Journal of European Tort Law* 2022, Vol. 13 nr. 3, s. 211; 221 f; 237.

16 Jfr Knetsch, ”The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases”, *Journal of European Tort Law* 2022, Vol. 13 nr. 2, s. 145.

17 Domen p. 59.

18 Domen p. 58.

19 Se bl. a. mål C-687/21 och C-741/21.

Hvordan samspiller risikovurderingene i AI Act med risikovurderingene i GDPR?

Av Anna J.M. Tamuly

1. Innledning

De siste årene har kunstig intelligens («KI») fått større utbredelse enn noen gang før. Det utvikles stadig flere produkter og tjenester som inneholder KI i en eller annen form og både offentlig og privat sektor i Norge er i gang med å kartlegge mulige bruksområder for KI fremover. Selv om teknologien utvilsomt er nyttig, kan den også utgjøre en stor risiko for menneskene som er utsatt for den. For å minimere risikoen forbundet med utvikling og bruk av KI, er det enighet om at det er behov for rettslig regulering. Det store spørsmålet er imidlertid hvordan vi best mulig skal klare dette.

Den 21. april 2021 la Europakommisjonen frem et forslag til en KI-forordning («AI Act»)¹. Den 6. desember 2022 publiserte Rådet et endringsforslag², og den 14. juni 2023 publiserte Europaparlamentet sin holdning.³ I tiden fremover skal partene inn i «trilog»-forhandlinger før endelig forordningsvedtak er



Anna J.M. Tamuly

ventet i slutten av 2023 eller starten av 2024.⁴

AI Act er verdens første forslag til et juridisk rammeverk som regulerer KI spesifikt. Når KI behandler personopplysninger innenfor EU eller om personer bosatt i EU, faller behandlingen imidlertid samtidig under personvernforordningen («GDPR»)⁵. Dette reiser spørsmål om samspillet mellom GDPR og fremtidens AI Act, og hvor godt regelverkene er harmonisert.

I min masteravhandling fra våren 2023 undersøkte jeg hvordan risikovurderingene i forslaget til AI Act samspiller med risikovurderingene som må foretas etter GDPR, samt hvordan dette påvirker sentrale aktører under de to regelverkene. For

å kunne besvare problemstillingen ble det identifisert hvilken rolle de sentrale aktørene under GDPR har under AI Act og hvordan rollefordelingen endrer seg i livsløpet til en KI. Avhandlingen inneholder videre en analyse av ulikhetene i de risiko-baserte tilnærmingene i henholdsvis GDPR og forslaget til AI Act, samt mulige konsekvenser av dette. Oppgaven og konklusjonen er rettet mot utviklere og tilbydere av KI som i fremtiden kommer til å måtte forholde seg til både GDPR og AI Act.

” Når KI behandler personopplysninger innenfor EU eller om personer bosatt i EU, faller behandlingen imidlertid samtidig under personvernforordningen («GDPR»).

I denne artikkelen skal jeg oppsummere funnene mine, med utgangspunkt i Rådets forslag. I ettertid, 14. juni 2023, har Europaparlamentet publisert sitt forslag. Betydningen av dette for mine funn fra våren 2023 vil bli kommentert underveis og avslutningsvis.

2. Rolleavklaring

Aktørene som er involvert i behandlingen av personopplysninger etter GDPR er *behandlingsansvarlig*, *databehandler* og *den registrerte*. De fleste forpliktelsene etter GDPR pålegges den behandlingsansvarlige.⁶ Be-

1 European Commission COM/2018/237

2 Council of EU, «Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights», pressemelding, 6. desember 2022. [Tilgjengelig her: Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights] (lest 17.8.2023).

3 European Parliament, «MEPs ready to negotiate first-ever rules for safe and transparent AI». [Tilgjengelig her: MEPs ready to negotiate first-ever rules for safe and transparent AI | News | European Parliament (europa.eu)] (lest 17.8.2023).

4 Trilog-forhandlinger er uformelle forhandlinger om lovforslag mellom representanter for Europaparlamentet, Rådet og Kommisjonen. Formålet er å oppnå en enighet mellom Europaparlamentet og Rådet om en lovtokst. Europaparlamentet har skrevet om disse på sine sider: Inter-institutional negotiations | Ordinary Legislative Procedure | European Parliament (europa.eu) (lest 17.08.2023).

5 GDPR artikkel 4 nr. 2.

6 NOU 2022: 11, s. 38.



Illustrasjon: Colourbox.com

handlingsansvarlig bestemmer formålet med en behandling og hvilke hjelpemidler, eksempelvis kunstig intelligens, som skal brukes.⁷ Behandlingsansvarlig er videre ansvarlig for risikoen og må gjennomføre de fleste risikovurderingene etter GDPR. Behandlingsansvarlig er imidlertid ikke nødvendigvis den som utfører selve behandlingen. En *databehandler* behandler personopplysninger på vegne av behandlingsansvarlig.⁸ *Den registrerte* er den identifiserte eller identifiserbare fysiske personen det behandles personopplysninger om.⁹

Under forslaget til AI Act er det *leverandøren* («provider») som er underlagt flest forpliktelser. En leverandør er en som utvikler et KI-system, setter dette på markedet el-

ler som tar det i bruk under eget navn eller varemerke.¹⁰ Videre er *brukeren* (tidligere «users», men foreslått endret til «deployers» av Europaparlamentet) en sentral aktør under AI Act. Brukere er definert som «any natural or legal person, including a public authority, agency or other body, under whose authority the system is used».¹¹ Dette kan eksempelvis være en arbeidsgiver som anvender et KI-system til å bistå med ansettelsesprosesser, eller en bank som anvender KI til å identifisere risikolånetakere. Brukere er også underlagt forpliktelser i forslaget til AI Act, men i mer begrenset omfang enn leverandøren. Europaparlamentets forslag innebærer imidlertid at flere av forpliktelsene som opprinnelig kun ble pålagt le-

verandør, nå også er foreslått pålagt brukerne.

Sett i lys av GDPR vil definisjonen av brukere i AI Act i mange tilfeller være *behandlingsansvarlige* etter GDPR artikkel 4 nr. 7, mens leverandørene opptre som *databehandlere* jf. GDPR artikkel 4 nr. 8. Dette medfører at selv om brukernes forpliktelser etter AI Act er begrenset, vil disse ha en rekke forpliktelser som behandlingsansvarlige etter reglene i GDPR. Samtidig er leverandøren selv behandlingsansvarlig for behandling av personopplysninger som gjøres med et eget satt mål om å utvikle, trene opp og videreutvikle KI-systemet sitt. Leverandører opptre derfor i mange tilfeller som databehandler og behandlingsansvarlig samtidig, eller er behandlingsansvarlig i utviklingsperioden og databehandler overfor en bruker av systemet når dette er ferdigutviklet. Med andre

7 GDPR art. 4 nr. 7.

8 GDPR art. 4 nr. 8.

9 GDPR art. 4 nr. 1.

10 Rådets forslag art. 3 nr. 2.

11 Rådets og Europaparlamentets forslag artikkel 3 nr. 4

ord vil rollefordelingen i mange tilfeller endres i løpet av livsløpet til en KI og for ulike deler av en behandling.

” Sett i lys av GDPR vil definisjonen av brukere i AI Act i mange tilfeller være behandlingsansvarlige etter GDPR artikkel 4 nr. 7, mens leverandørene opptrer som databehandlere jf. GDPR artikkel 4 nr. 8.

Dette har flere konsekvenser. For det første at det kan være utfordrende og ressurskrevende for hovedaktørene å forstå hvilken rolle de har i relasjon til de to regelverkene til enhver tid. Videre kan det være utfordrende å forstå hvilke forpliktelser de har og når.

3. To risikobaserte rettsakter

Både AI Act og GDPR er risikobaserte rettsakter. At GDPR har en risikobasert tilnærming kan forankres i GDPR artikkel 24, 32 m.fl., men fremgår også allerede i et av de grunnleggende prinsippene for behandling av personopplysninger, ansvarlighetsprinsippet.¹² Den risikobaserte tilnærmingen i GDPR følger et *nedefra-og-opp*-perspektiv.¹³ Med dette menes at de ulike bestemmelsene legger opp til at det er behandlingsansvarlige som er nærmest å vurdere risikoen og iverksette risikoreducerende tiltak. Det er behandlingsansvarlig som kjenner behandlingen best, og egen ressurs-situasjon, og dermed har forutsetning for å vurdere hvilke tiltak som vil virke best.¹⁴

12 Gellert (2020) s. 138.

13 De Gregorio og Dunn (2022) s. 4.

14 De Gregorio og Dunn (2022) s. 4.

AI Act representerer det motsatte synspunktet. Selve risikokategoriseringen overlates ikke til aktørene som forordningen retter seg mot. Det er AI Act som selv, fra en *ovenfra-og-ned*-tilnærming, direkte identifiserer fire ulike risikokategorier og pålegger aktører forpliktelser avhengig av risikogruppen systemet faller innunder.¹⁵

Ulikhetene i de risikobaserte tilnærmingene kan føre til at det blir utfordrende å få en helhetlig forståelse av risiko og hvilket ansvar risikoen medfører. Selv om det må vurderes hvilken risikokategori et KI-system ligger innunder, ansvarliggjøres leverandørene i mindre grad for denne vurderingen enn hva behandlingsansvarlig gjør etter GDPR hvor rommet for skjønn er større.

På den andre siden er det det samme konstitusjonelle målet om å fremme EUs grunnleggende rettigheter og friheter, herunder personvern, som er bakgrunnen for de to regelverkene.¹⁶ GDPR og forslaget til AI Act deler et mål om å regulere, og dermed minimere, risikoen nye teknologier kan utgjøre. Selv om de gir uttrykk for EUs risikobaserte tilnærming på svært ulike måter, er dette overordnede målet en samlende faktor.¹⁷ Når GDPR ikke alene har klart å begrense risikoene KI utgjør for menneskers rettigheter og friheter på en tilstrekkelig måte, er det kanskje nødvendig at AI Act anvender en annen tilnærming.

4. Risikovurderingene som må foretas etter de to regelverkene

Behandlingsansvarlig må etter GDPR artikkel 24, 25, 32 og 35 nr. 1 foreta risikovurderinger av risikoen en behandling av personopplysninger utgjør for de registrerte for et KI-system tas i bruk eller ut-

15 Ibid.

16 GDPR fortalepunkt 12; Rådets forslag fortalepunkt 2.

17 Ibid.

vikles. Disse risikovurderingene skal blant annet avklare om det er sannsynlig at systemet utgjør en høy risiko, slik at plikten til å foreta en vurdering av personvernkonsekvenser (DPIA) etter GDPR artikkel 35 foreligger.

Etter AI Act må leverandører foreta en vurdering av hvilken kategori systemet som utvikles faller inn under for å identifisere hvilke forpliktelser de har. Som nevnt identifiseres de ulike risikokategoriene direkte i lovverket og risikovurderingen som må foretas på dette tidspunktet er gjennomregulert, i motsetning til vurderingene etter GDPR.

” Ulikhetene i de risikobaserte tilnærmingene kan føre til at det blir utfordrende å få en helhetlig forståelse av risiko og hvilket ansvar risikoen medfører.

I likhet med GDPR artikkel 35 er det imidlertid også i AI Act lovfestet andre risiko-fokuserte legislative teknikker som ulike aktører må foreta og løpende oppdatere, slik som kravet til opprettelsen av et risikostyringssystem etter AI Act artikkel 9.¹⁸ Forpliktelsene artikkelen oppstiller var tidligere pålagt leverandøren alene, men Europaparlamentet har foreslått at dette også skal gjelde brukere.¹⁹ Formålet med artikkel 9 er å sørge for at det tas ytterligere grep for å redusere risiko som, etter overholdelse av de øvrige reglene i kapittel to, enda ansees å være for

18 Mahler (2022) s. 252.

19 Europaparlamentets forslag artikkel 16 nr. 1 bokstav a. At forpliktelsen ikke er pålagt en konkret aktør kan potensielt resultere i at samme prosesser risikovurderes flere ganger.

høy.²⁰ Artikkel 9 er dermed en viktig sikkerhetsventil som åpner opp for mer skjønsmessige risikovurderinger enn i AI Act for øvrig.

I likhet med en DPIA etter GDPR artikkel 35, krever risikovurderingsprosessen etter artikkel 9 nr. 1 og 2 systematisk oppdatering og oppfølging. Forpliktelsen foreligger kun for systemer som er høyrisiko etter AI Act. DPIA-prosessen foreligger derimot allerede om det er «sannsynlig» at behandlingen er høyrisiko etter GDPR.

Selv om AI Act ikke gir rettigheter til enkeltindivider på samme måte som GDPR, er leverandøren nødt til å vurdere risikoen for fysiske personer som er utsatt for leverandørens KI-system.²¹ Første steg i risikostyringssystemet er å identifisere og analysere kjente og forutsigbare risikoer for helse, sikkerhet og grunnleggende rettigheter i lys av det tiltenkte formålet med systemet. Europaparlamentet krever i tillegg at risiko for negativ påvirkning av like rettigheter, demokrati og mer må vurderes.²²

Leverandørens forpliktelse til å løpende vurdere de grunnleggende rettighetene til individer som kan være utsatt for KI-systemet, medfører at leverandøren må foreta noen av de samme vurderingene som behandlingsansvarlig/brukeren må foreta i sin DPIA etter GDPR artikkel 35. Det er derfor viktig at AI Act forsøker å harmonisere vurderingen foretatt etter AI Act artikkel 9 og etter GDPR artikkel 35. Dette poenget har Rådet sett. Derfor er det inntatt et krav om at leverandøren må dele funnene sine etter artikkel 9 nr. 2 med brukeren av systemet.²³ I Europaparlamentets forslag er bestemmelsen endret og det er ikke lenger slik at informasjon kun

skal formidles fra leverandøren til brukerne, men informasjonsflyten skal gå begge veier. Dette er en naturlig følge av at risikovurderingsplikten er pålagt begge aktører.



Selv om AI Act ikke gir rettigheter til enkeltindivider på samme måte som GDPR, er leverandøren nødt til å vurdere risikoen for fysiske personer som er utsatt for leverandørens KI-system.

Det fremgår imidlertid fremdeles i Europaparlamentets forslag at brukere av systemer som utgjør høy risiko skal bruke informasjonen de har fått av leverandøren i artikkel 9-vurderingen til å overholde forpliktelsen sin til å foreta en DPIA etter GDPR artikkel 35.²⁴ At begge disse risikovurderingssystemene skal oppdateres løpende medfører at overholdelse av GDPR artikkel 35 og AI Act artikkel 9 fordrer et nært samarbeid mellom leverandøren og brukeren av KI-systemet. Dersom den ene parten ikke gir tilstrekkelig informasjon, risikerer den andre parten å bryte sine forpliktelser etter ett eller begge regelverk.

Kommunikasjonen mellom leverandører og behandlingsansvarlige/brukere av KI-systemer er en utfordring. Dette kan kanskje forklares med at det hittil hovedsakelig har vært behandlingsansvarlig som har blitt ansvarliggjort for risikoen behandling av personopplysninger utgjør. Dermed har ikke databehandleren hatt det samme initiativet til å gi tilstrekkelig informasjon til behandlingsansvarlig. Der databe-

handler er tilknyttet et land utenfor EU har den vanskelige kommunikasjonen også kunnet forklares med at databehandler ikke har tilstrekkelig kunnskap om hvilken informasjon behandlingsansvarlig trenger og hvorfor. Med AI Act vil også leverandøren/databehandler få et større risikoansvar og vil ha et større initiativ til å opprettholde en løpende, åpen og god kommunikasjon med brukeren. Slik sett kan vedtakelsen av AI Act være med på å gjøre kommunikasjonen lettere.

5. Ytterligere risikovurderinger i Europaparlamentets forslag

I Kommisjonens og Rådets forslag skal KI-systemer listet opp i vedlegg III til forordningen som hovedregel automatisk regnes som høyrisiko.²⁵ Dette inkluderer blant annet KI-systemer som brukes i drift og styring av kritisk infrastruktur, systemer som brukes til utdannings- og yrkesopplæringsformål og systemer brukt i ansettelsesprosesser eller av en arbeidsgiver overfor sine ansatte. Etter Europaparlamentets forslag må det derimot foretas en konkret risikovurdering av om disse systemene utgjør en betydelig risiko for helse, sikkerhet eller EUs grunnleggende rettigheter. Først dersom det er tilfellet, vil KI-systemene regnes som høyrisiko.²⁶

I Europaparlamentets forslag er det videre lagt til en ny artikkel 29 a som pålegger brukere av høyrisiko AI-systemer å foreta en «Fundamental rights impact assessment» før første bruk av KI-systemet og på nytt hvis nødvendig. Denne vurderingen er omfattende og det er oppstilt 9 punkter som minimum skal vurderes. Dette inkluderer blant annet det tiltenkte geografiske og tidsmessige omfanget av systemets bruk, kategorier av fysiske personer og grupper som sannsynligvis vil bli påvirket av bruken av systemet, spe-

20 Schuett (2023) s. 4.

21 Schuett (2023) s. 8.

22 Europaparlamentets forslag artikkel 9 nr. 2 bokstav a.

23 Rådets forslag artikkel 13 nr. 3 bokstav b(iii)

24 Rådets og Europaparlamentets forslag artikkel 29 nr. 6

25 Rådets forslag artikkel 6 nr. 3.

26 Europaparlamentets forslag artikkel 6 nr. 2.

sifikke risikoer for skade som sannsynligvis vil påvirke marginaliserte personer eller sårbare grupper og de forutsigbare uønskede virkningene av bruk av systemet på miljøet.

For å unngå overlapp med GDPR er det spesifisert i punkt 3 at dersom brukeren allerede er pålagt å utføre en DPIA etter artikkel 35 i GDPR skal risikovurderingen i AI Act artikkel 29 gjennomføres sammen med DPIAen. DPIAen skal publiseres som et tillegg. I realiteten medfører dette at brukere må gjøre en mer omfattende vurdering enn det som er nødvendig etter GDPR artikkel 35. Det kan også diskuteres hvor lett det vil være å besvare alle de 9 punktene vurderingen krever, det kan være utfordrende for brukeren av et nytt system å vite svarene. Dermed kommer brukeren til å være avhengig av gode tidligere vurderinger og svar fra leverandøren/utvikleren.

6. Hvordan kan utviklere og tilbydere av kunstig intelligens bistås?

Det er som gjennomgått flere av de konkrete kravene til risikovurderinger i AI Act som ikke er harmonisert med de allerede eksisterende kravene til risikovurderinger etter

bestemmelsene i GDPR kapittel IV. Videre er kravene pålagt ulike aktører i løpet av livsløpet til en KI og for ulike deler av en behandling.



Det er som gjennomgått flere av de konkrete kravene til risikovurderinger i AI Act som ikke er harmonisert med de allerede eksisterende kravene til risikovurderinger etter bestemmelsene i GDPR kapittel IV.

Dette har flere konsekvenser. For det første at det kan være utfordrende for aktørene å forstå hvilken rolle de har i relasjon til de to regelverkene og følgelig hvilke forpliktelser de har og når. Videre må det utføres flere risikovurderinger enn de som allerede må gjennomføres etter GDPR. De fleste av disse kan neppe samordnes fullt ut om det skal sikres overholdelse av begge regelverk. Dette kommer til å medføre økte kostnader og kompleksiteten

av overholdelse vil øke ytterligere utover hva som allerede er tilfellet etter GDPR.

Det finnes flere måter å begrense utfordringene på. En måte er å lage gode veiledninger med et helhetlig syn på begge regelverkene. Disse veiledningene må identifisere overlappende krav, mål, risikovurderinger og proporsjonalitetsvurderinger. På den måten vil de kunne trekke linjer til hvor informasjon innhentet etter kravene i den ene forordningen kan brukes til å overholde forpliktelsene etter den andre forordningen. Det er etter min mening ikke tilstrekkelig med organer som veileder bedrifter til overholdelse av ett av regelverkene isolert sett, slik som EDPB. Der regelverkene overlapper eller regulerer samme tilfelle, må veiledningene legge til rette for det. Gode modeller, figurer og andre verktøy vil være til hjelp i veiledningsprosessen. Videre må også pliktsubjektene selv sørge for at de har en helhetlig tilnærming til risikovurderingene som må foretas etter både GDPR og AI Act.

Anna Tamuly er advokatfullmektig i Advokatfirmaet BÅHR AS.

Litteraturliste

Norske lover og forarbeider

1. NOU 2022: 11 Ditt personvern – vårt felles ansvar. Tid for en personvernpolitikk.
2. Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven).

EU-rett

Direktiver og forordninger

1. Europaparlamentets- og Rådsforordning (EU) nr. 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) [GDPR].

Uttalelser, veiledninger og retningslinjer

1. Council of the EU, «Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights», pressemelding, 6. desember 2022. Tilgjengelig her: [link Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights - Consilium \(europa.eu\)](#) (lest 29.08.2023).
2. European Commission, «Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence», pressemelding, 21. april 2021. Tilgjengelig her: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682. (lest 29.08.2023).
3. European Commission COM/2021/206, «Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts», Brussel, 21. april 2021 COM/2021/206 endelig. Tilgjengelig her: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206> (lest 29.08.2023).
4. European Parliament, «MEPs ready to negotiate first-ever rules for safe and transparent AI». [Tilgjengelig her: <https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai>] (lest 17.8.2023).

Bøker

1. Gellert, Raphaël, *The risk-based approach to data protection*, 1. utgave, Oxford University Press, 2020.
2. Schartum, Dag Wiese, *Personvernforordningen – en lærebok*, 1. utgave, Fagbokforlaget, 2020.

Artikler

1. De Gregorio, Giovanni og Dunn, Pietro, «The European Risk-based Approaches: Connecting Constitutional Dots in the Digital Age», *Common Market Law Review* 59, 2 (2022) s. 473-500. DOI: <https://dx.doi.org/10.2139/ssrn.4071437>
2. Mahler, Tobias, «Between Risk Management and Proportionality: The Risk-Based Approach in the EU's Artificial Intelligence Act Proposal», *The Swedish Law and Informatics Research Institute*, 1 (2022) s. 247–270. DOI: <https://doi.org/10.53292/208f5901.38a67238>.
3. Schuett, Jonas, «Risk Management in the Artificial Intelligence Act», *European Journal of Risk Regulation*, First View (2023) s. 1-19. DOI: <https://doi.org/10.1017/err.2023.1>

Internettadresser

1. Bertuzzi, Luca, «AI Act: European Parliament headed for key committee vote at end of April», *Euractive*, 30. mars 2023, oppdatert 31. mars 2023 [Tilgjengelig her: <https://www.euractiv.com/section/artificial-intelligence/news/ai-act-european-parliament-headed-for-key-committee-vote-at-end-of-april/>] (lest 08.04.2023).
2. Bertuzzi, Luca, «MEPs seal the deal on Artificial Intelligence Act», *Euractive*, 27. april 2023, oppdatert 28. april 2023. [Tilgjengelig her: <https://www.euractiv.com/section/artificial-intelligence/news/meps-seal-the-deal-on-artificial-intelligence-act/>] (lest 03.05.2023).

Er informasjon om fostre ansett som personopplysninger?

Av Ove A. Vanebo og Ann-Helen Sveino Schøyen

1. Innledning

Spørsmålet om et fosters moralske status aktualiserer både vanskelige etiske og følelsesmessig krevende problemstillinger. Innenfor jussens verden er det krevende gråsoner og ulike reguleringer som bestemmer når et foster anses for å være en person.

En særlig problemstilling innenfor personvernretten er om informasjon om fostre vil kunne utgjøre «personopplysninger» i henhold til personopplysningsloven, som gjør EUs personvernforordning («GDPR») til norsk rett.

Artikkelen redegjør for rettskildet bildet, og vil drøfte hvorvidt personvernforordningens personopplysningsbegrep omfatter informasjon om fostre. For enkelthetens skyld vil «foster» i artikkelen betegne mennesket fra unnfangelse og frem til fødsel.

Problemstillingen har potensielt stor rekkevidde, blant annet fordi ulike helse- og forskningsinstitusjoner behandler mye informasjon om fostre. Her kan for øvrig særlovgivningen nedfelle et særlig vern «forstre».

Ettersom vår vurdering er at svaret er uklart, vil vi mot slutten av artikkelen forsøksvis komme med noen antakelser.

2. Kan et foster være en «fysisk person» i henhold til GDPR?

2.1 Hva kan utledes av forordningen?

Personopplysninger er informasjon om en bestemt fysisk person, jf. GDPR artikkel 4 nr. 1.

Personvernforordningen uttrykker ikke klart hva som kreves for å være ansett som en «person». At fostre ikke er nevnt eller behandlet eksplisitt, kan tas til inntekt for både at de inkluderes og at de ikke er omfattet.



Ove A. Vanebo



Ann-Helen Sveino Schøyen

” En særlig problemstilling innenfor personvernretten er om informasjon om fostre vil kunne utgjøre «personopplysninger» i henhold til personopplysningsloven.

Det er imidlertid verdt å merke seg at forordningens fortalepunkt 27 fastslår at kun levende personer er omfattet av forordningens regulering, slik at informasjon om avdøde personer ikke er omfattet av personopplysningsbegrepet. Det kan anføres at den klare henvisningen til avdøde personer, men ikke til ufødte personer, kan tas til inntekt for at fosterinformasjon neppe er utelukket av uttrykket «personopplysninger».¹ Her

er det likevel viktig å huske at en slik antitetisk slutning neppe bør tillegges for mye vekt.

På den annen side kan det også argumenteres for at ordlyden «levende» sikter til personer som er født.² Vi oppfatter riktignok dette som et lite vektig argument, siden fostre jo også er levende i biologisk forstand.

Selv om GDPR også benytter uttrykket «barn», er heller ikke dette begrepet klart definert i forordningen.³

I forarbeidene til endringen i barnevernsloven ser departementet ut til forutsetningsvis å legge til grunn at informasjon om ufødte barn er personopplysninger: «Departementet foreslår videre i kapittel 4 at adgangen til å behandle nødvendige personopplysninger om gravide og ufødte barn blir presisert i

1 Manuel Klar og Jürgen Kahlings kommentar til GDPR artikkel 4(1). I: Jürgen Kühling and Benedikt Buchner (red.), Datenschutz-Grundverordnung; Kommentar, 1. utgave, 2017.

2 Sören Öman, Dataskyddsförordningen (GDPR) m.m.: En kommentar, 2019, s. 58; se også Peter Golas kommentar til artikkel 4. I: Peter Gola, Datenschutz-Grundverordnung VO (EU) 2016/679; Kommentar, 1. utgave, 2017.

3 Se f.eks. GDPR artikkel 8 nr. 1.

barnevernslov».⁴ Ettersom departementet verken begrunner eller drøfter denne forutsetningen, bør uttalelsen ikke tillegges nevneverdig vekt.

Personvernforordningens bestemmelser må tolkes i lys av andre internasjonale konvensjoner og kilder. Dette gjelder blant annet Den europeiske menneskerettskonvensjonen (EMK), Den europeiske unions pakt om grunnleggende rettigheter («pakten») og Europarådets konvensjon av 28. januar 1981 om personvern i forbindelse med elektronisk databehandling av personopplysninger («DPC»).

Paktens bestemmelser om personvern er inspirert av de tilsvarende bestemmelsene i EMK og DPC,⁶ og vil derfor ikke inngå i en separat drøftelse.

Etter EMK artikkel 8 nr. 1 har «enhver» rett til respekt for sitt privatliv og familieliv. Den europeiske menneskerettsdomstolen (EMD) har slått fast at artikkel 8 også omfatter personopplysningsvernet.⁷ Uttrykket «enhver» benyttes også i EMK artikkel 2 nr. 1. Om denne bestemmelsen har EMD uttalt at det ufødte barn generelt sett ikke vil være beskyttet av EMK artikkel 2.⁸ Domstolen holder likevel muligheten åpen for at et foster kan være vernet i enkelte tilfeller, og henviser i denne forbindelse til artikkel 8: «Article 8 § 1 cannot be interpreted as meaning that the pregnancy and its termination are, as a principle, solely a matter of the private life of

the mother». Det er derfor uavklart om det kan utelukkes at uttrykket «enhver» i EMK artikkel 8 omfatter fostre – og det er tenkelig at spørsmålet om abortrettigheter o.l. må bedømmes annerledes enn persondatarettslige spørsmål.⁹

Etter DPC artikkel 2 bokstav a) defineres personopplysninger som enhver opplysning som gjelder en bestemt eller identifiserbar «enkeltperson». Det er ikke spesifisert om «enkeltperson» også omfatter fostre.

Imidlertid har Europarådets ministerkomité utstedt en anbefaling om beskyttelse av medisinsk data, med utgangspunkt i konvensjonens bestemmelser.¹⁰ Etter anbefalingens punkt 4.5 skal «[m]edical data concerning unborn children [...] be considered as personal data and enjoy a protection comparable to the protection of the medical data of a minor». Rådet foreslår at dette kan gjennomføres ved at data om fosteret klassifiseres som morens personopplysninger.¹¹ Enkelte land har innført en lignende praksis.¹² Rådets anbefaling er imidlertid ikke rettslig bindende for medlemslandene.

Det er altså ingen klar oppfatning som kan utledes av forordningen eller øvrig internasjonal rett når det gjelder hvorvidt et foster er en «fysisk person» – og i det minste utelukkes det ikke at informasjon om fostre kan anses som personopplysninger.

9 Janne Rothmar Herrmann, *Retsbeskyttelsen af fostre og befrugtede ag og håndteringen af retlige hybrider*, 2008, s. 185-187; se også Portmeister og Drożdżowski 2018 s. 58.

10 Europarådets ministerkomité, *Recommendation R (97) 5 of the Committee of Ministers to Member States on the Protection of Medical Data*. Lest 29. august 2023: <https://rm.coe.int/cmrec-97-5-on-the-protection-of-medical-data/1680a43b64>

11 *Explanatory Memorandum to the Recommendation No R (97) 5 on the Protection of Medical Data* punkt 87. Lest 29. August 2023: <https://rm.coe.int/16806846cb>

12 Are genetic data of unborn children subject to data protection under the GDPR?

2.2 Særlig om oppfatningen i juridisk teori

Flere teoretikere har drøftet spørsmålet om hvorvidt informasjon om fostre er personopplysninger.

Nielsen og Lotterup antar at informasjon om fostre i alminnelighet må anses å være personopplysninger.¹³

” Det er altså ingen klar oppfatning som kan utledes av forordningen eller øvrig internasjonal rett når det gjelder hvorvidt et foster er en «fysisk person» – og i det minste utelukkes det ikke at informasjon om fostre kan anses som personopplysninger.

Sören Öman mener derimot at informasjon om «ännu inte födda, dvs. foster», ikke omfattes av definisjonen av personopplysninger, og synes å forankre dette i at de ikke er «levende fysiske personer».¹⁴

Kärt Pormeister og Łukasz Drożdżowski argumenterer for at fostre må anses som ufødte barn, som er «registrerte» med rettigheter i den forstand som brukes i GDPR – og vil at det skal tas hensyn til beskyttelse av deres genetiske data.¹⁵ De påpeker det problematiske ved at foreldre blir «registrerte» i relasjon til informasjon om fosteret, siden det skaper problemer etter at barnet født og dermed selv kan bli «registrert» i forordningens forstand.¹⁶

13 Kristian Korfits Nielsen og Anders Lotterup, *Databeskyttelsesforordningen og databeskyttelsesloven*, 2020, s. 252.

14 Öman 2019 s. 58.

15 Portmeister og Drożdżowski 2018 s. 58.

16 Portmeister og Drożdżowski 2018 s. 61.

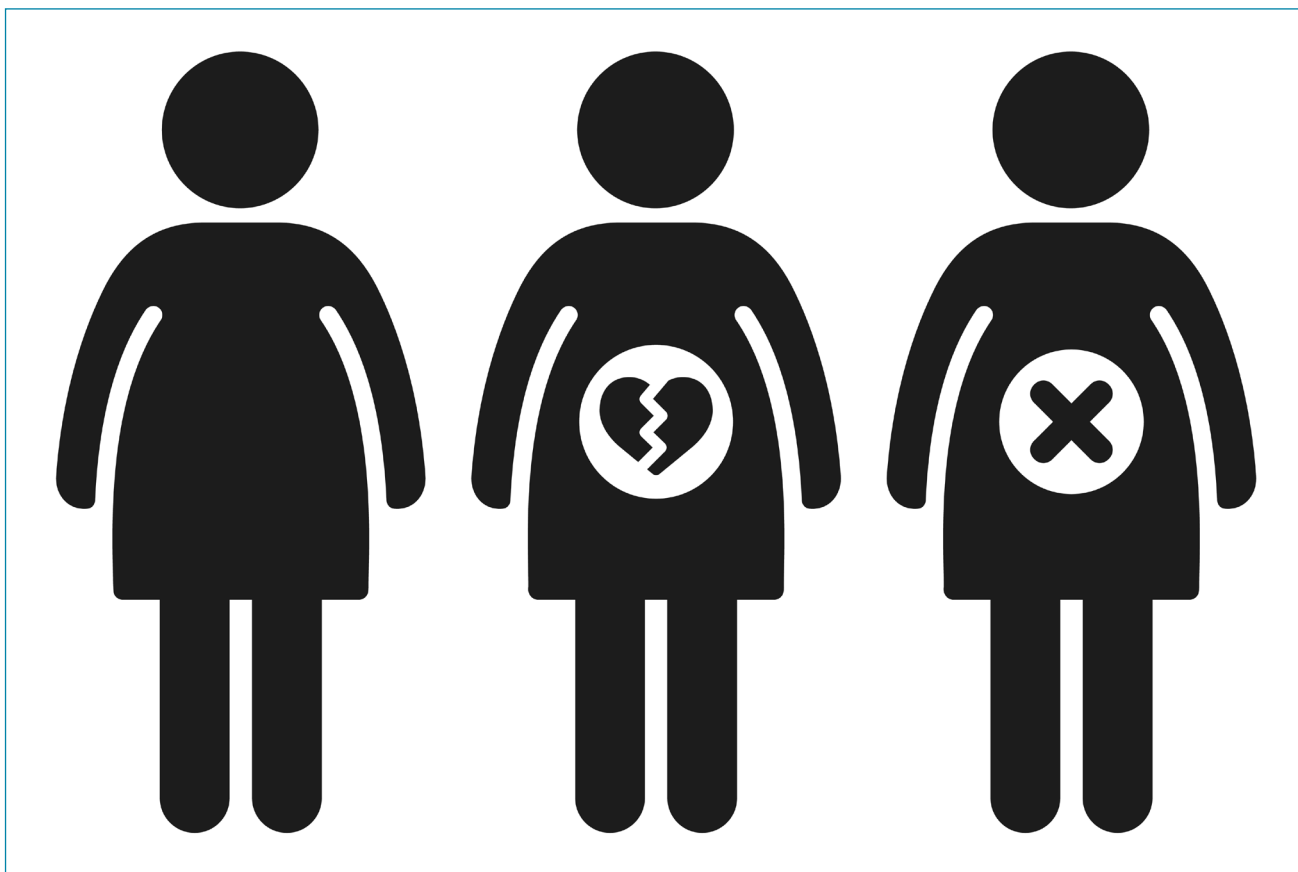
4 Prop.64 L (2022-2023) Endringer i barnevernsloven m.m. (formidling av opplysninger, meldinger om ufødte barn, politiattest) s. 5.

5 Se GDPR fortalepunkt 4 og 105, og Åste Marie Bergseng Skullerud mfl., *Personvernforordningen*. Lovkommentar, *Artikkel 1*, Juridika.

6 Kärt Pormeister og Łukasz Drożdżowski, *Protecting the Genetic Data of Unborn Children*. I: *European Data Protection Law Review*, nr. 1, 2018, sidene 53 - 64, s. 57.

7 Se f.eks. *Liebscher v. Austria* avsnitt 31.

8 *Vo v. France* avsnitt 80.



Illustrasjon: Colourbox.com

Suzanne Dibble påpeker at «*Natural person* isn't defined in the GDPR, but it is unlikely that a fetus would be deemed a natural person».¹⁷

Peter Blume anfører på sin side at fostre antakeligvis kan være «fysiske personer» – iallfall i de tilfeller hvor det er mer meningsfylt, blant annet siden fosteret normalt vil bli et barn med behov for vern av sensitiv informasjon.¹⁸ Basert på Blumes resonnement, antar Hanne Marie Motzfeldt at det bør anlegges en formålsoverordnet forståelse, der fostre har en slags «antesipert beskyttelse», i det minste når det er tilsiktet at fosteret skal bli et barn.¹⁹

2.3 Situasjonen etter

personvernordningen

Begrepet «personopplysning» er i all hovedsak en videreføring av tilsvarende begrep i personvernordningen.²⁰ Det kan derfor være relevant å se til om direktivet avklarer spørsmålet om klassifisering av informasjon om fostre.

Begrepet «fysisk person» brukes ikke i direktivet, er legaldefinisjonen av «personopplysninger» ment å være den samme som i GDPR.

Heller ikke i direktivet er det en definisjon på hva som utgjør en «fysisk person».²¹ Imidlertid har EU-

kommisjonens tidligere rådgivende organ, Artikkel 29-gruppen, kommet med en uttalelse om hva som utgjør personopplysninger, der den også omtaler fosterdata.²² Ifølge gruppen må det vurderes konkret hvorvidt nasjonale personvernregler også gjelder opplysninger om fostre. Vurderingen avhenger av «the general approach of the national legal system» og «the idea that the purpose of data protection rules is to protect the individual».²³ Det kan derfor synes som om spørsmålet er overlatt til den enkelte medlemsstat. Enkelte teoretikere oppfatter imidlertid at uttalelsen kan tas til inntekt for at informasjon om fostre generelt faller utenfor direktivets definisjon av «personopplysning».²⁴

17 Suzanne Dibble, *GDPR for dummies*, 2019.

18 Peter Blume, *Databeskyttelsesret*, 5. utgave, 2018, s. 18-19.

19 Hanne Marie Motzfeldt, *Grundleggende databeskyttelsesret*, 2022, s. 54.

20 Justisministeriet, *Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning*; Betænkning nr. 1565, 2017, s. 71.

21 I den norske oversettelsen av direktivet brukes ikke begrepet «fysisk person» i legaldefinisjonen av «personopplysninger», jfr. art. 2 bokstav a). Imidlertid benyttes uttrykket «natural person» både i den engelske oversettelsen av direktivet og i GDPR. Dette indikerer at legaldefinisjonen er ment å være den samme i direktivet og forordningen.

22 Artikkel 29-gruppen, *Opinion 4/2007 on the concept of personal data*.

23 Artikkel 29-gruppen 2007 s. 23.

24 Pormeister og Droidowski 2018 s. 54.

Også for direktivets del har ulike teoretikere drøftet spørsmålet om informasjon om fostre er personopplysninger. Peter Blume anfører at fostre, i det omfang det gir mening, skal gis rettslig beskyttelse og betraktes som individer innenfor databeskyttelsesretten.²⁵

2.4 Oppsummering av rettskildebildet

Rettskildebildet gir ingen klare svar på om informasjon om fostre omfattes av personvernlovgivningen. Vi antar derfor at det per nå ikke er mulig å konstatere en felles oppfatning av om informasjon om fostre anses for å være personopplysninger.

Så vidt oss bekjent, finnes det verken forvaltnings- eller rettspraksis som har tatt stilling til spørsmålet. Det er heller ikke klart om dette spørsmålet har et generelt unionsrettslig svar, der man kan komme til en felles definisjon, eller om avgjørelsen må tas på nasjonalt nivå.²⁶

3. Vår vurdering/noen antakelser

Vi mener at det i enkelte tilfeller er nokså klart at informasjon om fostre må anses for å være personopplysninger. Dette gjelder tilfeller der informasjonen knytter seg til personer som *er blitt* født. Det synes også på det rene at informasjon om fostre som kan gi informasjon om foreldre også er personopplysninger – om foreldrene.

25 Peter Blume, *Databeskyttelsesret*, 3. utgave, 2008, s. 17-18.

26 Sören Öman mener at denne problemstillingen «*har ett EU-gemensamt svar och altså inte ska avgöras enligt nationell rätt*», jf. Öman 2019 s. 58.

Motsetningsvis er det lite som tilsier at informasjon om et abortert foster bør klassifiseres som personopplysninger.

De mer krevende tilfellene melder seg der det ikke er avklart om fosteret bæres til levedyktig alder. Det kan være problematisk dersom informasjon som senere kan være ytterst sensitiv og i verste fall skadelig for en person nyter et mer begrenset vern enn GDPR inneholder inntil personen blir født. Det kan da være for sent å iverksette avbøtende tiltak for å begrense informasjonens skadevirkninger.

” Rettskildebildet gir ingen klare svar på om informasjon om fostre omfattes av personvernlovgivningen.

Etter vårt skjønn er det gode grunner for at informasjon om iallfall fostre som etter alt å dømme vil bli født, beskyttes som personopplysninger. Dette kan sies å være logisk siden informasjon som først på et senere tidspunkt kan knyttes til en fysisk person, vil være personopplysninger, selv om det på et bestemt tidspunkt ikke er mulig.²⁷ Siden dette

27 Artikkel 29-gruppen 2007 s. 15. I slike tilfeller mener vi at Blumes tilnærming kan være hensiktsmessig – så lenge det er meningsfylt, f.eks. hvis det er mest sannsynlig at fosteret vokser opp til å bli et menneske, bør fosterinformasjonen klassifiseres som personopplysninger.

i praksis er svært vanskelig å avgjøre, kan det være hensiktsmessig å operere med en presumsjon for at informasjon om fostre er personopplysninger – ikke minst fordi informasjonen ofte kan si noe om andre personer, særlig foreldrene.

” Etter vårt skjønn er det gode grunner for at informasjon om iallfall fostre som etter alt å dømme vil bli født, beskyttes som personopplysninger.

En utfordring er imidlertid at vitenskapelig kunnskap er i utvikling og at det krever også annen fagspesifikk kunnskap for å forstå hva slags informasjon som kan knyttes til bestemte personer. Vi har derfor liten tro på enkle enten-eller-standpunkter her, og mellom disse to ytterpunktene kan det utvilsomt oppstå vanskelige grensetilfeller.

Ove A. Vanebo, advokat og assosiert partner i CMS Kluge Advokatfirma, og Ann-Helen Sveino Schøyen, advokatfullmektig i CMS Kluge Advokatfirma.

Overtredelsesgebyr for forsinket avviksmelding – når begynner fristen å løpe?

Av Line Helen Haukalid og
Carl Emil Bull-Berg

Den 8. mars 2023 vedtok Datatilsynet et overtredelsesgebyr på 2,5 millioner kroner til det amerikanske selskapet, Argon Medical Devices (heretter omtalt som «Argon»). Bakgrunnen for gebyret var manglende overholdelse av 72 timers-fristen for avviksmelding.



Line Haukalid



Carl Emil Bull-Berg

Kort om 72-timers fristen

Meldeplikten til behandlingsansvarlige er regulert i GDPR artikkel 33. I henhold til artikkel 33 nr. 1 skal brudd på personopplysningsikkerheten meldes senest 72 timer etter at den behandlingsansvarlige har fått kjennskap til bruddet, dersom mulig. Dette gjelder ikke dersom bruddet sannsynligvis ikke vil medføre risiko for fysiske personers rettigheter og friheter.

Hva skjedde?

Argon opplevde sommeren 2021 et sikkerhetsbrudd. Bruddet bestod i at uautoriserte tredjepart hadde fått tilgang til epostkontoen til en av selskapets ansatte. Dette gav tilgang til personopplysninger om lønn og tilhørende informasjon om Argons ansatte, inkluderte én ansatt i Norge. Etter å ha undersøkt bruddet nærmere, sendte Argon den 24. september 2021 inn en avviksmelding til Datatilsynet.

Datatilsynet la i vedtaket til grunn følgende tidsforløp:

- 14. juni 2021. Argons IT-sikkerhetsteam får beskjed fra en ansatt at det er uvanlig aktivitet i epostkontoen til vedkommende. Etter nærmere undersøkelse oppstår

mistanke om at en utenforstående har fått tilgang til epostkontoen. Argon har grunn til å tro at vedkommende har hatt dette siden 21. mai 2021.

- 15. juni 2021. Argon melder hendelsen til FBI Cybercrime Unit i USA.
- 19. juli 2021. Argons undersøkelser avdekker at personopplysninger om europeiske ansatte har blitt påvirket av hendelsen
- 24. september 2021. Argon sender avviksmelding til europeiske datatilsyn, herunder det norske Datatilsynet. Dette da etter at Argon, ved hjelp av juridisk bistand, konkluderer med at hendelsen er meldepliktig.

Når fikk Argon kjennskap til bruddet?

I denne saken var det særlig sentralt for Datatilsynet å fastslå når Argon fikk *kjennskap* til bruddet. Som nevnt innledningsvis, begynner 72 timers-fristen å løpe fra og med dette tidspunktet. Spørsmålet er imidlertid hva som ligger i dette kriteriet. En mulig tolkning er at den behandlingsansvarlige får kjennskap (og tidsfristen derfor

begynner å løpe) på det tidspunktet den behandlingsansvarlige får kunnskap til at det foreligger et *meldepliktig* brudd på personopplysningsikkerheten. Dette innebærer blant annet at den behandlingsansvarlige må ha kjennskap til de faktiske forholdet som tilsier at bruddet vil kunne innebære risiko for fysiske personers rettigheter og friheter. Det er først på dette tidspunktet den behandlingsansvarlige har tilstrekkelig informasjon til å vite at hendelsen er meldepliktig.

” Tidsfristen kan altså begynne å løpe før den behandlingsansvarlige har tilstrekkelig kunnskap for å konkludere med at hendelsen er meldepliktig [...]

Datatilsynet (i tråd med veiledning fra EDPB) legger imidlertid til grunn at 72 timers-fristen begynner å løpe på tidspunktet når den behandlingsansvarlige blir klar over at det har



Illustrasjon: Colourbox.com

forekommet et brudd på personopplysningsikkerheten. Tidsfristen kan altså begynne å løpe før den behandlingsansvarlige har tilstrekkelig kunnskap for å konkludere med at hendelsen er meldepliktig (altså før den behandlingsansvarlige har kjennskap til de faktiske forholdene som tilsier at det foreligger risiko).

Dette betyr at tre kumulative vilkår må være oppfylt for at fristen skal begynne å løpe. *For det første*, må det ha funnet sted et sikkerhetsbrudd.

For det andre, må den behandlingsansvarlige være klar over at hendelsen innebærer brudd på konfidensialitet, tilgjengelighet og/eller integritet.

For det tredje, at bruddet omfatter personopplysninger. EDPB har i sin veileder om avviksmeldinger lagt til grunn at 72 timers-fristen begynner å løpe når den behandlingsansvarlige *med en rimelig grad av sikkerhet* forstår at disse vilkårene er oppfylt. Det er imidlertid interessant å merke seg at Datatilsynet slår fast at Argon burde vært klar over bruddet på et enda tidligere tidspunkt. Bakgrunnen for dette er et sitat fra EDPB, som også er gjengitt i vedtaket. EDPB skriver: *“the controller may*

undertake a short period of investigation in order to establish whether or not a breach has in fact occurred”.

Datatilsynets bemerkninger i vedtaket mot Argon kan muligens indikere at tilsynet mener at tidsfristen i artikkel 33 nr. 1 også kan begynne å løpe før den behandlingsansvarlige har kjennskap til sikkerhetsbruddet, dersom den behandlingsansvarlige har gått utover hva som ligger i en «short period of investigation».

” Det er imidlertid interessant å merke seg at Datatilsynet slår fast at Argon burde vært klar over bruddet på et enda tidligere tidspunkt.

Tolkningen har noe forankring i EDPB veiledning, men har liten støtte i ordlyden til artikkel 33 nr. 1. Artikkel 33 nr. 1 slår tydelig fast at fristen på 72 timer begynner å løpe fra den behandlingsansvarlige blir klar over bruddet. Ikke fra tidspunktet den behandlingsansvarlige *burde* fått slik kjennskap et-

ter en «short period of investigation». Datatilsynets tolkning bærer preg av å innføre et aktsomhetskrav (med en tilhørende ny tidsfrist).

Dette virker i så fall som en unødvendig innfortolkning. De fleste virksomheter er pålagt å ha rutiner for håndtering av avvik, da i henhold til artikkel 24 nr. 2. Dersom virksomheten ikke har slike rutiner, eller disse viser seg å ikke være operative i praksis, kan brudd muligens konstateres etter artikkel 24 – eller andre tilsvarende bestemmelser. At de organisatoriske og tekniske tiltakene skal sørge for at den behandlingsansvarlige klarer å håndtere avvik (herunder melde til Datatilsynet og/eller de registrerte) følger også blant annet av fortalepunkt 87. Det er derfor ikke nødvendig å innfortolke et aktsomhetskrav i artikkel 33 nr. 1. Det finnes altså andre bestemmelser som rammer samme forhold, uten behov for å innfortolke et aktsomhetskrav i artikkel 33.

Line Helen Haukalid, Managing Associate i Advokatfirmaet Wiersholm.

Carl Emil Bull-Berg, Senior Associates i Advokatfirmaet Wiersholm.



Halvor Manshaus

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

AI og åndsverk – fersk avgjørelse fra USA

18. august 2023 kom det en interessant avgjørelse fra U.S. District Court for the District of Columbia i sivil sak 22-1564 (BAH). Dette er en føderal domstol som utgjør førsteinstans for det særskilte distriktet Columbia som har sammenfallende grense med hovedstaden Washing-

ton i USA. Saken tar for seg et prinsipielt spørsmål i forholdet mellom kunstig intelligens og opphavsrett. Avgjørelsen er såpass ny at den ikke er rettskraftig i skrivende stund, men selv om saken ankes er det etter min vurdering lite sannsynlig at vi vil se noe annet utfall.

Saksøkeren Stephen Thaler har forklart at han har utviklet og eier flere dataprogrammer som han selv hevder bygger på kunstig intelligens (Artificial Intelligence – AI). Blant disse har han utviklet et datasystem som han ga navnet «the Creativity Machine». Thaler hevder at dette



systemet har skapt et billedkunstverk på egenhånd. Han har deretter forsøkt å registrere dette verket for at det skal få sterkere opphavsrettslig status i USA.

Verket heter «A Recent Entrance to Paradise» og er inntatt nedenfor. Det er uklart fra avgjørelsen om tittelen stammer fra Thaler eller data-programmet.

I USA får opphavsmannen vern for verket samtidig som det frembringes, forutsatt at dette skjer i et format som er fiksert og i en form som kan observeres enten direkte eller ved bruk av hjelpemidler. Som utgangspunkt kan opphavsmannen imidlertid ikke gå til inngreps sak for amerikanske domstoler uten at verket først er registrert. Det vern som opphavsmannen nyter er altså begrenset fordi håndhevelse av opphavsretten forutsetter registrering. Registrering har også en praktisk betydning ved at det innebærer tidfesting av verket og har betydning for rettens bevisvurdering etter nærmere angitte bevisregler. Regelverket i USA avviker dermed fra det vi er kjent med i Norge, hvor det ikke er krav til registrering.

Registrering skjer ved U.S. Copyright Office (USCO), som er en avdeling under det amerikanske kongressbiblioteket. I dette tilfellet ble registrering nektet under henvisning til at verket ikke var menneskeskapt. USCO tolket regelverket slik at dette er et absolutt krav for at verk skal oppnå status som åndsverk og inn tas i registeret.

Thaler påklaget avgjørelsen og bekreftet igjen at verket «*was autonomously generated by an AI*» og at det ikke forelå «*traditional human authorship*». Det var altså enighet om faktum, men Thaler fremholdt at en slik autonom frembringelse burde kunne registreres der vilkårene ellers var tilstede. Thaler argumenterte for at eierskapet til verket i slike tilfeller skal ligge hos eieren av det kunstige systemet som har laget verket. Argumentasjonen er her overlappende med saker tidligere

omtalt av undertegnede i artikkel i Lov & Data (LoD-2020-142-16), der oppfinnelser skapt av kunstige systemer er blitt søkt patentert i en rekke ulike jurisdiksjoner for å aktualisere debatten om kunstige frembringelser. USCO av slo klagen og oppsummerte sitt standpunkt slik: «*[b]ecause copyright law is limited to „original intellectual conceptions of the author;“ the Office will refuse to register a claim if it determines that a human being did not create the work.*»

Nærmere undersøkelser viser at det er den samme Stephen Thaler som går igjen i disse sakskompleksene. Thaler samarbeider med Dr. Ryan Abbot som er professor ved University of Surrey School of Law i England. Sistnevnte startet AIP, som står for «Artificial Inventor Project». Det er dette prosjektet som står bak en rekke patentsøknader som har vært og delvis fortsatt er til behandling i flere ulike jurisdiksjoner. Disse søknadene har til felles at det er en AI som står bak oppfinnelsen, og dette åpner for en diskusjon om slike oppfinnelser lar seg patentere – og hvem som i så fall skal ha rett til oppfinnelsen. Dette er da også hele poenget med AIP, å skape debatt og diskusjon rundt AI og innovasjon. Nærværende sak gjelder altså ikke en oppfinnelse, men et kunstverk i form av et AI-generert bilde. Dette åpner opp for en tilsvarende debatt på opphavsrettens område.

Etter at klagen var blitt forkastet fremmet Thaler ytterligere en klage, som ble behandlet av Copyright Office Review Board. Klagen førte ikke frem, og klageorganet ga sin tilslutning til synspunktet om at det kun er menneskelige frembringelser som kan registreres.

Thaler brakte deretter saken inn for retten. Slik saken var lagt frem, skulle retten kun ta stilling til det ene spørsmålet om et verk som utelukkende er skapt av et kunstig system og uten noen menneskelig innblanding kan få status som et åndsverk. Faktum var altså ubestridt og

saken gjaldt bare spørsmål om rettsanvendelsen. Samtidig var det fra begge sider bedt om en såkalt «summary judgment», en form for forenklet rettsbehandling som retten fant at det var åpning for i denne saken.

” Disse søknadene har til felles at det er en AI som står bak oppfinnelsen, og dette åpner for en diskusjon om slike oppfinnelser lar seg patentere – og hvem som i så fall skal ha rett til oppfinnelsen.

Thaler argumenterte med at det forelå flere eksempler knyttet til overgang av rettigheter fra dataprogram tilbake til utvikleren, og hevdet at dette ga anvisning på at opphavsrett måtte følge et slikt spor. Retten var imidlertid ikke overbevist, og viser til at saken ikke gjelder overgang av opphavsrett, men først og fremst spørsmålet *om det på noe tidspunkt har eksistert en slik rett overhodet*. Retten spissformulerer dette på følgende måte: «These arguments concern to whom a valid copyright should have been registered, and in so doing put the cart before the horse.»

I en fotnote viser retten samtidig til at Thaler i denne sammenheng overfor retten har argumentert med at hans egen menneskelige innsats ved utviklingen av dataprogrammet, den konkrete anvendelsen og kommandoer til Creativity Machine innebærer tilstrekkelig menneskelig aktivitet. Her får formen for avgjørelsen sentral betydning, ved at en «summary judgment» innebærer at domstolen fungerer som et ankeorgan som etter common law-systemet kun skal vurdere det samme faktum som underinstansen. Retten

peker dermed på at det ikke er rom for å vurdere nye anførsler, og at Thaler overfor USCO eksplisitt og gjentatte ganger hadde forklart at frembringelsen var autonom og uten hans innblanding. Dette innebærer at saken er avgjort på dette grunnlaget, som kun tar stilling til den autonome situasjon. Vi får med andre ord ikke trukket opp grensen for hvor mye eller lite menneskelig innsats som skal til, eller hva slags innsats som betyr mest for å møte vilkåret for registrering.

Retten kan dermed enkelt tiltre beslutningen fra USCO: «*By denying registration, the Register concluded that no valid copyright had ever existed in a work generated absent human involvement, leaving nothing at all to register and thus no question as to whom that registration belonged.*»

Thaler hadde vist til at regelverket rundt opphavsrett er utformet med sikte på å fange opp alle relevante intellektuelle frembringelser, og at det her har skjedd en utvikling fra rene skriftverk til en rekke ulike former for verk som kan registreres. Retten drøfter dette og viser blant annet til the Copyright Act i 17 U.S.C. § 102(a) forutsetter en slik «malleability», altså en fleksibilitet og tilpasningsevne, ved at den omfatter «*original works of authorship fixed in any tangible medium of expression, now known or later developed.*» (*rettens utheving*). Det fremheves imidlertid at dette kun går på ulike typer verk, der loven åpner for stadig nye former og utførelser. Den grunnleggende forutsetningen, selve *sine qua non* som retten formulerer det, er imidlertid at det er den menneskelige kreativitet og skapertrang som skal stå bak frembringelsen. Som eksempel viser retten til en gammel høyesterettsdom fra 1884 i en tvist mellom fotografen Napoleon Sarony og Burrow-Giles Lithographic Company.

Fotografen Sarony anla inngreps-søksmål for markedsføring og salg av fotografens litografi av Oscar Wilde med tittelen «Oscar Wilde

No. 18» inntatt nedenfor. Det var snakk om om lag 85.000 solgte kopier av bildet. Saksøkte anførte at den amerikanske grunnloven kun omtalte opphavsrett opp mot «writings» og verk frembragt av en «author», slik at de underordnede reglene i Copyright Act av 1865 måtte anses som ugyldige ettersom disse også omfattet fotografier. Saksøkte la til grunn at fotografier var resultatet av en rent mekanisk prosess som ikke sammenlignes med en kreativ frembringelse, og at et slik verk ikke kunne bære frem noe kreativt konsept eller ide. Sarony vant saken i første instans og ble tilkjent \$610. Sarony vant også frem i den føderale US Supreme Court som gjengir følgende oppsummering fra underinstansen om bildet:

«*[a] useful, new, harmonious, characteristic, and graceful picture, and that said plaintiff made the same at his place of business in said city of New York, and within the United States, entirely from his own original mental conception, to which he gave visible form by posing the said Oscar Wilde in front of the camera, selecting and arranging the costume,*



draperies, and other various accessories in said photograph, arranging the subject so as to present graceful outlines, arranging and disposing the light and shade, suggesting and evoking the desired expression, and from such disposition, arrangement, or representation, made entirely by the plaintiff, he produced the picture in suit...»

Supreme Court diskuterer deretter om det er rom for å utvide begrepet «writing» til å omfatte fotografier, og levner ikke mye tvil på dette punkt: «*We entertain no doubt that the constitution is broad enough to cover an act authorizing copyright of photographs, so far as they are representatives of original intellectual conceptions of the author.*»

„ [...] så viser retten til at loven aksepterer nye former for verk, men at det alltid står et krav om menneskelig kreativitet og innsats som en forutsetning.

Tilbake til vår sak om Creativity Machine, så viser retten til at loven aksepterer nye former for verk, men at det alltid står et krav om menneskelig kreativitet og innsats som en forutsetning. Dette oppsummeres presist av dommeren: «*Human involvement in, and ultimate creative control over, the work at issue was key to the conclusion that the new type of work fell within the bounds of copyright. Copyright has never stretched so far, however, as to protect works generated by new forms of technology operating absent any guiding human hand, as plaintiff urges here. Human authorship is a bedrock requirement of copyright.*»

Det er altså snakk om en «bedrock requirement», et ufravikelig

krav som retten ikke kan unngå å legge til grunn i sin vurdering. Samtidig fremgår det av sammenhengen at dette kravet må anses å ligge innbakt på samme trinnhøyde som grunnloven og dens krav til «author». Det følger en diskusjon om dette ordet, om «author» kan åpne for noe ikke-menneskelig. Dette avvises kategorisk. Riktignok anerkjenner retten i en fotnote at det kan åpnes for en diskusjon om ikke-menneskelig levende intelligens kan omfattes av begrepet, men inntar deretter et spenstig sitat i følgende uttalelse i samme fotnote: «*Nonetheless, delving into this debate is an unnecessary detour since “[t]he day sentient refugees from some intergalactic war arrive on Earth and are granted asylum in Iceland, copyright law will be the least of our problems.”*»

Det slutter imidlertid ikke her, for retten trekker også inn et annet interessant eksempel som må sies å ligge godt ute i grenseland. I saken *Urantia Found. v. Kristen Maaherra* (1997) var det et spørsmål om opphavsrett knyttet til et skriftverk angivelig frembrakt av et guddommelig vesen. Saken ble behandlet av domstolen i Ninth Circuit, som la til grunn at «it is not creations of divine beings that the copyright laws were intended to protect». Uansett la domstolen til grunn at den «Contact Commission» som hadde mottatt guddommens uttalelser selv hadde bidratt, først ved å formulere spørsmålene som ble stilt til det guddommelige vesen, deretter ved å gjøre utvalg og sammenstille åpenbaringene slik at helheten i alle fall delvis var et resultat av menneskelig innsats. De guddommelige skrifter not dermed også opphavsrettslig beskyttelse.

Tilsvarende gjaldt i saken *Penguin Books U.S.A., Inc. v. New Christian Church of Full Endeavor*, der en kvinne hadde fylt ut 30 steno­grafibøker med ord hun mente ble diktert til henne fra en stemme utenifra. Hun hadde deretter arbeidet sammen med to andre personer for å redigere teksten til en bok,

som også innebar tilstrekkelig menneskelig innsats.

I en litt annen retning lå saken *Kelley v. Chicago Park District, the Seventh Circuit* der retten besluttet å ikke anerkjenne opphavsrett knyttet til en kultivert hage, ettersom dette lå utenfor hva som kunne omfattes av begrepet menneskelig frembringelse.

Selvfølgelig måtte retten også omtale en sak som verserte i media en tid tilbake, der en apekatt hadde tatt en selfie. I saken *Naruto v. Slater* holdt en makak kameraet og knipset et bilde av seg selv. I den saken ble det først vist til at dyr ikke er prosessdyktige, samt at retten la til grunn at lovreglene om opphavsrett utelukkende tildeler rettigheter til mennesker og ikke dyr. I vår sak viser dommeren til at poenget med denne opprøpsingen er å underbygge at det ikke foreligger noen rettspraksis i USA der opphavsrett er anerkjent i et verk som ikke opprinner fra menneskelig innsats.

Når man leser denne dommen, er det altså ikke mye tvil underveis om hva som blir rettens slutning. Som nevnt åpner ikke en slik «summary judgment» for å behandle Thalers nye anførsler om hans innsats, men retten drøfter dette på generelt grunnlag i et obiter dictum i de siste avsnittene:

«The increased attenuation of human creativity from the actual generation of the final work will prompt challenging questions regarding how much human input is necessary to qualify the user of an AI system as an “author” of a generated work, the scope of the protection obtained over the resultant image, how to assess the originality of AI-generated works where the systems may have been trained on unknown pre-existing works, how copyright might best be used to incentivize creative works involving AI, and more.»

Denne avgjørelsen avgjør altså en sak der utfallet var gitt og går ikke særlig langt inn på den spennende grenselinjen for hvor lavt terskelen kan legges for slik registrering. I Norge, der det ikke er noe krav om registrering, vil diskusjonen gå på selve begrepet åndsverk og hvordan dette oppstår. Det er for eksempel ikke tvil om at det foreligger betydelig skapende og kreativ innsats ved å beskrive et tenkt bilde for en AI. En AI som deretter frembringer ulike alternativer som igjen er gjenstand for videre bearbeiding i et samvirke mellom menneske og maskin. Et slikt eksempel er inntatt i en tidligere artikkel (LoD-2023-153-32) der det er et AI-generert bilde av en kybernetisk AI som utarbeider lover om regulering av AI. Her ligger det en rekke juridiske utfordringer som vi skal få gruble over i tiden som kommer.

” I Norge, der det ikke er noe krav om registrering, vil diskusjonen gå på selve begrepet åndsverk og hvordan dette oppstår.

Som sagt innledningsvis er avgjørelsen ikke rettskraftig i skrivende stund. Vi kan legge til grunn at Thaler vil følge linjen vi har satt fra AIP tidligere, der avgjørelser ankes gjennom systemet og drives frem mot siste instans. I akkurat denne saken hadde det likevel vært mer interessant å få en avgjørelse som hensyntar de nye argumentene fremsatt av Thaler. Dersom retten må ta stilling til terskelen for det menneskeskapte der det har vært en arbeidsfordeling mellom AI og en eller flere medvirkende personer, vil dette være spennende lesing. Slik saken er lagt opp nå er det imidlertid ikke sannsynlig at Thaler har noen reell mulighet til å vinne frem.



Opphavsrett for begynnere 3. utgave

Olav Torvund

Sider: 264

Språk: Bokmål

ISBN: 9788215066257

Utgivelsesdato: 07.07.2023

Den som skaper et åndsverk, har opphavsrett til verket, står det i åndsverkloven. Men hva betyr det for deg som eier, bruker eller forvalter et åndsverk? Og hva er egentlig et åndsverk?

Opphavsrett er en engasjerende, praktisk og oversiktlig innføring i grunnleggende opphavsrett, skrevet for deg som møter opphavsrett i praksis. Boka er egnet for alle fra juris-

ter som trenger et oppslagsverk, til journalister og ansatte i mediehus som har behov for et verktøy i møte med opphavsrettslige problemstillinger.

Boka kommer nå i 3. utgave, og ny lovgivning og nye rettsavgjørelser er tatt inn.

Omtalen er hentet fra Universitetsforlaget.no: <https://www.universitetsforlaget.no/opp-havsrett-for-begynnere-2>

Tele- og datautstillingen I/O – Teknisk museum

Kunstig intelligens (AI) hjelper deg til en museumsopplevelse i spektakulære omgivelser, der fortid møter nåtid – med engasjerende pekere mot fremtiden.

I/O sprenger skalaen for hva du forventer når du hører ordet utstilling. Ved nyvinnende bruk av AI setter blir du en del av utstillingen på måter du aldri før har opplevd. Du får til og med ditt eget uttrykk gjennom en avatar! Siden utstillingen blir «ny» hver gang du legger inn dine valg, vil utstillingen presentere deg for gjenstandene og historien (og historiene) på forskjellige måter – hver gang.

Logg deg på utstillingens AI ved hjelp av en identifikator og svar på ulike spørsmål. I/O svarer med å tilby ulike løyper gjennom utstillingen som er tilpasset dine valg. Når du opplever utstillingen vil du legge igjen anonyme data som igjen danner grunnlaget for opplevelsen du får i Reaktor.



Les mer: <https://www.tekniskmuseum.no/io>



Stein Schjøberg

Av Trine Shil Kristiansen

Stein Schjøberg er aktuell med sin nye bok *Cyberkriminalitet – nasjonal og global utvikling* (2023). Schjøberg har en lang karriere innenfor arbeidet med cyberkriminalitet. Det hele startet med et forskningsopphold om computer crime ved Stanford Research Institute (SRI-International) i California. Han har samarbeidet med Jon Bing i mange år, og sammen skapte de begrepet *datakriminalitet*.

Redaksjonen i Lov&Data har snakket med Schjøberg om hans arbeid og om fagfeltet cyberkriminalitet.

Stein deltok på kurset *Informasjon om EDB for saksbehandlere* om datamaskinens oppbygning og virkemåte i 1976. Foredragsholder var Jon Bing. Etter foredraget satte de seg ned og snakket sammen om det amerikanerne kalte «computer crime» – et fenomen som også vil skape problemer i Norge. På den tiden var det i hovedsak misbruk av datamaskiner, altså data og kriminalitet. De ble

enige om å kalle det «datakriminalitet». Schjøberg sendte betegnelsen inn i en innberetning til Justisdepartementet, og en kopi til Bing.

– Jeg hadde gleden av å kjenne Jon Bing fra 1976 og ble hans «disippel», forsker og utreder i grenseflaten mot etterforskning og påtale i straffesaker, og i strafferettens område av rettsinformatikken. Vårt samarbeid varte i mer enn 30 år.

I sommer ble tolv departementer utsatt for hacking – truslene er mange. Hva er de største truslene innenfor cyberkriminalitet i Norge i dag?

– Globale cyberangrep fra statlige aktører. Alvorlig cyberkriminalitet forårsaket av at de private globale IT-selskapene nå styrer utviklingen av cyberspace uten nasjonale eller globale reguleringer og retningslinjer. En slik mangel på regulering av private aktører kan forårsake desinformasjon som igjen truer demokratiet.

Det å være ekspert innenfor et felt som cyberkriminalitet fører med seg en rekke ledende verv og oppgaver. Selv trekker han frem som sitt viktigste arbeide:

– Nasjonalt å ha ledet Datakrimutvalget som i 2003 fremmet forslag om lovtiltak for tilpassning og ratifikasjon av Europarådets konvensjon om cybercrime. Internasjonalt å ha ledet en High Level Experts Group i FN organet ITU i Genève med nesten 100 internasjonale eksperter fra hele verden. Jeg har bistått forskjellige FN organer helt frem til 2023, samt bistått Interpol i flere år.

I januar 2022 ble Schjøberg som den eneste personen fra de nordiske land oppnevnt av FN som Civil society delegate in the United Nations Ad Hoc Committee for developing a convention on countering the use of information and communications technologies for criminal purposes. Komiteen skal utarbeide et forslag om en FN konvensjon for cyberkriminalitet innen 2024.

– I dag har Ad Hoc komiteen ledet seks Sessions i 2022 og 2023, med innspill fra medlemsland og oppnevnte eksterne deltakere. Som en oppnevnt Civil Society delegate, har jeg sendt inn flere forslag, blant annet *A Proposal for a United Nations Convention on Cybercrime*. Et forslag til FN konvensjon om cybercrime kan forventes foreslått av Ad Hoc komiteen når den har sin Concluding Session i New York på nyåret 2024.

Det jobbes nasjonalt og globalt med å bekjempe cyberkriminalitet. Hvilke tips til våre lesere har du for de som ønsker å holde seg oppdatert om tema?

– Jeg vil foreslå at de følger med i virksomheten til det *nasjonale cyberkriminalitetssenteret (NC3)* på Kripos som holder et meget høyt internasjonalt nivå. I tillegg er det nyttig å lese om de forebyggende tiltak og råd som Nasjonal Sikkerhetsmyndighet (NSM) gir ut årlig.

Har du lyst til å lære mer om cyberkriminalitet holder Schjøberg et etterutdanningskurs for advokater, 19. mars 2024, se: <https://advokatenes-br.no/kurs/introduksjon-til-cyberkriminalitet>



Gorrissen Federspiel

Tue Goldschmieding

Domstolen afviser minimumsgrænse for erstatning efter GDPR

Domstolen traf den 4. maj 2023 afgørelse i sag C-300/21. Sagen var en præjudiciel forelæggelse indgivet af den østrigske højesteret, Oberster Gerichtshof, og vedrørte GDPR artikel 82 om retten til erstatning for enhver, der har lidt materiel eller immateriel skade som følge af en overtrædelse af GDPR.

Den østrigske højesteret skulle træffe afgørelse i en sag mellem en privatperson, UI, og Österreichische Post AG, som er et østrigsk selskab, der sælger adresseoplysninger til andre virksomheder til marketingsformål. Sagen angik Österreichische Post AG's behandling af personoplysninger i form af oplysninger om politisk tilhørsforhold for personer med bopæl i Østrig. UI nedlagde påstand, som en af de registrerede, om erstatning for den immaterielle skade, som UI havde lidt som følge af behandlingen af UI's personoplysninger. Den immaterielle skade, som UI gjorde gældende at have lidt, angik følelsen af stor ærgrelse, tab af tillid og ydmygelse.

Tvivlsspørgsmålet for den nationale ret drejede sig om, hvorvidt det var et krav for at få erstatning efter GDPR artikel 82 for en overtrædelse af en bestemmelse i GDPR, at sagsøger havde lidt en skade og i bekræftende fald, om ubehagelige følelser i så fald udgjorde en immateriel skade omfattet af GDPR artikel 82, eller hvorvidt erstatning var betinget af, at den skade der var lidt, overskred en vis minimumstærskel. Både den regionale domstol og den øverste regionale domstol i Østrig

var forud for sagen ved den østrigske højesteret, kommet frem til, at UI ikke kunne opnå erstatning for negative følelser, som følge af Österreichische Post AG's overtrædelse af GDPR.

Domstolen slog fast, at GDPR artikel 82, stk. 1 skal fortolkes således, at en overtrædelse af en bestemmelse i GDPR ikke i sig selv giver ret til erstatning, men at det er en betingelse for erstatning, at den registrerede tillige har lidt skade, samt at der er en årsagsforbindelse mellem overtrædelsen og skaden. Domstolen fastslog, at »skade« er et EU-retligt begreb, som skal fortolkes som et selvstændigt kriterie ved siden af en overtrædelse af GDPR.

Herefter fastslog Domstolen, at GDPR artikel 82, stk. 1 er til hinder for en national regel eller praksis, hvorefter erstatning for immateriel skade efter GDPR er betinget af, at en vis minimumstærskel er overskredet for den skade, der er lidt. Domstolen lagde vægt på, at det ikke vil være i overensstemmelse med hverken ordlyden, sammenhængen eller formålet med forordningen at opstille en sådan tærskel. Domstolen bemærkede, at der ikke ved en overtrædelse af GDPR, automatisk også vil være sket en »skade« i forordningens forstand.

Afgørelsen fastslår således, at den registrerede, hvis oplysninger er blevet behandlet i strid med GDPR, alene kan opnå erstatning, hvis den har lidt en »skade« i EU-retlig forstand, og at dette skal vurderes selvstændigt. Afgørelsen slår imidlertid samtidig fast, at skaden ikke skal have en vis alvorsgrad eller overgå en minimumsgrænse for at

kunne opfylde betingelsen om, at der er lidt en skade.

Endeligt var der stillet spørgsmål om fastlæggelsen af omfanget af erstatningen. Hertil bemærkede Domstolen, at erstatningen skal fastlægges ud fra de nationale regler, der gælder i det enkelte medlemsland om omfanget af økonomisk erstatning, så længe dette er sket i overensstemmelse med effektivitetsprincippet og ækvivalensprincippet.

Læs hele dommen her: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=273284&page-Index=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=5942936>

EU-Domstolen træffer afgørelse om omfanget af indsigtsretten, herunder retten til at få udleveret en kopi

EU-Domstolen traf den 4. maj 2023 afgørelse i en præjudiciel forelæggelse i sag C-487/21, som blev indgivet af den tyske forbundsdomstol (Bundesverwaltungsgericht).

Sagen handlede om en registreret, F.F., som anmodede et kreditoplysningsbureau, CRIF, om at få udleveret en kopi af de dokumenter, som indeholdt F.F.'s personoplysninger. CRIF udleverede herefter en sammenfattet liste med de personoplysninger, de havde behandlet. F.F. mente ikke det var tilstrækkeligt at fremsende en liste, men ønskede konkrete dokumenter som mails og udskrifter fra databaser fremlagt. FF klagede på denne baggrund til de østrigske databeskyttelsesmyndigheder (Österreichische Datenschutzbehörde), som gav CRIF medhold, hvorfor sagen blev påklaget til de østrigske domstole.

Den østrigske domstol udsatte sagen og forelagde denne for EU-Domstolen som et præjudicielt spørgsmål. Hovedspørgsmålet angik GDPR artikel 15, stk. 3, 1. pkt., hvorefter (d)en dataansvarlige skal udlevere en kopi af de personoplysninger, der behandles. Konkret blev spurgt om denne bestemmelse (i) også medfører en generel ret for en registreret til at få udleveret en kopi af hele dokumenter, hvori den registreredes personoplysninger behandles, eller (ii) kun giver den registrerede ret til en nøjagtig gengivelse af de personoplysninger, der skal gives adgang til?

EU-Domstolen bemærkede, at det er afgørende, at den dataansvarlige indretter sig på en måde, der gør det muligt for den registrerede effektivt at udøve sine rettigheder i henhold til GDPR. Det er ligeledes et krav, at oplysningerne bliver formidlet på en letforståelig måde. Endelig bemærkede EU-Domstolen, at GDPR artikel 15, stk. 3, 1. pkt., skal fortolkes bredt. EU-Domstolen konkluderede derfor, at den registrerede har ret til at få en kopi af uddrag af dokumenter, såvel som hele dokumenter og uddrag fra databaser, hvis udleveringen er nødvendig for at udøve forordningens øvrige rettigheder. Det er afgørende, at der indledningsvist foretages en afvejning til andres rettigheder ved udlevering af dokumenterne til den registrerede.

Endelig kom frem til EU-Domstolen, at den dataansvarlig udelukkende er pålagt at udlevere oplysninger, som er omfattet af GDPR artikel 15, stk. 3, 1. pkt. Der foreligger således ikke noget krav om at udlevere en kopi af oplysninger, der ikke er omfattet direkte af bestemmelsens ordlyd, f.eks. metadata.

Læs hele afgørelsen her: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=273286&page-Index=0&doclang=da&mode=lst&dir=&occ=first&part=1&cid=65870>

EU-Domstolen om grænsefladen mellem konkurrenceretten og databeskyttelse

EU-Domstolens har den 4. juli 2023 afsagt dom i sag C-252/21 om beføjelserne for en national konkurrencemyndighed til at fastslå, om en virksomhed har handlet i strid med GDPR. Afgørelsen blev indgivet af den regionale ret i Düsseldorf som en præjudiciel forelæggelse.

Domstolen fastslog, at en konkurrencemyndighed kan undersøge om den pågældende virksomhed har brudt databeskyttelsesregler eller andre regelsæt, som led i vurderingen af, om der er sket misbrug af dominerende stilling. Dette var blandt andet under henvisning til, at sådanne brud kan være indicier på, at virksomhedens adfærd fordrejer eller kan forventes at fordreje konkurrencen på det indre marked.

I lyset heraf præciserede Domstolen kompetencefordelingen mellem henholdsvis nationale konkurrencemyndigheder og tilsynsmyndighederne efter GDPR. Navnlige følger, at hvor en konkurrencemyndighed fastlægger en virksomheds tilsidesættelse af GDPR erstatter den ikke tilsynsmyndighederne. Domstolen fandt, at medlemsstaternes loyalitetsforpligtelse efter artikel 4, stk. 3, i Traktaten om Den Europæiske Union medfører, at nationale konkurrencemyndigheder har pligt til at samarbejde loyalt med den kompetente tilsynsmyndighed.

Herudover behandlede Domstolen spørgsmålet om den indsamling og behandling af personoplysninger, herunder særlige kategorier af personoplysninger, som der foretages af sociale onlinenetværk.

Sagen havde sit udspring i en tysk konkurrencesag om det mulige misbrug af dominerende stilling af Meta Platforms Ireland («Meta»), som udbyder de sociale netværkstjenester Facebook, Instagram og WhatsApp. Særligt fokus var forretningsmodellen, som hovedsageligt består af personlig tilpasning af indhold, baseret på oprettelsen af

detaljerede profiler på Metas online-tjenester. Profilerne bliver dels oprettet på baggrund af (i) data leveret af brugerne direkte til Meta, når de tilmelder sig Facebook, dels (ii) data om brugerne fra de øvrige sociale netværkstjenester leveret af Meta, samt tredjepartswebsteder og – apps, hvorved Meta linker sådanne data til brugernes konti. Den samlede visning af oplysningerne muliggør, at Meta kan drage detaljerede konklusioner om brugernes præferencer og interesser.

Hertil bemærkede den forelæggende ret, at denne behandling kan vedrøre særlige kategorier af personoplysninger, også selvom de pågældende oplysninger ikke var indtastet af brugeren selv, men at de kan hidrøre fra besøg og anvendelse af andre websteder og applikationer. Domstolen udtalte i den forbindelse, at hvor en social netværkstjeneste behandler personoplysninger, skal det efterprøves om dette afslører oplysninger, som omfattes af GDPR artikel 9. I bekræftende fald er behandlingen principielt forbudt, medmindre der kan identificeres en behandlingshjemmel i GDPR artikel 9, stk. 2.

Hertil præciserede Domstolen, at behandlingen af særlige kategorier af oplysninger undtagelsesvist kan være tilladt, hvor de »tydeligvis er offentliggjort af den registrerede« efter undtagelsen til forbuddet i GDPR artikel 9, stk. 2, litra e). Den blotte omstændighed, at en bruger besøger et websted eller anvender en app, er imidlertid ikke tilstrækkeligt til at konstituere, at denne tydeligvis har offentliggjort sine oplysninger. Det gælder både hvor brugeren indtaster oplysninger, trykker på valgknapper (f.eks. »synes godt om«) eller tilknytter en konti til webstedet, medmindre det på forhånd er tilkendegivet af brugeren med fuld kendskab til sagen, at denne ønsker at gøre oplysningerne offentligt tilgængelige for et ubegrænset antal personer.

For det tredje undersøgte Domstolen, om Metas behandlingsaktiviteter kunne udføres uden den registreredes samtykke, men i stedet baseres på en anden behandlingshjemmel, fx når behandlingen er nødvendig for opfyldelse af en kontrakt efter GDPR artikel 6, stk. 1, litra b).

Domstolen fandt, at behovet for at opfylde den kontrakt, som brugeren indgår med Meta, kun kan retfærdiggøre den pågældende praksis på betingelse af, at behandlingen er objektivt uundværlig. Domstolen udtrykte dertil tvivl om, hvorvidt et personaliseret indhold eller problemfri brug af Metas egne tjenester opfylder dette kriterie.

I stedet fandt Domstolen, at behandlingen kan foretages som del i Metas legitime interesse, forudsat at den foretages inden for rammerne af det strengt nødvendige – og således ikke går forud for brugernes interesser og grundlæggende rettigheder.

Afslutningsvist bemærkede Domstolen, at det forhold at en virksomhed er dominerende på et marked, ikke per se afskærer brugerne muligheden for at afgive et gyldigt samtykke. Det påhviler imidlertid operatøren at føre bevis herfor, idet dennes status af dominerende virksomhed i sig selv kan påvirke det frie valg for brugeren, og hvorfor dette dermed indgår som et element i vurderingen af, om et gyldigt, herunder særligt et frivilligt, samtykke er givet.

Læs hele dommen her: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=275125&pageIndex=0&doclang=DA&mode=req&dir=&occ=first&part=1&cid=5978970>

Domstolen afgør spørgsmål om omfanget af indsigt retten i oplysninger i logfiler, der genereres af et behandlingssystem

Domstolen traf den 22. juni 2023 afgørelse i sag C-579/21. Sagen var en præjudiciel forelæggelse indgivet

af den østfinske forvaltningsdomstol, Itä-Suomen hallinto-oikeus.

Den østfinske forvaltningsdomstol skulle træffe afgørelse i en sag mellem to parter angående retten til indsigt i information efter GDPR artikel 15, stk. 1. Den registreredes, J.M., anmodning om indsigt i information om behandlingen af dennes personoplysninger ved den bank, Pankki S, J.M. arbejdede i og samtidig var kunde ved, var i første omgang blevet afslået af den stedfortrædende repræsentant for det finske datatilsyn, Apulaistietosuojavaltuutettu.

Sagen gav for den nationale ret anledning til at genoverveje sin fortolkning af rækkevidden af GDPR artikel 15, stk. 1, og hvorvidt J.M. faktisk havde ret til indsigt i en række logfiler, der var genereret ved behandlingen af den registreredes oplysninger. Disse logfiler indeholdt information om søgningerne foretaget i J.M.'s personoplysninger i en periode på cirka to måneder. Informationerne vedrørte specifikt datoerne og formålet med søgningerne, samt identiteten på de fysiske personer, der havde gennemført søgningerne.

Domstolen fandt, at oplysningerne om datoerne for- og formålet med søgninger i J.M.'s personoplysninger udgjorde informationer, som den registrerede havde ret til at få indsigt i efter GDPR artikel 15, stk. 1. Domstolen bemærkede, at retten til indsigt efter GDPR artikel 15, stk. 1 er nødvendig for, at den registrerede kan udøve sine øvrige rettigheder efter GDPR. Datoen for behandlingen er blandt andet med til at sikre, at den registrerede kan vurdere lovligheden af den behandling, der er sket af vedkommendes personoplysninger.

Domstolen fandt desuden, at identiteten på de fysiske personer, der havde gennemført søgningerne, ikke er omfattet af retten til indsigt efter GDPR artikel 15, stk. 1., da disse personer ikke kunne anses for at være »modtagere« efter GDPR arti-

kel 15, stk. 1, litra c. Herved slog Domstolen fast, at retten til indsigt ikke omfatter information om identiteten på de ansatte, som under ledelse og instruks fra den dataansvarlige, har behandlet personoplysningerne som led i arbejde for den dataansvarlige. Afslutningsvist bemærkede Domstolen, at dette dog ikke gælder, såfremt en sådan information ville være nødvendig for, at den registrerede kan udøve sine øvrige rettigheder efter GDPR.

Endeligt afviste Domstolen, at det på nogen måde har betydning for omfanget eller påvirkede retten til indsigt, i hvilken sammenhæng der er anmodet om indsigt. Det var derfor uden betydning, at den registrerede både arbejdede for og var kunde hos banken.

Læs hele dommen her: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=274867&pageIndex=0&doclang=da&mode=lst&dir=&occ=first&part=1&cid=65870>

EDPB vedtager endelig udgave af retningslinjer om registreredes rettigheder – Indsigtsretten

EDBP har den 28. marts 2023 på baggrund af en offentlig høring, vedtaget den endelige udgave af retningslinjer om registreredes indsigtsret.

Retningslinjerne tager sigte på at udvide forståelsen og anvendelsen af indsigtsretten efter GDPR artikel 15, på baggrund af den hidtil udviklede praksis ved EU-Domstolen. GDPR artikel 15 hjemler den registreredes ret til, efter anmodning, indsigt i- og adgang til de personoplysninger, som en dataansvarlig behandler om den pågældende.

Blandt andet præciserer retningslinjerne (i) omfanget af indsigtsretten, (ii) de oplysninger, som den dataansvarlige skal give den registrerede, (iii) formatet for den registreredes anmodning om indsigt, (iv) de vigtigste måder hvorpå informationen kan udleveres til den registrerede samt (v) en uddybning af undtagelsen til indsigt, navnlig

hvor anmodningen er åbenbart grundløs eller overdreven.

Læs EDBP's pressemeddelelse her: https://edpb.europa.eu/news/news/2023/edpb-adopts-final-version-guidelines-data-subject-rights-right-access_en

Læs EDBP's nye retningslinjer her: https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf

Det irske datatilsyn udsteder bøde på € 1,2 mia. til Meta

Den 13. april 2023 vedtog EDPB en bindende tvistbilægelsesafgørelse efter proceduren i GDPR artikel 65 (»Bindende afgørelse 1/2023«).

Afgørelsen vedrørte Meta Platforms Ireland Limited (»Meta«) og dets overførsler af personoplysninger til USA på grundlag af standardkontraktbestemmelser (SCC'er) siden 16. juli 2020. Som ledende tilsynsmyndighed, havde den irske databeskyttelsesmyndighed (»DPC«) i sit udkast til afgørelse fundet, at dataoverførslerne fandt sted i strid med GDPR artikel 46, og at dataoverførslerne under disse omstændigheder burde suspenderes.

DPC blev mødt af indsigelser fra de øvrige berørte tilsynsmyndigheder vedrørende de korrigerende beføjelser, som DPC foreslog at udøve. DPC valgte imidlertid ikke at følge disse, hvorved tvistbilægelsesproceduren blev indledt.

Med afsæt i EDPB's Bindende afgørelse 1/2023 traf DPC sin endelige afgørelse den 12. maj 2023, hvorefter Meta bl.a. skal suspendere fremtidige overførsler af personlige data til USA inden for en periode på fem måneder. DPC udstedte derudover en bøde på € 1,2 mia. til Meta som følge af Metas overtrædelse af GDPR. Desuden blev Meta meddelt påbud om at bringe sine behandlingsaktiviteter i overensstemmelse med GDPR inden 6 måneder.

Læs Datatilsynets pressemeddelelse her: *Bøde på 1,2 milliarder euro til Meta*

Irland som følge af bindende afgørelse fra EDPB (datatilsynet.dk)

Læs det irske datatilsyns pressemeddelelse her: Data Protection Commission announces conclusion of inquiry into Meta Ireland | 22/05/2023 | Data Protection Commission

Læs EDPB's pressemeddelelse her: 1.2 billion euro fine for Facebook as a result of EDPB binding decision | European Data Protection Board (europa.eu)

EDPB vedtager beslutning om at nedsætte en taskforce vedrørende ChatGPT

EDPB har nedsat en særlig taskforce målrettet ChatGPT.

Den 13. april 2023 afholdte EDPB møde, hvorpå det italienske datatilsyns foranstaltninger mod OpenAI i relation til ChatGPT blev drøftet. EDPB besluttede på mødet at nedsætte en taskforce for at fremme samarbejdet og udvekslingen af oplysninger imellem de europæiske databeskyttelsesmyndigheder hvad angår Open AI's ChatGPT-tjeneste.

Læs hele EDPB's pressemeddelelse her: https://edpb.europa.eu/news/news/2023/edpb-resolves-dispute-transfers-meta-and-creates-task-force-chat-gpt_en

EDPB vedtager retningslinjer for myndigheders brug af ansigtsgenkendelsesteknologi

EDPB offentliggjorde den 26. april 2023 retningslinjer for anvendelsen af ansigtsgenkendelsesteknologi inden for retshåndhævelse.

Retningslinjerne henvender sig til EU-lovgivere samt de nationale lovgivere og retshåndhævende myndigheder og har til formål at vejlede om, hvordan myndighederne kan implementere og anvende ansigtsgenkendelsesteknologi. Retningslinjerne gennemgår, hvordan myndighederne sikrer overholdelse af Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 (»retshåndhævelsesdirektivet«) ved anvendelse af ansigtsgenkendelsesteknologi, og at anvendelsen sker i overensstemmelse med nødven-

digheds- og proportionalitetskravet i Den Europæiske Unions Charter om Grundlæggende Rettigheder.

Retningslinjerne vedrører den praktiske anvendelse af en ansigtsgenkendelsesteknologi og gennemgår også en række typiske tilfældegrupper, hvor ansigtsgenkendelsesteknologi anvendes og hvilke overvejelser myndighederne bør gøre sig, såfremt de anvender teknologien i det pågældende tilfælde.

Herudover gentager EDPB en opfordring om et fuldstændigt forbud mod anvendelse af teknologien i en række nærmere bestemte situationer, herunder ansigtsgenkendelse til aflæsning af menneskelige følelser og biometrisk fjernidentifikation af personer, som bevæger sig på et offentligt tilgængeligt sted.

Læs EDPB's pressemeddelelse her: https://edpb.europa.eu/news/news/2023/edpb-adopts-final-version-guidelines-facial-recognition-technology-area-law_da

Læs EDPB's retningslinjer her: https://edpb.europa.eu/system/files/2023-06/edpb_guidelines_042022_calculationofadministrativefines_en.pdf

EDBP vedtager uddybende retningslinjer om udmåling af bøder til private virksomheder efter GDPR

For at sikre en mere harmoniseret tilgang til udmåling af bøder til private virksomheder, for overtrædelser af GDPR, har EDBP på et plenarmøde den 24. maj 2023 vedtaget et sæt uddybende retningslinjer.

Udmålingen af administrative bøder er som udgangspunkt underlagt den enkelte databeskyttelsesmyndigheds skøn under iagttagelse af reglerne efter GDPR. Administrative bøder udregnes i første række ud fra virksomhedens omsætning samtidig med, at de skal være effektive, afskrækkende og stå i rimeligt forhold til overtrædelsens alvorlighed.

Retningslinjerne følger således på tilsvarende vis udgangspunktet efter GDPR for bødeberegningen, og

udstikker en metodisk fem-trins-model for udmålingen, herunder identifikation af behandlingsaktiviteterne, kategoriseringen af overtrædelsen og dennes grovhed samt skærpene og formildende omstændigheder.

Læs EDBP's pressemeddelelse her: https://edpb.europa.eu/news/news/2023/edpb-adopts-final-version-guidelines-calculation-administrative-fines-following_en

Læs EDBP's retningslinjer her: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042022-calculation-administrative-fines-under_en

Nordiske tilsyn øger fokus på data- og risikodrevet tilsyn gennem forstærket samarbejde

De nordiske datatilsyn mødtes den 15. og 16. maj 2023 til det årlige møde, hvor det fællesnordiske værdifællesskab blev diskuteret.

Ved dette årsmøde blev en ny erklæring, Reykjavik-erklæringen, vedtaget. Erklæringen skal ændre databeskyttelsesmyndighedernes måde at føre tilsyn på via en mere data- og risikobaseret tilgang. Med erklæringen tilstræbes ligeledes en øget vidensdeling de europæiske lande imellem ift. tilsynsstrategier og sanktionsmuligheder ved en dataansvarliges manglende efterlevelse af databeskyttelsesreglerne.

Læs Reykjavik-erklæringen her: <https://www.datatilsynet.dk/Media/638199319850756338/Reykjavik%20Declaration.pdf>

Den danske regering fremlægger initiativer for bedre databeskyttelse af børn

Den danske regering meddelte den 12. juni 2023, at de vil fremkomme med konkrete tiltag for bedre beskyttelse af børn i forbindelse med behandling af børns personoplysninger.

Tiltagene sker på baggrund af en række anbefalinger fra en af regeringen nedsat ekspertgruppe. Ekspertgruppen fremkom, i en rapport

fra juni 2023, med en række anbefalinger målrettet de udfordringer, der relaterer sig til tech-giganters platforme og forretningsmodeller. I rapporten fremkom ekspertgruppen blandt andet med tre konkrete anbefalinger til tech-giganters ansvar over for børn og unge i forhold til aldersverificering og sikringen af, at børn ikke tilgår ikke-alderssvarende indhold på internettet.

På baggrund af ekspertgruppens anbefalinger meddelte regeringen, at de ønsker at indføre et krav om, at tech-giganterne indhenter samtykke fra børns forældre, før de kan indhente og behandle børnenes personoplysninger.

På sigt ønsker regeringen at ændre reglerne for databeskyttelse af børn og øge aldersgrænsen for, hvornår en registreret skal anses for at være barn og dermed være omfattet af de databeskyttelsesregler, som gælder særligt for dem. Herudover vil regeringen indføre et krav om en digital bekræftelse af brugerens alder, når der tilgås upassende indhold på internettet.

Læs Erhvervsministeriets pressemeddelelse her: <https://em.dk/nyhedsarkiv/2023/juni/tech-giganterne-skal-begraenses-regeringen-vil-beskytte-boern-bedre/>

Læs ekspertgruppens rapport her: <https://em.dk/media/19630/anbefalinger-fra-tech-ekspertgruppe.pdf>

EU-Kommissionen fremsætter forslag til ny lovgivning for at sikre en stærkere håndhævelse af GDPR i grænseoverskridende sager

EU-Kommissionen har den 4. juli 2023 forelagt et forslag til en ny forordning for at strømline samarbejdet mellem databeskyttelsesmyndighederne ved håndhævelse af GDPR i grænseoverskridende sager. Reglerne har til formål at lette samarbejdet for databeskyttelsesmyndighederne og øge effektiviteten af håndhævelsen af GDPR. Den nye forordning opstiller konkrete procedureregler for myndighederne, når de anvender GDPR i sager, der be-

rører personer, der befinder sig i mere end én medlemsstat.

I sager, hvor behandlingen af GDPR påvirker registrerede i mere end én medlemsstat, gælder GDPR's »one-stop-shop« håndhævelsessystem, som skal hjælpe databeskyttelsesmyndighederne med at samarbejde og opnå konsensus om anvendelsen af GDPR i grænseoverskridende sager. Hvis det ikke er muligt for databeskyttelsesmyndighederne at opnå konsensus, giver GDPR mulighed for tvistbilæggelse ved EDPB.

Kommissionen bemærkede i sin 2020-rapport om anvendelsen af GDPR, at procedureforskelle anvendt af databeskyttelsesmyndighederne hindrer effektiviteten af GDPR's samarbejds- og tvistbilægelsesmekanismer. Forslaget fra Kommissionen tager afsæt i EDPB's forslag til at strømline og forbedre proceduremæssige aspekter for at styrke samarbejdet mellem databeskyttelsesmyndighederne og sikre levering af hurtige retsmidler til enkeltpersoner.

Den nye forordning forsøger bl.a. at varetage klagers rettigheder ved at harmonisere kravene for, at en grænseoverskridende klage kan antages, og fjerne de nuværende hindringer, som er fremsat af databeskyttelsesmyndighederne efter forskellige nationale regler. Desuden er der i forslaget fastsat regler for, at klagerne inddrages ordentligt i de tilfælde, hvor en klage undersøges. Derudover varetager forordningen rettigheder for parter under undersøgelse, ved at give parterne ret til at blive hørt på centrale tidspunkter i proceduren samt ved at præcisere indholdet af den administrative sag og parternes ret til indsigt i sagen. Forordningen forsøger ligeledes at sikre strømliningen af samarbejde og tvistbilæggelse mellem databeskyttelsesmyndighederne ved at give myndighederne mulighed for at give deres synspunkter til kende tidligt i efterforskningen og ved at give dem mulighed for at

gøre brug af alle de samarbejdsværktøjer, som GDPR giver. Forslagets specificering af reglerne og fælles frister for grænseoverskridende samarbejde og tvistbilæggelse skal lette en hurtig færdiggørelse af GDPR's tvistbilæggelsesmekanisme og sikre en rettidig afslutning af undersøgelser.

Læs Kommissionens pressemeddelelse her: [New rules to ensure stronger enforcement of the GDPR \(europa.eu\)](https://commission.europa.eu/press-releases/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf)

Læs lovforslaget her: [Proposal for a Regulation laying down additional procedural rules relating to the enforcement of GDPR \(europa.eu\)](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023P0100&from=do)

EU-Kommissionen vedtager ny og længe ventet tilstrækkelighedsafgørelse vedrørende dataoverførsler fra EU til USA

EU-Kommissionen vedtog den 10. juli 2023 en ny tilstrækkelighedsafgørelse for dataoverførsler mellem EU og USA under det såkaldte EU-U.S. Data Privacy Framework.

Den nye tilstrækkelighedsafgørelse erstatter sin forgænger; EU-U.S. Privacy Shield, som blev kendt ugyldig af EU-domstolen i Schrems II-afgørelsen.

Med den nye tilstrækkelighedsafgørelse udvides forpligtelserne, som virksomhederne skal overholde, når data overføres mellem EU og USA. Amerikanske virksomheder kan tilslutte sig beskyttelsesrammen ved aktivt at forpligte sig til disse regler via certificering.

Der indføres ligeledes en databeskyttelsesappelret, hvor registrerede kan påklage afgørelser, der vedrører overførsel af vedkommendes personoplysninger. Desuden sikres registrerede med den nye beskyttelsesramme en indsigt i de oplysninger, som den respektive virksomhed eller myndighed behandler om den pågældende.

Den nye rammeaftale imødekommer også EU's betænkeligheder ift. de amerikanske efterretningstjenesters brug af data, som kom til udtryk i Schrems II-afgørelsen. En-

deligt vil Kommissionen i samarbejde med såvel europæiske og amerikanske databeskyttelsesmyndigheder føre tilsyn med ordningen for at sikre, at den virker efter formålet.

Læs hele afgørelsen her: https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf

Datatilsynet udtaler kritik af arbejdsgiver for at orientere bredere kreds om baggrund for afskedigelse

Datatilsynet traf den 19. december 2022 afgørelse i sag 2021-31-5737 vedrørende en arbejdsgiver, der i flere orienteringsmails til samtlige kolleger havde angivet årsagen til en medarbejders afskedigelse.

Sagen blev indledt på baggrund af den afskediget medarbejders henvendelse til Datatilsynet med en klage over arbejdsgiverens videregivelse af medarbejderens oplysninger. Klager anførte, at arbejdsgiverens orienteringsmails var i strid med GDPR, og at oplysningerne om klager i de pågældende e-mails var urigtige. Arbejdsgiveren gjorde gældende, at formålet med orienteringen om årsagen til afskedigelsen var at sikre, at alle fik samme information for at undgå rygtedannelse. Arbejdsgiveren afviste endvidere, at oplysningerne om baggrunden for klagers afskedigelse var urigtige.

Datatilsynet udtalte kritik af arbejdsgiveren, idet oplysningerne om klagers fratrædelse i e-mails til hele arbejdspladsen gik ud over, hvad der var nødvendigt og, behandlingen kunne derfor ikke ske med hjemmel i interesseafvejningsreglen i GDPR artikel 6, stk.1, litra f.

Datatilsynet fandt, at arbejdsgiverens orientering om årsagen til klagers fratrædelse ikke kunne ske med henblik på at undgå rygtedannelse, da hensynet til klager gik forud herfor. Datatilsynet lagde i denne forbindelse vægt på, at det i en orienteringsmail om en medarbejders fratrædelse på en arbejdsplads, som

udgangspunkt ikke vil være nødvendigt at informere om baggrunden for fratrædelsen. Det indgik i vurderingen, at orienteringen skete til en bredere kreds af personer, og at der blev videregivet detaljerede oplysninger om baggrunden for afskedigelsen.

Læs Datatilsynets pressemeddelelse her: <https://www.datatilsynet.dk/pressesognyheder/nyhedsarkiv/2023/apr/kritik-af-arbejdsgiver-for-at-orientere-bredere-kreds-om-baggrund-for-afskedigelse>

Læs hele Datatilsynets afgørelsen her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/dec/kritik-af-arbejdsgiver-for-at-orientere-bredere-kreds-om-baggrund-for-afskedigelse>

Securitas A/S' videregivelse af personoplysninger lever op til GDPR

Datatilsynet traf den 22. december 2022 afgørelse i sag 2021-31-5654 vedrørende Securitas A/S' (»Securitas«) videregivelse af personoplysninger i forbindelse med en sikkerhedsgodkendelse af en medarbejder.

Sagen blev indledt af Datatilsynet på baggrund af en klage fra en tidligere vagtmedarbejder, der klagede over, at Securitas, uden klagers samtykke og viden, havde videregivet oplysninger om vedkommendes jobtitel, fulde navn og personnummer til Politiets Efterretningstjeneste og Forsvarets Efterretningstjeneste i forbindelse med en sikkerhedsgodkendelse. Klager påpegede således, at videregivelsen skete uden klagers samtykke og viden, idet klager ikke havde udfyldt oplysningsskema 2, og dermed heller ikke samtykkeerklæringen.

Securitas anførte, at klager på tidspunktet for videregivelsen af personoplysningerne var ansat som vagtmedarbejder ved Securitas, og at alle vagtmedarbejdere var informeret om kravet om sikkerhedsgodkendelse via kommunikationsportalen. Securitas påpegede endvidere, at klager havde udfyldt oplysningsskema 2 og samtykkeerklæringen,

da ansøgningen om sikkerhedsgodkendelse ville være blevet afvist, såfremt klager ikke havde udfyldt, underskrevet og samtykket til det.

Datatilsynet fandt, at det samtykke, som klager og Securitas henviste til, ikke udgjorde et databeskyttelsesretligt samtykke, da et samtykke efter GDPR artikel 6, stk. 1, litra a, kun sjældent vil opfylde gyldighedsbetingelsen om at være afgivet frivilligt grundet det ulige forhold, der typisk består mellem arbejdsgiveren og den ansatte.

Datatilsynet fandt imidlertid, at Securitas havde hjemmel til at videregive klagers personoplysninger i medfør af interesseafvejningsreglen i GDPR artikel 6, stk. 1, litra f. Herved lagde Datatilsynet vægt på, at indhentelsen af den pågældende sikkerhedsgodkendelse var nødvendig for, at Securitas som arbejdsgiver kunne sikre sig, at klager som arbejdstager kunne varetage de opgaver, som var nødvendige i forbindelse med ansættelsen.

Afslutningsvis fandt Datatilsynet, at videregivelsen af klagers personnummer lå inden for rammerne af lov nr. 502 af 23. maj 2018 (»den danske databeskyttelseslov«) § 11, stk. 2, nr. 3, hvorefter videregivelse af oplysninger om personnummer bl.a. kan ske med henblik på entydig identifikation.

Læs Datatilsynets pressemeddelelse her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/apr/videregivelse-af-personoplysninger-levede-op-til-gdpr>

Læs hele Datatilsynets afgørelse her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/dec/videregivelse-af-personoplysninger-levede-op-til-gdpr>

Radius behandler personoplysningerne indhentet ved fjernaflæsning af elmålere i overensstemmelse med GDPR og nationale regler

Datatilsynet traf den 10. februar 2023 afgørelse i sag 2021-31-5478 vedrørende Radius Elnet A/S's (»Radius«), en dansk distributions-

nettsvirksomhed, fjernaflæsning af deres kunders elmålere. Sagen havde været behandlet i Datarådet.

Sagen blev indledt på baggrund af, at en række borgere havde klaget over Radius' behandling af borgernes personoplysninger i forbindelse med, at Radius fjernaflæste borgernes elforbrug og indhentede andre tekniske oplysninger via deres elmålere, og herefter delte oplysningerne med Energinet.

Radius gjorde gældende, at de indhentede oplysningerne i forbindelse med deres retlige forpligtelse efter elforsyningsloven. Derudover var indhentningen af oplysninger nødvendig for afregning samt sikring af forsyning, opbygning og balancerings af elmarkedet.

Datatilsynet fandt, at adgangen til måleenhederne og behandlingen af de her indhentede oplysninger var en forudsætning for, at Radius kunne efterleve deres retlige forpligtelser. Datatilsynet lagde dels vægt på, at det fremgik klart af lovgivningen, hvad Radius forpligtelser indebærer, og dels at behandlingen af oplysningerne indhentet på den omtalte måde var en forudsætning for at efterleve disse forpligtelser.

Datatilsynet fandt samtidig, at behandlingen var i overensstemmelse med proportionalitetsprincippet i GDPR.

Læs Datatilsynets pressemeddelelse her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/maj/klage-over-radius-fjernaflaesning-af-elmaalere>

Læs hele Datatilsynets afgørelse her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/feb/klage-over-radius-fjernaflaesning-af-elmaalere>

Intern deling af oplysninger mellem myndigheder underlagt skatteforvaltningen ikke i strid med GDPR

Datatilsynet traf d. 14. marts 2023 afgørelse i sagen 2021-32-2645, hvor en borger havde klaget over, at Skattestyrelsen havde delt oplysninger om vedkommende med Gældstyrelsen.

Skattestyrelsen modtog oplysninger om klagerens arv fra Skifteretten, og delte disse oplysninger med Gældstyrelsen med henblik på inddrivelse af klagers gæld til det offentlige. Spørgsmålet var således, om videregivelsen af oplysningerne var forenelige med databeskyttelsesreglerne, idet klager mente, at delingen var sket til et uvedkommende formål og dermed var i strid med reglen om formålsbegrænsning i GDPR artikel 5, stk. 1, litra b.

Datatilsynet lagde indledningsvist til grund, at både Skattestyrelsen og Gældstyrelsen havde hjemmel til at behandle oplysningerne som led i deres almindelige myndighedsopgaver. Det var således udelukkende et spørgsmål om videregivelsens lovlighed.

Videregivelse af personoplysninger må udelukkende ske til udtrykkeligt angivne og legitime formål. I den forbindelse konkluderede Datatilsynet, at der i den konkrete sag var tale om et legitimt formål, idet der foreligger en betydelig sammenhæng mellem de udvekslende myndigheders opgaver og formålene med disse opgaver. Det blev særligt fremhævet, at begge myndigheders virke handler om statens »provenu«, og at klager måtte kunne forvente, at oplysninger om dennes indtægter (arv) vil blive anvendt i forbindelse med gældsinddrivelsen.

Datatilsynet konkluderede derfor, at videregivelsen af oplysningerne internt mellem myndighederne, der begge er en del af skatteforvaltningen, ikke var i strid med GDPR.

Læs hele Datatilsynets afgørelse her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/mar/berettiget-at-skatteforvaltningen-delte-personoplysninger-internt>

Datatilsynet udtaler kritik af Hovedstadens Beredskab for mangelfuld behandlingssikkerhed i deres ESDH-system

Datatilsynet traf den 22. marts 2023 afgørelse i sag 2022-442-21566. Sa-

gen vedrørte Hovedstadens Beredskab I/S (»Hovedstadens Beredskab«), som havde haft en brud på persondatasikkerheden ved at samtlige brugere af virksomhedens elektroniske sags- og dokumenthåndteringssystem (»ESDH-system«) i perioden mellem maj 2022 og november 2022 havde haft adgang til i alt 2.029 nuværende og tidligere medarbejderes personoplysninger.

Hovedstadens Beredskab anmeldte selv bruddet til Datatilsynet i november 2022, da de blev opmærksomme på problemet. Bruddet skyldtes en manglende differentiering i de enkelte brugeres adgangsrettigheder til oplysningerne i ESDH-systemet. Dette medførte, at seks brugere af systemet i perioden havde tilgået personoplysninger for hvem oplysningerne var uvedkommende, mens alle brugere havde haft mulighed for at tilgå oplysningerne.

Datatilsynet udtalte kritik af Hovedstadens Beredskab, idet virksomheden ikke havde sikret differentieringen af brugeradgange til personoplysningerne i ESDH-systemet og Datatilsynet fandt på den baggrund, at Hovedstadens Beredskab ikke havde iagttaget sin pligt efter GDPR artikel 32, stk. 1 om en tilstrækkelig sikkerhed ved behandling af personoplysninger.

Datatilsynet tillagde det vægt, at de mere end 190 brugere af systemet alle havde haft adgang til oplysningerne i hele perioden, og at det til dels på tidspunktet for afgørelsens afsigelse fortsat var muligt at tilgå oplysninger. Derudover blev det tillagt vægt, at der var tale om fortrolige oplysninger om blandt andet beskyttede adresser og personnumre, som alene en HR-afdeling burde have haft adgang til.

Datatilsynet fastslog vedrørende kravet om tilstrækkelig behandlingssikkerhed efter GDPR artikel 32, at dette indebærer, at de enkelte brugeres adgang til systemer med personoplysninger skal være begrænset til hvad der er et nødvendigt, ar-

bejdsbetinget behov for den enkelte bruger.

Læs Datatilsynets pressemeddelelse her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/maj/kritik-af-hovedstadens-beredskabs-mangelfulde-rettighedsstyring>

Læs hele Datatilsynets afgørelse her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/mar/kritik-af-hovedstadens-beredskabs-mangelfulde-rettighedsstyring>

Alvorlig kritik af Rigspolitiet

Datatilsynet traf den 28. marts 2023 afgørelse i sag 2022-32-2939 vedrørende Rigspolitiets videregivelse af oplysninger til Aalborg Universitet om en borger, der havde modtaget en fartbøde, men gjort indsigelse mod bødeforelægget, og afventede domstolens behandling af sagen.

Sagen blev indledt af Datatilsynet på baggrund af en række henvendelser fra borgere, hvis oplysninger om, at de havde modtaget en fartbøde, var videregivet af Rigspolitiet til Aalborg Universitet til brug for forskningsprojektet Intervention Against Speed Offenders (EASE). Forskningsprojektet havde til formål at forebygge hastighedsovertrædelser i trafikken gennem onlinelæring om trafikikkerhed. En af henvendelserne til Datatilsynet var fra en borger, der havde gjort indsigelse mod bødeforlægget og afventede domstolens behandling af sagen.

Borgeren gjorde gældende, at oplysningen ikke kunne videregives, før lovovertrædelser var endeligt stadfæstet, uanset at videregivelsen skete til forskningsformål. Borgeren anførte, at det ikke var nødvendigt for Rigspolitiet at videregive oplysningerne til Aalborg Universitet, idet Rigspolitiet havde mulighed for at skelne mellem bilister, som havde vedtaget bøden, og bilister, som havde klaget over bøden.

Datatilsynet fandt, at oplysningerne var nødvendige for, at Aalborg Universitet kunne invitere relevante personer til at deltage i

forskningsprojektet, som havde til formål at forebygge hastighedsovertrædelser i trafikken.

Datatilsynet fandt imidlertid, at Rigspolitiets videregivelse af klagers personoplysninger var sket i strid med GDPR artikel 5, stk. 1, litra b og c, da Rigspolitiets videregivelse af oplysninger om klager ikke var sket til et sagligt og relevant formål, fordi det på tidspunktet for videregivelsen fortsat måtte anses for at have haft formodningen imod sig, at klager havde overtrådt færdselsloven, indtil sagen var blevet afgjort, og at forskningsprojektets målgruppe var personer, der havde overtrådt færdselsloven. På baggrund af dette udtalte Datatilsynet alvorlig kritik af Rigspolitiet.

Afslutningsvis fandt Datatilsynet grundlag for at påbyde Rigspolitiet at ophøre med at videregive oplysninger til Aalborg Universitet om personer, der har modtaget et bødeforlæg og gjort indsigelse, førend sagen er endeligt afgjort ved domstolene.

Læs Datatilsynets pressemeddelelse her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/apr/alvorlig-kritik-af-rigspolitiet>

Læs hele Datatilsynets afgørelse her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/mar/alvorlig-kritik-af-rigspolitiet>

Datatilsynet udtaler alvorlig kritik af Boligportalen for deres behandling af personoplysninger for besøgende på Boligportalens hjemmeside og giver et påbud

Datatilsynet traf den 20. april 2023 afgørelse i sag 2021-7329-0052. Sagen vedrørte BoligPortal.dk ApS's (»Boligportalen«) indsamling af personoplysninger på deres hjemmeside ved brug af Facebook Business Tools.

Sagen blev indledt på baggrund af en klage over Boligportalens brug af Facebook Business Tools på deres hjemmeside. Klagen blev indsendt af nonprofit organisationen None of Your Business

(»NOYB«) og blev behandlet som en del af den såkaldte »Taskforce 101«, som en af de 101 klager der blev indsendt af NOYB til en række europæiske datatilsyn i 2020.

Boligportalen anvendte de såkaldte Facebook Business Tools til at indsamle personoplysninger om besøgende på deres hjemmeside, men kunne ikke påvise, at denne indsamling blev foretaget i overensstemmelse med GDPR. Datatilsynet udtalte kritik af, at Boligportalen således ikke overholdte deres forpligtelse efter GDPR artikel 5, stk. 2, hvorefter den dataansvarlige skal være i stand til at påvise, at de behandler personoplysninger efter principperne om blandt andet lovlighed, rimelighed og gennemsigtighed efter GDPR artikel 5, stk. 1.

Udover at Boligportalen ikke kunne påvise, at de overholdte GDPR, fandt Datatilsynet det endvidere kritisabelt, at Boligportalen ikke havde en tilstrækkelig rolle- og ansvarsfordeling, som forpligtet til efter GDPR artikel 26, mellem Boligportalen og Meta Ireland, som var fælles dataansvarlige for behandlingen af personoplysninger indsamlet ved de besøgende på Boligportalens hjemmeside.

Datatilsynet kritiserede Boligportalen for ikke at have undersøgt, i samarbejde med Meta Ireland, om personoplysninger fra hjemmesiden blev behandlet uden for EU/EØS. Boligportalen havde derfor ikke sikret, at reglerne for overførsel af data til lande uden for EU/EØS blev overholdt.

Samlet udtalte Datatilsynet alvorlig kritik Boligportalen, som samtidig fik et påbud om at bringe deres behandling af personoplysninger på deres hjemmeside i overensstemmelse med GDPR artikel 5, stk. 1, litra a, artikel 5, stk. 2, artikel 24, stk. 1 og artikel 26. inden den 18. maj 2023.

Læs Datatilsynets pressemeddelelse her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/jun/alvorlig-kritik-og-paabud-til-boligportal-for-brug-af-facebook-business-tools>

Læs hele Datatilsynets afgørelse her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/apr/alvorlig-kritik-og-paabud-til-boligportal-for-brug-af-facebook-business-tools>

Nyt vejledningsunivers om GDPR til mindre virksomheder

Datatilsynet offentliggjorde den 4. maj 2023 et nyt vejledningsunivers om GDPR til mindre virksomheder.

Formålet med vejledningsuniverset er at gøre databeskyttelsesreglerne mere overskuelige for mindre virksomheder, der ikke har egne juridiske afdelinger eller en ansat jurist. Vejledningsuniverset er indrettet på en måde, der har til formål at formidle reglerne på en letforståelig og tilgængelig måde. Ved hjælp af konkrete eksempler, en step-by-step guide og uddybende ekstramateriale gøres GDPR mere pædagogisk og spiseligt.

Step-by-step guiden består af syv trin og skal tjene som en huskeliste til virksomhederne og dermed medvirke til at skabe et overblik over tiltag, som måtte være relevante for den respektive virksomhed. Hvert trin beskrives i lægmandstermer og indeholder konkrete eksempler, som kunne være relevante for virksomhederne.

Ekstramaterialet består af en række relevante begrebsdefinitioner og en udførlig FAQ, hvor virksomhederne kan finde svar på nogle ofte stillede spørgsmål.

Derudover tilbyder Datatilsynet også en udvidet telefonservice, hvor virksomhederne har mulighed for at konsultere hjælp.

Læs Datatilsynets pressemeddelelse her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/maj/gdpr-for-smaa-virksomheder>

Datatilsynet indskærper, at indsigt retten er en personlig rettighed – også for umyndige

Datatilsynet udtalte sig i en pressemeddelelse den 8. maj 2023 om omfanget af den databeskyttelsesretlige indsigt ret angående børn.

Udtalelsen kom i forlængelse af en undersøgelse af Gribskov kommune, efter at Datatilsynet i november 2022 blev opmærksom på, at kommunen generelt afviste at give en forældremyndighedsindehaver indsigt i personoplysninger om et fælles barn, medmindre der forelå tilsagn fra begge forældremyndighedsindehavere.

Ifølge GDPR artikel 15, stk. 1, har den registrerede ret til bekræftelse på og oplysninger om behandlingen af dennes personoplysninger. Det følger herudover af GDPR artikel 12, stk. 2, at den dataansvarlige skal lette udøvelsen af den registreredes rettigheder.

Datatilsynet understregede, at indsigt retten er en personlig rettighed, og at barnet således er selvstændig rettighedshaver. Datatilsynet bemærkede dog, at denne indsigt ret kan udøves af en forældre på barnets vegne for at understøtte muligheden for, at barnet kan nyde den fulde beskyttelse af sine rettigheder.

Datatilsynet udtalte i den forbindelse, at det er tilstrækkeligt, hvis én forældremyndighedsindehaver udøver retten, uden at der hertil kan kræves tilsagn fra en eventuel anden forældre.

Kommunens praksis om at kræve tilsagn fra begge forældremyndighedsindehavere ville således besværliggøre udøvelse af indsigt retten og dermed være i strid med GDPR artikel 12, stk. 2.

Læs Datatilsynets pressemeddelelse her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/maj/naar-foraeldre-soeger-om-indsigt-i-barnets-oplysninger>

Læs Datatilsynets brev til Gribskov kommune her: <https://www.datatilsynet.dk/Media/638188008150537548/Brev%20til%20Gribskov%20Kommune.pdf>

Datatilsynet udtaler kritik af Kriminalforsorgen for at undlade undersøgelse af muligt brud på persondatasikkerhed

Datatilsynet har den 31. maj 2023 truffet afgørelse i sag 2021-816-

0292 om den danske Kriminalforsorgs (»Kriminalforsorgen«) behandling af et brud på persondatasikkerheden. I sagen udtalte Datatilsynet kritik af Kriminalforsorgen, idet myndigheden ad flere omgange blev bekendt med oplysninger om et muligt brud, men trods henvendelserne undlod at undersøge forholdet før efter seks måneder fra første henvendelse.

De faktiske omstændigheder, som dannede ramme om sagen, var en personalegruppes oprettelse af en chatgruppe på Facebooks beskedtjeneste Messenger. Heri foregik tjenstlig kommunikation hos de ansatte i Kriminalforsorgen om såvel indsatte i Storstrøm Fængsel som de ansatte. I den forbindelse delte en medarbejder over for ledelsen i Storstrøm Fængsel den 11. november 2020, at chatgruppen eksisterede, og at medarbejderen var af den overbevisning, at der blev delt arbejdsrelaterede oplysninger. Først den 12. april 2021 rettede fængslets ledelse imidlertid henvendelse til Kriminalforsorgens databeskyttelses- og informationssikkerhedsmedarbejder, og ikke før den 4. august 2021 blev hændelsen anmeldt som et brud på persondatasikkerheden til Datatilsynet.

Datatilsynet lægger i den forbindelse til grund, at en dataansvarlig som udgangspunkt er bekendt med et brud på persondatasikkerheden, når en medarbejder hos den dataansvarlige gøres bekendt med bruddet. I den forbindelse tillagde Datatilsynet det således vægt, at medarbejderen, der indgav den oprindelige henvendelse, allerede den 11. november 2020 var bekymret for, at der i chatgruppen blev delt arbejdsrelaterede oplysninger. Sådanne indikationer på brud på persondatasikkerheden bør ifølge Datatilsynet foranledige den dataansvarlige til at foretage yderligere undersøgelser med henblik på at afklare forholdet.

På baggrund heraf udtalte Datatilsynet kritik over, at Kriminalforsorgen, ved ikke at have undersøgt

hændelsen med fornøden hastighed og i forlængelse heraf indgivet rettidig anmeldelse af bruddet til Datatilsynet, ikke havde handlet i overensstemmelse med lov nr. 410 af 27. april 2017 § 28, stk. 1 (»retshåndhævelsesloven«). Efter denne bestemmelse skal den dataansvarlige myndighed uden unødigt forsinkelse og om muligt, senest 72 timer efter at den dataansvarlige blevet bekendt med bruddet, indgive anmeldelse til Datatilsynet.

Læs Datatilsynets pressemeddelelse her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/jun/kritik-af-kriminalforsorgen-for-ikke-at-afklare-muligt-brud-i-tide>

Læs hele Datatilsynets afgørelse her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/maj/kritik-af-kriminalforsorgen-for-ikke-at-afklare-muligt-brud-i-tide>

Datatilsynet træffer afgørelse om Statens Serum Instituts opfyldelse af oplysningspligten

Datatilsynet traf den 2. juni 2023 afgørelse 2021-432-0070 i en tilsynssag mod Statens Serum Institut (»SSI«). Sagen, som blev behandlet i Datarådet, handlede om, hvorvidt SSI kunne undlade at opfylde sin databeskyttelsesretlige oplysningspligt med henvisning til, at denne opfyldelse ville være forbundet med en uforholdsmæssig stor indsats.

Sagen opstod, efter Datatilsynet blev bekendt med, at SSI ikke foretog underretning om behandling af personoplysninger til de registrerede i forbindelse med modtagelse af blodprøver mv. fra regionerne med henblik på analyse samt i de tilfælde, hvor SSI besluttede at gemme restmateriale i Danmarks Nationale Biobank.

Det følger af GDPR artikel 14, stk. 1-3, at den dataansvarlige, når personoplysninger ikke indsamles hos den registrerede, skal give oplysninger om behandlingen til den registrerede. Det følger dernæst af artikel 14, stk. 4, at når den dataansvarlige vil viderebehandle person-

oplysninger til et andet formål end oprindelige indsamlingsformål, skal den dataansvarlige give den registrerede underretning om dette formål. Der knytter sig imidlertid den undtagelse til bestemmelserne, at oplysningspligten kan undlades, såfremt det vil være forbundet med uforholdsmæssigt store vanskeligheder at give denne underretning jf. GDPR artikel 14, stk. 5, litra b.

SSI gjorde gældende, at undtagelsen fandt anvendelse, eftersom SSI modtager og gemmer et meget stort antal prøver, og at en manuel og individuel underretning til de registrerede ville kræve en uforholdsmæssigt stor administrativ og en ikke ubetydelig økonomisk byrde. Det blev i den forbindelse bemærket, at SSI's IT-system ikke var indrettet til at kunne givet automatiseret underretning.

Datatilsynet fandt, at undtagelsen i 14, stk. 5 litra b, skal fortolkes indskrænkende, at formålet med oplysningspligten er at sikre gennemsigtighed med behandling af personoplysninger, og at den dataansvarlige derfor som udgangspunkt skal sikre dette. Dernæst udtalte Datatilsynet, at det er en betingelse for anvendelse af undtagelsesbestemmelsen, at vanskelighederne forbundet med opfyldelse af oplysningspligten skal skyldes det forhold, at oplysningerne er indsamlet hos andre end den registrerede. Dette var ikke tilfældet, eftersom vanskelighederne skyldtes indretningen af SSI's eget system, der ikke understøttede en mulighed for på nemmere vis at underrette de registrerede.

Datatilsynet anmodede derfor SSI om en redegørelse for, hvordan instituttet fremadrettet vil opfylde sin oplysningspligt inden for en frist på 3 måneder.

Læs Datatilsynets pressemeddelelse her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/maj/afgoerelse-om-statens-serum-instituts-opfyldelse-af-oplysningspligten>

Læs hele Datatilsynets afgørelse her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/feb/statens-serum-instituts-opfyldelse-af-oplysningspligten>

Brøndby IF får lov til udvidet brug af ansigtsgenkendelse

Datatilsynet gav den 9. juni 2023 Brøndby IF tilladelse til at anvende ansigtsgenkendelse i forbindelse med kampe på andre stadions end Brøndby Stadion. Datatilsynet gav ydermere Brøndby IF lov til at anvende overvågningsbilleder fra stadion til at registrere personer, der overtræder ordensreglementet, i systemet til automatisk ansigtsgenkendelse.

Tilbage i maj 2019 gav Datatilsynet, i henhold til § 7, stk. 4, i lov nr. 502 af 23. maj 2018 (»den danske databeskyttelseslov«), Brøndby IF tilladelse til at behandle særlige kategorier af personoplysninger i forbindelse med Brøndby IF's etablering af automatisk ansigtsgodkendelse som led i adgangskontrol ved indgangene til Brøndby Stadion. Efterfølgende anmodede Brøndby IF om udvidelse af denne tilladelse, således at Brøndby IF fremover også kunne anvende ansigtsgenkendelse i forbindelse med Brøndby IF's udebanekampe, dvs. kampe på andre stadions end Brøndby Stadion. Brøndby IF anmodede endvidere om tilladelse til at anvende billeder fra overvågningskameraer på stadion som grundlag for at registrere personer, der overtræder ordensreglementet, i systemet til automatisk ansigtsgodkendelse.

Datatilsynets opfattelse var, at de forhold, der begrundede tilladelse til brug af automatisk ansigtsgenkendelse i forbindelse med adgangskontrol ved indgangene til Brøndby Stadion, ligeledes gjorde sig gældende for så vidt angik Brøndby IF's udebanekampe. Datatilsynet vurderede også, at Brøndby IF inden for rammerne af tilladelsen kan anvende overvågningsbilleder fra kameraer på stadion som grundlag for at registrere personer, der overtræder ordensreglementet, i systemet til automatisk ansigtsgodkendelse.

Brøndby IF skal dog fortsat overholde tilladelsens vilkår.

Ydermere påpegede Datatilsynet, at anvendelsen af overvågningsbilleder kan være omfattet af reglerne i § 4 c, stk. 4 og 5, i lovekendtgørelse nr. 182 af 24. februar 2023 om tv-overvågning (»den danske tv-overvågningslov«). I den forbindelse finder Datatilsynet det nærliggende at anse Brøndby IF's meddelelse og håndhævelse af en karantæne som behandling af en konkret tvist, hvorfor opbevaringen af overvågningsbilleder vil kunne forlænges udover den generelle slettefrist på 30 dage i den danske tv-overvågningslov.

Læs Datatilsynets pressemeddelelse her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/jun/brondby-if-bar-faaet-lov-til-udvidet-brug-af-ansigtsgenkendelse>

Læs hele Datatilsynets afgørelse her: <https://www.datatilsynet.dk/afgoerelser/tilladelser/2023/jun/2022-51-0375>

Datatilsynet udtaler alvorlig kritik af utilstrækkelig sikkerhed ved MitID

Datatilsynet traf den 23. juni 2023 to afgørelser i sagerne 2022-431-0171 og 2022-432-0079 over for henholdsvis Digitaliseringsstyrelsen og Signaturgruppen.

Begge afgørelser angik det samme hændelsesforløb i januar 2022, hvor flere borgere fejlagtigt fik adgang til andre borgers konti ved forsøg på login i deres netbank via MitID. Fejlen skyldtes, at flere login-anmodninger til samme netbank inden for millisekunder kunne resultere i udstedelsen af et adgangsgivende token fra MitID til en anden brugers session. Fejlen kunne være undgået ved hjælp af en valideringsteknologi kaldet *Broker Security Context*, som Digitaliseringsstyrelsen havde anbefalet, men ikke stillet som krav. Signaturgruppen havde ikke implementeret *Broker Security Context* i overensstemmelse med anbefalingens nærmere specifikationer.

Signaturgruppens rolle i sagen som såkaldt *broker* var at viderefor-

midle loginoplysninger fra Digitaliseringsstyrelsen til netbanken, hvilket grundet samtidighedsfejlen i systemet medførte behandling af ukorrekte data. Signaturgruppen var i denne henseende selvstændigt dataansvarlig for behandling og videregivelse af data, mens Digitaliseringsstyrelsen var dataansvarlig for MitID.

Ifølge Datatilsynet var der i sagerne tale om en skærpet risikoprofil, da der forelå en netbank-løsning med risiko for bl.a. utilsigtet adgang til andres personoplysninger om økonomiske forhold samt dispositionsadgangen til at kunne foretage transaktioner med retskraft.

Datatilsynet fandt, at hverken Signaturgruppen eller Digitaliseringsstyrelsen havde overholdt deres forpligtelser efter GDPR artikel 32, stk. 1. Digitaliseringsstyrelsen skulle således, henset til de betydelige risici, have stillet det som et obligatorisk krav at anvende *Broker Security Context* i modsætning til blot at anbefale dette. Signaturgruppen skulle efter en tilsvarende risikobetragtning have fulgt anbefalingen til trods for, at den ikke var fremsat som et obligatorisk krav.

På den baggrund udtalte Datatilsynet alvorlig kritik af såvel Digitaliseringsstyrelsen som Signaturgruppen. Digitaliseringsstyrelsen gjorde efterfølgende anbefalingen til et obligatorisk krav, mens Signaturgruppen har implementeret *Broker Security Context* i overensstemmelse med anbefalingen og de dertilhørende specifikationer.

Læs datatilsynets pressemeddelelse her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/jun/alvorlig-kritik-af-utilstraekkelig-sikkerhed-ved-mitid>

Læs hele afgørelsen over for Digitaliseringsstyrelsen her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/jun/alvorlig-kritik-af-digitaliseringsstyrelsen-for-utilstraekkelig-sikkerhed-ved-mitid>

Læs hele afgørelsen over for Signaturgruppen her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2023/jun/alvorlig-kritik-af-signaturgruppen-for-utilstraekkelig-sikkerhed-ved-mitid>

Datatilsynet offentliggør en opdateret vejledning om adfærdskodekser

Datatilsynet offentliggjorde den 26. juni 2023 en revideret udgave af Datatilsynets vejledning om adfærdskodekser. Datatilsynet reviderede deres vejledning på baggrund af ny praksis på området som fulgte af et nyt adfærdskodeks fra Kirkeministeriet samt offentliggørelsen af en vejledning om adfærdskodekser fra EDPB.

Den reviderede vejledning uddyber processen for udarbejdelse af en adfærdskodeks med det formål at præcisere og lette processen for udarbejdelsen, for ansøgerne. Herudover er vejledningen opdateret i overensstemmelse med de krav EDPB opstiller i deres vejledning fra 2019. På baggrund heraf fastlægger Datatilsynet også i den reviderede vejledning, hvilke minimumskrav Datatilsynet selv stiller til en adfærdskodeks.

Datatilsynet har til vejledningen tillagt en ansøgningsblanket til godkendelse af adfærdskodeks ved Datatilsynet med det formål at lette processen herfor og dermed fremme flere godkendelser af adfærdskodekser. Datatilsynet har tillige inkluderet en tjekliste, som kan gennemgås inden indsigelse af et adfærdskodeks til Datatilsynet.

Læs Datatilsynets pressemeddelelse her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/jun/datatilsynets-vejledning-om-adfaerdskodekser-er-revideret>

Læs Datatilsynets vejledning her: <https://www.datatilsynet.dk/Media/638233755631220855/Vejledning%20om%20adf%C3%A6rdskodekser.pdf>

Læs Datatilsynets ansøgningsblanket her: <https://view.officeapps.live.com/op/view.aspx?src=htp%3A%2F%2Fwww.datatilsynet.dk%2FMedia%2F638233760790882718%2FAns%25C3%25B8gningsblanket%2520af%2520adf%25C3%25A6rdskodeks.docx&wdOrigin=BROWSELINK>

Datatilsynet offentliggør vejledning om brugen af tv-overvågning i private virksomheder

Datatilsynet offentliggjorde den 27. juni 2023 en ny vejledning om tv-overvågning. Denne vejledning er målrettet private virksomheder og giver et samlet overblik over, hvilke love og regler private virksomheder skal være opmærksomme på, når de anvender tv-overvågning.

Vejledningen gennemgår de krav, som virksomhederne skal opfylde, for at måtte anvende tv-overvågning, herunder hvilke behandlingsgrundlag, der skal eksistere for, at virksomhederne må anvende tv-overvågning, samt hvor og hvornår virksomhederne må tv-overvåge. Vejledningen gennemgår også en række sikkerhedsmæssige foranstaltninger, som virksomhederne skal overveje i forbindelse med brug af tv-overvågning.

Herudover vejledes der om, hvilke pligter virksomheden har i forbindelse med udførelse og opbevaring af tv-overvågningsbilleder ved en gennemgang af blandt andet pligten til at skiltning og oplysningspligten. Vejledningen præciserer også den registreredes indsigt i tv-overvågningsoptagelserne, og hvornår virksomheden er forpligtet til at imødekomme en sådan anmodning om indsigt fra den registrerede.

Endeligt bemærker Datatilsynet i deres pressemeddelelse, at der planlægges udgivelser af yderligere vejledninger om tv-overvågning, som vil være målrettet blandt andet offentlige myndigheder og boligorganisationer.

Læs Datatilsynets pressemeddelelse her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/jun/ny-vejledning-om-tv-overvaagning-maalrettet-private-virksomheder>

Læs Datatilsynets vejledning her: <https://www.datatilsynet.dk/Media/638234600620556007/Vejledning%20om%20tv-overv%C3%A5gning%20-%20private%20virksomheder.pdf>

Datatilsynet udsteder ny vejledning om direkte markedsføring

Datatilsynet offentliggjorde den 30. juni 2023 en ny vejledning om virksomheders brug af direkte markedsføringsaktiviteter.

Vejledningen har sit primære fokus på de databeskyttelsesretlige regler, der finder anvendelse i forbindelse med direkte markedsføring. Vejledningens målgruppe er rådgivere og andre, der har erfaring med databeskyttelse. Foruden de databeskyttelsesretlige regler kaster vejledningen lys over andre retsreglers relevans og samspil med databeskyttelsesretten i forskellige sammenhænge, herunder navnlig markedsføringsretten og forbrugerretten.

Vejledningen beskriver, hvordan man som dataansvarlig skal indtænke de databeskyttelsesretlige regler allerede inden markedsføringsaktiviteten igangsættes, særligt princippet om »privacy by design and default« i GDPR artikel 25 og de grundlæggende principper i GDPR artikel 5.

Vejledningen giver herudover eksempler på nogle af de mest udbredte markedsføringsaktiviteter, såsom telefonisk markedsføring, brevpost, elektroniske henvendelser på e-mail og sms, sociale medier, og deres forenelighed med de databeskyttelsesretlige regler. Endelig forklarer vejledningen, hvordan de databeskyttelsesretlige regler skal overholdes, når der udføres segmentering, profilering og automatiske afgørelser.

Læs Datatilsynets pressemeddelelse her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/jun/ny-vejledning-om-direkte-markedsfoering>

Læs Datatilsynets vejledning her: <https://www.datatilsynet.dk/Media/638237218449834564/Vejledning%20om%20direkte%20markedsfoering%20-%20markedsfoering.pdf>

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



Delphi

David Suh og Rebecka Undén

Sanktionsavgift mot Bonnier för otillåten profilering och reprimand mot Vklass för otillräckligt skyddad lärplattform

Sanktionsavgift om 13 miljoner kronor för profilering av kunder utan samtycke

Den svenska Integritetsskyddsmyndigheten ("IMY") meddelade den 27 juni 2023 beslut i ett tillsynsärendet mot Bonnier News AB ("Bonnier") efter en granskning av hur Bonnier samlade in och hanterade personuppgifter i syfte att använda dessa för marknadsföring. Granskningen resulterade i en administrativ sanktionsavgift om 13 miljoner kronor. Bonnier har överklagat sanktionsbeslutet till förvaltningsrätten.

Bolag inom Bonnierkoncernen samlade in personuppgifter från kunder och personer som besökte bolagens webbplatser. De insamlade uppgifterna överfördes sedan till koncerngemensamma databaser där profiler skapades om enskilda personer. Datan användes sedan för riktad annonsering online, marknadsföring via fysisk post och telefonsförsäljning. Uppgifterna som samlades in innefattade bland annat köpinformation från olika företag inom koncernen samt analyser av internetanvändares beteenden på företagens webbplatser. I vissa fall kombinerades denna information även med externa personuppgifter såsom kundens kön, hushållets bilägande, postnummer och ytterligare statistik baserat på individens bostadsområde. Denna statistik inklu-

derade aspekter som livsfas, köpkraft och boendesituation. Bonnier behandlade uppgifterna med stöd av den rättsliga grunden berättigat intresse i artikel 6.1. f) GDPR och menade att de hade ett berättigat intresse i att bl.a. förstå sina kunders önskemål och behov för att kunna uppnå relevans i innehåll och annonsering.

IMY framhöll inledningsvis att uppgifterna som användes för profilering ursprungligen samlades in genom webbkakor och att det samtyckeskrav som gäller för webbkakor enligt lag (2022:482) om elektronisk kommunikation ger ett starkt integritetsskydd för de registrerade. Integritetsskyddet riskerar att undermineras om de insamlade personuppgifterna i ett senare led kan behandlas med stöd av andra rättsliga grunder t.ex. berättigat intresse.

IMY uttalade även att profileringen i fråga var omfattande till sin karaktär och inte någonting som en registrerad kan förvänta sig utan att ha lämnat sitt samtycke. De registrerade kan inte heller förvänta sig att beteendedata samlas in i marknadsföringssyfte endast eftersom de besöker en webbsida, eller att datan kommer att sammanställas med information från andra köpsituationer och information från externa källor. Vid en sammantagen bedömning

fann IMY därför att de registrerades integritetsintresse vägde tyngre än Bonniers marknadsföringsintresse. Profileringen krävde därför samtycke, och hade därmed skett i strid med GDPR.

Vid bestämmandet av sanktionsavgiftens storlek tog IMY bl.a. hänsyn till att profileringen i fråga hade varit omfattande till sin karaktär, pågått under lång tid och berört ett stort antal registrerade vilket motiverande en hög sanktionsavgift. IMY beaktade dock även att Bonnier hade vidtagit omfattande åtgärder i form av satta lagringsfrister, att uppgifter inte registrerades på produktnivå och att inte fler uppgifter än nödvändigt lämnades ut till anslutna bolag för att begränsa intrånget i de registrerades personliga integritet. Detta gjorde att överträdelsernas allvarlighetsgrad minskades i betydande mån. Beslutet fattades i samarbete med övriga dataskyddsmyndigheter i EU eftersom Bonnier har användare i flera länder.

Tillsynsärendet visar på det starka integritetsskydd som de registrerade har vid beteendeprofilering. Av intresse är även den koppling som görs till att uppgifterna i fråga ursprungligen samlades in genom webbkookies med stöd av samtycke.



Reprimand för otillräckligt skydd av personuppgifter på lärplattform

IMY inledde den 18 oktober 2022 ett tillsynsärende mot lärplattformsbolaget Vklass AB ("Vklass") mot bakgrund av flera anmälningar om personuppgiftsincidenter. Anmälningarna hade inkommit från före detta samt befintliga kunder, vilka utgjordes av aktörer inom skol- och utbildningsverksamhet.

En elev som använde lärplattformen lyckades komma åt personuppgifter och ladda ner dem till en egen databas, för att sedan publicera dem online. Detta möjliggjordes genom att systemövervakning avseende an-

rop mot lärplattformens adressböcker saknades. Vklass hade på grund av detta ingen möjlighet att upptäcka vare sig incidenterna eller vilka som hade drabbats.

IMY konstaterade att Vklass hade behandlat personuppgifter i strid med GDPR, genom att inte i adekvat utsträckning skydda personuppgifterna genom lämpliga tekniska och organisatoriska säkerhetsåtgärder. Lärplattformen innehöll även personuppgifter tillhörande barn, vilka är särskilt skyddsvärda enligt GDPR. Dock hade Vklass agerat snabbt så snart incidenten uppdagats, samt därefter vidtagit säkerhetsåtgärder. IMY

gjorde därför bedömningen att förseelserna var att betrakta som en mindre överträdelse och tilldelade Vklass en reprimand.

Av särskilt intresse i tillsynsärendet är att Vklass är personuppgiftsbiträde i relation till sina kunder. Beslutet påvisar att både den personuppgiftsansvariga och personuppgiftsbiträdet har ett ansvar för att säkerställa att personuppgifterna hanteras och skyddas på ett korrekt sätt.

David Sub, Associate, Advokatfirman Delphi

Rebecka Undén, Associate, Advokatfirman Delphi



Bird & Bird

Gunnar Hjalt

Svensk domstol baserar skälig ersättning till anställd uppfinnare på royalty, PMT 9596-21

Kärandens talan avsåg vid Patent- och marknadsdomstolen (PMD) krav på ersättning grundat på reglerna i lagen om rätten till arbetstagarers uppfinningar (LAU). Det var ostridigt att uppfinningen inte utgjorde en forskningsuppfinning utan en uppfinning av kategorin ”annan tjänsteuppfinning”. PMD ogillade kärandens talan i dess helhet på grund av att kärandens anställning haft stor betydelse för tillkomsten av uppfinningen, att uppfinningen haft ett förhållandevis

begränsat värde och att käranden genom lön och förmåner hade fått skälig ersättning för uppfinningen.

Patent- och marknadsöverdomstolen (PMÖD) ansåg liksom PMD att anställningen hade haft stor betydelse för uppfinningens tillkomst och ett förhållandevis stort avdrag måste göras med anledning av detta. PMÖD bedömde att uppfinningens värde för svaranden hade begränsat värde ur teknisk synvinkel men det kommersiella värdet var betydande.

Den skäliga ersättningen som käranden ansågs berättigad till, efter en helhetsbedömning, utgjordes dels av en engångsersättning, dels en royalty

om 1% av svarandens omsättning för aktuell produkt under tiden 1 januari 2020 t.o.m. den 7 december 2029. Omständigheten att det saknades förtroende mellan parterna hindrade alltså inte PMÖD att välja en ersättningsmodell baserat på royalty, vilket är en mycket ovanlig modell i den här typen av mål.

Se avgörandet i sin helhet här: <https://www.domstol.se/globalassets/filer/domstol/patentochmarknadsoverdomstolen/avgoranden/2023/pmt-9596-21.pdf>

Gunnar Hjalt, Senior Counsel, Bird & Bird Advokat



Illustration: Colourbox.com



Gorrissen Federspiel

Tue Goldschmieding

Betegnelsen »Emmentaler« kan ikke beskyttes som EU-varemærke for oste

Den Europæiske Unions Ret (»Retten«) afsagde den 24. maj 2023 dom i sag T-2/21 mellem Emmentaler Switzerland og Den Europæiske Unions Kontor for Intellectuel Ejendomsret (»EUIPO«). Tvisten omhandlede Emmentaler Switzerlands anmodning om annullation af EUIPO's afgørelse, der blev truffet den 28. oktober 2020.

Den 4. oktober 2017 fik Emmentaler Switzerland en international registrering af ordmærket »Emmentaler« for varer, der henhører under klasse 29. Den 7. december 2017 blev den internationale registrering meddelt EUIPO, som den 9. september 2019 afviste registreringsansøgningen med henvisning til Europa-Parlamentets og Rådets forordning 2017/1001 af 14. juni 2017 om EU-varemærker (»varemærkeforordningen«) artikel 7, stk. 1, litra b og c i samt artikel 7, stk. 2, der omhandler absolutte registreringshindringer. Afslaget blev begrundet med, at ordmærket var beskrivende for en type af ost.

Emmentaler Switzerland hævdede, at ordmærket udgjorde et EU-kollektivmærke, som indikerede den geografiske oprindelse af osten i overensstemmelse med varemærkeforordningens artikel 74, stk. 2 om certificeringsmærker. Emmentaler Switzerland argumenterede desuden for, at ordmærket ikke udtrykte en egenskab specifikt forbundet med denne type ost.

Retten konkluderede, at den relevante kundekreds umiddelbart opfattede ordmærket »Emmentaler«

som en betegnelse for en bestemt type ost. Under sagen fremlagde EUIPO ordbogen Dudens definition på ordet »Emmentaler«, der ikke skriver noget om oprindelsen, men alene om ostetypen.

Hvad angik spørgsmålet om, hvorvidt ordmærket var et kollektivmærke, fastslog Retten, at undtagelsen i varemærkeforordningens artikel 74, stk. 2, giver mulighed for, at tegn eller angivelser, der i handlen kan fungere som betegnelser for de pågældende varers geografiske oprindelse, kan udgøre kollektivmærker uanset bestemmelsen i forordningens artikel 7, stk. 1, litra c. Retten bemærkede imidlertid, at undtagelsen bør fortolkes snævert navnlig for at sikre en præcis anvendelse af bestemmelsen. Alene tegn, der utvetydigt angiver varernes geografiske oprindelse, kunne således nyde beskyttelse som kollektivmærker. Tegn, der alene angiver varers art, beskaffenhed, mængde, anvendelse eller andre egenskaber, kunne derimod ikke nyde samme beskyttelse.

På baggrund af dette konkluderede Retten, at »Emmentaler« ikke kunne beskyttes som et kollektivmærke, og Retten bekræftede således EUIPO's tidligere afgørelse.

Læs hele dommen her: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=274062&page-Index=0&doclang=DA&mode=req&dir=&occ=first&part=1&cid=3566030>

EUIPO indgår samarbejdsaftale med Ukraine

Den Europæiske Unions Kontor for Intellectuel Ejendomsret (»EUIPO«) og Ukraines Nationale Kon-

tor for Intellectuel Ejendomsret og Innovation (»UANIPIO«) indgik den 5. juli 2023 en ny samarbejdsaftale med henblik på at fremme Ukraines system for immaterielle rettigheder samt styrke dets institutionelle kapacitet.

Aftalen udmønter sig som en underskrevet Memorandum of Understanding (MoU), hvis primære fokus er at styrke EU's samarbejde med Ukraine på området for intellektuel ejendomsret. Aftalen må desuden ses i lyset af Ukraines status som EU-kandidatland, hvor den udgør skridt i retning af Ukraines tættere integrering med EU's indre marked.

MoU'en giver UANIPIO mulighed for at drage fordel af værktøjer til IP-management og undersøgelse, harmonisering af varemærke- og designregistrering samt undersøgelsespraksisser. Hertil kommer nye muligheder for træning af og samarbejde mellem medarbejdere.

MoU'en vil også styrke håndhævelsesrelaterede aktiviteter såsom gensidig udveksling af information angående IP-relaterede undersøgelser eller anti-scam. Herudover muliggøres integrering af Ukraines varemærke- og designdata i EUIPO's varemærke- og designdatabaser.

Ifølge Andrea Di Carlo, EUIPO's vicedirektør, vil harmoniseringen med EU-regler forventeligt øge udenlandske investeringsmuligheder i Ukraine samt facilitere internationaliseringen af lokale virksomheder i Ukraine. Di Carlo mener endvidere, at opgraderingen af Ukraines IP-system vil spille en positiv rolle i Ukraines vej mod integration med EU.

Læs EUIPO's pressemeddelelse her: <https://www.euipo.europa.eu/da/news/euipo-and-ukraine-forge-new-partnership>

Karikaturtegning og fotografi af Den Lille Havfrue ikke i strid med ophavsretten

Højesteret afsagde den 17. maj 2023 dom i sagen BS-24506/2022-HJR mellem den ansvarshavende chefredaktør på Berlingske («Berlingske») og Billedhuggeren Edvard Eriksens Arvinger I/S («arvingerne»). Højesteret frikendte og underkendte dermed Østre Landsrets afgørelse af 9. februar 2022 i sagen BS-47536/2020-OLR, hvorved Berlingske var blevet dømt til at betale 300.000 kroner i erstatning til arvingerne.

Skulpturen af Den Lille Havfrue blev skabt i 1913 af billedhuggeren Edvard Eriksen. Ophavsretten til et værk varer indtil 70 år efter ophavspersonens dødsår. Edvard Eriksen døde i januar 1959,

hvilket betyder, at ophavsretten til Den Lille Havfrue fortsat består.

Berlingske offentliggjorde en tegning den 18. maj 2019, der viste Den Lille Havfrue med et zombilignende ansigt påført titlen »Ondskaben i Danmark«. Tegningen blev udgivet sammen med en artikel om debatkulturen i forbindelse med valgkampen til folketingsvalget i 2019. Den 22. april 2020 offentliggjorde Berlingske en artikel, der viste et fotografi af Den Lille Havfrue med et mundbind på. Artiklen diskuterede et forskningsprojekt, der undersøgte forholdet mellem frygt for Covid-19 smitte og politisk observans.

Spørgsmål var således, om Berlingske havde krænket arvingernes ophavsret til Den Lille Havfrue ved at offentliggøre tegningen og fotografiet. Højesterets skulle afgøre, hvorvidt tegningen og fotografiet udgjorde selvstændige værker, og om der var tale om lovlige parodier eller karikaturer.

Højesteret fastslog først og fremmest, at der findes et parodiprincip i dansk ophavsret. Højesteret fremhævede, at en parodi som sit væsentligste kendetegn skal minde om et allerede eksisterende værk, men samtidig skal udvise synlige forskelle, så der ikke er risiko for forveksling. Dommen understregede desuden, at det ikke er et selvstændigt krav, at parodien skal have sin egen originale karakter. I den konkrete sag konkluderede Højesteret dog, at zombietegningen rent faktisk fremstod som en karikatur, der med sine forskellige elementer opfyldte kravene til at udgøre et selvstændigt værk.

Højesteret konkluderede, at tegningen tydeligt refererede til Den Lille Havfrue som et nationalt symbol og altså ikke Den Lille Havfrue som et kunstnerisk værk. Højesteret understregede, at tegningen klart havde karakter af en karikatur, der med sine forskellige elementer havde et formål, der var meget forskel-



Illustration: Mara Zengalite / Scandinavian StockPhoto

ligt fra det originale værk, og derfor var omfattet af parodiundtagelsen.

Hvad angik fotografiet, var det ikke et spørgsmål om, hvorvidt der var tale om en karikatur omfattet af parodiundtagelsen. Berlingske gjorde derimod gældende, at fotografiet var beskyttet af ytringsfriheden efter Den Europæiske Menneskerettighedskonventions artikel 10. Højesteret fastslog, at forskellige aspekter tages i betragtning for at afgøre, om en given ytring har samfundsmæssig betydning. Disse omfatter pressens centrale rolle i samfundet, det politiske indhold i udtrykket og den grundlæggende ret til kunstnerisk frihed. Der foretages en konkret vurdering af, om håndhævelsen af den påberåbte IP-rettilighed resulterer i en bredere indskrænkning af ytringsfriheden, end hvad der er nødvendigt i et demokratisk samfund.

Højesteret fastslog i den konkrete sag, at fotografiet var en del af pressens generelle dækning af et emne af samfundsmæssig interesse, og at brugen af værket ikke medførte urimelig skade for arvingerne. Højesteret fremhævede også, at det var Den Lille Havfrues symbolske værdi, som var afgørende, og ikke Den Lille Havfrue som kunstværk. På den baggrund konkluderede Højesteret, at fotografiet ikke gik længere, end formålet med artiklen kunne begrunde.

Efter en samlet vurdering konkluderede Højesteret, at hverken tegningen eller fotografiet af Den Lille Havfrue krænkede arvingernes ophavsret. Berlingske blev også frikendt for overtrædelse af lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«) § 3 om god markedsføringsetik, idet både tegningen og fotografiet var en del af Berlingskes redaktionelle arbejde.

Læs hele dommen her: https://domstol.fe1.tangora.com/media/-300016/files/24506-2022_Dom_til_hjemmesiden.pdf

Betegnelsen »legaltech« er for alle
Østre Landsret afsagde den 28. juni dom i sag BS-34153/2022-OLR mellem Legaltech ApS (»Legal-Tech«) og Legal IT ApS (»Legal IT«). Tvisten drejede sig om, hvorvidt Legal IT's brug af betegnelsen »LEGALTECH DENMARK« krænkede LegalTechs rettigheder i henhold til den danske lovbekendtgørelse nr. 88 af 29. januar 2019 (»varemærkeloven«) og den danske lovbekendtgørelse nr. 866 af 15. juni 2022 om markedsføring (»markedsføringsloven«).

Legal IT leverer legaltech-ydelser og rådgiver virksomheder om bl.a. GDPR og informationssikkerhed. På tilsvarende vis rådgiver i Legal-Tech om informationsteknologi.

Landsretten fastslog, at LegalTechs varemærkerettigheder til betegnelsen »LEGALTECH DENMARK« skulle fortolkes snævert. Landsretten fremhævede bl.a., at begrebet »legaltech« har et bredt anvendelsesområde og omfatter teknologier og digitale løsninger, der bruges inden for den juridiske branche. Brug af betegnelsen for ydelser, der har karakter af legaltech, eller som kendetegn for virksomheder, der udbyder sådanne ydelser, vil derfor ikke udgøre en krænkelse af LegalTechs varemærkeret.

Da LegalTech ikke havde godtgjort, at Legal IT havde anvendt den omtvistede betegnelse til andre formål end markedsføring af tjenesteydelser, der var inden for kernen af begrebet »legaltech« fandt Landsretten, at der ikke forelå nogen krænkelse af LegalTechs varemærkerettigheder. Endeligt fandt Landsretten, at LegalTech ikke kunne forhindre Legal IT's brug af betegnelsen »LEGALTECH DENMARK« i medfør af markedsføringsloven.

Læs hele Østre Landsrets dom her: <https://domstol.dk/media/1flbg-mbb/dombog.pdf>

Læs hele Sø- og Handelsrettens dom her: https://domstol.fe1.tangora.com/media/-300011/files/BS-37430-2021-SHR_Dom.pdf

[com/media/-300011/files/BS-37430-2021-SHR_Dom.pdf](https://domstol.fe1.tangora.com/media/-300011/files/BS-37430-2021-SHR_Dom.pdf)

Østre Landsret ophæver Sø- og Handelsrettens forbud i sag om varemærkekrænkelse

Østre Landsret afsagde den 7. juli 2023 kendelse i sag BS-10051/2023-OLR mellem Forza Fighting Gear BV (»Forza Fighting«) og EPC Alternative Source (»EPC«) over for Victor Rackets Ind. Corp (»Victor Rackets«) og Sports Group Denmark A/S. (»Sports Group«)

Sagen angik, om der var grundlag for at opretholde eller ophæve et overfor Forza Fighting og EPC nedlagt forbud mod at anvende ordet »FORZA« samt to ordkombinationer med ordet »FORZA« og dertilhørende figurmærker i forbindelse med salg og markedsføring af sportstøj og -udstyr i Danmark. Sø- og Handelsretten nedlagde det pågældende forbud den 25. januar 2023.

Ifølge lovbekendtgørelse nr. 1655 af 25. december 2022 (»den danske retsplejelov«) § 413, nr. 2, er det en betingelse for at meddele forbud, at den anmodende part sandsynliggør, at modpartens adfærd nødvendiggør et sådant forbud. Victor Rackets og Sports Group skulle således sandsynliggøre, at Forza Fighting og EPC's salgs- og markedsføringsaktiviteter, herunder navnlig anvendelsen af deres hjemmeside, medførte risiko for overtrædelse af Victor Racket og Sports Groups varemærkerettigheder.

Østre Landsret udtalte i den forbindelse, at det må vurderes fra sag til sag, om der er konkret tegn på, at udbud til salg på en hjemmeside, der er tilgængelig på et andet varemærkes område, også henvender sig til forbrugere på dette område.

I modsætning til Sø- og handelsretten mente Østre Landsret, at dette ikke var tilfældet, eftersom det ved bevisførelsen blev lagt til grund, at der ikke var foretaget salg til Danmark, og at der heller ikke var

udsigt til, at dette ville ske i fremtiden. Den omstændighed, at det havde været muligt at vælge Danmark som leveringssted på hjemmesiden, samt at der var foretaget nogle danske testkøb, som alle blev annulleret, var ikke tilstrækkeligt til at sandsynliggøre nødvendigheden af et forbud. Østre lagde herudover til grund, igen i modsætning til Sø- og Handelsretten, at der var indgået en sameksistensaftale om anvendelse af det registrerede varemærke »FORZA SPORTSWEAR«, og at parterne var bundet af denne.

Østre Landsret fandt det derfor ikke sandsynliggjort, at der var udsigt til, at Forza Fighting og EPC ville krænke Victor Rackets og Sports Groups varemærkerettigheder i Danmark.

Østre Landsret tiltrådte således Sø- og Handelsrettens mindretals vurdering, hvorved forbuddet blev ophævet.

Læs hele Østre Landsrets kendelse her: <https://domstol.dk/media/hx-knrylf/kendelse-bs100512023.pdf>

Læs hele Sø- og Handelsrettens kendelse her: https://domstol.fe1.tangora.com/media/-300011/files/BS-37996-2021-SHR_Kendelse.pdf

Animerede reklamer krænker ikke rettighederne til det danske landshold

Sø- og Handelsretten afsagde den 20. april 2023 dom i sag BS-26458/2022-SHR mellem Power A/S (»Power«) og DBU A/S samt DANSK BOLDSPIL-UNION (samlet »DBU«). Tvisten vedrørte dels om en række af Powers reklamer krænkede DBU's kommercielle rettigheder til det danske landshold, dels om visse udsagn, fremsat af DBU's kommercielle direktør, udgjorde en overtrædelse af lovbestemt nr. 866 af 15. juni 2022 (»den danske markedsføringslov«).

I forbindelse med fejringen af EM-slutrunden i 2021 lancerede Power tre forskellige reklamer under temaet »Den store fodboldfest«.

De omtvistede reklamer viste en jublende animeret figur iført en fodboldtrøje på et stadion, hvor flere fodboldspillere befandt sig i baggrunden. I en radioudsendelse vedrørende konflikten mellem parterne udtrykte den kommercielle direktør hos DBU kritik af Powers markedsføringsmetoder. Han påpegede bl.a., at Power tidligere havde været involveret i flere sager ved den danske Forbrugerombudsmand.

Sø- og Handelsretten fandt, at Powers reklamer ikke krænkede DBU's rettigheder til det danske fodboldlandshold. Det skyldtes, at reklamerne skildrede en generisk situation i en professionel fodboldkamp, som ikke skabte konkrete associationer til det danske fodboldlandshold. Retten lagde bl.a. vægt på, at de omstridte reklamer ikke indeholdt nuværende eller tidligere landsholdsspillere og at trøjens design var væsentligt forskellig fra den rød/hvide landsholdstrøjetrøjen. Endvidere fastslog retten, at detailvirksomheder generelt har ret til at markedsføre sig i forbindelse med store nationale begivenheder.

Med hensyn til udsagnene fremsat af DBU's kommercielle direktør, fandt Sø- og Handelsretten, at disse udtalelser ikke havde karakter af misrekommandering af Power. Desuden fandt retten, at udsagnene ikke kunne betragtes som aggressive eller utilbørlige i markedsføringsammenhæng.

Dommen er anket til Østre Landsret.

Læs hele Sø- og Handelsrettens dom her: [https://domstol.fe1.tangora.com/media/-300011/files/Dom_\(Power_mod_DBU\).pdf](https://domstol.fe1.tangora.com/media/-300011/files/Dom_(Power_mod_DBU).pdf)

Krænkelse af personlighedsretten ved brug af prominente sportsudøvere på Facebook og Twitter

Sø- og Handelsretten afsagde den 8. maj 2023 dom i sag BS-968/2022-SHR mellem Spillerforeningen, som mandatar for en lang række kendte danske fodboldspil-

re (heriblandt Christian Eriksen, Lasse Schöne, Kasper Schmeichel og Simon Kjær), Danske Elite-sportsudøveres Forening, som mandatar for Viktor Axelsen, og Håndbold Spiller Foreningen, som mandatar for Mikkel Hansen, mod Hillside (New Media Malta) Plc, der står bag bettingsitet Bet365 (»Bet365«).

I perioden fra februar 2019 til marts 2021 havde Bet365 offentliggjort indhold på Facebook og Twitter, der afbildede sportsudøverne i aktion med tilhørende beskrivelser. Dette skete oftest i forbindelse med større sportsbegivenheder. Eksempelvis delte Bet365 i forbindelse med semifinalen i Champions League i 2019 et opslag på Facebook med teksten: »Hvilken dansker håber du at se i Champions League finalen? Lasse Schöne eller Christian Eriksen«. I kommentarsporet til opslaget linkede Bet365 til deres bettingsite, hvor det var muligt at placere væddemål på kampen.

Spørgsmålet var således, hvorvidt Bet365 lovligt kunne bruge billeder og navne på sportsudøverne på Facebook og Twitter uden deres forudgående tilladelse. Navnlig om billedernes brug kunne betegnes som legitim redaktionel anvendelse, eller om der var tale om ulovlig kommerciel brug.

Personlighedsretten sikrer enhver mod ulovlig brug af ens navn og billede. På baggrund af lovbestemt nr. 866 af 15. juni 2022 (»den danske markedsføringslov«) § 3, stk. 1 om god markedsføringsetik, og særligt almindelige retsgrundsætninger, der blev fastslået i Buster Larsen-dommen (U.1965.126H), kan det udledes, at enhver har ret til selvstændigt at bestemme i hvilket omfang og med hvilket formål ens navn og billede benyttes kommercielt.

I den konkrete sag kom Sø- og Handelsretten efter en samlet vurdering frem til, at opslagene indhold var prægede af en kommerciel

hensigt. Sø- og Handelsretten fremhævede særligt et vidneudsagn, der konkluderede, at flere opslag tydeligt reklamerede for betting. Sø- og Handelsretten påpegede også, at den overordnede beskrivelse af Bet365's Facebook-side indikerede muligheden for en startbonus for nye kunder, hvilket indikerede det kommercielle islæt.

Idet indholdet blev betragtet som kommercielt, og eftersom sportsudøverne ikke havde givet samtykke til brug af deres billeder, blev det konkluderet, at der var sket en krænkelse af sportsudøvernes rettigheder til deres eget billede og navn.

Sø- og Handelsretten vurderede, at sportsudøverne normalt ville have modtaget en betaling på 50.000 kr. for opslagene. Bet365 blev derfor pålagt at betale 50.000 kr. for hvert opslag.

Bet365 har anket dommen til Østre Landsret.

Læs hele Sø- og Handelsrettens dom her: https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-968-2022-SHR.pdf

Gyldigt patent medfører midlertidigt forbud og påbud

Sø- og Handelsretten afsagde den 15. juni 2023 kendelse i sagen BS-45856/2022-SHR anlagt af Novartis AG, Novartis Pharma AG og Novartis Healthcare A/S (»Novartis«) mod Viatrix ApS (»Viatrix«).

Omdrejningspunktet for sagen var, hvorvidt der skulle nedlægges midlertidigt forbud og påbud overfor Viatrix på baggrund af en påstået krænkelse af Novartis' patentret til lægemidlet fingolimod til behandling af multipel sklerose (»Stridspatentet«). Viatrix gjorde i sagen gældende, at Stridspatentet var ugyldigt.

Det skulle i sagen afgøres, hvorvidt Viatrix på tilstrækkelig vis svækkede Stridspatentets gyldighedsformodning, herunder om Stridspatentet manglede basis og nyhed, hvorefter der ikke ville kunne nedlægges forbud og påbud, jf.

kapitel 40 i lovbekendtgørelse nr. 1655 af 25. december 2022 (»den danske retsplejelov«).

For så vidt angår Stridspatentets manglende basis fandt Sø- og Handelsretten, at der ikke var grundlag for at tilsidesætte Den Europæiske Patentmyndigheds vurdering om, at Stridspatentet opfyldte betingelserne i Den Europæiske Patentkonventions artikel 76, stk. 1 og artikel 123, stk. 2 om basis. Dels blev dette begrundet i, at der i sagen bestod en gyldighedsformodning baseret på Den Europæiske Patentmyndigheds udstedelse af patentet, dels at kravet om, at den tekniske effekt skal være »opnået eller plausibel« ikke indgår i vurderingen af basis for kravændringer, hvorfor dette ikke var relevant i nærværende sag.

For så vidt angår Stridspatentets manglende nyhed fandt Sø- og Handelsretten, at Novartis' tidligere pressemeddelelse af 6. april 2006 samt præsentation af 21. juni 2005 ikke bevirkede, at Stridspatentet manglede nyhed. Retten fastslog, at en fagmand ikke ville kunne anvende metoden fra Stridspatentet (grundet kravet om »enablement«), da pressemeddelelsens indhold ved offentliggørelsen ikke indikerede, at behandlingen havde en effekt.

Sø- og Handelsretten fandt således samlet, at Viatrix ikke i tilstrækkelig grad havde svækket formodningen om, at Stridspatentet var gyldigt, samt at Novartis netop havde sandsynliggjort, at de havde den rettighed, som blev søgt beskyttet jf. den danske retsplejelovs § 413, nr. 1. På baggrund heraf fandt retten, at betingelserne i den danske retsplejelovs § 413 for at nedlægge midlertidigt forbud og påbud således i det hele var opfyldt. Følgelig kunne der mod Novartis' sikkerhedsstillelse nedlægges midlertidigt forbud og påbud overfor Viatrix' kommercielle anvendelse af Fingolimod.

Læs hele Sø- og Handelsrettens kendelse her: https://domstol.fe1.tangora.com/media/-300011/files/BS-45856-2022-SHR_Kendelse.pdf

Byretten: Forbrugslån må ikke markedsføres som kassekreditter

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) oplyste i en pressemeddelelse den 7. juli 2023, at kviklånselskabet 4Finance (vivas.dk) for nyligt blev idømt en bøde på 1 mio. kr. for vildledende markedsføring. Københavns Byret afgjorde, at virksomheden ved at markedsføre almindelige forbrugslån som kassekreditter, selvom der var tale om almindelige forbrugslån, havde vildledt forbrugerne. Byretten afgjorde endvidere, at virksomheden havde undladt at oplyse om den månedlige ydelse i markedsføringen af kreditaftalerne.

I 2019 politianmeldte Forbrugerombudsmanden 4Finance, bl.a. grundet virksomhedens markedsføring af kreditaftaler med betegnelsen »kassekredit« på sin hjemmeside vivas.dk. Dette udgjorde ifølge Forbrugerombudsmanden mod vildledende markedsføring, da der netop ikke var tale om kassekreditter, men derimod almindelige forbrugslån. Reglerne for kassekreditter er mere lempelige end for almindelige forbrugslån og ifølge Forbrugerombudsmanden var der således tale om forsøg på omgåelse af lovgivningen.

For så vidt angår kassekreditspørgsmålet udtalte byretten bl.a. at »tiltalte ved sin markedsføring har fremkaldt en forkert forventning hos gennemsnitsforbrugere om, at det udbudte låneprodukt var en kassekredit, ligesom tiltaltes handelspraksis har gjort det svarere for gennemsnitsforbrugeren at sammenligne priser fra forskellige udbydere, idet gennemsnitsforbrugeren blev vildledt omkring låneproduktets art og væsentligste egenskaber.«

Endvidere blev 4Finance fundet skyldig i manglende oplysning af den månedlige ydelse på de markedsførte kreditaftaler.

Forbrugerombudsmand Christina Toftgaard Nielsen udtalte:

»Dommen bidrager til at skabe klarhed, om hvorvidt et lån er en kassekredit eller ej. Det er vigtigt, fordi der gælder lempeligere regler for kassekreditter end for for-

brugslån. Det er mit indtryk, at der er virksomheder, som forsøger at udnytte de lempeligere regler ved at kalde deres forbrugslån for kassekreditter, og jeg forventer, at de ophører med det nu.»

Læs Forbrugerombudsmandens pressemeddelelse her: <https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2023/byretten-forbrugslaan-maa-ikke-markedsfoeres-som-kassekreditter/>

Bøde for skjult reklame i flere Facebook-opslag, der har til formål at få forbrugere til at investere

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) oplyste i en pressemeddelelse den 22. juni 2023, at Retten i Roskilde har idømt indehaveren af en enkeltmandsvirksomhed en bøde på 30.000 kr. for overtrædelse af reglerne i lovbekendtgørelse nr. 866 af 15. juni 2022 (»den danske markedsføringslov«) om skjult reklame ved at have markedsført virksomheder på Facebook.

Forbrugerombudsmanden politianmeldte indehaveren i marts 2021. For nyligt blev indehaveren dømt for i perioden november 2018 til maj 2020 at have markedsført en række opslag på Facebook uden tydeligt at oplyse, at der var tale om reklame. Nærmere præcist var der tale om 16 Facebook-opslag, som indehaveren ikke havde markeret tydeligt som reklame. Retten udtalte, at opslagene havde til formål at påvirke læserne af opslagene til at foretage investeringsmæssige dispositioner.

Retten fastslog, at indehaveren ved at have lavet et opslag, en kommentar til et opslag og en meningsmåling havde reklameret for at investere i virksomhederne. Retten fandt også, at der var en kommerciel hensigt med opslag, som ifølge

indehaveren ikke var omfattet af indehaverens aftaler med virksomhederne. Ydermere fastslog retten, at oplysningen om, at et opslag udgør reklame, skal placeres indledningsvist, således at forbrugeren, når denne vælger at læse indholdet, er klar over, at der er tale om reklame. Retten fandt, at ord som »i samarbejde med« eller »sponseret af« ikke udgjorde en klar oplysning om, at opslagene var reklame.

I henhold til den danske markedsføringslovs § 6, stk. 4, skal erhvervsdrivende klart oplyse den kommercielle hensigt med enhver form for handelspraksis, herunder reklame. Heri ligger, at man, uanset medium, skal oplyse, hvis der er kommercielle interesser bag en omtale af virksomheder eller produkter. Dette skal fremgå klart af opslaget og desuden være tydeligt for modtagerne, så modtagerne er klar over det, før de ser nærmere på opslaget.

Forbrugerombudsmanden Christina Toftegaard Nielsen udtalte: *»Det skal fremgå meget klart, når der reklameres for at investere i en eller flere virksomheder på de sociale medier. Man må ikke være i tvivl, når man ser opslaget. Retten har fastslået, at det ikke er nok at skrive „i samarbejde med“ eller „sponseret af“.«*

Læs Forbrugerombudsmandens pressemeddelelse her: <https://www.forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2023/boede-for-skjult-reklame-i-flere-facebook-opslag-der-havde-til-formaal-at-faa-forbrugere-til-at-investere/>

Ny dansk ophavsretslov vedtaget

Den 1. juni 2023 vedtog det danske Folketing den danske lov nr. 680 af 06. juni 2023 om ændring af lov om ophavsret. Loven har til formål at implementere den resterende del af

Europa-Parlamentets og Rådets direktiv 2019/790 af 17. april 2019 om ophavsret og beslægtede rettigheder på det digitale indre marked, der ikke blev dækket af den danske lov nr. 2607 af 28. december 2021 om ændring af lov om ophavsret. Målet med loven er at modernisere ophavsretten, så lovgivningen følger med udviklingen af digitale teknologier, især den øgede adgang til ophavsretligt beskyttet materiale via internettet.

Loven søger at styrke kunstnerens position i forhold til aftaler indgået med producenter og streamingtjenester. Loven indfører en ny § 11 b, der er særligt relevant ift. nye AI-modeller, der bruger beskyttede værker som træningsdata. Efter bestemmelsens stk. 2 er det tilladt at foretage tekst- og datamining med mindre rettighedshaveren aktivt har frabedt sig denne brug.

Samtidig giver loven øget adgang for biblioteker, museer og andre institutioner til at benytte materiale fra deres samlinger, såsom plakater, bøger og tidsskrifter, der ikke længere er i handel. Med loven bekræftes den danske aftalelicensmodel, hvilket gør det nemmere at opnå tilladelser til masseudnyttelse, hvor flere rettighedshavere er involveret.

Den nye lov trådte i kraft den 7. juni 2023.

Læs hele lovforslaget som vedtaget her: *Til lovforslag nr. L 125, Folketinget 2022-23 (2. samling), Forslag til Lov om ændring af lov om ophavsret (Gennemførelse af dele af direktiv om ophavsret og beslægtede rettigheder på det digitale indre marked) (ft.dk)*

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



simonsen vogtviig

Hedda Baumann Heier og Henning Wahlberg

Høyesterett avsier dom om vederlagsberegning for bruk av vernet musikk

Høyesterett avsa dom den 12. juni 2023 i en sak om vederlagsberegning mellom TONO og Stiftelsen Oslo-Filharmonien. TONO er en kollektiv organisasjon som forvalter opphavsrett til musikkverk på vegne av sine medlemmer. Oslo-Filharmonien er et norsk symfoniorkester. For offentlig fremføring av vernet musikk fra TONOs repertoar i konserter må Oslo-Filharmonien betale et vederlag til TONO. Saken gjaldt beregningen av dette vederlaget.

Bakgrunnen for saken er at TONO har en egen konserttariff som beregner vederlag ut fra bruttoinntekter per konsert. TONO har imidlertid også hatt særskilte avtaler med fire større norske orkestre, herunder Oslo-Filharmonien. TONO sa opp sin avtale med Oslo-Filharmonien med virkning fra 2016, uten at partene klarte å enes om en ny avtale. Oslo-Filharmonien har krevd å betale vederlag etter den alminnelige konserttariffen, mens TONO har motsatt seg en slik modell. TONO har krevd at Oslo-Filharmonien skal betale et årlig beløp som utgjør 0,55% av Oslo-Filharmoniens billettinntekter og tildelt statstilskudd per år, og der prosent-satsen justeres forholdsmessig hvis omfanget av relevante fremføringer er større eller mindre enn en viss størrelse. En sentral forskjell mellom den vederlagsmodellen Oslo-Filharmonien ønsket og den TONO ønsket, var altså at vederlaget etter førstnevnte modell ble beregnet på bakgrunn av billettinntektene ved hver konsert, mens sist-

nevnte modell også tok i betraktning den statsstøtten som Oslo-Filharmonien mottar.

Spørsmålet for Høyesterett var om TONOs vederlagsmodell oppfyller kravene i lov om kollektiv forvaltning av opphavsrett mv. § 28. Denne bestemmelsen sier at lisensvilkår skal baseres på «objektive og ikke-diskriminerende» kriterier, og at vederlaget skal være «rimelig».

Høyesterett startet den konkrete vurderingen med å konstatere at konserttariffen er den alminnelige modellen for å beregne vederlag for bruk av vernede musikkverk i konsertvirksomhet og at den modellen som TONO krevde skulle gjelde for Oslo-Filharmonien avviker fra dette, både med hensyn til beregningsgrunnlag, prosentandel, justeringsfaktor og sluttsum. Dette illustreres ved at differansen mellom de to modellene for årene 2018-2020 var nærmere 1,7 millioner kroner.

Lov om kollektiv forvaltning av opphavsrett m.m. krever som nevnt at vilkårene for beregningen av vederlaget er «objektive og ikke-diskriminerende». Ettersom det forelå en forskjellsbehandling, vurderte deretter Høyesterett om det var gitt en objektiv begrunnelse for forskjellsbehandlingen.

Begrunnelsen til TONO for forskjellsbehandlingen var at det skal legges vekt på statstilskudd ved fastsetting av vederlaget. Høyesterett fant at dette kriteriet etterlot flere åpne spørsmål med hensyn til konkret hvordan det påvirker vederlaget, og at vilkårene i stor utstrekning syntes å være basert på individuelle vurderinger knyttet til sær egne forhold hos

Oslo-Filharmonien. Videre fant Høyesterett at den alminnelige konserttariffen samsvarer bedre med formålet i forarbeidene om at den mest nøyaktige beregningsmodellen skal foretrekkes.

Høyesterett kom dermed til at kravene til objektivitet og ikke-diskriminering ikke var oppfylt. Vederlagsmodellen som TONO krevde skulle gjelde for Oslo-Filharmonien derfor ikke kunne tas til følge, og TONOs anke ble forkastet. Høyesterett fant det ikke nødvendig å gå inn på kriteriet om vederlaget var «rimelig».

Høyesterett utelukker imidlertid ikke i avgjørelsen at en vederlagsmodell der statstilskuddet inngår kan begrunnes på en måte som oppfyller kravene i lov om kollektiv forvaltning av opphavsrett, men Høyesterett gikk ikke nærmere inn på dette, ettersom TONOs kriterier uansett var for generelle og skjønnsmessige til å begrunne en forskjellsbehandling.

Les hele avgjørelsen med saksnummer HR-2023-1077-A i Lovdatabasen.

Dom fra Oslo tingrett om manglende kreditering av fotograf i digitalmarkedsføring

Saken stod mellom K19 Foods AS (K19), som eier flere restauranter, og en fotograf. Dom ble avsagt 23. juni 2023 og har saksnummer 23-010693TVI-TOSL/05.

I 2021 inngikk partene avtale om at fotografen (gjennom sitt selskap Visuella) skulle lage en bildebank med fotografier av mat, drikke m.m. til bruk blant annet på sosiale medier. Avtalen spesifiserte at ved pu-

blisering av bilder på sosiale medier skal fotograf nevnes på en spesifikk måte («Foto: Visuella med tagg»).

K19 benyttet senere flere bilder uten å tagge/kreditere fotografen – i alt 37 ulike bilder som ble publisert til sammen 83 ganger, noe som ikke var omstridt. Spørsmålet for tingretten gjaldt erstatning for denne manglende krediteringen.

Retten fant at dette utgjorde et kontraktsbrudd som gir grunnlag for økonomisk tap etter alminnelige kontraktsrettslige regler. Retten vurderte imidlertid også om dette kunne utgjøre et brudd på åndsverkloven § 5, som sier at opphaver har krav på å bli navngitt når et åndsverk gjøres tilgjengelig for allmennheten (regelen gjelder også for den som lager et fotografisk bilde jf. åndsverkloven § 23 fjerde ledd jf. § 5). Det kunne i så fall ha betydning for erstatningsutmålingen, ettersom åndsverkloven § 81 gir rettighetshaveren krav på flere alternativer for å utmåle erstatning eller vederlag.

Åndsverkloven § 5 gir opphaveren krav på å bli navngitt slik som «god skikk tilsier». Spørsmålet var dermed om god skikk tilsier at fotografens navn skal framgå hver gang markedsføringsmateriell som inneholder foto vises frem. Retten viste til at mye markedsføringsmateriell ikke inneholder opplysninger på selve reklamen om hvem som er fotograf, og at en slik hovedregel vil kunne vanskeliggjøre formålet med markedsføring. Retten fant dermed at det ikke forelå noe brudd på åndsverkloven § 5.

Erstatningsutmålingen måtte altså bero på alminnelige kontraktsrettslige regler.

Fotografen anførte at utmålingen måtte ta utgangspunkt i den antatte verdien av markedsføringen, og la ned påstand om erstatning oppad begrenset til 166.000 kr. Kontraktsverdien var 12.500 kr.

Retten fant at det beste grunnlaget var fotografens egne opplysninger om hvordan hun priset tilbud med og uten betingelsen om å kre-

diteres. Fotografen opplyste at hun tok dobbel pris for bilder uten krediteringsklausulen. Retten la dette til grunn, og viste til at som nyetablert bedrift var verdien av å bli kreditert høy. Ettersom kontraktssummen var 12.500 kr, ble derfor også vederlaget for den manglende krediteringen fastsatt til 12.500 kr.

Fotografen la også ned påstand om at K19 måtte pålegges å kreditere fotografen ved fremtidig bruk. Ettersom retten fant at fotografens krav på kreditering måtte baseres på kontrakten (og ikke åndsverkloven § 5), kunne ikke fotografen få medhold i påstanden ettersom påstanden hadde en annen ordlyd enn det kontrakten fastslo.

Les hele avgjørelsen med saksnummer TOSL-2023-10693 i Lovdatas database.

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



Illustrasjon: Colourbox.com



Wikström
& PARTNERS

Christina Wikström

Ny vägledning från eSam om utkontraktering

eSamverkansprogrammet (eSam) har i juli 2023 publicerat en ny uppdaterad vägledning om outsourcing, *Utkontraktering – sekretess och dataskydd* (ES2023-06). eSam består av 36 svenska myndigheter som samarbetar kring digital utveckling och publicerar löpande rättsliga uttalanden, vägledningar och it-avtalsvillkor på www.esamverka.se.

Den uppdaterade vägledningen har tagits fram mot bakgrund av utvecklingen på dataskyddsområdet och den nya sekretessbrytande bestämmelsen i 10 kap. 2 a § offentlighets- och sekretesslagen (2009:400) (OSL) som trädde i kraft den 1 juli 2023.¹ Den uppdaterade vägledningen ersätter en tidigare vägledning² på samma ämne och ger en allmän orientering om de rättsliga överväganden som en myndighet behöver göra vid en utkontraktering.

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

2 Outsourcing 2.0 – En vägledning om sekretess och dataskydd.



Illustration: Colarbox.com

Fokus i vägledningen ligger på sekretess och dataskydd, men även andra rättsområden som handlingars offentlighet, it-avtalsrätt och informationssäkerhet behandlas. Stort utrymme i vägledningen lämnas åt en beskrivning av den nya sekretessbrytande regeln i 10 kap. 2 a § OSL, begreppet ”endast teknisk bearbetning eller teknisk lagring” och den

olämplighetsbedömning som ska genomföras i samband med uppgifternas utlämnande i enlighet med den nya sekretessbrytande regeln.

Christina Wikström, advokat och partner verksam vid Wikström & Partners Advokatbyrå i Stockholm och specialiserade på IT, IP och dataskydd.



Selmer

Maren Tveten og André Istad Johansen

Endringer i innleiereglene – misforståelser og frykt for feilvurderinger skaper utfordringer for IT-bransjen

1. innledning

I april 2023 fikk vi en rekke endringer i arbeidsmiljøloven knyttet til reglene om innleie. Lovendringene skal styrke vernet om faste ansettelser i norsk arbeidsliv.

Etter at endringene ble innført er innleie av arbeidskraft til prosjektarbeid og annet arbeid av midlertidig karakter, med noen viktige unntak, ikke lenger tillatt. Som følge av denne innstramningen mente lovgiver det var behov for å tydeliggjøre grensen mellom innleie som reguleres av de strenge reglene i arbeidsmiljøloven, og oppdragsavtaler/entrepriser, som faller utenfor arbeidsmiljøloven. Det ble derfor vedtatt en ny bestemmelse i arbeidsmiljøloven § 14-12 (5) som er ment å klargjøre det rettslige skillet mellom innleie og oppdrag. Bestemmelsen innebærer en viss innskjerping sammenlignet med tidligere rettstilstand.

Endringene i innleiereglene har ført til fornyet fokus på grensen mellom oppdragsavtaler og innleie innenfor en rekke tjenesteytende næringer, inkludert i IT-bransjen.

Historisk har ansvarsdelingen i IT-kontrakter vært konsentrert rundt ytterpunktene, hvor det enten skal leveres en på forhånd

entydig og spesifisert løsning, eller det skal leveres en ren innsatsforpliktelse. I dag leveres komplekse IT-prosjekter normalt etter agile/smidige gjennomføringsmodeller, hvor fordeling av ansvar og risiko på en tenkt skala ligger et sted imellom de tradisjonelle ytterpunktene resultatansvar og bistand. Denne måten å strukturere avtaleverk og prosjekter på, kan i enkelte tilfeller gjøre det vanskelig å avgjøre om man har å gjøre med en oppdragsavtale eller innleie.

” Etter vår oppfatning kan det imidlertid ikke være slik at endringene i arbeidsmiljøloven skal få den effekt at alle IT-prosjekter basert på agil/smtidig metodikk vil falle innenfor arbeidsmiljølovens innleieregler. Det må skje en konkret vurdering av det enkelte avtaleforhold.

Grensedragningen har blitt ytterligere komplisert etter endringene i arbeidsmiljøloven. Etter lovendringene ser vi en trend der mange kjøpere av IT-tjenester stiller ulike typer krav til leverandørene i et forsøk på å redusere egen risiko for brudd på innleiereglene, eksempelvis ved å kreve at leverandøren følger reglene om innleie selv om det er snakk om tjenesteleveranser som kunne vært klassifisert som oppdrag utenfor arbeidsmiljøloven.

Etter vår oppfatning kan det imidlertid ikke være slik at endringene i arbeidsmiljøloven skal få den effekt at alle IT-prosjekter basert på agil/smtidig metodikk vil falle innenfor arbeidsmiljølovens innleieregler. Det må skje en konkret vurdering av det enkelte avtaleforhold.

I denne artikkelen skal vi se nærmere på hvilke momenter som er relevante ved vurderingen av om IT-prosjekter som skjer etter agile gjennomføringsmodeller skal klassifiseres som oppdrag eller innleie. Vi skal også se nærmere på konsekvensene av å basere seg på at en tjenesteavtale må følge reglene om innleie.

2. Vurdering av IT-prosjekter opp mot terskelen for innleie

2.1 Nærmere om

arbeidsmiljøloven § 14-12 (5)

Den nye bestemmelsen i arbeidsmiljøloven § 14-12 (5) trekker opp grensen mellom oppdragsavtaler på den ene siden, og innleie av arbeidskraft på den andre siden. Den nye bestemmelsen har følgende ordlyd:

“Ved vurderingen av om en oppdragsavtale mellom to virksomheter innebærer innleie, skal det særlig legges vekt på om oppdragsgiver har ledelsen av arbeidet og ansvar for resultatet. Andre relevante forhold er blant annet om det i hovedsak skal leveres arbeidskraft, om arbeidet skjer i nær tilknytning til oppdragsgivers virksomhet, om arbeidet dekker et vedvarende arbeidskraftbehov hos oppdragsgiver og om arbeidet skjer innenfor oppdragsgivers kjerne- eller hovedaktivitet.”

Bestemmelsen angir to hovedkriterier og fire tilleggsmomenter som skal vektlegges ved vurderingen av om det foreligger innleie. Hovedkriteriene om *arbeidsledelse* og *ansvar for arbeidsresultatet* innebærer en lovfesting av gjeldende rett. Tilleggsmomentene kan også delvis utledes av gjeldende rett.

Bestemmelsen innebærer likevel en endring i forhold til tidligere rettsstilstand. Før lovendringen var de to hovedkriteriene avgjørende for vurderingen. Ifølge rettspraksis skulle de øvrige momentene mest tjene som sperre mot forsøk på omgåelser. Etter lovendringen er tilleggsmomentene gitt større betydning, særlig når det gjelder avtaler hvor arbeidskraft utgjør det bærende elementet i leveransen.

I forarbeidene til bestemmelsen fremgår det at dersom alle tilleggsmomentene er oppfylt, taler det for at¹:

“... kontrakten bør klassifiseres som innleie, også i de tilfellene oppdragstaker har ansvar for arbeidsledelsen og/eller arbeidsresultatet.”

Det fremgår videre at² tilleggsmomentene vil:

“... være av særlig betydning for å avklare om oppdragsavtalen utfordrer lovens formål om trygge ansettelsesforhold på en slik måte at oppdragsavtalen bør omfattes av de strengere reglene om innleie.”

Det er særlig den lovforståelsen som følger av ovennevnte uttalelser som vil lede til en viss innskjerping sammenlignet med tidligere rettsstilstand. Det har vært en bevegelse fra at de to hovedkriteriene er avgjørende, til at det har blitt en mer sammensatt vurdering.

2.2 De ulike momentene som inngår i helhetsvurderingen

2.2.1 Ledelsen av arbeidet

Det første hovedkriteriet i vurderingen av om en tjenestekjøpsavtale mellom to virksomheter innebærer innleie er om det er leverandøren eller kunden som *utøver arbeidsledelsen*. Dersom kunden kontrollerer og leder leveransen av leverandørens tjenester og enkeltpersoner, vil det være et moment som taler for innleie.

I vurderingen av hvem som utøver arbeidsledelsen, er det blant annet relevant hvem som er ansvarlig for den faglige ledelsen av prosjektet og ressursene. Det er også av betydning hvem som er ansvarlig for å sette sammen team og finne en erstatter dersom en konsulent slutter eller av andre grunner tas ut av et oppdrag. Et annet element er om det er kunden eller leverandø-

ren som har de administrative arbeidsgiver- og ledelsesfunksjonene overfor egne ansatte, herunder ansvar for å kontrollere arbeidstiden, innvilge permisjoner, drive sykefraværsoppfølging osv.

Dersom det i all hovedsak er leverandøren som er ansvarlig for å utføre denne typen oppgaver, tilsier det at det er leverandøren som i det vesentlige utøver reell styring og arbeidsledelse over egne ansatte. Dette vil i så fall være et moment som taler imot klassifisering som innleie.

2.2.2 Ansvar for resultatet

Når det gjelder det andre hovedkriteriet, hvem som har *ansvaret for resultatet*, er det sentrale å fastslå hvilken risiko og hvilket ansvar leverandøren påtar seg gjennom kontraktsforholdet. Dersom leverandøren har ansvaret for resultatet, taler det for at foreligger et reelt oppdragsforhold, og ikke innleie. Derom leverandøren ikke har forpliktet seg til noe mer enn en innsatsforpliktelse, er det et argument i motsatt retning.

Ved vurderingen av dette momentet er det avgjørende å forstå den kontrakts- og prosjektmetodikk som ligger til grunn for de fleste komplekse IT-prosjekter. Avtalene som inngås er normalt omfattende, nettopp som følge av kompleksiteten i de tjenestene kunden kjøper. Ved vurdering av de forpliktelser leverandøren er underlagt må hele avtaleverket ses under ett, inkludert eventuelle konkurransegrunnlag, rammeavtaler, og de underliggende avropsavtaler for det enkelte oppdrag. Selv om SSA-B eller lignende avtaler er utgangspunktet, vil disse gjennom den konkrete reguleringen i bilag etc. kunne resultere i en annen ansvars- og risikofordeling enn hva tilfellet er ved en tradisjonell bistandsavtale.

Dersom avtaleverket inneholder klare forventninger om gjennomføring etter konkrete modeller og oppnåelse av definerte mål, taler det

1 Prop. 131 L 2021-2022 s. 47.

2 Prop. 131 L 2021-2022 s. 45.

for at leverandøren har en resultatforpliktelse. Tilsvarende gjelder der kunden kan gjøre gjeldende misligholdsbeføyelser, inkludert krav om erstatning. Det er også relevant å se hen til om leverandøren har tegnet ansvarsforsikring som dekker ansvar ved brudd på kontraktsforpliktelser.

Det følger videre av lovforarbeidene at det taler for oppdragsforhold når det angis tydelige kvalitetskrav til den tjenesten som skal leveres³, slik som krav til helhetlig arkitektur, sikkerhet, kompatibilitet, skalerbarhet og innebygget personvern. Mer generelle krav, slik som at leverandøren plikter å utføre oppdraget profesjonelt, effektivt og med høy faglig standard, er også relevante i vurderingen.

Det forhold at avtaleverket åpner for endringer underveis kjennetegner iterative/agile IT-prosjekter. Slike endringsmekanismer kan ikke være diskvalifiserende for klassifisering som oppdragsforhold. En slik lovtolking har også støtte i forarbeidene⁴, som angir at selv om hyppige endringer i arbeidsoppgaver i løpet av avtaleperioden kan tale for innleie, betyr ikke dette at det ikke kan foretas endringer i en oppdragsavtale underveis.

2.2.3 Om det i hovedsak leveres arbeidskraft

Det vil være et moment som trekker i retning av innleie dersom et oppdrag i hovedsak består i å levere arbeidskraft. Dersom en slik leveranse likevel skal anses som oppdragsforhold bør avtalen, etter lovgivers syn, inneholde tydelige elementer av at det foreligger en resultatforpliktelse og at det skal leveres noe mer enn arbeidskraft og den kompetansen leverandørens ansatte besitter.

Et element ved denne vurderingen er om leverandørens leveranse bare omfatter en forpliktelse til å

stille et bestemt antall kvalifiserte arbeidstakere til kundens disposisjon, eller om den utgjør en mer komplett tjenesteleveranse. Sentralt i så henseende er om leverandøren leverer tjenester basert på en opparbeidet system-/strukturkapital, altså om den samlede organisasjonens kompetanse og erfaring er strukturert og systematisert gjennom for eksempel metodeverk, standardiserte prosesser, opplæringsystemer, egne IT-systemer mv. som setter leverandøren i stand til å levere den komplette tjenesten kunden etter spør. En slik komplett tjenesteleveranse krever noe langt mer fra leverandøren enn bare å stille med kvalifisert personell basert på kundens kravspesifikasjon, og vil være et moment som taler imot innleie.

Det er også relevant om det er leverandøren eller kunden som stiller utstyr mv. til disposisjon ved gjennomføring av oppdraget. Det faktum at leverandørens ansatte jobber på kundens utstyr der dette anses nødvendig av hensyn til leveransen og/eller eksempelvis sikkerhetsmessige årsaker, kan likevel ikke tillegges avgjørende betydning ved klassifiseringen av en tjenesteleveranse innen IT-sektoren. Her vil selve leveransen i de fleste tilfeller nettopp måtte utføres i kundens egne systemer og med hjelp av kundens utstyr, uten at dette i seg selv må bety at det er snakk om innleie.

2.2.4 Om arbeidet skjer i nær tilknytning til oppdragsgivers virksomhet

Et annet moment som kan trekke i retning av innleie er at arbeidet skjer i nær tilknytning til kundens virksomhet. Dersom arbeidet som utføres like gjerne kunne vært utført av kundens egne ansatte, kan det ifølge forarbeidene være en indikasjon på at aktiviteten skjer i nær tilknytning til kundens virksomhet.

I en del IT-prosjekter er det imidlertid en forutsetning eller forventning fra kunden at leverandørens team, i alle fall i perioder, utfører oppdraget fra kundens lokasjo-

ner. Isolert sett vil dette tale for innleie.

Det må likevel kunne legges vekt på at gjennomføringen av moderne IT-prosjekter i praksis skjer på en måte som krever samhandling med kunden og derfor også hel eller delvis tilstedeværelse på kundens lokasjoner. Forarbeidene uttaler også at oppdragsavtaler som gjennomføres "on-site" fortsatt vil være en naturlig og legitim del av norsk arbeidsliv⁵. Det er derfor først og fremst i de tilfeller der arbeid "on-site" utfører lovens formål om trygge ansettelsesforhold at momentet vil ha betydning i tvilstilfeller.

2.2.5 Om oppdraget dekker et vedvarende arbeidskraftsbehov hos oppdragsgiver

Ved vurderingen skal det også legges vekt på om leverandøren leverer tjenester som dekker et vedvarende arbeidskraftsbehov hos kunden. I så fall vil det tale for at kontrakten bør klassifiseres som innleie.

Særlig relevant i den forbindelse er om oppdraget er tidsbegrenset eller ikke. Dersom en leverandør utfører oppdrag under tidsbegrensete kontrakter, vil det naturlig nok tale imot at oppdraget dekker et vedvarende arbeidskraftsbehov. Eksempelvis er statens standardavtaler tidsbegrensete med mindre det gjøres endringer i den generelle avtaleteksten. Kunden vil som regel ha rett til forlengelse, men en slik rett er også tidsbegrenset. At et oppdrag har en definert start og slutt vil altså være et moment i retning av at det ikke er tale om innleie.

2.2.6 Om arbeidet skjer innenfor oppdragsgivers kjerne- eller hovedaktivitet

Det siste momentet som inngår i arbeidsmiljøloven § 14-12 (5) er om arbeidet skjer innenfor kundens kjerne- eller hovedaktivitet. Det taler for oppdragsforhold dersom det arbeid leverandøren utfører skiller

3 NOU 2021:9 s 304

4 NOU 2021:9 s 304

5 NOU 2021:9 s. 304

seg fra det kundens egen arbeidsstyrke arbeider med, mens det taler for innleie dersom arbeidet skjer innenfor kundens kjerne- eller hovedaktivitet. I forarbeidene⁶ uttaler departementet følgende om dette momentet:

“For private virksomheter vil kjerne- eller hovedaktiviteten som regel være det virksomheten tjener penger på. For offentlige virksomheter vil det være relevant å se hen til hvilken aktivitet som oppfyller samfunnsoppdraget. Det kan i alle tilfeller være relevant å se hen til hvilken del av virksomheten det investeres mest tid og ressurser i, herunder andelen av den samlede arbeidsstokken som utfører den aktuelle aktiviteten. Administrative funksjoner og støttefunksjoner som regnskap, HR, økonomi, renhold og kantine vil typisk falle utenom, med mindre dette anses som en del av virksomhetens kjerne- eller hovedaktivitet.”

I praksis kan ingen større aktører drive virksomhet i Norge i 2023 uten ganske betydelige og kontinuerlige investeringer i IT og digitalisering. Dette kan likevel ikke bety at alle norske virksomheter har rådgivning og utvikling knyttet til IT og digitale løsninger som sin kjerne- og hovedaktivitet. Selv om disse virksomhetene har behov for (til dels betydelig) støtte til å gjennomføre IT- og digitaliseringsprosjekter, og selv om de kan ha store IT-avdelinger, vil kjerne- og hovedaktiviteten være en annen.

2.2.7 Helhetsvurdering der formålet med reglene skal tillegges vekt

Vurderingen av grensen mellom oppdragsforhold og innleie skal skje basert på en konkret helhetsvurde-

ring, der alle de ulike momentene nevnt over må ses i sammenheng.

Ved denne helhetsvurderingen gir forarbeidene anvisning på at man må se hen til om det aktuelle avtaleforholdet utfordrer lovens formål om å sikre trygge ansettelsesforhold, slik at innleiereglene bør få anvendelse. Sentralt i denne vurderingen er om lovens formål er ivarettatt gjennom trygge og faste ansettelsesforhold hos leverandøren. Her vil det være relevant om leverandøren har gode lønns- og arbeidsvilkår, godt arbeidsmiljø og velfungerende organer for ansatte-representasjon mv.

Et annet moment er om de ansatte har større fordeler hos leverandøren enn kunden når det gjelder arbeids- og fagfelleskap, karrieremuligheter og systematisk kompetanseheving innenfor sine spesialiserte fagområder. Dette vil for eksempel være tilfellet dersom kundens kjerne- og hovedaktivitet ligger utenfor det leverandøren driver med og utenfor hva de ansatte har som sine arbeids- og fagområder.

3. I hvilken grad kan kunder og leverandører basere seg på unntakene i innleieregelverket?

Dersom en tjenesteleveranse må klassifiseres som innleie, eller avtalepartene velger å klassifisere tjenesten som innleie selv om tjenesten kunne vært klassifisert som oppdrag, må arbeidsmiljølovens regler om innleie følges.

Dersom en tjenesteleverandør innen IT-sektoren regelmessig baserer seg på å levere prosjekter basert på innleiereglene, vil leverandøren som klar hovedregel måtte regnes som en virksomhet som har utleie av arbeidskraft til formål. Tjenesteleverandøren vil da regnes som bemanningsforetak og vil måtte følge de strenge reglene i arbeidsmiljøloven §§ 14-12 flg. Som nevnt vil utleie av ansatte til prosjekter mv. som hovedregel være forbudt når man omfattes av disse re-

glene, med unntak for utleie av vikarer. Det oppstilles likevel to viktige unntak, det såkalte spesialistunntaket og tariffunntaket. Begge disse unntakene forutsetter imidlertid at en rekke vilkår er oppfylt. Videre kan innleie av en ansatt i alle tilfeller ikke pågå i mer enn tre år, noe som naturligvis kan være problematisk ved større prosjekter. Innleie fra bemanningsforetak må også følge omfattende regler om likbehandling av innleide med kundens ansatte når det gjelder lønns- og arbeidsvilkår, noe som blant annet kan påvirke de kommersielle forutsetningene for kontrakten.

En del leverandører forsøker å unngå de strenge reglene for innleie fra bemanningsforetak ved å definere seg som en såkalt «produksjonsbedrift». Denne typen innleie reguleres av arbeidsmiljøloven § 14-13, og innebærer at det er tillatt med innleie fra «virksomhet som ikke har til formål å drive utleie» uten de strenge begrensningene i § 14-12 flg.

” En del leverandører forsøker å unngå de strenge reglene for innleie fra bemanningsforetak ved å definere seg som en såkalt «produksjonsbedrift». Denne typen innleie reguleres av arbeidsmiljøloven § 14-13.

Etter vår vurdering er dette unntaket snevert, og kan som utgangspunkt ikke benyttes av en leverandør som grunnlag for å drive kommersiell utleie som ledd i leverandørens løpende tjenesteleveranser til markedet.

Arbeidsmiljøloven § 14-13 er primært innrettet mot utleiers behov, inkludert at virksomheter skal kunne leie ut overskuddskapasitet i pe-

6 Prop. 131 L 2021-2022 s. 47

rioder med manglende oppdragsmengde. Lovgiver har særlig tenkt på at slik utleie vil være et bedre alternativ enn at ansatte må permitteres eller sies opp. Det oppstilles videre noen minstevilkår for at slik utleie er tillatt, herunder at det må skje innenfor det som utgjør virksomhetens hovedbeskjeftigelse og ikke omfatte mer enn 50 prosent av de ansatte. Selv om disse minimumskravene er oppfylt, vil imidlertid en skjønsmessig helhetsvurdering kunne resultere i at virksomheten likevel anses for å ha utleie til formål. I forarbeidene nevnes som eksempel at en IT-virksomhet som permanent leier ut 30 % av sine tilsatte vil kunne anses for å drive ordinær utleie.

” Etter vår vurdering er dette unntaket snevert, og kan som utgangspunkt ikke benyttes av en leverandør som grunnlag for å drive kommersiell utleie som ledd i leverandørens løpende tjenesteleveranser til markedet.

En kjøper av IT-tjenester vil altså ikke uten videre kunne basere seg på leverandørens egen klassifisering som produksjonsbedrift. Det avgjørende er en konkret helhetsvurdering av hva som er formålet bak utleien og realiteten vil være avgjørende, ikke leverandørens egen klassifisering. For utleie som har et klart kommersielt siktemål og utgjør

et forretningsområde for utleier, vil aktiviteten som klar hovedregel omfattes av § 14-12 (bemanningsforetak) og ikke av § 14-13.

” Pliktsubjektet ved brudd på arbeidsmiljølovens regler er først og fremst innleier, altså kjøpere av IT-tjenester. Det er dermed viktig å være bevisst på hva man kjøper, grensen mellom tjenesteleveranser på oppdragsbasis og innleie, og ikke la misforståelser eller frykt for feilvurderinger medføre at en avtale som i realiteten faller utenfor innleieregelverket likevel klassifiseres som innleie.

Et poeng i denne forbindelse er at det vil kunne være i strid med anskaffelsesregelverket dersom en offentlig tjenesteinnkjøper setter som vilkår for en anskaffelse at kun bemanningsforetak eller “produksjonsbedrift” kan delta i konkurransen. Dette fordi et slikt vilkår vil kunne begrense konkurransen unødvendig.

4. Oppsummering

De nye reglene i arbeidsmiljøloven innebærer vesentlige innstramminger i adgangen til å leie inn arbeids-

kraft fra bemanningsforetak, i tillegg til at flere kontrakter om tjenestekjøp nå risikerer å bli klassifisert som innleie. Dette betyr imidlertid ikke at alle IT-prosjekter som skjer etter agile gjennomføringsmodeller utgjør innleie. Det må foretas en konkret vurdering i hvert enkelt tilfelle, og hele avtaleverket må sees under ett.

Hvis man først skal basere seg på at en tjenesteavtale må følge reglene om innleie i arbeidsmiljøloven, er det ikke rett frem å konkludere med at innleien vil være lovlig. Spesialistunntaket er ment å være snevert, og partene kan i mange tilfeller ikke basere seg på en avtale med fagforeningen hos innleier. Spesialistunntaket og tariffunntaket omfattes også av bestemmelsen om at ansatte som har vært sammenhengende innleid i mer enn tre år, har rett til fast ansettelse hos innleier. Når det gjelder unntaket for produksjonsbedrift, vil dette etter vår vurdering i utgangspunktet ikke kunne brukes som grunnlag for utleie som har et klart kommersielt siktemål og utgjør et forretningsområde hos leverandøren.

Pliktsubjektet ved brudd på arbeidsmiljølovens regler er først og fremst innleier, altså kjøpere av IT-tjenester. Det er dermed viktig å være bevisst på hva man kjøper, grensen mellom tjenesteleveranser på oppdragsbasis og innleie, og ikke la misforståelser eller frykt for feilvurderinger medføre at en avtale som i realiteten faller utenfor innleieregelverket likevel klassifiseres som innleie.

Maren Tveten, fast advokat i avdelingen HITEK i Advokatfirmaet Selmer, og André Istad Jobansen, partner i samme avdeling.



Gorrissen Federspiel

Tue Goldschmieding

Ny afgørelse om grænserne for fastsættelse af tekniske specifikationer i IT-systemer i udbud

Det Danske Klagenævn for Udbud (»Klagenævnet for Udbud«) traf den 22. marts 2023 afgørelse i sag 22/14579 mellem en filial af Trend Micro Emea (»Trend Micro«) over for Region Hovedstaden. Sagen vedrørte, hvorvidt Region Hovedstaden havde handlet i strid med udbudsreglerne i forbindelse med indkøb af endpoint-beskyttelsessoftware.

Trend Micro fremsatte i sagen, at Region Hovedstaden havde handlet i strid med reglerne lovbestemt nr. 10 af 06. januar 2023 (»den danske udbudslov«) § 40 og § 42, ved i de tekniske specifikationer at stille krav om, at endpoint-beskyttelsessoftwaret i vidt omfang skulle være kompatibelt med regionens eksisterende firewalls og sandkasseløsning fra producenten Palo Alto.

Ifølge den danske udbudslov § 42, stk. 1, jf. § 40, må en ordregiver ikke angive et bestemt fabrikat, en bestemt oprindelse eller en bestemt fremstillingsproces, som kendetegner de produkter eller tjenesteydelser, en bestemt aktør leverer. Ifølge Trend Micro var det en uberettiget indsnævring af konkurrencen, som var usaglig og proportional, idet kun ganske få tilbudsgivere ville kunne levere en kompatibel løsning. Region Hovedstaden havde heroverfor anført, at kravene var saglige, fordi de bidrog til øget it- og driftsmæssig sikkerhed og samtidig undgik øget ressourceforbrug.



Illustration: Colourbox.com

Formanden for Klagenævnet for Udbud udtalte med henvisning til forarbejderne til den danske udbudslov § 42, stk. 1, at en ordregiver efter omstændighederne kan stille krav om kompatibilitet med et eksisterende produkt, selv hvis det udelukker visse tilbudsgivere under betingelse af, at disse krav er saglige. Formanden mente med henvisning til Region Hovedstadens begrundelser om sikkerhed, at kravene var saglige.

Det andet medlem af Klagenævnet for Udbud lagde i sin dissenterende udtalelse vægt på, at det efter den danske udbudslov § 40 og § 42, er ordregiveren, der skal løfte bevisbyrden for saglighed og proportionalitet i en konkurrencebegrænsende kravspecifikation. Med hensyn til saglighed og proportionalitet lagde medlemmet vægt på, at der var tale om køb af +50.000 licenser, og at disse reelt kun kunne leveres af én producent, sådan som

kravene var udformet. Bevisbyrden var derfor skærpet, og medlemmet vurderede, at bevisbyrden ikke blev løftet med Region Hovedstadens »generelle vendinger« om »sikkerhedsmæssige, organisatoriske, tekniske og økonomiske grunde«.

Da der var stemmelighed, blev formandens udtalelse afgørende, og Trend Micros påstand blev derfor ikke taget til følge.

Læs hele Klagenævnet for Udbuds afgørelse her: https://kelfu.naevnenesbus.dk/media/documents/Filial_af_Trend_Micro_Emea_Limited_mod_Region_Hovedstaden_8Nc7eZo.pdf

De Europæiske tilsynsmyndigheder lancerer offentlig høring om DORA

De europæiske tilsynsmyndigheder (»EBA«, »EIOPA« og »ESMA«, samlet »ESA'erne«) lancerede den 19. juni 2023 en offentlig høring om den første serie af fælles udkast til tekniske standarder under

Digital Operational Resilience Act («DORA»). Navnlige omfatter det fire udkast til reguleringsmæssige tekniske standarder («RTS») og et udkast til gennemførelsesmæssige tekniske standarder («ITS»). Disse tekniske standarder har til formål at sikre en ensrettet og harmoniseret juridisk ramme inden for områderne af IKT-rikostyring, rapportering af større IKT-relaterede hændelser og IKT-rikostyring for tredjeparter. Det regulatoriske afsæt herfor følger af artikel 15, 16, stk. 3, 18, stk. 3, og 28, stk. 9 og 10, i DORA.

Læs Finanstilsynets pressemeddelelse her: https://www.finanstilsynet.dk/Nyheder-og-Presse/Sektornyt/2023/DORA_boering_070723

Andet nyt

EU-Kommissionen og Rådet opnår politisk enighed om en europæiske dataforordning

Den 28. juni 2023 offentliggjorde Europa-Kommissionen, at de sammen med Rådet for Den Europæiske Union var nået til politisk enighed om en europæisk dataforordning.

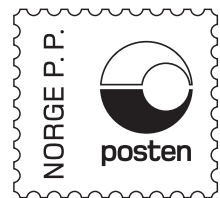
Formålet med dataforordningen er at skabe et indre marked for deling af data inden for EU og derved samtidig sikre et tilgængeligt, konkurrencedygtigt, pålideligt og dataøkonomisk cloudmarked inden for EU.

Dataforordningen indeholder forskellige foranstaltninger relateret til deling af data inden for EU. Foranstaltningerne indebærer blandt

andet en styrkelse af virksomheder i EU i forbindelse med deres aftaleindgåelse og forhandlinger inden for det digitale område. Herudover omfatter forordningen mekanismer, der letter og muliggør offentlige myndigheders adgang og anvendelse af den private sektors data. Dataforordningen opstiller herudover blandt andet også en række nye regler, som sikrer konkurrencen på cloudmarkedet.

Læs EU-Kommissionens pressemeddelelse her: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3491

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



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

Nytt fra

 **LOVDATA**



Lovdata Pro
gratis ut året for
nye kunder

 **LOVDATA
PRO**