Lov & Data

Mars 2026
Nr. 165 1/2026

Innhold

Leder 2
Tue Goldschmieding
Cybersikkerhed bliver produktsikkerhed

Artikler

Lars Arnesen, Sebastian Schwemer og Emily Mary Weitzenboeck
Den digitale omnibus-pakken: forenkling eller regulatorisk kursendring? 4

Fredrik Sandström, Hanna Bogsjö Österberg, Staffan Malmgren
Att dela det odelbara 16

Nicholas Foss Barbantonis og Eilert Midttun Rostrup
Kreativt vern mot kommersiell utnyttelse av AI-genererte stemmeimitasjoner 19

Kjersti Wilson, Thomas T. Roskifte og Peter Lenda
Pårørendeopplysninger: Kontaktopplysninger til ansattes pårørende i arbeidslivet – personvernprinsipper, behandlingsgrunnlag og praksis etter GDPR 23

Kristian Foss og Sara Lamøy Engberg
Hvordan praktiserer norske virksomheter NIS2-direktivet? 26

Mira Levånd Bergsland og Ole Martin Moe
Konkursboets behandling av personopplysninger – hvordan håndtere it-leverandører som holder igjen nødvendige opplysninger 29

Camilla Vislie
AI-trening: Gema mot Open AI. 33

JusNytt 42
Halvor Manshaus
EU og Norden: Ny tilnærming til IP og teknologi i forsvarsleveranser

Nytt om immaterialrett 51
Nytt om personvern 60
Annet nytt 69

Lov & Data er et nordisk 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
Alias: www.lovogdata.no
www.lawanddata.no

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

Ansvarlig redaktør er Sara Habberstad, advokat, VP Legal & Compliance i LINK Mobility Group.
Medredaktør er Trine Shil Kristiansen, rettsinformatiker, Lovdata.
Redaktør for Danmark er Tue Goldschmieding, partner i firmaet Gorrissen Federspiel, København.
Redaktør for Sverige er Daniel Westman, uavhengig rådgiver og forsker.
Redaktør for Finland er Viveca Still, senior ministerial adviser, legal affairs, at Ministry of Finance.
Fast spaltist er Halvor Manshaus, partner i advokatfirmaet Schjødt.

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

Lov & Data er medlemsblad for foreningene Norsk forening for Jus og EDB, Dansk forening for Persondataret, Danske IT-advokater, Svenska föreningen för IT och juridik (SIJU) og Finnish IT Law Association.

Fra 2024 er Lov & Data kun tilgjengelig på nett, lod.lovdata.no.

Layout: Aksell AS

Leder

Cybersikkerhed bliver produktsikkerhed

Tue Goldschmieding

EU's ambitioner om regulering af det digitale marked omsættes i disse år til konkret handling, og med introduktionen af ny lovgivning bevæger IT-retten sig for alvor fra anvendelse af generel lovgivning i det digitale rum til selvstændig regulering af den digitale verden, med fokus på de særlige problemstillinger, der udspringer af de digitale teknologier og øget brug af data. En af de seneste tilføjelser til denne regulatoriske bølge er Cyber Resilience Act. Cyber Resilience Act adskiller sig fra anden informations- og cybersikkerhedslovgivning som NIS2-direktivet ved at være egentlig produktsikkerhedslovgivning. Cyber Resilience Act opstiller således ikke alene krav til producentens tekniske foranstaltninger og efterlevelse af best practice, men opstiller krav til informations- og cybersikkerheden i produkter, der er bestemmende for producentens produktansvar og markedsadgang.

Cyber Resilience Act konkretiserer informations- og cybersikkerhedskravene. Når sårbarheder opdages, er håndteringen ikke længere alene et internt anliggende, men et krav med direkte betydning for salg, udbud, kontrakter og kundetillid. Sårbarhedsrapportering bliver et markedskrav frem for blot et potentielt kontraktkrav. For produkter med digitale elementer bliver forventningen, at leverandøren ikke bare kan håndtere sårbarheder, men skal have en systematisk proces for at modtage og behandle sårbarhedsrapporter, vurdere risiko og påvirkning, informere relevante myndigheder ved alvorlige forhold, informere kunder og brugere når det er nødvendigt og levere rettelser og opdateringer som en del af produktets livscyklus.

Ticket to play

Udsagn som »vi tager sikkerhed alvorligt« vil i fremtiden ikke længere være tilstrækkeligt. Informations- og cybersikkerhed i produkter er en

verificerbar størrelse, og troværdig sårbarhedshåndtering en konkurrenceparameter på linje med kvalitet og pris.

Udbud og indkøb vil i stigende grad stille ufravigelige krav til sikker produktudvikling, sårbarhedsprocesser, opdateringspolitik og dokumentation. Leverandører, der kan svare klart og konsistent, vil vinde. Samtidig vil kunder i stigende grad kræve klare kontraktlige forpligtelser om patching, responstider, advisering og transparens. Når et sikkerhedshul udnyttes, handler tvisten ofte ikke om, hvem der fandt fejlen, men om hvem der gjorde hvad, hvornår, og hvorvidt leverandøren kan dokumentere sin proces.

Tiden er knap

Cyber Resilience Act stiller krav til producentens håndtering af det digitale produkts cybersikkerhed gennem hele produktets livscyklus og forudsætter, at producenten har etableret den organisation og de interne processer, der er nødvendige for at håndtere de stillede krav.

På trods af at Cyber Resilience Act har indflydelse langt ind i producentens organisation og forretningsgange, er Cyber Resilience Act for mange producenter gået under radaren eller er blevet sat til side, mens producenten har forholdt sig til NIS2 eller den megen anden digitale lovgivning, der er blevet introduceret.

Det fulde sæt af forpligtelser under Cyber Resilience Act træder i kraft for digitale produkter, der bringes på markedet fra den 11. december 2027 og reglerne om rapportering af sårbarheder træder i kraft allerede den 11. september 2026.

Dette giver producenterne mindre end to år til at etablere de processer og funktioner, der er nødvendige for producentens overholdelse af de materielle krav under Cyber Resilience Act. Disse krav forudsætter, blandt andet, at producenten har implementeret processer til sikring af cybersikkerhed i design fasen, håndtering af cybersikkerhed i tredjepartskomponenter, udarbejdelse af dokumentation og håndtering af sårbarheder, og rapportering.

> Cyber Resilience Act adskiller sig fra anden informations- og cybersikkerhedslovgivning som NIS2-direktivet ved at være egentlig produktsikkerhedslovgivning.

For mange producenter vil denne tidsfrist være udfordrende henset til, den tid, det tager at udvikle nye digitale produkter og fordi implementeringen kræver omfattende organisatoriske og tekniske ændringer.

Mange producenter bør derfor allerede nu påbegynde implementeringen af de mange krav, der sikrer, at de nødvendige processer, dokumentation og organisatoriske kapaciteter er på plads inden ikrafttrædelsen.

Udfordringen i softwareforsyningskæden og rapporteringskrav

For producenter af digitale produkter er identifikation og håndtering af sårbarheder hidtil blevet foretaget efter bedste evne, når producenten blev opmærksom på en sårbarhed. Derfor har mange kontrakter alene opstillet krav om, at producenten skulle håndtere sårbarheder, som producenten måtte blive bekendt med. Cyber Resilience Act er et opgør med denne praksis. Producentens identifikation og håndtering af sårbarheder i produkters cybersikkerhed og informationssikkerhed er ikke længere blot et internt kvalitetsmål, men et lovgivningsmæssigt krav, som kunder, partnere og myndigheder kan måle producenten på, og er afgørende for producentens markedsadgang og konkurrenceposition.

I de fleste tilfælde opstår sårbarheder ikke i den kode, producenten selv har udviklet, men i de tredjepartskomponenter, der anvendes i produktudviklingen. Cyber Resilience Act stiller derfor også krav til, at producenten har styr på sin softwareforsyningskæde. Grundlæggende skal producenter have afdækket og forstået, hvilke softwarekomponenter, der indgår i producentens produkter (Software Bill of Materials) og skal have implementeret processer, der sikrer, at producenten kan identificere og adressere sårbarheder i disse komponenter.

Cyber Resilience Act opstiller også krav til producentens deling af oplysninger om sårbarheder og rapportering af sårbarheder, der har været udnyttet. Producenter skal derfor agere efter en præmis om transparens for både kunder og myndigheder i producentens håndtering af sårbarheder og den potentielle ansvarseksponering, der kan opstå, hvis producenten ikke håndterer sårbarheder korrekt.

Producentens identifikation og håndtering af sårbarheder i digitale produkter bliver således ikke blot en compliance-øvelse, men en multidisciplinær proces, der kræver forståelse af både regulatoriske krav, tekniske forhold, kommunikation og kontraktuelle forpligtelser og rettigheder i forholdet til kunder og leverandører.

Tue Goldschmieding, partner i Gorrissen Federspiel og dansk redaktør for Lov & Data.

Den digitale omnibus-pakken: forenkling eller regulatorisk kursendring?

Av Lars Arnesen, Sebastian Schwemer og Emily Mary Weitzenboeck

Lars Arnesen

Sebastien Schwemer

Emily Mary Weitzenboeck

1. Bakgrunn

De siste ti årene har vært preget av en markant regulering av det digitale indre markedet gjennom rettsakter med flotte akronymer, blant annet GDPR, DGA, DA, DSA, DMA, NIS 2, eller CDSM-direktivet.[1] EU-kommisjonen har imidlertid endret kurs under von der Leyen II-kommisjonen. Allerede i juli 2024 varslet von der Leyen en ny reguleringsretning i sine «politiske retningslinjer».[2] Budskapet i Draghi-rapporten om at EUs konkurranseevne må styrkes,[3] samt fornyede spenninger i EUs transatlantiske relasjoner, danner grunnlaget for en hittil usett regulatorisk utvikling i form av et bredt spekter av forenklings- og deregulerings-pakker mot et «Et enklere og hurtigere Europa».[4] EU-medlemsstatene har sluttet seg opp om denne «simplifiseringsrevolusjonen»,[5] og det danske EU-formannskapet har i 2025 aktivt tatt til orde for deregulering av det digitale markedet.[6]

På det digitale området presenterte EU-kommisjonen sin syvende såkalte «omnibuspakke» 19. november 2025. Den digitale omnibuspakken, bestående av to separate regulatoriske forslag: en pakke som omfatter endringer i personvernforordningen og en rekke øvrige

1 I denne artikkelen har vi oversatt engelsk og dansk tekst til norsk. Med mindre annet er spesifisert er den norske teksten vår egen uoffisielle oversettelse. Originaltekst er som hovedregel angitt i fotnote.

2 European Commission, *Political Guidelines for the Next European Commission 2024–2029* (18 July 2024) *https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en accessed 17 February 2026*, 5.

3 Mario Draghi, *The Future of European Competitiveness* (European Commission 2024) 3.

4 European Commission, *'Et enklere og hurtigere Europa: Meddelelse om gennemførelse og forenkling'* COM(2025) 47 final (11 February 2025)

5 European Commission, *EU leaders commit to boost Europe's competitiveness* (Press release AC/24/5786, 11 November 2024) *https://ec.europa.eu/commission/presscorner/detail/en/ac_24_5786* accessed 17 February 2026.

6 Council of the European Union, *Programme of the Danish EU Presidency: A Strong Europe in a Changing World* (2025) — digital policy section *https://danish-presidency.consilium.europa.eu/media/xv5jn5nx/programme-of-the-danish-eu-presidency-2025.pdf*, 16-17.

datareguleringer,[7] et eget særskilt forslag om KI-forordningen,[8] samt en ny strategi for dataunionen og forslaget om en europeisk bedriftslommebok. Overordnet sett, er målet å forenkle en rekke digitale rettsakter, særlig innen områdene kunstig intelligens, data, personvern og cybersikkerhet.[9]

1.1. Et markant kursskifte i EU-lovgivningen

EU-kommisjonen vurderer selv at sin digitale forenklingspakke inneholder «en rekke tekniske endringer i et stort antall digitale lover, valgt med sikte på å gi umiddelbar bistand til bedrifter, offentlige forvaltninger og borgere og stimulere konkurranseevnen».[10] EU-kommisjonen fant det derfor ikke nødvendig å utarbeide en konsekvensutredning, ettersom «justeringene av regelverket er av teknisk art, ikke endrer lovgivningens ånd, men snarere optimaliserer den».[11]

Begge forordningsforslagene går imidlertid tydelig utover rene tekniske justeringer, noe vi vil gå nærmere inn på nedenfor. Dette reiser tvil om hvorvidt prinsippene og retningslinjene for regulering, de såkalte retningslinjene for bedre regulering, er overholdt.[12] I forbindelse med den første omnibus-pakken, knyttet til landbrukspolitikk, fant den europeiske ombudsmannen til eksempel feil og mangler ved måten EU-kommisjonen utarbeidet hastelovforslag på.[13]

> Overordnet sett, er målet å forenkle en rekke digitale rettsakter, særlig innen områdene kunstig intelligens, data, personvern og cybersikkerhet.

Den digitale omnibus-pakken tiltrakk seg på kort tid betydelig interesse. Noen ønsker endringsforslagene velkommen,[14] mens andre, herunder sivilsamfunnsorganisasjoner og forbrukerorganisasjonen[15] såsom danske IT-pol[16] og det norske Likestillings- og diskrimineringsombudet (LDO)[17] stiller seg kritiske til dem. 10. februar 2026 vedtok Det europeiske tilsynsførende for personvern (EDPS) og Det europeiske personvernrådet (EDPB) en felles uttalelse om EU-kommisjonens forslag og uttrykte betydelige bekymringer.[18] At regelverk med jevne mellomrom gjennomgås i form av en såkalt «REFIT», er ikke uvanlig. Den nåværende foreslåtte omnibus-pakken er derimot langt mer omfattende og

---

7 European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus) Brussels 19.11.2025, COM(2025) 837 final.

8 European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), Brussels 19.11.2025, COM(2025)837.

9 Det bemerkes at EU-kommisjonen – utenfor Omnibus-agendaen – har foreslått omfattende endringer i Cybersecurity Act, se *Proposal for a Regulation for the EU Cybersecurity Act* (20 januar 2026) *https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act*.

10 European Commission, *'Commission Staff Working Document Accompanying the Proposal for a Regulation on the Simplification of the Digital Legislative Framework and on Artificial Intelligence (Digital Omnibus)'* SWD(2025) 836 final (19 november 2025) 3.

11 European Commission, *'Call for Evidence: Digital Omnibus (Digital Package on Simplification)'* Ref Ares(2025)7724296 (16 september 2025).

12 European Commission, *Better regulation: guidelines and toolbox* (3 November 2021; updated 20 July 2023) *https://commission.europa.eu/law/law-making-process/better-regulation/better-regulation-guidelines-and-toolbox_en*.

13 European Ombudsman, *Ombudsman finds maladministration in how Commission prepared urgent legislative proposals* (Press release No 01/2025, 26 november 2025) *https://www.ombudsman.europa.eu/en/press-release/en/215989*.

14 Dansk Erhverv, *EU fortsætter gode takter mod regeltsunami med digital omnibus* (19 November 2025) *https://www.danskerhverv.dk/presse-og-nyheder/nyheder/2025/november/eu-fortsatter-gode-takter-mod-regeltsunami-med-digital-omnibus/*.

15 Se, for eksempel, det norske Forbrukerrådet, *Forslag om «forenkling» av digitale regelverk svekker forbrukerrettigheter* (18 november 2025) *https://www.forbrukerradet.no/siste-nytt/digital/forslag-om-forenkling-av-digitale-regelverk-svekker-forbrukerrettighet/* og den europeiske forbrukerorganisasjonen BEUC, *BEUC concerns on Digital Omnibus - keep protections under GDPR and uphold the AI Act* (12 november 2025).

16 Access Now, *A call to EU legislators: protect rights and reject the call to delete transparency safeguard in AI Act* (10 februar 2026) *https://www.accessnow.org/press-release/a-call-to-eu-legislators-protect-transparency-safeguard-in-ai-act/*.

17 Likestillings- og diskrimineringsombudet, *'Ombudet ut mot utvanning av menneskerettigheter på det digitale området'* (13 november 2025) *https://ldo.no/blog/2025/11/13/ombudet-ut-mot-utvanning-av-menneskerettigheter-pa-det-digitale-omradet/*.

18 European Data Protection Board and European Data Protection Supervisor, Joint Opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus) (10 februar 2026).

ekstraordinære i en EU-rettslig kontekst.[19]

1.2. Den politiske dimensjonen

Det er viktig å merke seg at utviklingen har en tydelig politisk dimensjon. For det første spiller EU-kommisjonen en sentral rolle i det digitale *acquis*, både gjennom sin initiativrett til å fremme lovforslag og gjennom håndhevingen av regelverket. Mens selvstendige EU-byråer på andre områder (f.eks. Det europeiske miljøbyrået i København eller Den Europeiske Unions Agentur for Cybersikkerhet i Athen) har ansvaret for å forvalte og håndheve regelverk, utføres dette i økende grad av EU-kommisjonens egne enheter på det digitale området (f. eks. KI-kontoret). De fleste digitale rettsakter er forankret i generaldirektoratet for kommunikasjonsnett, innhold og teknologi (DG CONNECT), hvor interne enheter kan konkurrere om ressurser og innflytelse. Reguleringsutviklingen skjer heller ikke i et institusjonelt vakuum. For det andre er teknologiregulering politisk sensitiv, og de endelige rettsaktene er kompromisser fremforhandlet i trilogforhandlinger mellom Rådet, Europaparlamentet og EU-kommisjonen. Kommisjonens forslag kan dermed inneholde elementer som fungerer mer som forhandlingsposisjoner enn som det endelige normative målet. For det tredje er det digitale området preget av betydelig interessepåvirkning. Reguleringsprosessen påvirkes av sterke næringsinteresser og sivilsamfunnsaktører, noe som kan få betydning for både prioriteringer og utformingen av forslagene, og i siste instans det endelige regelverkets materielle innhold.

1.3. Veien videre

Den digitale omnibus-pakken er bare første del av et større initiativ knyttet til EUs teknologiregelverk. Parallelt med høringsfristen for omnibus-pakken vil det bli gjennomført en såkalt «Digital Fitness Check».[20] Denne skal vurdere hvordan det digitale regelverket påvirker og understøtter EUs konkurranseevne, med særlig vekt på områder av strategisk betydning. Den vil også analysere samspillet mellom ulike regelverk, herunder identifisere synergier, god praksis samt eventuelle gjenværende hull, overlapp og inkonsistenser.

2. De sentrale byggeplassene i korte trekk

I denne korte artikkelen vil vi i hovedsak fokusere på fem hovedpunkter knyttet til vern av personopplysninger i punkt 3. I det følgende gir vi derfor kun en kort oversikt over andre relevante endringsforslag i omnibus-pakken.

2.1. Data acquis: En samlet data regulering

På dataområdet er det mest markante elementet den foreslåtte konsolideringen av sentrale EU-rettsakter i én samlet dataforordning. Dataforordningen (Data Act), Dataforvaltningsforordningen (Data Governance Act), Åpne datadirektivet, og onlineplattformforordning med regler for rimelig forretningspraksis (P2B-forordningen) foreslås samlet med sikte på økt juridisk klarhet og administrativ forenkling. Forslaget innebærer samtidig materielle justeringer, herunder endringer i reglene om skifte mellom databehandlingstjenester, med formål å redusere administrative byrder og skape større fleksibilitet. Som ledd i omnibus-pakken er det også foreslått å oppheve forordning (EU) 2018/1807 om fri flyt av ikke-personlige data. Samtidig opprettholdes ambisjonen om å motvirke leverandørlåsing og styrke et åpent og konkurransedyktig skymarked, riktignok med særlige tilpasninger for små og mellomstore virksomheter (SMB-er) og små midcap-virksomheter.

2.2. KI-forordningen

De foreslåtte endringene i KI-forordningen har fått stor oppmerksomhet. Endringene fremmes i et særskilt lovforslag som del av Den digitale omnibus-pakken. At det allerede halvannet år etter vedtakelsen foreslås nye, materielle endringer, er i seg selv bemerkelsesverdig. Ifølge fortalepunkt nr. 3 dreier det seg om «målrettede endringer» for å håndtere implementeringsutfordringer.[21]

For det første foreslås et såkalt «stop-the-clock», hvor anvendelsen av høyrisikoreglene kobles til tilgjengeligheten av bl.a. harmoniserte standarder. I praksis innebærer dette en mulig utsettelse av sentrale forpliktelser og er et sentralt diskusjonspunkt.

For det andre foreslås endringer i bestemmelsen om KI-ferdigheter (art. 4 i KI-forordningen). Leverandører og idriftsettere har ansvar for å sikre tilstrekkelig KI-kompetanse. Dette forslås endret, slik at ansvaret i større grad legges på EU-kommisjonen og medlemsstatene for å fremme KI-kompetanse.[22] Videre foreslås en reduksjon av registreringsbyrden for leverandører av KI-systemer som anvendes i høyrisikoområder, men som leverandøren selv har klassifisert som ikke-høyrisiko. Samtidig styrkes KI-kontorets kompetanse gjennom ytterligere

---

19 Alberto Alemanno, *'The Legality of Omnibus Legislation Under EU Law: A Preliminary Analysis of Omnibus I Simplification Directive of CSRD and CSDD and its Legal Consequences on the EU Legal Order'* (9 november 2025) SSRN *https://ssrn.com/abstract=5727822*.

20 European Commission, *'Digital fitness check – testing the cumulative impact of the EU's digital rules'* (Have Your Say, 2024) *https://ec.europa.eu/info/law/better-regulation/info/law/better-regulation/have-your-say/initiatives/15554-Digital-fitness-check-testing-the-cumulative-impact-of-the-EUs-digital-rules*.

21 Omnibus-pakken om KI, fortalepunkt nr. 3.

22 KI-forordningen artikkel 1(4); Omnibus-pakken om KI, fortalepunkt nr. 5.

sentralisering av tilsynet med KI-systemer basert på generelle formålsmodeller eller integrert i svært store nettplattformer og søkemotorer, hvor det også foreligger en overlapp med forordningen om digitale tjenester (Digital Services Act).[23]

Forslaget om en «ny» bestemmelse om «bias detection and correction» (art. 4a KI-forordningen) er særlig interessant.[24] Bestemmelsen etablerer et uttrykkelig rettsgrunnlag for behandling av særlige kategorier av personopplysninger med sikte på å identifisere og korrigere skjevheter i KI-systemer. Den flyttes i hovedsak ordrett fra art. 10 i KI-forordningen (krav til høyrisikosystemer) til kapittel I om generelle bestemmelser. Dermed løftes reguleringen ut av høyrisikokonteksten og gis et bredere anvendelsesområde. Dette er ikke bare en redaksjonell endring, men en systematisk forskyvning av bestemmelsens karakter. Den sentrale formuleringen åpner for at hjemmelen kan anvendes av leverandører og idriftsettere av KI-systemer og -modeller, samt av idriftsettere av høyrisikosystemer, der behandlingen er nødvendig og forholdsmessig og skjer innenfor de fastsatte formålene og garantiene. Bestemmelsen må også ses i sammenheng med forslaget om en ny artikkel 88c i personvernforordningen om behandling i forbindelse med utvikling og drift av kunstig intelligens.[25]

Til tross for endringenes rekkevidde forventes forhandlingene å forløpe raskt, både som følge av tidsmessig press knyttet til «stop-the-clock»-forslaget og den generelle hurtigbehandlingen av omnibus-pakken. Europaparlamentets komiteer, IMCO (indre marked og forbrukerbeskyttelse) og LIBE (sivile rettigheter, justis og indre anliggender), offentliggjorde allerede 17. februar et utkast til betenkning,[26] og trilogforhandlinger mellom Europaparlamentet, Rådet og Kommisjonen forventes i mars og april, med sikte på avstemning i parlamentet i juni.

3. Noen sentrale endringsforslag i personvernregelverket

I det følgende vil vi se nærmere på fem sentrale endringsforslag fra EU-kommisjonen, med et særskilt fokus på hvorvidt endringene medfører en forenkling. De fem utvalgte endringene er:

- Det nye tillegget til definisjonen av personopplysningsbegrepet, der EU-kommisjonen foreslår å innføre et relativt og personbetinget personopplysningsbegrep.
- Nytt behandlingsgrunnlag for særlige kategorier av personopplysninger til bruk og utvikling av KI.
- Berettiget interesse som behandlingsgrunnlag for utvikling og bruk av kunstig intelligens i kombinasjon med en særskilt hjemmel for bruk av sensitive personopplysninger til å oppdage og korrigere skjevheter i datagrunnlaget.
- Den foreslåtte innskrenkningen til den registrertes rett til innsyn via en ny artikkel 12(5) GDPR.
- De nye samtykkereglene for bruk av informasjonskapsler («cookies») med nye begrensinger for å redusere omfanget av samtykkeforespørsler.

3.1. Nytt tillegg til definisjonen av personopplysninger – en forhastet forenkling?

EU-kommisjonen har foreslått et nytt og omfattende tillegg til definisjonen av personopplysninger.[27] Formålet med den foreslåtte endringen er å kodifisere rettspraksis fra EU-domstolen.[28] Ifølge kommisjonen har nyere rettspraksis fra EU-domstolen slått fast at informasjonen skal ikke anses å være personopplysninger for en gitt enhet dersom denne enheten ikke har midler som det med rimelighet kan brukes til å identifisere den fysiske personen som informasjonen gjelder.[29] Kort oppsummert innebærer dette at en opplysning kan være en personopplysning for noen, uten at opplysningen nødvendigvis er en personopplysning for alle andre. Det er derfor behov, ifølge kommisjonen, for å avklare når pseudonymiserte opplysninger utgjør personopplysninger.[30] Det nye tillegget består av tre setninger, som i uoffisiell norsk oversettelse (av oss), lyder som følger:

- Informasjon om en fysisk person er ikke nødvendigvis personopplysninger for alle andre personer eller enheter, bare fordi en annen enhet kan identifisere den fysiske personen.

23 Forordning om digitale tjenester (EU) 2022/2065 OJ L 277/1. (på engelsk: Digital Services Act).

24 KI-forordningen artikkel 1(5); Omnibus-pakken om KI, fortalepunkt nr.6.

25 KI-forordningen artikkel 3(15); Omnibus-pakken om KI, fortalepunkt nr.6.

26 European Parliament, *Report on the proposal for a regulation of the European Parliament and of the Council amending Regulations (EU) No 765/2008, (EU) 2016/424, (EU) 2016/425, (EU) 2016/426, (EU) 2023/1230, (EU) 2023/1542 and (EU) 2024/1781 as regards digitalisation and common specifications* (A10-0024/2026, 17 February 2026) *https://www.europarl.europa.eu/doceo/document/A-10-2026-0024_EN.html.*

27 Omnibus-pakken om personvernforordningen m.m. 54-55.

28 Omnibus-pakken om personvernforordningen m.m. 10-11, og fortalepunkt nr. 27.

29 *Commission Staff Working Document* SWD (2025) 836 final, 38 og fortalepunkt nr. 27.

30 Omnibus-pakken om personvernforordningen m.m. 6, 10-11, og European Commission, *Commission Staff Working Document* SWD (2025) 836 final, 38.

- Informasjon skal ikke være personlig for en gitt enhet når denne enheten ikke kan identifisere den fysiske personen som informasjonen gjelder, med hensyn til de midler som enheten med rimelighet kan forventes å bruke.
- Slik informasjon blir ikke personlig for den enheten bare fordi en potensiell senere mottaker har midler som med rimelighet kan forventes å bli brukt til å identifisere den fysiske personen som informasjonen gjelder.

Den første setningen introduserer et forbehold: Informasjon som knytter seg til en fysisk person (en registrert), er ikke nødvendigvis alltid en personopplysning for andre. De neste to setningene forsøker å presisere dette, men ordlyden er uklar, tvetydig og går utover nyere rettspraksis fra EU-domstolen. Vi utdyper dette senere.

I forslaget er det ikke nevnt hvilke avgjørelser det nye tillegget til personopplysningsbegrepet bygger på. Kommisjonens forslag inneholder heller ingen detaljert analyse av rettspraksis som kan underbygge den nye definisjonen.[31] I fortalepunkt nr. 27 til Omnibus-pakken fremkommer det kun følgende: «Ut fra rettspraksis» så er det ifølge kommisjonen nødvendig «å gi ytterligere klarhet om når en fysisk person skal anses som identifiserbar».[32] Slik den nye definisjonen er formulert, kan det imidlertid antas at forslaget i hovedsak bygger på *EDPS mot SRB* (C-413/23 P), avsagt 4. september 2025.[33]

Kommisjonen ønsker altså å stadfeste at en opplysning som er en personopplysning for noen, ikke nødvendigvis er en personopplysning for enhver. En opplysning kan for eksempel utgjøre en personopplysning for den behandlingsansvarlige, uten å være en personopplysning for en tredjepart, som kun har tilgang til avidentifiserte opplysninger utlevert av den behandlingsansvarlige.

Dette kan illustreres med et enkelt eksempel: Et sykehus har etablert et helseregister som inneholder avidentifiserte helseopplysninger knyttet til pasienter som har mottatt behandling på sykehuset. I tråd med etablerte rutiner, foreligger det en koblingsnøkkel mellom pasientens journal og de avidentifiserte registeropplysningene. Det er dermed mulig å identifisere pasientene, men denne koblingsnøkkelen har kun tre autoriserte ansatte på sykehuset tilgang til. De avidentifiserte opplysningene er personopplysninger for sykehuset (behandlingsansvarlig) ettersom sykehuset har koblingsnøkkelen. For andre eksterne personer, som ikke har tilgang til koblingsnøkkelen, er ikke helseopplysningene *nødvendigvis* personopplysninger. Gjennom pseudonymisering fjernes den direkte koblingen til pasientens navn og andre direkte identifiserbare indikatorer. Spørsmålet etter gjeldende rett blir da om disse eksterne fysiske eller juridiske personer, har tatt hensyn til «alle midler som det med rimelighet kan tenkes at den behandlingsansvarlige eller en annen person kan ta i bruk», kan identifisere en fysisk person direkte eller indirekte, jf. personvernforordningen fortalepunkt nr. 26 og *EDPS mot SRB*. Identifikasjon er likevel mulig for noen få autoriserte ansatte på sykehuset, gjennom koblingsnøkkelen, og dermed er helseopplysningene i helseregisteret, tross pseudonymisering, personopplysninger for sykehuset, den behandlingsansvarlige.[34]

Det har lenge vært uenighet om hvor bredt personopplysningsbegrepet skal tolkes. I en omfattende artikkel om personopplysningsbegrepet fra 2018, skiller Purtova mellom den såkalte «relative» og «absolutte» tilnærmingen til personopplysningsbegrepet.[35] Den relative tilnærmingen er risikobasert, og betinget av en konkret vurdering i hvert enkelt tilfelle. Den absolutte tilnærmingen regner alt som ikke er irreversibelt anonymisert som en personopplysning. Ut fra den absolutte tilnærmingen må det kunne påvises at en opplysning er anonymisert for enhver. Ifølge Purtova kan dette i praksis være en umulig oppgave, sett i lys av den teknologiske utviklingen. Hva som regnes som irreversibelt anonymisert i dag, kan være identifiserbart med ny teknologi om få år.[36] Utgangspunktet, ut fra den absolutte tilnærmingen, er likevel at enhver opplysning kan utgjøre en personopplysning, med mindre den er irreversibelt anonymisert.[37]

Det er støtte for både den relative og den absolutte tilnærmingen i personvernforordningen. Denne tvetydigheten kommer klart til uttrykk i fortalepunkt nr. 26, som peker mot en konkret risikovurdering som samtidig skal dekke enhver person:

> *Når det skal fastslås om en fysisk person er identifiserbar, bør det tas hensyn til alle midler som det med rimelighet kan tenkes at den behandlingsansvarlige eller en annen person kan ta i bruk for å identifisere vedkommende direkte eller indirekte, f.eks. utpeking.*

31 Se f.eks. European Commission, *Commission Staff Working Document* SWD(2025) 836 final, 38.

32 Omnibus-pakken om personvernforordningen m.m. 9.

33 Case C-413/23 P *European Data Protection Supervisor v Single Resolution Board* ECLI:EU:C:2025:645, Judgment of 4 September 2025.

34 Se *EDPS mot SRB (n 33)*, avsnitt 76.

35 Nadezhda Purtova, 'The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10(1) *Law, Innovation and Technology* 40, 46 *https://doi.org/10.1080/17579961.2018.1452176*.

36 Ibid. 47-48.

37 Article 29 Data Protection Working Party (Artikkel 29-gruppen), *Opinion 05/2014 on Anonymisation Techniques* (10 April 2014) (WP216) 3, 5-7.

Det er altså ikke kun situasjonen til den behandlingsansvarlige som skal vurderes, men risikoen for at «den behandlingsansvarlige eller en annen person» kan identifisere de registrerte, enten direkte eller indirekte. Alle midler som enhver person «med rimelighet kan tenkes» å bruke for å identifisere noen skal tas i betraktning.

I fortalepunkt nr. 26 i personvernforordningen fremgår det også at motsatsen til personopplysninger er anonyme opplysninger. En anonym opplysning er beskrevet som «opplysninger som ikke kan knyttes til en identifisert eller identifiserbar fysisk person, eller personopplysninger som er blitt anonymisert på en slik måte at den registrerte ikke lenger kan identifiseres.» Samlet sett *kan* fortalepunkt nr. 26 tolkes i retning av den absolutte tilnærmingen til personopplysningsbegrepet, der enhver opplysning er en personopplysning inntil det motsatte er bevist: Det må kunne påvises at opplysningen er irreversibelt anonymisert.[38] Dette er standpunktet inntatt av forløperen til EDPB, Artikkel 29-gruppen, i retningslinjene om anonymiseringsteknikker fra 2014.[39] EDPB har bygget videre på denne forståelsen av personopplysningsbegrepet i de nye retningslinjene om pseudonymisering fra januar 2025.[40]

EU-domstolen har imidlertid en litt annen tilnærming i den nylig avsagte avgjørelsen *EDPS mot SRB (C-413/23 P)*.[41] Spørsmålet i denne saken var om opplysninger som utgjorde personopplysninger for Single Resolution Board (SRB) også gjorde dette for konsulentselskapet Deloitte. SRB er et EU-organ som engasjerte Deloitte til å gjennomgå en verdivurdering.[42] Saken ble derfor behandlet under forordning (EU) 2018/1725, som regulerer behandling av personopplysning for EU-organer. Forordningen har den samme definisjonen av personopplysninger som personvernforordningen,[43] med tilsvarende beskrivelse av anonymiserte og pseudonymiserte opplysninger i fortalen.[44]

SRB satt på en koblingsnøkkel som kunne identifisere hvem som hadde svart på en spørreundersøkelse. Formålet med spørreundersøkelsen var å innhente synspunkter fra berørte parter knyttet til verdivurderingen. For hvert svar ble en 33-siffret globalt unik identifikator tilfeldig generert.[45] Deloitte hadde kun tilgang til svarene samt den 33-siffret unik identifikator, uten koblingsnøkkelen.[46] EU-domstolen stadfestet at opplysningene var pseudonymiserte.[47] I utgangspunktet kunne man forvente at opplysningene er personopplysninger, ettersom de ikke er anonymiserte. EU-domstolen avviser dette:

> *I motsetning til hva EDPS anfører, må pseudonymiserte data ikke anses å utgjøre personopplysninger i alle tilfeller og for alle personer i forbindelse med anvendelsen av forordning 2018/1725.*[48]

Domstolen viste til at pseudonymisering kan medføre at tredjeparter, slik som Deloitte, ikke kan identifisere de registrerte, noe som medfører at opplysningene gitt til Deloitte ikke kan regnes som personopplysninger ettersom den registrerte ikke lengre er identifiserbare.[49]

Dommen gikk mot EDPS, og det kommer derfor ikke som noen stor overraskelse at EDPS er kritisk til avgjørelsen. Tillegget til personopplysningsbegrepet i omnibuspakken virker i utgangspunkt å vær ment å kodifisere *EDPS mot SRB*, der EU-domstolen stadfester at pseudonymiserte opplysninger ikke nødvendigvis alltid er personopplysninger. EDPS og EDPB uttrykker i en felles uttalelse fra 10. februar 2026 uenighet i kommisjonens tolkning av EU-domstolens praksis.[50] De fremfører at de foreslåtte endringene «går klart utover EU-domstolens rettspraksis». Etter deres syn foreligger det derfor ikke grunnlag for å utlede en ny generell definisjon av personopplysningsbegrepet, med hovedvekt på det som ser ut til å være en enkeltstående avgjørelse fra september 2025.[51]

Den tredje setningen i den foreslåtte definisjonen synes verken å kodifisere EU-domstolens praksis eller å være i tråd med det EU-dom-

38 Fortalepunkt nr. 26 kan imidlertid også tolkes i retning av den relative tilnærmingen til personopplysningsbegrepet, se Weitzenboeck, Lison, Cyndecka og Langford, 12 (2022) 3 *International Data Privacy Law*, 184, 191, *https://doi.org/10.1093/idpl/ipac008*.

39 Artikkel 29-gruppen (n 36).

40 European Data Protection Board, *Guidelines 01/2025 on Pseudonymisation* (16 January 2025) *https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf* 10.

41 *EDPS mot SRB* (n 33).

42 *EDPS mot SRB* (n 33) avsnitt 10-11.

43 Forordning 2018/1725 artikkel 3(1).

44 Fortalepunkt nr. 26 i personvernforordningen tilsvarer fortalepunkt nr. 16 i forordning 2018/1725.

45 *EDPS mot SRB* (n 33) avsnitt 23. Engelsk originaltekst: «That alphanumeric code consisted of a 33-digit globally unique identifier randomly generated at the time the responses to the form were received.»

46 *EDPS mot SRB* (n 33) avsnitt 22-28.

47 Ibid. avsnitt 68.

48 Ibid. avsnitt 86. Engelsk originaltekst: «It follows, contrary to what the EDPS maintains, pseudonymised data must not be regarded as constituting, in all cases and for every person, personal data for the purposes of the application of Regulation 2018/1725»

49 Ibid. avsnitt 87. Engelsk originaltekst: «pseudonymisation may, depending on the circumstances of the case, effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable.»

50 EDPS og EDPB (n 18).

51 Ibid. 9-11.

stolen uttalte i *EDPS mot SRB*. Etter å ha først henvist til domstolens tidligere dom i *Gesamtverband Autoteile-Handel,* som gjaldt tilgang til kjøretøyinformasjon (sak C-319/22, 9. november 2023) gjentok EU-domstolen i *EDPS mot SRB* avsnitt 84 at:

> *«data som i seg selv er upersonlige, kan bli 'personlige' når den behandlingsansvarlige stiller dem til rådighet for andre personer som har midler som med rimelighet kan gjøre det mulig å identifisere den registrerte. Det fremgår særlig av sistnevnte dom [*dvs. Gesamtverband Autoteile-Handel] *at når disse dataene stilles til rådighet for disse personene, er de personopplysninger for disse personene og, indirekte, for den behandlingsansvarlige.»*

EU-domstolen fastslår dermed at opplysningene i den ovennevnte saken er personopplysninger både for mottakeren (tredjeparten) og for virksomheten som deler opplysningene med mottakeren. Videre fastslår EU-domstolen i avsnitt 85:

> *«I den grad det ikke kan utelukkes at disse tredjepartene har midler som rimeligvis gjør det mulig for dem å knytte pseudonymiserte opplysninger til den registrerte, for eksempel ved å krysssjekke med andre opplysninger de har til rådighet, må den registrerte anses som identifiserbar både med hensyn til overføringen og enhver senere behandling av disse opplysningene av disse tredjepartene. Under slike omstendigheter bør pseudonymiserte opplysninger anses å være personlige.»*

Det nye tillegget står også potensielt i motstrid med flere sentrale elementer i personvernforordningen, som ikke ble nærmere vurdert av EU-domstolen i *EDPS mot SRB*. Systematikken i personvernforordningen bygger på at pseudonymiserte opplysninger er personopplysninger:

- I fortalepunkt nr. 26, fremkommer det at motsatsen til personopplysninger ikke er pseudonymisering, men anonymisering.[52]
- I artikkel 4(5) er pseudonymisering definert som «behandling av personopplysninger på en slik måte at personopplysningene ikke lenger kan knyttes til en bestemt registrert uten bruk av tilleggsopplysninger.»[53]
- Artikkel 11 har egne regler om «behandling av personopplysninger» som ikke krever identifikasjon. Det er gitt unntak for en rekke rettigheter i personvernforordningen kapittel III, i de tilfeller der den behandlingsansvarlige ikke kan identifisere den registrerte.[54]

Det er altså en systematikk i personvernforordningen som tar høyde for at den behandlingsansvarlige ikke nødvendigvis alltid kan identifisere den registrerte. EU-domstolen ser derimot ut til å forutsette, i *EDPS mot SRB*, at en personopplysning må være identifiserbar for mottakeren for at vedkommende skal kunne ta på seg forpliktelser som behandlingsansvarlig.[55] I tidligere praksis, har EU-domstolen imidlertid slått fast at man kan ha behandlingsansvar, selv uten å ha tilgang til de aktuelle personopplysningene som er under behandling.[56] Ansvaret mellom flere behandlingsansvarlige er ikke nødvendigvis likt fordelt.[57]

Diskusjonen om personopplysningsbegrepet er absolutt eller relativt, og i hvilken grad pseudonymiserte opplysninger utgjør personopplysninger, er langt fra over. Spørsmålet reiser komplekse problemstillinger, som trolig ikke lar seg fange i en enkel og generell legaldefinisjon. Det er i tillegg en rekke uklarheter i ordlyden presentert av kommisjonen, for eksempel knyttet til formuleringen «ikke nødvendigvis» i den første setningen av den nye definisjonen. Fra forslaget følger det at en opplysning er «ikke nødvendigvis» en personopplysning for en part, kun fordi den er en personopplysning for en annen. Det er uklart hvordan forbeholdet «ikke nødvendigvis» («not necessarily») skal tolkes. I hvilke tilfeller vil en personopplysning kunne være en personopplysning for en annen part? Et annet eksempel er ordet «enhet» i den nye definisjonen. Hva betyr «enhet»? Er «enhet» en person, og i så fall, hva betyr «for alle andre personer eller enheter»? Ordet «enhet» kan mistolkes som en seksjon eller avdeling av en juridisk person, og ytterligere utvanne begrepet «personopplysninger» og dermed personopplysningslovens og personvernforordningens saklige virkeområde, jf. pol. § 2 jf. personvernforordningen artikkel 2. Et tredje eksempel av uklarhet er følgende. Etter personvernforordningen fortalepunkt nr. 26 «det bør tas hensyn til *alle* midler som med rimelighet kan antas å bli brukt» (vår kursivering), mens den foreslåtte ordlyden i den andre setningen av den nye definisjonen glemmer kvalifikasjonen «alle» og kun oppgir «med hensyn til de midler som med rimelighet kan antas å bli brukt av den enheten». Den foreslåtte definisjonen ser derfor ikke til å sammenfalle med fortalepunkt nr. 26 i personvernforordningen. Det vil derfor ikke overraske om kommisjonens forslag til nytt personvernbegrep kommer til å være gjenstand for in-

52 Tilsvarer fortalepunkt nr. 16 i forordning (EU) 2018/1725.

53 Tilsvarer artikkel 3(6) I forordning (EU) 2018/1725.

54 Tilsvarer artikkel 12 i forordning (EU) 2018/1725.

55 *EDPS mot SRB* (n 33), avsnitt 89. Engelsk originaltekst: «Such obligations [to provide information] cannot be imposed on an entity which is in no way in a position to carry out that identification.»

56 Case C-25/17 *Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta* ECLI:EU:C:2018:551, avsnitt 69; Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, avsnitt 38.

57 Wirtschaftsakademie (n 44), avsnitt 43.

tensiv diskusjon i lovgivningsprosessen og til å bli modifisert.

3.2. Nytt behandlingsgrunnlag for særlige kategorier personopplysninger ved utvikling og bruk av KI

Utviklingen av KI-systemer og KI-modeller kan innebære behandling av særlige kategorier av personopplysninger, og slike personopplysninger kan ende opp i datasettene for trening, testing eller validering, eller i KI-systemet eller KI-modellen, selv om de ikke er nødvendige for formålet med behandlingen. Kommisjonen har derfor foreslått en ny hjemmel i personvernforordningen artikkel 9(2) for å legge til rette at slik behandling «ikke hindrer på en uforholdsmessig måte utviklingen og driften av KI».[58] Den foreslåtte artikkel 9(2)(k) hjemler behandling av særlige kategorier personopplysninger for:[59]

> *«(k) behandling i forbindelse med utvikling og drift av et KI-system i henhold til definisjonen i artikkel 3 nr. 1 i forordning (EU) 2024/1689 eller en KI-modell, forutsatt at vilkårene i femte ledd er oppfylt.»*

I artikkel 3(3) bokstav b foreslås det et nytt femte ledd til artikkel 9, som lyder som følger:

> *«(5) For behandling etter andre ledd bokstav (k), skal det iverksettes egnede organisatoriske og tekniske tiltak for å unngå innsamling og ellers behandling av særlige kategorier av personopplysninger. Dersom den behandlingsansvarlige, til tross for iverksettelsen av slike tiltak, identifiserer særlige kategorier av personopplysninger i datasettene som brukes til trening, testing eller validering eller i KI-systemet eller KI-modellen, skal den behandlingsansvarlige fjerne slike opplysninger. Hvis fjerning av disse opplysninger krever uforholdsmessig stor innsats, skal den behandlingsansvarlige likevel uten unødig opphold effektivt beskytte slike opplysninger mot å bli brukt til å produsere utdata, mot å bli utlevert eller på annen måte gjort tilgjengelig for tredjeparter.»*

Den foreslåtte artikkel 9(5) innfører flere betingelser og kvalifikasjoner for behandling av særlige kategorier av personopplysninger i henhold til artikkel 9(2)(k), som interessant nok, og i motsetning til mange av de andre behandlingsgrunnlagene i artikkel 9(2), ikke gjelder behandling som er «nødvendig», men kun «i forbindelse med»[60] utvikling og drift av et KI-system eller en KI-modell. Det kan også spørres om bestemmelsene er tilstrekkelig teknologinøytrale, i tråd med fortalepunkt nr. 15 i personvernforordningen.[61] Disse to foreslåtte bestemmelsene svekker beskyttelsen som personvernforordningen ellers gir til særlige kategorier av personopplysninger, da de kan fort føre til at behandlingsansvarlige hevder at deres behandling er «i forbindelse med utvikling og drift av et KI-system» eller en KI-modell, og at fjerning av slike personopplysninger krever «uforholdsmessig stor innsats».

Det er heller ikke enkelt å forene de to bestemmelsene, siden artikkel 9(2)(k) er et nytt rettslig grunnlag for behandling av særlige kategorier av personopplysninger for de angitte formålene, mens utgangspunktet i artikkel 9(5) er at særlige kategorier av personopplysninger *ikke* skal behandles på grunnlag et slikt rettslig grunnlag, nemlig at det må treffes organisatoriske og tekniske tiltak for å unngå slik behandling, og hvor den behandlingsansvarlige oppdager at slike personopplysninger behandles, skal slike personopplysninger fjernes fra datasettene. Ordlyden her skaper en lacuna, et rettslig tomrom, da det er opp til den behandlingsansvarlige å oppdage at det finnes særlige kategorier av personopplysninger i datasettet. Artikkel 9(5) synes å straffe den mer årvåkne eller seriøst behandlingsansvarlige. Den mindre aktsomme behandlingsansvarlige kan faktisk hevde, ved «oppdagelse» av slike opplysninger på et senere tidspunkt, at fjerning av slike personopplysninger krever en «uforholdsmessig stor innsats».

3.3. Berettiget interesse som behandlingsgrunnlag for utvikling og bruk av kunstig intelligens

EU-kommisjonen viser til at en rekke interessenter på tvers av sektorer i høringsprosessen anså adgangen til å påberope seg berettiget interesse som særlig viktig.[62] Med henvisning til at «pålidelig kunstig intelligens er afgørende for at skabe økonomisk vækst og støtte innovation med socialt gavnlige resultater,»[63] foreslår Kommisjonen en egen bestemmelse i personvernforordningen som spesifiserer at berettiget interesse kan brukes som behandlingsgrunnlag

58 Se Omnibus-pakken om personvernforordningen m.m., fortalepunkt nr. 33.

59 Se Omnibus-pakken om personvernforordningen m.m. 55.

60 Engelsk originaltekst er: «in the context of».

61 Etter fortalepunkt nr. 15 GDPR, «For å unngå at det oppstår en alvorlig risiko for at bestemmelsene omgås bør vernet av fysiske personer være teknologisk nøytralt og ikke avhenge av teknikkene som benyttes. Vernet av fysiske personer bør få anvendelse på automatisert behandling av personopplysninger samt manuell behandling dersom personopplysningene inngår i eller skal inngå i et register. Saksmapper eller samlinger av saksmapper samt deres forsider som ikke er strukturert etter bestemte kriterier, bør ikke omfattes av denne forordnings virkeområde.»

62 European Commission, *'Commission Staff Working Document Accompanying the Proposal for a Regulation … on the Simplification of the Digital Legislative Framework and on Artificial Intelligence (Digital Omnibus)'* SWD(2025) 836 final (19 November 2025) 53.

63 Digital Omnibus, Fortalepunkt 30.

for utvikling av KI-modeller.[64] Forslaget må også ses i lys av EDPBs uttalelse fra desember 2024, hvor det presiseres at behandlingsansvarlige i prinsippet kan støtte seg på berettiget interesse ved utvikling og bruk av KI-modeller, forutsatt at den klassiske tretrinnsvurderingen etter artikkel 6 nr. 1 bokstav f er oppfylt.[65] Spørsmålet i uttalelsen var dermed ikke om berettiget interesse kan anvendes, men hvordan behandlingsansvarlige kan dokumentere at vilkårene er oppfylt.

Kommisjonens forslag går et skritt videre ved å kodifisere adgangen uttrykkelig i forordningen. Samtidig oppstilles viktige begrensninger. Berettiget interesse er ikke tillatt som behandlingsgrunnlag i tilfeller der EU-lovgivning eller nasjonal lovgivning krever samtykke fra den registrerte. Et eksempel, der samtykke er påkrevd, er for plattformer designert som «gatekeepers» etter forordningen om digitale markeder (Digital Markets Act).[66]

Videre presiseres at behandlingsgrunnlaget ikke kan anvendes dersom den berettigede interessen «overstyres av interessene eller grunnleggende rettigheter og friheter til den registrerte som krever beskyttelse av personopplysninger, særlig når den registrerte er et barn.»[67] Dette unntaket spesifiserer for så vidt kun noe som allerede er tilfelle knyttet til berettiget interesse som behandlingsgrunnlag: Berettiget interesse er kun et gyldig behandlingsgrunnlag forutsatt at interessen er forholdsmessig, tatt i betraktning de personvernmessige konsekvensene for de registrerte.[68]

Samlet sett fremstår forslaget dels som en kodifisering og klargjøring av EDPBs fortolkning, dels som et politisk signal om at berettiget interesse anses som et sentralt rettsgrunnlag for KI-utvikling. Spørsmålet er imidlertid om presiseringen reelt endrer terskelen for interesseavveiningen, eller om den primært gir økt rettsteknisk klarhet uten å forskyve balansen i personvernforordningen. Forslaget klargjør også de tilfellene der samtykke alltid er nødvendig, slik som i tilfelle for «gatekeepers» etter forordningen om digitale markeder.

Forslaget må også leses i sammenheng med endringsforslagene i KI-forordningen. I KI-forordningen artikkel 10(5) er det gitt anledning for tilbydere av høy-risiko KI-systemer å bruke sensitive personopplysninger for å rette opp skjevheter i datagrunnlaget. Dette gjelder kun dersom det er «strengt nødvendig» («strictly necessary»). Dette er foreslått endret til kun «nødvendig».[69]

Forslaget i omnibus-pakken om KI vil flytte eksisterende artikkel 10(5) inn som ny artikkel 4(a). Dette er etter vårt syn lovteknisk uheldig. Artikkel 10(5) er konstruert som en forpliktelse for tilbydere av høyrisiko KI-systemer, og passer dermed ikke direkte inn i delen som omhandler generelle forpliktelser for alle KI-systemer. Kommisjonen forsøker å reparere dette, ved å legge til et nytt punkt:

> *«Punkt 1 kan gjelde for leverandører og distributører av andre KI-systemer og -modeller, og distributører av høyrisiko-KI-systemer der det er nødvendig og forholdsmessig (...).»*[70]

Det første punktet retter seg kun mot tilbydere av høy-risiko KI-systemer, og er hentet fra den eksisterende artikkel 10(5). Deretter, på slutten, i andre avsnitt, får vi vite at bestemmelsen også kan anvendes for tilbydere og idriftsettere «av andre KI-systemer og modeller». Her ville det vært mer hensiktsmessig å skrive om hele bestemmelsen. Forslaget er ment som en forenkling, men lovteksten, slik den nå er foreslått, er gjort unødvendig utilgjengelig.

Et av vilkårene i artikkel 10(5), som skal flyttes til en ny artikkel 4a, er at de sensitive personopplysningene skal pseudonymiseres. Pseudonymiserte opplysninger skal ifølge forslaget til nytt personopplysningsbegrep ikke nødvendigvis utgjøre en personopplysning, se punkt 3.1 ovenfor. Ved å pseudonymere sensitive personopplysninger, i tråd med kravet i artikkel 10(5) (ny artikkel 4a), kan altså de sensitive personopplysningene miste sin juridiske status som personopplysning, i alle fall for enkelte mottakere. Dette il-

64 Art. 3 (15) Digital Omnibus vedr. Artikkel 88c om Behandling i forbindelse med udvikling og drift af kunstig intelligens.

65 EDPB, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models Adopted on 17 December 2024.

66 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L 265/1.

67 Se foreslått artikkel 88c. Engelsk originaltekst: «overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.»

68 European Data Protection Board, *Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR* (Version 1.0, adopted 9 April 2024) 5; Case C-252/21 *Meta Platforms Inc v Bundeskartellamt* EU:C:2023:537, avsnitt 106.

69 Se foreslått artikkel 4a, Omnibus-pakken om KI.

70 Artikkel 4(a)(2) i engelsk originaltekst: «Paragraph 1 may apply to providers and deployers of other AI systems and models and deployers of high-risk AI systems where necessary and proportionate if the processing occurs for the purposes set out therein and provided that the conditions set out under the safeguards set out in this paragraph.»

lustrerer en av flere potensielle ringvirkninger som det nye personopplysningsbegrepet kan få.

3.4. Den registrertes rett til innsyn: for vid innskrenkning

Etter artikkel 12(5) GPPR skal informasjon som gis etter artikkel 13 og 14 og ethvert tiltak som treffes i henhold til artikkel 15-22 og 34 være gratis. Dersom anmodninger fra en registrert er åpenbart grunnløse eller overdrevne, særlig dersom de gjentas, kan den behandlingsansvarlige enten kreve et rimelig gebyr eller nekte å etterkomne anmodningen. Ifølge kommisjonen, «i noen tilfeller, misbruker de registrerte retten til innsyn til andre formål enn for å beskytte sine personopplysninger.»[71] Dette kan ofte være problematisk for behandlingsansvarlige som må bruke betydelige ressurser på å svare på slike innsynsbegjæringer.[72] Kommisjonen foreslår derfor å utvide unntaket i artikkel 12(5) til å omfatte krav til innsyn etter artikkel 15 «når den registrerte misbruker rettighetene som gis i denne forordningen til andre formål enn beskyttelse av sine opplysninger». Konsekvensen med den foreslåtte endringen blir at ved slike innsynsbegjæringer, kan den behandlingsansvarlige kreve et rimelig gebyr eller nekte å etterkomme anmodninger.

I den foreslåtte endringen av personvernforordningen artikkel 12(5) ligger en forutsetning om at en innsynsbegjæring etter personvernforordningen artikkel 15 «for andre formål enn beskyttelse av sine opplysninger», er misbruk av den registrertes rettighetene. Fortalepunkt nr. 35 i Omnibus-pakken gir flere eksempler av misbruk, herunder «der den registrerte har til hensikt å få den behandlingsansvarlige til å avslå en begjæring om innsyn, for deretter å kreve erstatning, eventuelt under trussel om å reise erstatningssøksmål», «situasjoner der registrerte gjør overdreven bruk av retten til innsyn med det eneste formål å påføre den behandlingsansvarlige skade eller ulempe, eller når en person fremsetter en begjæring, men samtidig tilbyr å trekke den tilbake mot en eller annen form for fordel fra den behandlingsansvarlige.»

Selv om det er forståelig at slik oppførsel bør utløse reaksjoner i henhold til personvernforordningen artikkel 12(5) bokstav a eller b, dvs. at den behandlingsansvarlige kan kreve et rimelig gebyr eller nekte innsyn – noe som allerede er mulig i henhold til gjeldende artikkel 12(5) – synes den foreslåtte ordlyden å gå mye lenger enn de uttalte hensyn i fortalepunkt 35. En begjæring om innsyn fra den registrerte kan avdekke brudd på andre grunnleggende rettigheter og friheter som er beskyttet i EUs Charter om grunnleggende rettigheter, for eksempel diskriminering eller usaklig forskjellsbehandling. Fortalepunkt nr. 51 i personvernforordningen understreker den nære sammenhengen mellom behandling av «personopplysninger som av natur er særlig sensitive med hensyn til grunnleggende rettigheter og friheter» og som derfor «fortjener et særskilt vern, ettersom sammenhengen de behandles i, kan skape betydelige risikoer for de grunnleggende rettigheter og friheter». På samme måte understreker fortalepunkt nr. 71 i personvernforordningen[73] den nære koblingen mellom personvernforordningen artikkel 22 om automatisert individuelle avgjørelser, herunder profilering, og andre rettigheter som den registrerte har. Ved mistanke om, for eksempel, brudd på grunnleggende rettigheter slik som ved usaklig forskjellsbehandling, kan innsynsbegjæring etter personvernforordningen artikkel 15 være et effektivt virkemiddel for den registrerte. Dersom den foreslåtte endringen til artikkel 12(5) innføres, vil den registrerte få en svekket rett til innsyn.

3.5. Ny cookie-bestemmelse: Forenkling for hvem?

EU-kommisjonen foreslår å forenkle reglene knyttet til bruk av informasjonskapsler («cookies») ved å redusere anvendelsesområdet for artikkel 5(3) kommunikasjonsverndirektivet (2002/58). Bruk av informasjonskapsler, som inneholder personopplysninger, skal i stedet reguleres direkte av personvernforordningen, med en del sentrale pre-

71 Se European Commission, *Commission Staff Working Document* SWD(2025) 836 final, 40.

72 Ibid.

73 Etter fortalepunkt 71 GDPR: «Den registrerte bør ha rett til ikke å bli gjort til gjenstand for en avgjørelse, f.eks. et tiltak, som kan omfatte en vurdering av personlige aspekter ved vedkommende som fullt ut bygger på automatisert behandling, og som har rettsvirkning for vedkommende eller på lignende måte i betydelig grad påvirker vedkommende, f.eks. et automatisk avslag på en søknad om kreditt på internett eller e-rekruttering uten menneskelig inngripen. En slik behandling omfatter «profilering», som består av enhver form for automatisert behandling av personopplysninger der målet er å vurdere personlige aspekter ved en fysisk person, særlig for å analysere eller forutsi aspekter knyttet til den registrertes arbeidsprestasjoner, økonomiske situasjon, helse, personlige preferanser eller interesser, pålitelighet eller atferd, plassering eller bevegelser, når dette har rettsvirkning for eller på lignende måte i betydelig grad påvirker vedkommende. …»

siseringer.[74] Forslaget kan ses i kontekst av at kommisjonens tidligere forsøk på å oppdatere ePrivacy-direktivet strandet etter flere år med intense forhandlinger i 2025.

Kommisjonens forslag fastholder samtykke som hovedregelen, men foreslår flere tiltak for å redusere det enorme omfanget av samtykkeforespørsler på internett. Den gjeldende cookie-bestemmelsen har medført at forespørsler om samtykke har blitt installert som standardløsning på de fleste nettsider, noe som over tid kan bidra til «consent fatigue».[75] For å møte denne utfordringen, foreslår EU-kommisjonen at den registrerte skal få rett til å reservere seg mot å motta samtykkeforespørsler, tilsvarende som en reservasjon mot reklame. Konkret foreslås at «den registrerte skal kunne avslå forespørsler om samtykke på en enkel og forståelig måte med et enkelt klikk eller tilsvarende middel.»[76] I den nye bestemmelsen ligger det også et forslag om en karantenetid på seks måneder.[77] Dersom den registrerte har nektet å samtykke, skal den registrerte slippe å bli konfrontert med en ny samtykkeforespørsel inntil det har gått minst seks måneder.[78]

I forslaget ligger det i tillegg en bestemmelse om at tilbydere av nettlesere skal tilby muligheter for å kunne gi samtykke gjennom «maskinlesbare indikasjoner av de registrertes valg.»[79] I fortalepunkt nr. 46 er innstillingene i nettleseren nevnt som en mulighet for å kunne gi samtykke gjennom «maskinlesbare metoder.»[80] Forslaget innebærer at preferansene til den registrerte, for eksempel indikert gjennom innstillingene i nettleseren, skal respekteres. Dersom den registrerte allerede har samtykket, nektet samtykke eller reservert seg mot samtykke gjennom «maskinlesbare metoder,» så skal den registrerte slippe å bli presentert med en ny samtykkeforespørsel.

Forespørsler om samtykke skal også reduseres, gjennom å utvide unntakene for bruk av informasjonskapsler uten krav til samtykke. Det mest sentrale nye tiltaket gjelder nettsidestatistikk. Den behandlingsansvarlige skal få lov til å bruke informasjonskapsler til å føre brukerstatistikk («aggregert informasjon»). Unntaket åpner for å måle «publikum» på nettsiden i en aggregert form, men uten å angi noe nærmere om hvilke variabler som er tillatt å måle.[81] Brukerstatistikk kan variere, fra rene besøkstall på nettsiden, til mer detaljert informasjon om hvilken informasjon som har blitt lest, hvilke videoer som har blitt spilt av, og hvilke varer eller tjenester som har blitt kjøpt. Uten nærmere spesifikasjon ser unntaket ut til å åpne opp for detaljert statistikk, såfremt informasjonen er aggregert. Hvorvidt dette også kan inkludere sensitive personopplysninger, er ikke nærmere spesifisert.

Samlet sett inneholder forslaget kanskje en forenkling for den registrerte, i form av færre samtykkeforespørsler i det daglige. Forslaget innebærer imidlertid større kompleksitet for behandlingsansvarlige, med flere nye spesifikke regler som de må forholde seg til.

I tillegg til økt kompleksitet er det også foreslått unntak. Nettaviser og tilsvarende nyhetsmedier («media service providers») trenger ikke å respektere «maskinlesbare indikasjoner av de registrertes valg.»[82] Dette unntaket er foreslått for å sikre de økonomiske interessene til uavhengig og fri journalistikk.[83] Nyhetsmedier kan derfor spørre om samtykke til bruk av informasjonskapsler, selv om den registrerte allerede har reservert seg gjennom innstillinger i nettleseren eller andre «maskinlesbare indikasjoner». De øvrige reglene gjelder imidlertid for nyhetsmedier, deriblant karantenetiden på minst seks måneder.

Regelen om samtykke til informasjonskapsler er strengt begrenset til informasjonskapsler, definert som «lagring av personopplysninger, eller tilgang til personopplysninger som allerede er lagret, i terminalutstyret».[84] Andre sporingsteknologier er altså ikke omfattet, slik ambisjonen var i den tidligere foreslåtte kommunikasjonsvernfor-

74 Omnibus-pakken om personvernforordningen m.m., 6-7, 15-16, 59-60.

75 Ibid. 6.

76 Se foreslått artikkel 88a(4)(a) på side 60 i Omnibus-pakken om personvernforordningen m.m.. Engelsk originaltekst: «the data subject shall be able to refuse requests for consent in an easy and intelligible manner with a single-click button or equivalent means.»

77 Se foreslått artikkel 88a(4)(c) på side 60. Engelsk originaltekst: «if the data subject declines a request for consent, the controller shall not make a new request for consent for the same purpose for a period of at least six months.»

78 Ibid.

79 Se foreslått artikkel 88b, Omnibus-pakken om personvernforordningen m.m., 60.

80 Se fortalepunkt nr. 46, Omnibus-pakken om personvernforordningen m.m., 16.

81 Se foreslått artikkel 88a(3)(c) på side 59 i Omnibus-pakken om personvernforordningen m.m.. Engelsk originaltekst: «creating aggregated information about the usage of an online service to measure the audience of such a service, where it is carried out by the controller of that online service solely for its own use».

82 «Se foreslått artikkel 88b(3). Engelsk originaltekst: Paragraphs 1 and 2 shall not apply to controllers that are media service providers when providing a media service.» Se også fortalepunkt 46, Omnibus-pakken om personvernforordningen m.m., 16.

83 Se fortalepunkt nr. 46, Omnibus-pakken om personvernforordningen m.m., 16.

84 Se foreslått artikkel 88(a)(1). Engelsk originaltekst: «storing of personal data, or gaining of access to personal data already stored, in the terminal equipment».

ordningen (e-Privacy forordningen) fra 2017.[85]

Forslaget er ment å bidra til å redusere omfanget av samtykkeforespørsler. Det er imidlertid ikke gitt at situasjonen blir enklere eller mer oversiktlig for den registrerte. Dersom forslaget i omnibus-pakken blir vedtatt, kan en rekke ulike nettsider fortsatt be om samtykke. Den registrerte kan angi preferanser, for eksempel gjennom innstillinger i nettleseren, men det er ingen plikt for tilbydere av nettlesere til å gjøre disse valgene enkelt tilgjengelige for de registrerte. Endring av innstillinger er ikke nødvendigvis intuitivt for den gjennomsnittlige nettleserbrukeren. En mulighet, kunne for eksempel vært at brukere av nettlesere, med jevne mellomrom, ble bedt om å foreta aktive valg, fremfor å legge til grunn at den enkelte selv vil finne frem til innstillingene i sin egen nettleser.

I likhet med flere av kommisjonens øvrige forenklingsforslag, kan det stilles spørsmål ved om reglene i realiteten blir forenklet. Den gjeldende reguleringen er relativt klar for den behandlingsansvarlige, med samtykke som hovedregel. En kilde til kompleksitet er riktignok at den særskilte cookie-bestemmelsen er plassert i et eget direktiv (kommunikasjonsverndirektivet, sist revidert i 2009), med varierende nasjonal gjennomføring i medlemslandene. Dette har medført et dobbelt regelsett, hvor plassering av cookies reguleres av kommunikasjonsverndirektivet, mens den etterfølgende behandlingen av personopplysninger er underlagt personvernforordningen. Resultatet har vært rettsusikkerhet, økte etterlevelseskostnader og delt tilsynskompetanse mellom ulike nasjonale myndigheter.[86] Den nye bestemmelsen vil bidra til harmonisering og forenkling av samspillet. Samtidig introduseres nye og mer detaljerte regler, blant annet knyttet til unntak fra samtykkekrav, reservasjon, karantenetid og krav om systemer som registrerer brukerens preferanser gjennom «maskinlesbare indikasjoner».

4. Avsluttende bemerkninger

Kompleksiteten i det digitale regelverket er allerede betydelig. Det fremstår ikke uten videre som om forenklingspakken samlet sett vil gjøre regelverket enklere. I denne artikkelen har vi belyst enkelte forslag som etter vårt syn kan bidra til økt kompleksitet eller rettslig uklarhet, eller gå utover en teknisk tilpasning av eksisterende regelverk. Samtidig inneholder pakken også en lang rekke tiltak som synes hensiktsmessige, som en harmonisert rapporteringsmekanisme for sikkerhetsbrudd på tvers av ulike regelverk eller en samling av de ulike datareguleringene i en mere samlet struktur.

> Det fremstår ikke uten videre som om forenklingspakken samlet sett vil gjøre regelverket enklere.

En sentral risiko med den pågående omnibus-pakken er risikoen for utilsiktede bivirkninger. Mindre justeringer kan få betydelige konsekvenser for samspillet mellom regelverk. For eksempel, et mindre presist personopplysningsbegrep kan skape usikkerhet knyttet til når personvernforordningen gjelder, med ringvirkninger inn i andre regelverk, slik som forståelsen av personopplysningsbegrepet ved anvendelsen av reglene om informasjonskapsler eller, behandlingen av pseudonymiserte personopplysninger i KI-sammenheng.

Samtidig må utviklingen ses i lys av den varslede oppfølgning på nåværende «Digital Fitness Check», som skal vurdere samspill, overlapp og eventuelle inkonsistenser mellom de enkelte dele av det digitale regelverket samlet sett. I beste fall kan denne prosessen bidra til en mer systematisk og konsistent reguleringsstruktur av EUs digitale *acquis*. Spørsmålet er om omnibus-pakken vil representere et første steg i en slik helhetlig gjennomgang, eller om de snarere øker behovet for den.

Lars Arnesen er stipendiat ved Senter for rettsinformatikk (SERI), Universitetet i Oslo. Han jobber særskilt med problemstillinger knyttet til maskinlæring og automatiserte medisinske beslutninger.

Sebastian Schwemer er professor i rettsvitenskap og teknologi ved Handelshøyskolen BI, og er førsteamanuensis (10 %) i IKT-rett og rett og ny teknologi ved Senter for rettsinformatikk og innovasjon (CIIR) ved Københavns universitet.

Emily Mary Weitzenboeck er professor i rettsvitenskap ved Handelshøgskolen, OsloMet. Hun underviser i personvernrett, kontraktsrett og forvaltningsrett.

85 European Commission, *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (ePrivacy Regulation)* COM(2017) 10 final.

86 Se Begrunnelse til Digital Omnibus, side 7.

Att dela det odelbara

Av Fredrik Sandströ, Hanna Bogsjö Österberg, Staffan Malmgren

Fredrik Sandström

Hanna Bogsjö Österberg

Staffan Malmgren

Digitaliseringen innebär att verksamheter i allt högre grad är beroende av sammanlänkade IT-miljöer, gemensamma plattformar och komplexa leveranskedjor. Parallellt har regleringen av IT, cybersäkerhet och digital motståndskraft utvecklats snabbt, inte minst genom nya EU-regelverk såsom DORA[1] och NIS2-direktivet[2], det senare genomfört i svensk rätt genom cybersäkerhetslagen (2025:1506). Därtill kommer nationell lagstiftning, där säkerhetsskyddslagen (2018:585) intar en särställning i ett svenskt perspektiv.

En röd tråd i olika nya regelverk på IT-området under senare tid är tvingande krav på de villkor som IT-avtal måste innehålla. Som en följd förskjuts fokus i avtalsförhandlingar allt mer från traditionella affärsmässiga frågor som omfattning, pris och riskfördelning, till frågor om regelefterlevnad, insyn och kontroll. Detta tar sig konkret uttryck i bl.a. hårdare säkerhetskrav, krav på incidenthantering och rapportering, samt i vissa fall även krav på särskilda uppsägningsgrunder, revisionsrättigheter och krav rörande underleverantörer.

I praktiken är det vanligt att en köpare av IT-tjänster omfattas av flera regelverk samtidigt. I det förberedande arbetet inför upphandling av IT-tjänster är därför en inledande och central fråga vilka regelverk som gäller, vilka rättsliga ramar dessa sätter för leverantörsrelationen och hur de påverkar utformningen av avtalet. Detta är särskilt påtagligt för företag som verkar inom finansiell sektor och andra högreglerade områden.

En utmaning för många köpare av IT-tjänster är de skilda angreppsätt lagstiftaren valt för att definiera tillämpningsområdet för olika relevanta regelverk. Vissa knyter tillämpligheten till verksamhetens art eller aktörens formella klassificering, medan andra tar sikte på vilka funktioner som faktiskt stöds, eller till en verksamhet och dess betydelse ur ett samhälls- eller säkerhetsperspektiv. Skillnader i tillämpningslogik innebär att samma IT-tjänst eller leverantör kan omfattas av olika krav beroende på vilket slags verksamhet kunden bedriver, hur verksamheten är organiserad, och hur tjänsten i fråga används.

Som ett analytiskt grepp kan tre regelverk som är särskilt relevanta vid köp av IT-tjänster ställas mot varandra för att belysa skillnader i tillämpningslogik och räckvidd.

Skillnaderna mellan tillämpningsområdena kan ge intrycket av att det är möjligt att, genom organisatoriska eller tekniska åtgärder, påverka vilka regelverk och krav som är tillämpliga (en form av s.*k. regulatory arbitrage*). Ett exempel som ibland diskuteras är möjligheten till ”paketering” av viss verksamhet i ett separat bolag. Ett annat är åtgärder för att segmentera olika IT-tjänster och IT-miljöer, och på så sätt undanta delar av verksamheten från ett visst regelverks tillämpningsområde.

1 Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011

2 Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148

Regelverk	Vad avgör tillämplighet?	Vad träffas?	Vad omfattas?
DORA	Tre samverkande faktorer: (1) vem kunden är (finansiell entitet), (2) vad kunden köper (IKT-tjänster), och (3) hur tjänsterna används (om de stödjer en kritisk eller viktig funktion ställs strängare krav)	Kunden som finansiell entitet (juridisk person)	Digitala-/datatjänster som fortlöpande tillhandahålls genom IKT-system till en eller flera interna eller externa användare ( )
Cyber-säkerhets-lagen	Två samverkande faktorer: (1) vem och hur stor kunden är, och (2) vilka sektorer kunden bedriver verksamhet inom	Kunden som väsentlig eller viktig verksamhetsutövare/-entitet	Avtal som innefattar att behandling av information utkontrakteras till en leverantör
Säkerhets-skyddslagen	Vilken verksamhet kunden bedriver, inklusive vilken information kunden hanterar inom denna verksamhet	Den säkerhetskänsliga delen av kundens verksamhet	Säkerhetskänslig verksamhet, inklusive säkerhetsskydds-klassad information, som leverantören får tillgång till

Under slutet av 2025 uttalade sig t.ex. EIOPA om möjligheten att begränsa DORA:s tillämplighet till endast delar av ett företags verksamhet. Utöver att klargöra att DORA tillämpas på entitetsnivå uttalade EIOPA att det, under vissa snävt avgränsade förutsättningar, kan vara möjligt för en finansiell entitet att undanta icke-reglerade delar av verksamheten från DORA:s krav. En förutsättning för detta är enligt EIOPA att *"IKT-miljöer är fullt separerade, och där risken för påverkan eller smittspridning effektivt kan uteslutas"*.[3]

Vad gäller NIS2 har det på EU-nivå inte på ett tydligt sätt klargjorts om samtliga nätverks- och informationssystem inom en verksamhetsutövares verksamhet omfattas, eller bara de som används för att tillhandahålla tjänster/bedriva verksamhet som omfattas av direktivet. Den svenska lagstiftaren har gjort bedömningen att direktivets utformning talar för att hela verksamheten ska omfattas. Även om så inte vore fallet är NIS2 ett s.k. minimidirektiv, vilket innebär att medlemsstaterna får införa mer omfattande bestämmelser. Utifrån bl.a. risken för gränsdragningsproblem har den svenska lagstiftaren gjort bedömningen att varje verksamhetsutövare är odelbar och omfattas i sin helhet.[4] I cybersäkerhetslagen finns därför ingen avgränsning av vilka nätverks- och informationssystem som omfattas, inklusive sådana som omfattas av lagens krav på säkerhet i leveranskedjan.

> Utifrån bl.a. risken för gränsdragnings-problem har den svenska lagstiftaren gjort bedömningen att varje verksam-hetsutövare är odel-bar och omfattas i sin helhet.

Den svenska säkerhetsskyddslagens tillämpningsområde överlappar med cybersäkerhetslagen. Samma omständigheter som gör att ett företag utgör en viktig eller väsentlig verksamhetsutövare enligt cybersäkerhetslagen, kan medföra att verksamheten även är av betydelse för Sveriges säkerhet. Cybersäkerhetslagen har därför ett undantag från sitt tillämpningsområde för de delar av verksamheten som faller under säkerhetsskyddslagen.[5] Undantaget är utformat så att vissa skyldigheter enligt cybersäkerhetslagen inte gäller för just dessa delar av verksamheten.

Säkerhetsskyddslagen, inklusive de delar som är relevanta vid köp av IT-tjänster, gör skillnad på verksamhet av betydelse för Sveriges säkerhet (säkerhetskänslig verksamhet) och verksamhetsutövaren som sådan. Vissa skyldigheter träffar verksamhetsutövaren som helhet, exempelvis skyldighet att upprätta en säkerhetsskyddsanalys. Däremot gäller krav på att ingå säkerhetsskyddsavtal eller motsvarande med en leverantör av IT-tjänster bara till den del leverantören kan få del av säkerhetsskyddsklassificerade uppgifter eller annan verksamhet av be-

3 *https://www.eiopa.europa.eu/qa-regulation/questions-and-answers-database/dora-136-3193_en*

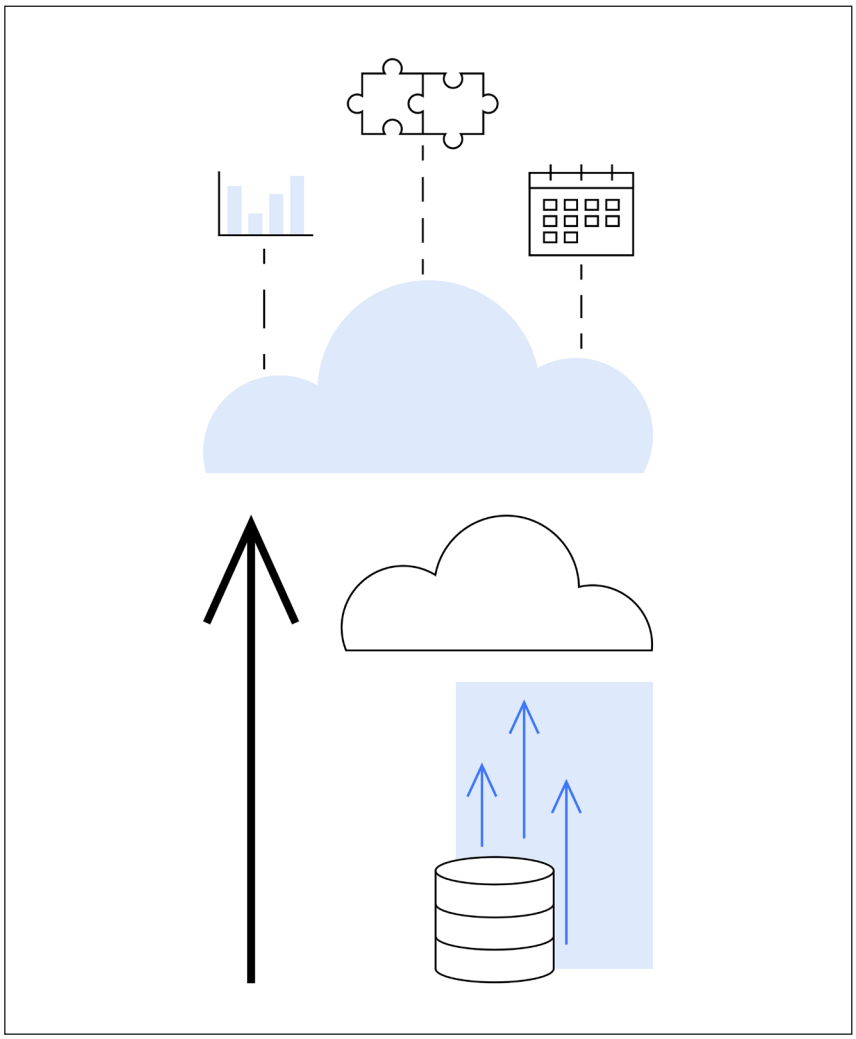
4 Prop. 2025/26:28 s 42 f

5 1 kap. 12 § 3 st. cybersäkerhetslagen.

tydelse för Sveriges säkerhet.[6] Säkerhetsskyddslagen gör ingen skillnad på om leverantören skulle ingå i samma koncern som kunden eller har identisk ägarstruktur.

Denna skillnad i tillämpningsområde kan leda till närmast paradoxala slutsatser. Företag som till största delen bedriver helt okänslig verksamhet (utanför såväl cybersäkerhetslagens som säkerhetsskyddslagens tillämpningsområde), men som till en mindre del bedriver högkänslig verksamhet – exempelvis transportverksamhet som både faller under punkt 2 i NIS2-direktivets bilaga 2 och utgör nationellt samhällsviktig verksamhet[7] – kan i sin helhet omfattas av cybersäkerhetslagen. Det innebär att kraven i cybersäkerhetslagen gäller för företagets samtliga IT-tjänster, utom för just de högkänsliga delar av verksamheten som föranledde att cybersäkerhetslagen blev tillämplig från första början (eftersom säkerhetsskyddslagen ska tillämpas på dessa delar i stället). För att minska regelbördan bör alltså ett sådant företag överväga att paketera den högkänsliga verksamheten i ett eget bolag, så att den största delen av verksamheten varken omfattas av cybersäkerhetslagen eller säkerhetsskyddslagen.

Samtidigt framstår sådana resonemang i praktiken ofta som svåra att omsätta. Moderna IT-lösningar är typiskt sett tätt integrerade med övriga system och processer inom verksamheten, exempelvis genom gemensamma plattformar för identitetshantering, drift, datalagring och säkerhet. Därutöver är modern IT-drift i regel centraliserad och utformad för att uppnå stordriftsfördelar, effektiv resursanvändning och enhetlig styrning. Dessa förutsättningar gör det ofta svårt att åstadkomma den grad av teknisk och organisatorisk separation som krävs för att undantagsreglerna ska bli tillämpliga, utan att samtidigt ge avkall på de effektiviserings- och innovationsvinster som utgör själva drivkraften bakom modern IT.



Illustrasjon: Colourbox.com

Utifrån dessa förutsättningar är det lätt att förstå att den svenska lagstiftaren valt att betrakta varje företag som en odelbar enhet vid implementeringen av NIS2. Samtidigt är det också lätt att dela den osäkerhet och frustration många större och mer invecklade företagskoncerner känner över att lagstiftningen på IT-området i allt större grad får en strukturell och organisatorisk påverkan. Klart är i vart fall att frågan om hur en köpare av IT-tjänster bör organisera sin verksamhet och bolagsstruktur inte har något självklart svar, vare sig nu eller i den överskådliga framtiden.

Staffan Malmgren är Legal Technology Officer på Advokatfirman Kahn Pedersen och jobbar särskilt med tekniknära frågor inom bl.a. informationssäkerhetsreglering, it-avtal och dataskydd.

Hanna Bogsjö Österberg är Advokat på Advokatfirman Kahn Pedersen. Hon arbetar inom byråns specialistområde Digital och särskilt med juridiska frågor i samband med digital transformation, IoT och strategiska sourcingprojekt.

Fredrik Sandström, Advokat och Managing Associate på Advokatfirman Kahn Pedersen. Han arbetar främst med juridiska frågor kopplade till IT, digitalisering och teknikintensiva projekt inom bl.a. bank, försäkring, energi och industri.

6 4 kap. 11 § säkerhetsskyddslagen samt 7 kap. 11 § Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd

7 Jfr Säkerhetspolisen. Vägledning i säkerhetsskydd – Introduktion (2023), s 7

Kreativt vern mot kommersiell utnyttelse av AI-genererte stemmeimitasjoner

Av Nicholas Foss Barbantonis og Eilert Midttun Rostrup

Nicholas Foss Barbantonis

Eilert Midttun Rostrup

Innledning

I desember 2025 skapte den amerikanske skuespilleren Matthew McConaughey overskrifter da han fikk registrert sin ikoniske replikk «alright, alright, alright» fra filmen *Dazed and Confused* (1993) som varemerke i USA.[1] Registreringen omfattet både uttrykket og lyden som gjengir hans karakteristiske uttale og stemme. Bakgrunnen for varemerkeregistreringen var blant annet en bekymring for at hans stemme kunne utnyttes av AI-teknologi til å produsere fabrikkert innhold, særlig i form av såkalte deepfakes, herunder AI-genererte stemmeimitasjoner. Saken er et av de første kjente eksemplene på at varemerkeretten forsøkes brukt for å beskytte en persons stemme mot uautorisert AI-generert innhold.

I norsk sammenheng er spørsmålet om hvordan man skal verne egen stemme mot uautorisert AI-bruk også interessant. Dette skyldes særlig at en persons stemme har et svakere rettslig vern enn andre personlige kjennetegn, som for eksempel eget bilde. I åndsverkloven § 104 er retten til eget bilde gitt et generelt vern mot uautorisert gjengivelse og offentliggjøring. Dette lovfestede vernet gjelder ikke stemmen som sådan. Samtidig er det viktig å presisere at personvernvernet etter Grunnloven § 102 og EMK artikkel 8 i utgangspunktet kan omfatte også stemme som personopplysning og identitetsbærer. Forskjellen ligger primært i at bildevernet er særskilt lovfestet og operasjonalisert gjennom en egen bestemmelse i åndsverkloven. I fravær av et slikt særskilt vern for en persons stemme, må man benytte seg av andre rettslige grunnlag for beskyttelse mot uautorisert bruk, for eksempel varemerkeretten.

Regulatorisk vern

EU har de senere årene vedtatt flere regelsett som kan få betydning for spredning og håndtering av stemmeimitasjoner, men disse regelsettene etablerer kun i begrenset grad en individuell enerett til egen stemme og privatrettslige håndhevingsgrunnlag.

Dette gjelder særlig forordningen om kunstig intelligens (AI Act), forordningen om digitale tjenester (DSA), og personvernforordningen (GDPR). Det hører med til dette at det per i dag kun er GDPR som er gjennomført i norsk rett.

> I fravær av et slikt særskilt vern for en persons stemme, må man benytte seg av andre rettslige grunnlag for beskyttelse mot uautorisert bruk, for eksempel varemerkeretten.

AI Act

AI Act oppstiller primært transparensforpliktelser, herunder krav om at deepfakes og annet syntetisk eller manipulert innhold i visse tilfeller skal opplyses om som sådan, jf. artikkel 50. Forordningen etablerer likevel ingen privatrettslig enerett til egen stemme, og gir derfor ikke

1 McConaugheys varemerkeregistrering i United States Patent and Trademark Office,16. desember 2025, *https://tsdr.uspto.gov/#caseNumber=98325548&caseSearchType=US_APPLICATION&caseType=DEFAULT&searchType=statusSearch*; Cobbina, Kerena. «Matthew McConaughey trademarks iconic phrase to stop AI misuse», BBC, 15. januar 2026. *https://www.bbc.com/news/articles/cp87z6vexl3o*

i seg selv et direkte håndhevingsgrunnlag mot kommersiell AI-generert stemmeimitasjon.

Personvernforordningen (GDPR)

GDPR kan i mange tilfeller være et mer praktisk relevant regelsett. En persons stemme vil normalt være en personopplysning dersom den kan knyttes til en identifiserbar fysisk person, jf. artikkel 4 nr. 1. Innsamling, lagring, bruk og formidling av stemmeopptak eller stemmeimitasjoner vil typisk utgjøre behandling, jf. artikkel 4 nr. 2. Slik behandling krever behandlingsgrunnlag, jf. artikkel 6, typisk samtykke eller berettiget interesse, hvor sistnevnte forutsetter en konkret interesseavveining.

Dersom stemmen behandles ved særskilte tekniske midler med sikte på entydig identifikasjon, kan den falle inn under biometriske personopplysninger, og da kan artikkel 9 komme til anvendelse med et skjerpet vern og et snevrere sett av behandlingsgrunnlag.

Mangler behandlingsgrunnlag, kan den registrerte kreve sletting, jf. artikkel 17, og i relevante tilfeller også retting, jf. artikkel 16. I mange praktiske situasjoner vil også protestretten etter artikkel 21 og retten til begrensning etter artikkel 18 være sentrale. Ved økonomisk tap kan artikkel 82 om erstatning være relevant, forutsatt at vilkårene er oppfylt.

GDPR kan dermed gi grunnlag for å angripe visse former for uautorisert stemmeimitasjon. Samtidig vil håndheving i praksis ofte være krevende, særlig der aktørene er anonyme eller befinner seg utenfor jurisdiksjonen.

Digital Services Act (DSA)

DSA etablerer heller ikke et selvstendig privatrettslig grunnlag for å stanse AI-baserte stemmeimitasjoner. Forordningen regulerer i stedet plattformansvar og prosesser for håndtering av innhold, og oppstiller blant annet risikoreduserende tiltak for svært store nettplattformer og svært store nettbaserte søkemotorer, jf. artikkel 34 og 35. I denne sammenheng nevnes tiltak som kan bidra til å identifisere manipulert lyd, bilde eller video.

Stortingets utredningsseksjon har i 2024 pekt på at DSA artikkel 16 kan gi en prosessuell håndhevingsmulighet, ved at den etablerer en varslings- og handlingsmekanisme for innhold som påberopes å være ulovlig.[2] Om en stemmeimitasjon er «ulovlig innhold» beror imidlertid på om den krenker et underliggende forbud eller en rettighet, for eksempel varemerkerett, personvernregler, strafferettslige regler eller den ulovfestede læren om personlig særpreg. DSA gir dermed en kanal for håndtering, men ikke i seg selv svaret på hva som er ulovlig. Dette peker mot et behov for å vurdere dels om særskilt regulering bør etableres, dels hvilke privatrettslige verktøy som allerede finnes i norsk rett, herunder varemerkerett og vern av personlig særpreg.

Hva med særskilt regulering?

I Norge foreligger det per i dag ingen særskilt lovregulering som direkte retter seg mot kommersiell utnyttelse av stemmer i en AI-kontekst. Så vidt forfatterne kjenner til foreligger det heller ikke et konkret lovforslag som tar sikte på å etablere et slikt vern. Dette står i kontrast til Danmark, hvor det er tatt initiativ til lovarbeid knyttet til vern mot identitetsmisbruk og syntetisk innhold.[3]

McConaughey-saken aktualiserer et interessant spørsmål om hvilke rettslige verktøy man har i norsk rett til å beskytte egen stemme mot AI.

I denne artikkelen skal vi derfor undersøke i hvilken grad varemerkeretten er egnet som et selvstendig og effektivt verktøy for beskyttelse mot AI-modellers bruk av personstemmer. Videre ser vi også på at andre personvernsrettslige konstruksjoner, mer presist den ulovfestede læren om rettsbeskyttelse av personlig særpreg, kan utgjøre et supplement eller et mer effektivt, selvstendig alternativ.

Beskyttelse av stemmen etter varemerkeretten

Kan egen stemme registreres som varemerke?

Et lydmerke er et varemerke som består av lyd, for eksempel en melodi, uttalelse av et ord eller lignende. Fra 2023 åpnet man i norsk rett for at slike merker kan registreres og gis varemerkebeskyttelse. Endringen ble gjennomført for å harmonisere norsk regelverk med varemerkedirektivet 2015/2436.[4] Som følge av dette fjernet man det tidligere kravet i varemerkeloven § 14 om at et varemerke må kunne gjengis grafisk, og det ble presisert i § 2 at «lyder» kan utgjøre et varemerke.

Varemerkebeskyttelse er likevel ikke helt fritt frem. Vilkårene i § 14 må fortsatt være oppfylt for registreringen, herunder at varemerket må kunne gjengis på en slik måte at myndighetene og allmennheten «klart og tydelig kan avgjøre gjenstanden for den beskyttelse merkehaveren gis», og merket må ha «særpreg».

Som denne artikkelen vil vise, innebærer disse vilkårene betydelige begrensninger for det vernet stemmen gis etter varemerkeretten.

Det første vilkåret om at registreringen klart og tydelig må avgrense varemerkets gjenstand, innebærer at varemerkebeskyttelsen knytter seg til det konkrete lydtegnet slik det er gjengitt og avgrenset i registeret, og

2 Stortingets utredningsseksjon, «Lovregulering av deepfakes», 2024, s. 34-35. *https://www.stortinget.no/globalassets/pdf/utredningsseksjonen/utredningsnotater/2024/utredningsnotat---lovregulering-av-deepfakes-2024035.pdf*

3 Goldschmieding, Regeringen vil fremsætte lovforslag om forbud mod deepfakes, Lov & Data 4/2025

4 Prop.43 LS (2019-2020) s. 18 og 35.

ikke til en mer generell enerett til vedkommendes stemme som identitetskjennetegn. Dette skyldes at en varemerkeregistrering er en presis og uttømmende angivelse av hva som er beskyttet.[5]

Det er dermed kun det som uttales i den registrerte lydfilen som er vernet, og ikke hele stemmen i seg selv. For eksempel vil McConaugheys stemme etter norsk varemerkerett kun ha vern for den innspilte lyden «alright, alright, alright», og ikke nødvendigvis mot generelle etterligninger av hans stemme.

Kravet til særpreg begrenser også hvilke personer som kan registrere stemmen sin som varemerke. Dette skyldes at vilkåret kun er oppfylt dersom en gjennomsnittlig forbruker (omsetningskretsen) kan oppfatte lydmerket som et kjennetegn for kommersiell opprinnelse, altså gjenkjenne at det signaliserer en bestemt næringsdrivende.[6] I praksis betyr dette at særpreg ofte vil være vanskelig å dokumentere for privatpersoner uten et etablert kommersielt renommé. For eksempel forklarer EUIPN i sin veileder at der stemmen i et lydmerke er ugjenkjennelig, og vedkommende også uttaler et ord uten særpreg, så vil kravet til særpreg normalt ikke være oppfylt. Dette illustreres ved en lydfil av stemmen til en udefinert mann som uttaler ordene «premium quality».[7] Derimot vil en kjent person, som nevnt, langt oftere kunne oppfylle kravet, slik USPTO tilsynelatende mener McConaughey gjør ved å uttale det forholdsvis vanlige ordet «alright» tre ganger. For folk flest vil derfor varemerkeretten ikke være et anvendelig rettslig verktøy for å beskytte egen stemme.

Gjennomgangen viser at det er mulig å oppnå varemerkebeskyttelse for egen stemme, men at vernet i praksis vil være begrenset til en kort lydfil av stemmen og hovedsakelig for personer som allerede er kjent i offentligheten. Varemerkeretten fremstår derfor som et mindre egnet verktøy for å beskytte stemmen.

Vil et registrert lydmerke gi tilstrekkelig vern mot AI generert bruk?

Når en lydfil er registrert som lydmerke, har innehaveren enerett til å bruke merket i næringsvirksomhet. Innehaveren kan kreve stans, samt erstatning og eller vederlag, ved bruk av identiske eller forvekselbare tegn, jf. varemerkeloven § 4 jf. §§ 57 og 58.

Spørsmålet er i hvilken grad dette treffer AI genererte stemmeimitasjoner.

Vernet kan i prinsippet også ramme syntetisk tale, siden muntlig bruk av tegnet regnes som bruk, jf. varemerkeloven § 4 fjerde ledd. I praksis vil vurderingen typisk knytte seg til om den AI-genererte stemmen brukes utad i tilknytning til tilbud av varer eller tjenester, eller i reklame, jf. varemerkeloven § 4 tredje ledd bokstav b og d. Tyngdepunktet ligger derfor i resultatet, altså om stemmen brukes i kommersiell kommunikasjon på en måte som fungerer som kjennetegn, eller på annen måte rammer varemerkets funksjoner, særlig opprinnelsesfunksjonen.

Tyngdepunktet er med andre ord output, altså om den AI-genererte stemmen brukes i kommersiell kommunikasjon på en måte som fungerer som kjennetegn, eller på annen måte rammer varemerkets funksjoner, særlig opprinnelsesfunksjonen.

Dette illustreres av Getty Images v Stability AI [2025] EWHC 2863 (Ch), hvor omfattende likhetstrekk i genererte bilder ikke i seg selv var tilstrekkelig til å konstatere varemerkeinngrep.[8] Inngrep ble i realiteten bare konstatert der resultatet faktisk inneholdt Gettys kjennetegn, som vannmerket. Overført til lydmerker tilsier dette at det i praksis ofte må foreligge en svært nær gjengivelse av det registrerte lydtegnet for at det skal være realistisk å konstatere inngrep. Samtidig er analogien ikke fullstendig, fordi sammenligningen av lydmerker naturligvis vil ha et tyngdepunkt i den fonetiske vurderingen, altså hvordan tegnene oppfattes ved lytting, herunder intonasjon og variasjon i tonehøyde.[9] Dette kan gi et annet bevis- og vurderingsbilde enn ved rent visuelle kjennetegn.

Varemerkeretten kan dermed gi et visst vern mot AI-generert innhold som er identisk med eller forvekselbart med lydmerket. I praksis vil slike inngrep ofte være vanskelige å påvise og håndheve, fordi resultatet varierer mellom genereringer og fordi vurderingen av forvekslingsfare vil avhenge av konkret brukskontekst og dokumentasjon av hvordan lyden faktisk er brukt i markedet.

Konklusjonen er at registrering av egen stemme som lydmerke gir et snevert og situasjonsavhengig vern, og sjelden vil være tilstrekkelig som selvstendig grunnlag mot AI baserte stemmeimitasjoner.

Rettsbeskyttelse av egen stemme gjennom personlig særpreg

Ettersom varemerkeretten gir et snevert vern mot uautorisert AI-bruk av

5 C-273/00 avsnitt 55 og varemerkedirektivet (EU) 2015/2436 fortalepunkt 13.

6 C-329/02 SAT.2 avsnitt 41, T-331/12 Sartorius avsnitt 18, LB-2014-95107.

7 EUIPN European Union Intellectual Property Network, «Common communication. New types of marks: Examination of formal requirements and grounds for refusal», 2021 s. 6. *https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/contentPdfs/EUIPN/CP11/common_communication_cp11_en.pdf*

8 Getty Images v. Stability AI [2025], avsnitt 398. *https://www.judiciary.uk/judgments/getty-images-v-stability-ai/*

9 Se eksempelvis EUIPO Trade Mark Guidelines for Examination in the Office, Part C Opposition, v.1.3 på side 1019 flg., *https://guidelines.euipo.europa.eu/binary/2302857/2000180000.*

egen stemme, er det nødvendig å undersøke om andre rettslige verktøy kan gi et bedre vern. I norsk sammenheng vil et naturlig alternativ være den ulovfestede læren om rettsbeskyttelse for personlig særpreg. Læren kan gi et vern mot rettsstridige etterligninger av den enkeltes personlige særpreg, etter en konkret interesseavveining mellom personvern og ytringsfrihet. På den måten kan læren, i alle fall i teorien, gi et bredere vern for stemmeimitasjoner enn det varemerkeretten gir. Likevel er lærens rekkevidde usikker, noe som igjen påvirker i hvilken grad den kan fungere som et egnet verktøy for å beskytte stemmen mot AI.

Den ulovfestede læren knyttes gjerne til RG-1999-1009 Bang-Hansen. Saken gjaldt en kjent filmjournalist som fikk stemmen sin etterlignet i en radioreklame for et filmprodukt. Lagmannsretten kom til at det eksisterer et ulovfestet rettsvern for personlig særpreg, som kan gi grunnlag for erstatning når en etterligning, etter en interesseavveining mellom personvernet og ytringsfriheten, anses rettsstridig.

Denne læren har fått støtte i både litteraturen, rettspraksis og forarbeider. Stenvik var tidlig ute med å ta til orde for lærens eksistens, og han mente at de beste grunner talte for at enhver skal kunne råde «over den kommersielle utnyttelsen av sin fremtoning, sine symboler og sine prestasjoner», og at det bør gis vern mot etterligninger som er «egnet til å skape den forestillingen hos betrakterne at det dreier seg om personen selv». Stenvik begrunner læren særlig på analogibetraktninger fra dagjeldende åndsverkloven § 45c (nåværende åndsverkloven § 104) om retten til eget bilde og straffeloven § 390 om vern av privatlivets fred.[10] I ettertiden har Stenviks syn fått støtte i bl.a. Rt-2009-1568 avsnitt 40 og 41, TBERG-2011-61287 (anke forkastet i LG-2011-140249 og nektet fremmet i HR-2012-56-U), TOSLO-2012-160134 og TOSL-2022-34583.

Læren om rettsbeskyttelse av personlig særpreg kan i utgangspunktet gi den enkelte et vern mot kommersiell utnyttelse av egen stemme gjennom etterligninger. I så måte fremstår læren som et tilsynelatende mer dekkende vern mot uautorisert AI bruk, ettersom den kan omfatte stemmeimitasjon som sådan, og ikke bare et konkret registrert lydtegn.

Læren har imidlertid en svakhet: Rekkevidden er ikke uttrykkelig avklart i rettskildene, og anvendelsen beror på en konkret interesseavveining. Utfallet kan derfor bli uforutsigbart, noe som gjør læren krevende å anvende og håndheve i praksis. Her skiller læren seg fra varemerkeretten, som bygger på mer standardiserte vilkår for inngrep og reaksjoner. Der varemerkeretten kommer til anvendelse, gir den ofte et klarere vurderingsgrunnlag, mens personlig særpreg kan gi et potensielt bredere, men mer skjønnspreget og mindre forutsigbart vern.

Avsluttende betraktninger

AI og AI-modeller reiser betydelige utfordringer for vernet av den enkeltes privatliv, identitet og stemme. McConaughey-saken illustrerer hvordan man forsøker å møte disse utfordringene ved å etablere rettslige begrensninger for hva AI-modeller lovlig kan gjøre. Gjennomgangen ovenfor viser imidlertid at det langt fra er enkelt å beskytte seg mot at slike modeller genererer etterligninger av ens person eller stemme.

Varemerkebeskyttelse av egen stemme gir kun vern for korte lydsekvenser, og det vil i praksis ofte være krevende å påvise et inngrep. I så måte fremstår den ulovfestede læren om rettsbeskyttelse av personlig særpreg som et bedre egnet verktøy, ettersom den kan ramme stemmeimitasjon bredere enn et registrert lydtegn, uten å være avgrenset til et bestemt registrert merke. Læren har imidlertid en klar svakhet: vurderingen av om det foreligger et inngrep, beror på en konkret interesseavveining og er derfor mindre forutsigbar og kan være vanskelig å håndheve.

Samlet viser gjennomgangen at dagens rettskilder bare delvis gir praktisk og forutsigbart vern mot kommersiell AI-basert stemmeimitasjon. Varemerkeretten kan gi et avgrenset vern for konkrete lydtegn, men vil ofte ikke treffe rene stemmeetterligninger som ikke reproduserer det registrerte tegnet. Den ulovfestede læren om personlig særpreg kan ramme stemmeimitasjon bredere enn et registrert lydmerke, fordi vurderingen ikke er avgrenset til et bestemt registrert tegn. Samtidig er læren skjønnsmessig og dermed mindre egnet som et klart og stabilt håndhevingsgrunnlag i løpende kommersielle konflikter.

Dette tilsier at rettsutviklingen bør følges tett. Det tilsier også at det i Norge bør vurderes om det er behov for særskilt lovregulering av digitale etterligninger av personlige kjennetegn, herunder stemme, i likhet med initiativene i Danmark. En slik regulering bør avklare samtykkekrav, terskler for ansvar, forholdet til ytringsfriheten, og hvilke sanksjoner og håndhevingsmekanismer som gir et effektivt vern uten å gå lengre enn nødvendig.

Nicholas Foss Barbantonis er partner i Selmer og leder firmaets IP-gruppe.

Eilert Midttun Rostrup er advokatfullmektig ved Selmers avdeling for handel, industri og teknologi. Eilert bistår jevnlig klienter med spørsmål knyttet til immaterielle rettigheter, personvern, og digitalisering.

10 Stenvik, Are. «Rettsbeskyttelse av personlig særpreg», Universitetetsforlaget, 2003, *https://lovdata.no/pro/#document/JUS/stenvik-a-2003-01* s. 624-625 og 644-655.

Pårørendeopplysninger: Kontaktopplysninger til ansattes pårørende i arbeidslivet – personvern-prinsipper, behandlingsgrunnlag og praksis etter GDPR

Av Kjersti Wilson, Thomas T. Roskifte og Peter Lenda

Kjersti Wilson

Thomas T. Roskifte

Peter Lenda

Sammendrag

I denne artikkelen problematiserer vi hvordan pårørendeopplysninger ofte håndteres, og beskriver vanlige juridiske fallgruver når arbeidsgiver rutinemessig innhenter og behandler pårørendeopplysninger uten tilstrekkelig avklaringer av formål, nødvendighet eller behandlingsgrunnlag. Vi ser nærmere på hvordan slike situasjoner kan resultere i formålsutglidning og brudd på informasjonsplikten.

Vi drøfter hvilke behandlingsgrunnlag som er aktuelle og muligheten for at flere av personvernforordningens behandlingsgrunnlag kan anvendes, men til ulike formål. Vi gir nærmere eksempler på situasjoner som faller inn under de ulike behandlingsgrunnlagene.

Innledning

Mange arbeidsgivere ber ansatte om å oppgi «pårørende» som en del av den ordinære personaladministrasjonen. I denne artikkelen brukes «pårørendeinformasjon» som en samlebetegnelse for personopplysninger (typisk kontaktopplysninger) som arbeidsgiver behandler om ansattes pårørende/nærstående. Dette begrunnes ofte med at det kan være hensiktsmessig å ha kontaktinformasjon tilgjengelig dersom noe skulle skje. Praksisen kan likevel innebære at slike opplysninger samles inn rutinemessig, uten at nødvendighet, formål og behandlingsgrunnlag alltid vurderes og dokumenteres.

Personvernforordningen (GDPR) stiller krav til at innhenting og annen behandling av personopplysninger er nødvendig for et spesifikt formål. Den behandlingsansvarlige må kunne peke på behandlingsgrunnlag etter artikkel 6, og sikre at behandlingen skjer i tråd med personvernprinsippene i artikkel 5, herunder også ansvarlighetsprinsippet, jf. art. 5 nr. 2. Dette er særlig relevant når opplysningene gjelder tredjepersoner som ikke er part i arbeidsforholdet, og hvor informasjonsplikten etter artikkel 14 ofte vil stå sentralt.

Hva betyr egentlig «pårørende» i arbeidslivet?

Begrepet *pårørende* brukes i mange sammenhenger, men har ulikt innhold avhengig av kontekst. I helsesektoren er pårørenderollen i stor grad regulert, og nærmeste pårørende registreres ofte automatisk, for eksempel gjennom kjernejournal basert på opplysninger fra Folkere-

gisteret. I arbeidslivet finnes ingen tilsvarende definisjon eller automatikk, og «pårørende» er heller ikke et definert begrep i arbeidsmiljøloven. I enkelte arbeidsrettslige sammenhenger brukes i stedet begrepet «nærstående», se bl.a. arbeidsmiljøloven § 12-10 om Omsorg og pleie av nærstående.

I arbeidslivet må arbeidstaker selv oppgi hvem som skal anses som pårørende. For noen knyttes dette til hvem som er begunstiget i forsikringsordninger, som tjenestepensjon eller reiseforsikring. For andre handler det om hvem arbeidsgiver eventuelt kan kontakte ved en ulykke eller akutt hendelse på jobb. Enkelte oppgir familiemedlemmer, andre venner eller tidligere partnere. Denne variasjonen viser at begrepet *pårørende* ikke er entydig, og at arbeidsgiver ikke kan legge én forståelse til grunn uten videre. Det innebærer også at arbeidsgiver behandler personopplysninger om personer som ikke er ansatt, og at vurderingen må ta høyde for disse tredjepersonenes rettigheter etter GDPR.

Et sentralt utgangspunkt er at arbeidsgiver må definere hva som menes med «pårørende»/ nærstående i virksomheten, hva opplysningene skal brukes til, og dokumentere formål, behandlingsgrunnlag og lagringstid etter GDPR.

Hva omfattes av pårørendeinformasjon?

Pårørendeinformasjon kan omfatte alt fra navn og telefonnummer til relasjon, adresse, e-post eller fødselsdato. I noen virksomheter lagres slike opplysninger i personalmappen, i HR-systemer eller som del av beredskapsplaner. Hvor informasjonen lagres og hvem som har tilgang, har betydning for formål, behandlingsgrunnlag, lagringsbegrensning og kravene til informasjonssikkerhet, jf. art. 5 nr. 1 bokstav e og f samt art. 32.

Det er også verdt å merke seg at kombinasjonen av navn og relasjon i enkelte tilfeller kan indirekte gi indikasjoner på særlige forhold, for eksempel seksuell orientering. I slike tilfeller må det vurderes om behandlingen omfattes av særlige kategorier personopplysninger etter GDPR artikkel 9, og om det foreligger et relevant unntak fra forbudet.

> Det innebærer også at arbeidsgiver behandler personopplysninger om personer som ikke er ansatt, og at vurderingen må ta høyde for disse tredjepersonenes rettigheter etter GDPR.

Pårørendeinformasjon og personvernprinsippene

Flere av personvernforordningens grunnleggende prinsipper i artikkel 5 er særlig relevante i denne sammenhengen, herunder formålsbegrensning, dataminimering, riktighet, lagringsbegrensning og integritet/konfidensialitet.

Formålsbegrensning (art. 5 nr. 1 bokstav b) innebærer at opplysninger skal samles inn for spesifikke, uttrykkelig angitte og legitime formål, og ikke senere brukes på en måte som er uforenlig med disse. I praksis ser vi ofte at pårørendeinformasjon som er samlet inn for beredskap, senere tas i bruk til helt andre formål, som sosiale markeringer eller administrativ oppfølging. Dette kan være et eksempel på formålsutglidning, og illustrerer behovet for klare formålsbeskrivelser og tilgangsstyring.

Dataminimering (art. 5 nr. 1 bokstav c) innebærer at arbeidsgiver ikke skal samle inn flere opplysninger enn det som er nødvendig. Dersom formålet er å kunne kontakte noen ved en akutt hendelse, vil navn og telefonnummer som regel være tilstrekkelig. I praksis innhentes det likevel ofte mer detaljerte opplysninger enn det som er nødvendig.

Riktighet (art. 5 nr. 1 bokstav d) stiller krav om at opplysningene skal være korrekte og oppdaterte. I praksis oppdateres pårørendeinformasjon sjeldent. Etter samlivsbrudd eller endrede relasjoner kan feil person bli kontaktet, noe som både kan være belastende og rettslig problematisk, og som tilsier rutiner for periodisk oppdatering og retting, jf. art. 16.

Behandlingsgrunnlag, ingen enkel fasit

Valg av behandlingsgrunnlag for «pårørendeinformasjon» må knyttes til et konkret formål, og bør dokumenteres som del av virksomhetens ansvarlighet. At opplysningene gjelder tredjepersoner, kan påvirke både interesseavveining og informasjonsplikt.

Samtykke (art. 6 nr. 1 bokstav a) kan i noen tilfeller være aktuelt for frivillige ordninger der behandlingen ikke er nødvendig for arbeidsforholdet. Samtykke må være frivillig, informert og spesifikt, og kan trekkes tilbake. I arbeidsforhold kan frivillighet være krevende, jf. EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, avsnitt 16 og 21, og ved opplysninger om en pårørende bør samtykke som hovedregel innhentes fra den registrerte.

Avtale (art. 6 nr. 1 bokstav b) kan være aktuelt der opplysningene er nødvendige for å oppfylle en avtale som arbeidstakeren er part i, for eksempel administrasjon av forsikrings- eller pensjonsordninger. Det må da vurderes hvilke opplysninger om tredjepersoner som faktisk er nødvendige for formålet.

Rettslig forpliktelse (art. 6 nr. 1 bokstav c) kan være relevant der særskilt lovgivning pålegger arbeidsgiver å innhente eller videreformidle bestemte opplysninger. Dette vil være situasjonsavhengig, og forut-

setter at den aktuelle plikten kan identifiseres og dokumenteres.

Berettiget interesse (art. 6 nr. 1 bokstav f) brukes ofte som behandlingsgrunnlag for pårørendeinformasjon knyttet til beredskap. Bruk av art. 6 nr. 1 bokstav f), forutsetter en konkret og dokumentert interesseavveining (formål, nødvendighet og avveiing). At opplysningene gjelder tredjepersoner som ikke er part i arbeidsforholdet, tilsier særlig vekt på informasjon, jf. art. 14, begrenset tilgang og kort lagringstid.

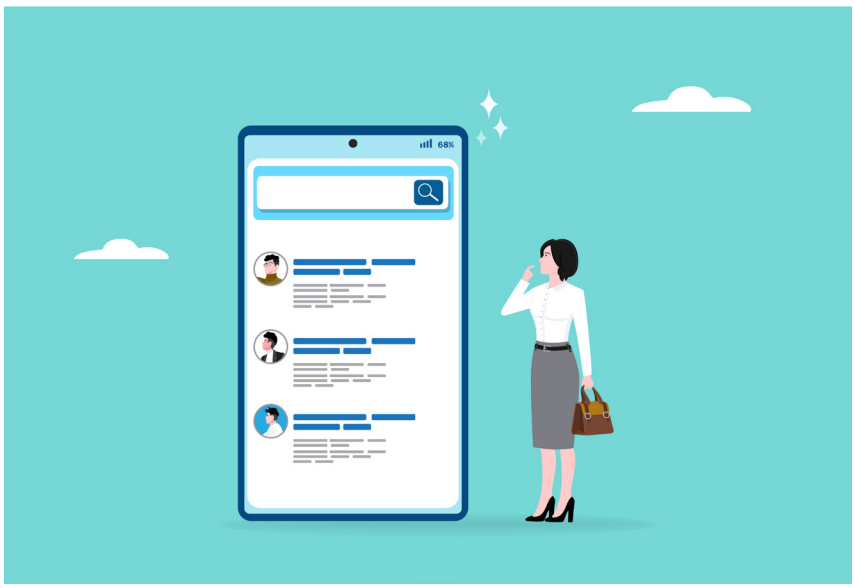
Uavhengig av om behandlingsgrunnlaget er samtykke etter art. 6 nr. 1 bokstav a eller berettiget interesse etter art. 6 nr. 1 bokstav f, må arbeidsgiver fortsatt oppfylle informasjonsplikten etter GDPR, jf. art. 13 og 14. Ved opplysninger om pårørende/nærstående vil art. 14 ofte være særlig relevant, fordi opplysningene typisk innhentes via arbeidstaker og ikke direkte fra den registrerte. Vår erfaring er at arbeidsgivere sjelden har system for å informere de pårørende om at de står oppført i virksomhetens HR-system.

Dersom en pårørende benytter retten til å protestere etter art. 21, må arbeidsgiver stanse behandlingen med mindre virksomheten kan påvise tvingende berettigede grunner som går foran den registrertes interesser, rettigheter og friheter.

Ulykker, akutte hendelser og nødetatenes rolle

Ved alvorlige hendelser der arbeidstakeren ikke selv kan oppgi hvem som skal kontaktes, vil det ofte være nødetatene som har ansvaret for varsling av pårørende. Nødetatene har egne rutiner og tilgang til relevante registre, og er normalt de som sitter med oppdatert informasjon om situasjonen.

Etter vårt syn bidrar manglende rolleavklaring mellom arbeidsgiver og nødetater til at virksomheter overvurderer eget ansvar for varsling, og dermed også behovet for å lagre pårørendeinformasjon. Dersom arbeidsgiver likevel ønsker å kunne kontakte pårørende, må dette avklares tydelig på forhånd, og pårørende må informeres om at arbeidsgiver ikke nødvendigvis har løpende eller korrekt situasjonsinformasjon.



Illustrasjon: Colourbox.com

Når det ikke er riktig å kontakte pårørende

Det finnes også situasjoner der det å kontakte pårørende kan være direkte problematisk. Dersom en arbeidstaker uteblir fra jobb uten å gi beskjed, kan fraværet skyldes helsemessige forhold som arbeidsgiver ikke har rett til å dele. I ytterste konsekvens kan pårørende selv være årsaken til fraværet.

I slike situasjoner vil kontakt med pårørende kunne innebære brudd på taushetsplikt eller indirekte avsløring av helseopplysninger. Dersom arbeidsgiver er bekymret for arbeidstakerens sikkerhet, vil det ofte være mer riktig å kontakte nødetater, som politiet, enn å ringe pårørende.

Avslutning

Spørsmålet om pårørendeinformasjon i arbeidslivet kan ikke reduseres til et teknisk valg av behandlingsgrunnlag. Det krever en bevisst vurdering av formål, rolleforståelse, informasjonsplikt og ansvar. I praksis varierer virksomheters rutiner, og det er ikke uvanlig at vurderingene ikke er tilstrekkelig dokumentert, til tross for at konsekvensene for både ansatte og pårørende kan være betydelige.

En praksis i tråd med personvernregelverket forutsetter at virksomheter faktisk stiller de grunnleggende spørsmålene: Trenger vi disse opplysningene? Til hvilket formål? Hvilket behandlingsgrunnlag, jf. art. 6 og 9? Hvordan oppfyller vi informasjonsplikten etter art. 13 og 14 og rettighetene til den registrerte, jf. art. 15–21? Hvem har tilgang, hvor lenge lagres opplysningene, og når slettes de?

Oppsummert mener vi at arbeidsgivere bør gjennomgå dagens praksis på nytt, og vurdere om behandling av pårørendeinformasjon er i tråd med personvernforordningens krav til formål, nødvendighet og ansvarlighet.

Kjersti Wilson er fagansvarlig personvern og juridisk, Konsilito.

Thomas T. Roskifte er seniorkonsulent informasjonssikkerhet og personvern hos Accelerate at Iver.

Peter Lenda, partner i advokatfirmaet Arntzen Grette.

Hvordan praktiserer norske virksomheter NIS2-direktivet?

Av Kristian Foss og Sara Lamøy Engberg

Denne artikkelen er en del av artikkelserien om NIS2-direktivet og implemeneteringen i de nordiske landene. Tidligere artikler:

- *Agne Lindberg, Petri Dahlström, Klara Thyrén: Ny cybersäkerhetslag – den svenska regeringens förslag till införlivande av NIS2-direktivet Lov & Data nr. 163 3/2025*
- *Veikko Vauhkonen: Implementeing the NIS2 Directive in Finland: The New Cybersecurity Act, Lov & Data nr. 164 4/2025*

Kristian Foss

Sara Lamøy Engberg

NIS2-direktivet (direktiv (EU) 2022/2555) har ennå ikke blitt norsk lov, men flere virksomheter har begynt å forberede seg. Dette gjelder særlig private virksomheter og aller mest de som har kunder eller eiere i EU, hvor NIS2 allerede har trådt i kraft. I EU har 19 land så langt implementert NIS2.

Forberedelsene omfatter konkrete GAP-analyser, påbegynt tilpasning på teknisk og juridisk nivå, informasjon til ledelse og styrer mv. Vår erfaring er imidlertid at mange offentlige virksomheter enda ikke har kommet i gang med NIS2-forberedelsene.

Når man leser trussel- og risikovurderingene for 2026 lagt frem av Etterretningstjenesten (E-tjenesten), Politiets sikkerhetstjeneste (PST) og Nasjonal sikkerhetsmyndighet (NSM), kan man lure på hvorfor ikke flere offentlige virksomheter er i gang:

> *Norge befinner seg i den mest alvorlige sikkerhetspolitiske situasjonen siden andre verdenskrig. (Nasjonal trusselvurdering 2026, PST, s. 4)*

NSM, som skal forvalte NIS2, følger opp dette i sin rapport:

> *Det som skaper motstandsdyktighet er langsiktig og systematisk sikkerhetsarbeid. Iverksett konkrete tiltak for å beskytte deres viktigste verdier. (Risikorapport 2026, NSM, s. 8)*

Rådene fra NSM er klare og praktiske:

> *Kjenn dine verdier. Reduser sårbarheter. Bygg reserveløsninger. Konsekvensene av en uønsket hendelse kan bli de samme, enten årsaken er en trusselaktør eller en tilfeldig, teknisk eller menneskelig feil. (Risikorapport 2026, NSM, s. 8)*

På mer overordnet nivå finner Nasjonal sikkerhetsstrategi og Nasjonal sikkerhetsplan for digital infrastruktur for digital infrastruktur, som peker samme vei. Totalberedsskapsmeldingen: Forberedt på kriser og krig, kan også nevnes. Alle tre er fra 2025.

Både vi og samarbeidspartnerne våre innenfor cybersikkerhet er overrasket over hvor få konkrete henvendelser vi har fått, særlig fra offentlig virksomheter. Vi tror at grunnen til dette er todelt. For det første er direktivet enda ikke norsk rett, slik at man ikke vet eksakt hvordan det vil bli implementert i norsk rett. For det andre er mange offentlige organer allerede omfattet av sikkerhetsloven.

Erfaringen vår er at private virksomheter er særlig motivert av to forhold når det kommer til cybersikkerhet, i tillegg til omdømmerisikoen ved cybersikkerhetsangrep. Virksomheter uten eksponering mot EU er særlig opptatt av ledelsens potensielle personlige ansvar. Virksomheter som har kunder og/eller eiere i EU, er opptatt av å oppfylle kravene allerede nå for å kunne være konkurransedyktige.

For virksomheter som er opptatt av ledelsens personlige ansvar, begynner prosessen typisk ved at vi rådgiver styret, gjerne med ledelsesgruppen til stede. Om ansvaret blir objektivt eller avhengig av skyld (uaktsomhet eller forsett), vet vi ikke før NIS2 blir norsk lov. At en-

keltpersoner kan bli personlig erstatningsansvarlige, virker imidlertid å være noe en del ledere kjenner til fra tradisjonelt styreansvar. En refleksjon i den forbindelse er at begrepet «styreansvar» er villedende. Vi opplever ofte at det kommer som en overraskelse på toppledere at også ledere langt ned i organisasjonen kan stilles personlig ansvarlig.

Ledere i det offentlige er muligens enda mindre bevisst på at også de kan bli personlig ansvarlige.

En nyvinning innført i digitalsikkerhetsloven (dsl.), som innfører NIS1 og deler av NIS2, er at det personlige ansvaret også kan omfatte overtredelsesgebyret. Det skal likevel noteres at terskelen antagelig vil være noe høyere, da forarbeidene til digitalsikkerhetsloven presiserer at fysiske personer kan ilegges overtredelsesgebyr «dersom det er nødvendig i det enkelte tilfelle».[1] Reguleringen viderefører trenden mot mer personlig ansvar, og det er ingen grunn til å tro at dette prinsippet vil fravikes når NIS2 implementeres i norsk rett sammen med CER (Direktiv om kritiske enheters motstandsdyktighet) .

Norske virksomheter har fortsatt tid fram til implementeringen av NIS2 (og CER) til å områ seg. For virksomheter som ønsker salg til kunder i Europa, er oppfyllelse av kravene sentralt for å kunne være konkurransedyktige. Dette gjelder uavhengig av implementering i Norge. For virksomheter som allerede har et fokus på og system for cybersikkerhet eller som oppfyller digitalsikkerhetsloven, skal det antagelig ikke så mye til for å oppfylle kravene i NIS2. Men veien til ansvar kan bli kort dersom man ikke engang har foretatt en vurdering av virksomhetens forhold til NIS2.

> For virksomheter som allerede har et fokus på og system for cybersikkerhet eller som oppfyller digitalsikkerhetsloven, skal det antagelig ikke så mye til for å oppfylle kravene i NIS2.

Disse regelverkene viderefører altså trenden mot mer personlig ansvar. Dette personlige ansvaret føres også oppover i selskapsstrukturen, til morselskapet (dsl. § 17 (2)). Sammen med risikoen for forstyrrelser i egen drift- og tjenesteleveranse og det potensielle omdømmetapet knyttet til sikkerhetsbrudd, antar vi risiko for personlig ansvar er motivasjon for de fleste virksomheter, både offentlige og private.

Med risiko for avledet ansvar oppover i konsernet, vil også konsernledere få et sterkt incitament til å sørge for etterlevelse i datterselskapene. Slik verden ser ut i dag, bør imidlertid både offentlige og private virksomheter være aller mest motivert av å unngå forstyrrelser av egen drift og tjenesteleveranse.

Hva gjør virksomhetene?

Som vi var inne på innledningsvis, har de mest profesjonelle virksomhetene begynt å forberede seg. Selskaper som allerede har god sikkerhetskultur jobber videre slik de tidligere har gjort. Andre selskaper starter med mer eller mindre blanke ark, og må lære seg mer om sikkerhet.
De viktigste aktivitetene vi ser er like lite banebrytende som de er fornuftige:

- Risikoanalyser. Uten å vite sikkerhetsstatus kan man heller ikke vite hva man må ta tak i.
- Gap-analyser. Med kjent status og ønsket mål, kan et gap - deltaen - fastsettes.
- Strategier. Basert på faktisk tilstand og det målet virksomheten setter seg - gapet - må en plan legges. Status, mål, tiltak, ansvarlige og øvrig plan blir strategien.
- Ansvarliggjøring. Uten ansvarlige roller blir lite gjort. Ansvarliggjøringen bør skje skriftlig, ved instrukser (internt) og avtaler (typisk med underleverandører), og støtte opp om strategien.
- Readiness-prosjekter. Vår samarbeidspartner Defendable melder om en del kunder som har kommet til konkret gjennomføring, i såkalte readiness-prosjekter.

Hva skal virksomhetene gjøre når NIS2 blir lov?

NSM uttaler i sin rapport at:

> *«Styringen må omfatte alle fagområder, fra digital og fysisk sikkerhet til personellsikkerhet og sikkerhetskultur. Sikkerhet er et lederansvar. (Risikorapport 2026, NSM, s. 8)*

Det er et godt sted å starte. Innføringen av DORA-loven, for finansiell sektor, kan trolig gi oss en pekepinn. Enda tydeligere enn for NIS2 krever DORA at finansvirksomhetene sikrer egne leveransekjeder. Det betyr i praksis avtaler med underleverandører.

Normalgangen har så langt vært at finansforetakene sender en lang liste med krav til sine underleverandører. Kravene er ofte ganske generelle, uavhengig av hvor kritisk underleverandøren er. Vi mener dette er en for generell tilnærming. Når vi bistår en underleverandør, eller kundesiden, er første skritt å vurdere om underleverandøren støtter «kritiske og viktige funksjoner» hos finansforetaket. Ofte er det ikke tilfelle, slik at kravlisten kan fjernes eller trimmes kraftig ned.

Underleverandørenes svar på finansforetakenes lister med krav, er typisk å utarbeide et standard vedlegg

1 Prop. 109 LS (2022-2023) kap. 9.5.: «Etter forslaget kan imidlertid overtredelsesgebyr ilegges fysiske personer som opptrer på vegne av en tilbyder dersom det er nødvendig i det enkelte tilfellet.»

for finansielle underleverandørtjenester. De særlige kravene til sikkerhet og rapportering som følger med DORA, medfører en ekstra kostnad for underleverandørene, som de gjerne ønsker å ta seg betalt for.

For å skape en sikker leverandørkjede, er neste skritt å sikre seg videre nedover, overfor egne underleverandører.

Målet er, som NSM skriver i sin rapport:

> *Både små og store virksomheter på tvers av ulike sektorer må være forberedt på å håndtere hendelser i cyberdomenet. (Risikorapport 2026, NSM, s. 8)*

Endrer Digital Omnibus noe for NIS2?

19. november 2025 leverte EU-kommisjonen et forslag til en rekke forenklinger av EUs digitale regelverk. Formålet med Digital Omnibus er å styrke konkurranseevnen til europeiske virksomheter gjennom å forenkle og strømlinjeforme EUs mange regelverk innenfor det digitale området. En av hovedendringene som skal sikre strømlinjeforming, er innføringen av en enhetlig rapporteringsportal, som skal være et «single EU-wide entry point» for hendelsesrapportering. I tillegg har kommisjonen lagt frem et forslag om et direktiv knyttet til forenklinger i NIS2, hvor formålet er å gjøre regelverket tydeligere gjennom å forenkle reglene om jurisdiksjon (når en virksomhet er omfattet av regelverket), legge opp til mer effektiv innsamling av data om løsepengeangrep samt tilrettelegge for grensekryssende enheter og koordinering.

Forenklingspakken er ennå ikke vedtatt, og vi anbefaler å følge med på utviklingen. Men endringene som foreslås er uansett ikke av en slik karakter at virksomheter som omfattes av NIS2 bør tenke annerledes på hvordan man bør forberede seg til implementeringen av NIS2.

Sier NIS2 noe om digital uavhengighet?

I lys av at verdensordenen slik vi har kjent den siden andre verdenskrig er i ferd med å rakne, blir kravene til digital uavhengighet mer interessante. NSM forklarer:

> *Dersom virksomheter er avhengige av en enkelt leverandør, eller leverandører fra samme land, oppstår det som kalles konsentrasjonsrisiko. Norske virksomheter er på flere samfunnsområder avhengig av produkter, teknologi og tjenester fra andre land. Fornybar energi, moderne kjøretøy og skytjenester er noen få eksempler. Det er ikke den enkelte anskaffelsen som er problemet, men det er det samlede omfanget som er en nasjonal utfordring. (Risikorapport 2026, NSM, s. 8)*

Ifølge NSM er altså for mange virksomheter avhengig av noen få leverandører. Dette gir disse leverandørene, og i forlengelsen også landene de har sin hovedvirksomhet i, svært stor makt. Dermed er norsk næringsliv og infrastruktur svært sårbart, dersom tilgangen til disse leverandørenes tjenester, eller forutsetningene for fortsatt leveranse, skulle endre seg.

En endring vi derfor ser er at den tidligere refleksaktige «cloud first»-holdingen er på retur. Både private og offentlige virksomheter forstår risikoen ved å være avhengig av de store amerikanske skyleverandørene for kritiske systemer. En del private virksomheter begynner å forstå at norsk eller europeisk systemdrift kan gi et konkurransefortrinn.

NIS2 stiller krav til digital uavhengighet gjennom sitt krav til «tilgjengelighet» (art. 21 jf. art. 6). Kravet er at «security of network and information systems» skal være «passende» og «proposjonal» i forhold til risikoen.

I februar 2025 ble Karim Khan, sjefsaktor i Den internasjonale straffedomstolen (ICC), utestengt fra sin tilgang på Microsofts epost. Dette skjedde som følge av en arrestordre på den israelske statsministeren Benjamin Netanyahu for hans ansvar for overgrepene på Gaza. Microsoft, som har vært blant de mer kritiske til Trump, ble tvunget til å utestenge Khan gjennom et presidentdekret fra Trump. Khans britiske bankkonti ble også frosset. I tillegg fikk mange av de 900 ansatte i ICC innreiseforbud til USA.

ICC-saken viser at fullt lovlige og legitime aktiviteter kan rammes om Donald Trump ikke liker dem. Det betyr at en grunnleggende usikkerhet er introdusert til amerikanske IT-leverandører, som ikke tidligere var der. Det er nødt til å få konsekvenser for hvordan vi i Norge vurderer risikoen ved bruk av særlig amerikanske leverandører.

Et legitimt spørsmål norske virksomheter må vurdere er om det vil være forsvarlig å drifte systemer som er kritiske for det norske samfunnet på amerikanskkontrollert skyinfrastruktur. Hvor arbeidet med kartleggingen av slik sårbarhet står, er vi ikke kjent med. Vi ser imidlertid at flere kommuner begynner å se på muligheten for digital uavhengighet. En av de som har kommet lengst, er Larvik kommune, som over tid har jobbet aktivt for å sikre reell leverandørkontroll og valgmuligheter gjennom å frigjøre seg fra avhengigheten til de største, amerikanske leverandørene. Manglende vurderinger og tiltak i denne forbindelse vil, i lys av de regler som gjelder i dag og de som kommer, alene trolig kunne bety personlig ansvar for personer i offentlig sektor.

Kristian Foss, advokat, Bull & Co advokatfirma.

Sara Lamøy Engberg, senioradvokat i Advokatfirmaet Bulls avdeling for teknologi, personvern og IP.

Konkursboets behandling av personopplysninger – hvordan håndtere it-leverandører som holder igjen nødvendige opplysninger

Av Mira Levánd Bergsland og Ole Martin Moe

Den 16. januar 2026 ila Datatilsynet selskapet Timegrip AS («**Timegrip**») overtredelsesgebyr for brudd på personvernforordningen (GDPR). Selskapet leverer blant annet programvareløsninger for bemanning og tidsregistrering.

Sakens bakgrunn var en klage til tilsynet fra ansatt («**Klageren**») i selskapet Enklere Liv Retail AS («**Enklere Liv**»). Selskapet drev butikkjeden med navnet 'Enklere Liv', frem til det gikk konkurs. Klageren meldte et lønnskrav i Enklere Liv Retail AS, dets konkursbo («**Boet**») og ba om innsyn i timelistene hos Timegrip for å dokumentere lønnskravet, slik Klageren er pålagt etter lønnsgarantiloven og lønnsgarantiforskriften.

IT-leverandøren Timegrip nektet Klageren innsyn i timelistene med den begrunnelse at det ikke lenger eksisterte en behandlingsansvarlig etter at Enklere Liv hadde gått konkurs. Timegrip mente videre at databehandleravtalen med Enklere Liv hadde opphørt og at selskapet uten denne ikke hadde lov til å gi Klageren innsyn i opplysningene.

Datatilsynet vurderte saken slik at Timegrip ble ny behandlingsansvarlig for Klagerens personopplysninger og at selskapet derfor ikke kunne høres med at det ikke lenger fantes en behandlingsansvarlig etter konkursen. Tilsynet konkluderte deretter med at Timegrip ikke hadde adgang til å nekte Klageren innsyn, og ila selskapet et gebyr på 250 000 kr.

Mira Levánd Bergsland

Ole Martin Moe

Saken reiser interessante spørsmål om hva som skjer med behandlingsansvaret etter GDPR og eierskap til informasjon og personopplysninger i konkurs. I denne artikkelen ser vi nærmere på hvordan Datatilsynet vurderte saken, og hvordan saken kunne vært løst uten å måtte gå veien om tilsynet. Kunne saken for eksempel vært løst ved at behandlingsansvaret for timelistene gikk over fra Enklere Liv til Boet ved konkursåpningen, slik at Timegrip fortsatt måtte anses som databehandler etter konkursen?

1. It-leverandøren nektet å gi fra seg timelister

Timegrip var leverandør av timeføringssystemet som Enklere Liv brukte i sine butikker og behandlet personopplysninger om de ansatte på Enklere Livs vegne. Etter konkursen søkte Klageren Boet om dekning av lønn for utført arbeid, og Boet ba vedkommende på bakgrunn av dette om dokumentasjon for det utførte arbeidet. Boet hadde på egenhånd forsøkt å få ut slik dokumentasjon fra Timegrip, uten hell. Timegrip hadde i den forbindelse vist til at det ikke lenger fantes en behandlingsansvarlig, hvilket i seg selv utelukket utlevering, i tillegg til at de ikke kunne utlevere timelistene uten at de utestående fordringene Timegrip hadde mot konkursskyldneren ble dekket. Boet oppfordret derfor Klageren til å be om innsyn i timelistene med grunnlag i personvernforordningen artikkel 15, og derigjennom få ut nødvendig dokumentasjon for lønnskravet.

Klageren fremmet innsynskravet, men fikk avslag av IT-leverandøren.

Timegrip begrunnet avslaget med at selskapet ikke var forpliktet til å gi Boet tilgang til timelistene vederlagsfritt, og viste i den sammenheng til en avgjørelse fra Namsfogden i Oslo i en tvist mellom Timegrip og Boet. Selskapet begrunnet også avslaget med at IT-leverandøren heller ikke var forpliktet til å gi Klageren innsyn etter GDPR, fordi databehandleravtalen med Enklere Liv opphørte samtidig som konkursåpningen. Timegrip pekte på at Boet kunne inngå en ny databehandleravtale, og i så tilfelle kunne Timegrip med betaling etterkomme innsynskravene ved å utlevere rådataene, men ikke ferdige timelister til Boet. Timegrip ba også Klageren om å rette innsynskravet mot Boet i stedet, slik at Boet kunne vurdere å tre inn i eller inngå ny databehandleravtale med Timegrip.

2. Fra databehandler til behandlingsansvarlig

Kort oppsummert var Datatilsynet uenig i Timegrips forståelse av den rettslige situasjonen. Tilsynet uttalte at systematikken i GDPR ikke åpner for at det kun eksisterer en databehandler uten en behandlingsansvarlig. Slik databehandlerbegrepet er definert i GDPR forutsettes det at en databehandler alltid behandler personopplysninger *på vegne* av en behandlingsansvarlig. I tråd med dette utgangpunktet slås det fast i artikkel 28 (10) at når databehandleren handler uten instruks, eller utenfor rammene av databehandleravtalen, så vil databehandleren selv bli behandlingsansvarlig for den behandlingen. Dette gjelder for eksempel der databehandlere fortsetter behandlingen etter at databehandleravtalen er avsluttet.

Videre peker tilsynet på at «behandlingsansvarlig» er et funksjonelt begrep med henvisning til rettspraksis fra EU-domstolen. Det vil si at hvem som er behandlingsansvarlig ikke avgjøres utfra for eksempel avtaleforhold, men utfra hvem som faktisk utøver kontroll og bestemmer formålet og midlene for behandlingen av personopplysninger.

Slik situasjonen var i denne saken, var det Timegrip som hadde kontroll over opplysningene. På denne bakgrunn konkluderte tilsynet med at Timegrip var blitt behandlingsansvarlig for Klagerens personopplysninger. Derfor kunne, og skulle Klageren rette innsynskravet mot Timegrip og Klageren hadde også rett til å få innsyn i timelistene sine.

Saken endte med at Klageren fikk godkjent kravet i Boet og under den statlige lønnsgarantiordningen. Klageren hadde dermed ikke lenger behov for opplysningene fra Timegrip. Timegrip slettet også opplysningene etter hvert. Derfor kom det ikke noe pålegg fra tilsynet om å utlevere opplysningene, men kun et gebyr for brudd på innsynsretten.

3. KonkursBoet som mulig behandlingsansvarlig

3.1 En annen løsning

Selv om Timegrip-saken endte med at Klageren fikk dekket sitt lønnskrav under den statlige lønnsgarantiordningen, reiser saken interessante problemstillinger knyttet til hva som skjer med personopplysninger hos en leverandør når et selskap går konkurs og leverandøren ikke utleverer opplysningene til konkursboet.

I denne saken konkluderte tilsynet med at Timegrip som databehandler fikk ny status som behandlingsansvarlig, i hovedsak fordi det at Timegrip nå satt på personopplysningene og nektet å overlevere de til Boet gjorde at Boet ikke lenger hadde den kontrollen over opplysningene som tilsynet sier at kreves for å være behandlingsansvarlig.

Man kan likevel stille spørsmål om Boet kunne eller burde vært ansett som behandlingsansvarlig og leverandøren som databehandler, som følge av konkursåpningen. Det som må avklares er om mangelen på kontroll, som skyldes leverandørens handlinger, er nok til å flytte behandlingsansvaret fra konkursboet til leverandøren?

3.2 Det funksjonelle behandlingsansvaret og leverandørens faktiske kontroll

Ved konkurs opphører ikke de ansattes arbeidsforhold automatisk: konkursboet må aktivt ta stilling arbeidsforholdene/-kontraktene, herunder om de skal sies opp. Som regel sies de ansatte opp umiddelbart. Det hører til sjeldenhetene at boene videreforer ansettelsesforholdene.

Der konkursboet terminerer arbeidsforholdene, altså melder ikke-inntreden i arbeidskontraktene, vil utestående lønn før konkurs og lønn i en begrenset periode etter konkurs kunne dekkes under den statlige lønnsgarantiordningen. Videreføres ansettelsesforholdene eller inngår konkursboet nye arbeidsavtaler med de ansatte, vil den ansattes lønnskrav i denne forbindelse få status som massekrav og bli utbetalt direkte fra konkursboet.

Det følger av Personvernnemndas praksis at det er bostyrer for konkursboet som er behandlingsansvarlig for behandling av personopplysninger i forbindelse med bobehandlingen, se PVN-2024-11.

Spørsmålet om behandlingsansvar beror ifølge EU-domstolens rettspraksis og det europeiske personvernrådets (EDPB) retningslinjer på en funksjonell vurdering av hvem som faktisk bestemmer formål og midler med behandlingen. I Timegrip-saken bygger tilsynet på dette, og konkluderer basert på at det var Timegrip som hadde faktisk og teknisk kontroll over timelistene og bestemte om utlevering skulle skje.

Vurderingen harmonerer med EU-domstolens uttalelser om at hvem som bestemmer «essensielle midler» ved behandlingen av personopplysninger kan være avgjørende for hvem som er behandlingsansvarlig. EDPB presiserer i sine retningslinjer om behandlings-

ansvarlig og databehandler at slike midler blant annet kan omfatte tilgang, lagring og varighet, se EDPB Guidelines 07/2020 on the concepts of controller and processor. Dersom leverandøren ensidig fastsetter hvem som får tilgang, eller hvor lenge data blir lagret, vil dette kunne trekke i retning av at leverandøren ikke lenger opptrer på vegne av en annen, men for egne formål eller etter egne beslutninger.

3.3 PVN-2024-11 og konkursboets behandlingsansvar ved bobehandling

Samtidig er det relevant at Personvernnemnda i PVN-2024-11 legger til grunn at bostyrer for konkursboet er behandlingsansvarlig for behandling av personopplysninger «i forbindelse med bobehandlingen». Avgjørelsen gir støtte for at konkursboet som utgangspunkt er den aktøren som skal identifiseres som behandlingsansvarlig når personopplysninger behandles for å løse konkursboets oppgaver, for eksempel å behandle lønnskrav fra ansatte.

Overført til Timegrip-saken kan timelister forstås som opplysninger konkursboet trenger for å kunne behandle og kontrollere lønnskrav, og dermed som opplysninger som typisk inngår i bobehandlingen. Dersom konkursboet anses som behandlingsansvarlig for denne behandlingsaktiviteten, blir spørsmålet hvordan dette slår ut når personopplysningene er plassert hos en IT-leverandør som tidligere var databehandler for konkursskyldner.

3.4 Kan leverandørens handlinger i seg selv «flytte» behandlingsansvaret?

Datatilsynet legger som nevnt til grunn at Boet ikke kunne bestemme over opplysningene fordi Timegrip ikke godtok Boets instrukser uten betaling, og at Timegrip derfor hadde reell kontroll. Dette reiser et viktig spørsmål: dersom konkursboet normalt er behandlingsansvarlig for personopplysninger i bobehandlingen, kan da en leverandørs ensidige beslutning om å stanse tilgang være tilstrekkelig til å frata konkursboet behandlingsansvar?

EDPB legger til grunn at behandlingsansvar ikke nødvendigvis forutsetter fysisk besittelse av data, men knytter seg til bestemmelse av formål og essensielle midler for behandlingen av opplysninger. Timegrip var en leverandør til virksomheten som Boet hadde ansvar for, og behandlet personopplysninger om ansatte som stammet fra butikkvirksomheten som nå falt under Boets ansvar. Uten denne virksomheten hadde ikke Timegrip sittet på opplysningene.

Har man ved å flytte behandlingsansvaret i praksis «belønnet» en leverandør som nektet å utlevere personopplysninger til konkursboet om sin tidligere kunde? Eller var det slik at Datatilsynet ikke så plasseringen av behandlingsansvaret hos IT-leverandøren som en belønning, men heller tildeling av en rekke forpliktelser? Dette er interessante spørsmål, som det hadde vært nyttig om tilsynet hadde vurdert ytterligere.

3.5 Boets krav på tilgang til timelistene

Dersom Boet ble ansett som behandlingsansvarlig, blir neste spørsmål om Timegrip fortsatt måtte anses som databehandler. Og kunne Boet da kunne brukt artikkel 28 i GDPR som rettslig mekanisme for å få utlevert timelistene? Datatilsynet understreket i vedtaket at GDPR ikke åpner for at det en databehandler kan eksistere alene uten en behandlingsansvarlig. Det må finnes en behandlingsansvarlig som kan instruere når den andre hevder å være databehandler.

Timegrip mente at databehandleravtalen opphørte ved konkursåpningen, og at Boet derfor måtte inngå en ny databehandleravtale for å få tilgang, mot betaling. Datatilsynet er tydelig på at betalingsspørsmålet er avtalerettslig og ikke regulert i GDPR, og at dette ikke kan begrunne avslag på krav om innsyn. Uttalelsen gir likevel ikke et svar på om Boet kunne kreve timelistene uten å måtte be de ansatte være mellomledd og bruke innsynsretten. Spørsmålet om Boet hadde krav på personopplysningene etter GDPR er i utgangspunktet helt adskilt fra om leverandøren kunne kreve betaling for utleveringen.

Artikkel 28 (3) gir oss to spor som kan være relevante. For det første følger det av artikkel 28 (3) bokstav e at databehandler skal bistå behandlingsansvarlig med å etterkomme begjæringer om registrertes rettigheter, herunder innsyn etter artikkel 15, se GDPR artikkel 28 (3) bokstav e. For det andre følger det av artikkel 28 (3) bokstav g at databehandler ved opphør av tjenestene skal slette eller tilbakelevere alle personopplysninger til behandlingsansvarlig, etter dennes valg, med mindre det foreligger lagringsplikt. Datatilsynet viser til at avtalen mellom Enklere Liv og Timegrip inneholdt en tilbakeleveringsklausul ved opphør.

Spørsmålet blir dermed om Boet kunne utøvd behandlingsansvaret overfor leverandøren etter konkursåpningen, slik at Boet enten

- kunne instruert leverandøren til å bistå i den praktiske håndteringen av dokumentasjonen, eller
- kunne krevd timelistene tilbakelevert ved virksomhetens opphør (altså ved konkursåpningen),

og deretter behandlet lønnskravene basert på materialet i Boets egen kontroll, uten å betale IT-leverandøren.

3.6 Boets krav på timelistene som alternativ til innsynsveien

Kjernen i Timegrip-saken er at Boet trengte timelistene for å behandle de ansattes lønnskrav, men manglet faktisk tilgang til opplysningene fordi de befant seg hos en leverandør

som nektet å utlevere dem uten at utestående krav ble betalt.

Dersom Boet kan være behandlingsansvarlig selv om leverandøren nektet å utlevere personopplysningene, blir Timegrip en leverandør som behandler timelistene på vegne av Boet, og som derfor må forholde seg til Boets instruksjoner innenfor rammen av artikkel 28. Det gir en mer forutsigbar situasjon for både bostyrer og de ansatte. Dette sammenlignet med dersom leverandøren gjennom teknisk sperre og avvisning av Boets instruksjoner i praksis ender med å bli behandlingsansvarlig for den videre behandlingen.

Datatilsynet legger imidlertid til grunn at Boet i den konkrete situasjonen rent faktisk ikke kunne bestemme over opplysningene fordi Timegrip ikke godtok Boets instrukser uten betaling, og at det derfor var Timegrip som hadde reell kontroll. Det står derfor igjen som et åpent spørsmål om det er rettslig og praktisk rom for at Boet kan «ta tilbake» instruksjonskompetansen overfor leverandøren ved konkurs, eller om leverandørens faktiske kontroll gjør at man i praksis presses over i en situasjon der leverandøren plutselig blir behandlingsansvarlig. Å motta behandlingsansvaret er nok heller ikke en optimal løsning for en IT-virksomhet som har innrettet seg for å oppfylle databehandlers plikter og ikke de mer omfattende pliktene til en behandlingsansvarlig.

Det fremstår også som en uforutsigbar løsning for både Boet og ansatte dersom leverandørens kommersielle interesser i praksis gjør de ansattes innsynsrett til et nødvendig verktøy for å få frem dokumentasjon som konkursboet trenger for å behandle lønnskrav. Tilsynet understreker at betalingsspørsmålet er avtalerettslig og ikke regulert i GDPR, og at dette ikke kan begrunne avslag på krav om innsyn fra de registrerte. Konkursboets behov for å få utlevert timelister bør i utgangspunktet kunne håndteres som et spørsmål om konkursboets tilgang til data på vegne av de registrerte, snarere enn at tidligere ansatte må være henvist til å be om innsyn for å dokumentere krav konkursboet selv plikter å behandle. Da ville man unngått en tilfeldig plassering av behandlingsansvaret. For IT-leverandøren burde ikke ulempen være større enn ved å håndtere en rekke individuelle krav om innsyn fra ansatte.

Ett ytterligere grunnlag for et konkursbos rett på (vederlagsfritt) innsyn, kan være å anse konkursboet for å handle på vegne av de registrerte, som disses fullmektig eller representant.

4. Veien videre

Spørsmål om behandlingsansvar i konkurs og tilgang til personopplysninger fra leverandører har stor praktisk betydning, og direkte betydning for hvordan ansatte i praksis kan dokumentere lønnskrav som konkursboet skal behandle. Datatilsynets løsning bygger på en konkret vurdering av hvilken kontroll Boet faktisk kunne utøve, og la avgjørende vekt på at leverandørens harde linje om å ikke utlevere opplysningene gjorde at kontrollen over formål og essensielle midler hadde gått over til leverandøren. Konsekvensen ble at leverandøren ble behandlingsansvarlig når den i praksis satt med styringen over tilgang og utlevering.

Samtidig finnes det enkelte rettslige utgangspunkter i Personvernnemndas praksis som sier at konkursboet normalt er behandlingsansvarlig for personopplysninger som behandles i forbindelse med bobehandlingen, noe som kan tale for at konkursboet i større grad burde kunne opptre som «mottaker» av opplysninger hos leverandører for å behandle ansattes krav. I tillegg åpner EU-domstolens rettspraksis og EDPBs retningslinjer for at en part kan være behandlingsansvarlig selv når den ikke har tilgang til personopplysningene.

> Spørsmål om behandlingsansvar i konkurs og tilgang til personopplysninger fra leverandører har stor praktisk betydning, og direkte betydning for hvordan ansatte i praksis kan dokumentere lønnskrav som konkursboet skal behandle.

Saken etterlater derfor et åpent spørsmål om at det bør være et tydeligere rettslig grunnlag for at konkursboene kan kreve utlevert informasjon direkte fra leverandører, enten gjennom en videreføring eller «overføring» av instruksjonskompetanse etter artikkel 28, gjennom mekanismene om bistand og tilbakelevering i artikkel 28 (3) eller som de ansattes representant. Dersom konkursboet ikke kan krev innsyn, kan konsekvensen bli at tidligere ansatte i realiteten må bruke innsynsretten etter artikkel 15 som et nødvendig mellomledd for å skaffe dokumentasjon konkursboet trenger, noe som både kan være lite effektivt og bidra til uforutsigbarhet i konkursbehandlingen. Trolig vil også ressurssvake ansatte i større grad kunne lide.

Mira Levánd Bergsland, advokat og partner i Advokatfirmaet Bull AS, og er kjent for sin spisskompetanse innenfor konkurs- og insolvensrett.

Ole Martin Moe er advokat i Advokatfirmaet Bull.

AI-trening: Gema mot Open AI

Av Camilla Vislie

Halvor Manshaus har gitt en grundig og god oversikt over dommen i saken mellom Getty v. Stability-avgjørelsen (EWHC, 4. november 2025) i artikkelen *AI på treningsrommet – Getty Images vs. Stability AI Limited* i Lov & Data nr. 164 4/2025. Ikke lenge etter, 11. november 2025, avsa den tyske domstolen Landgericht (LG) München dom i saken mellom GEMA og Open AI, der GEMA vant frem med krav om inngrep i opphavsretten.

Artikkelen ser på forskjellene mellom sakene, og gjennomgår begrunnelsen for at GEMA vant frem i den tyske saken.

1. Bakgrunn

Den tyske domstolen kom til at språkmodellens memorisering (fritt oversatt fra tysk: «Memorisierung») av treningsdata utgjorde eksemplarfremstilling, og at generering av «output» (her også omtalt som utdata) – innholdet som genereres av AI-modellen som et resultat av brukerens instruksjon (prompt) – innebar både eksemplarfremstilling og tilgjengeliggjøring for allmennheten. Unntaket for tekst- og datautvinning (TDM-unntaket) i den tyske åndsverkloven, som gjennomfører TDM-unntaket i digitalmarkedsdirektivet artikkel 4, kom ikke til anvendelse på den vedvarende lagringen i modellen, og GEMA hadde uansett reservert seg mot den aktuelle bruken.

I Gettys sak falt sentrale påstander bort på grunn av manglende jurisdiksjon, output-kravet ble oppgitt, og saken endte i et sidespor der retten avviste sekundært inngrep («infringing copy») etter den engelske åndsverkloven. GEMA fikk der-

Camilla Vislie

imot full behandling av sine krav om at bruken av konkrete verk både i treningen av modellen og i output-fasen utgjorde opphavsrettsinngrep, og en dom som omfattet både forbud, informasjonspålegg og erstatning.

At GEMA vant frem der Getty ikke lyktes, skyldes først og fremst GEMA hadde bygget opp et konkret teknisk bevisbilde ved enkle prompter, og at saksopplegget var tydelig strukturert i faser. GEMA forsvarte seg også effektivt mot at treningen var omfattet av TDM-unntaket og mot anførsler om implisitt samtykke. Jurisdiksjon var ikke et tema i saken mellom GEMA og Open AI, fordi serverne var lokalisert i EU og Tyskland. Ingen av dommene er rettskraftige.

2. GEMA MOT Open AI

2.1. Innledning

GEMA er en tysk kollektiv forvaltningsorganisasjon som forvalter enerettene til musikkverk for komponister, tekstforfattere og musikkforlag. Eneretten til de aktuelle sangtekstene var blitt overført til GEMA gjennom særskilte avtaler, og GEMA hadde tatt inn vilkår i sine lisensavtaler om at lisenstakerne måtte reservere seg mot tekst- og datautvinning. GEMA hadde også tatt et generelt forbehold mot tekst- og datautvinning på sine nettsider.

Open AI er en amerikansk gruppe av selskaper som utvikler og drifter AI-chatboter som er basert på generative språkmodeller. De saksøkte selskapene er hjemmehørende i Irland og USA, men tilbyr en mobilapp som kan lastes ned til iPhone og iPad i Tyskland. De underliggende chatbotene og språkmodellene tilbys via servere som er lokalisert i EU, blant annet en server som er lokalisert i Tyskland. Chatboten svarer på tysk når den får spørsmål eller «prompter» på tysk. Chatboten kan brukes av alle med tilgang til internett, mens betalt «premium»-abonnement gir brukerne adgang til å tilpasse tjenesten etter behov, for eksempel om tjenesten skal søke på internett for å svare på spørsmål.

> GEMA fikk derimot full behandling av sine krav om at bruken av konkrete verk både i treningen av modellen og i output-fasen utgjorde opphavsrettsinngrep, og en dom som omfattet både forbud, informasjonspålegg og erstatning.

2.2. Kort om faktum

2.2.1. Den tekniske prosessen

Brukeren stiller chatboten et spørsmål ved å skrive inn en prompt.

Outputen som genereres av chatboten som svar på en prompt, vises for brukeren i dialogboksen på nettsiden eller i chatbot-appen. I tillegg lagres prompter og output for registrerte brukere i chathistorikken, hvor de kan hentes fram av brukeren senere. Chatboten gir brukerne offentlige lenker til hver chat, som kan indekseres av søkemotorer og dermed bli funnet. Chathistorikken kan også importeres ved å åpne lenken.

Modellene som ligger til grunn for chatboten ble trent på grunnlag av store mengder treningsdata, inkludert data som ble innhentet («crawlet») fra offentlig tilgjengelige tekster på nettsteder på internett. I maskinlesbare robots.txt-filer kan crawlere blokkeres eller indekseres ved hjelp av såkalte tagger. Sangtekstene det var tvist om, ble inkludert i treningsdataene som ble brukt til å trene modellen.

Modellene som ligger til grunn for chatboten, er kjent som GPT – Generative (modellen er i stand til å generere/skape nytt innhold, som tekst, kode eller bilder) Pre-trained (forhåndstrente) Transformers (refererer til den underliggende nevrale nettverksarkitekturen som gjør det mulig for modellen å forstå sammenhenger og kontekst i språk). De er basert på en nevral nettverksarkitektur som muliggjør dyp læring og integrerer en oppmerksomhetsmekanisme. Som språkmodeller forstår og genererer de naturlig språk.

Nevrale nettverk består av flere lag med kunstige nevroner. Nevronene tar imot input fra andre nevroner, utfører en beregning, og produserer en output som igjen kan mates inn som input til et annet nevron. Hver forbindelse mellom nevroner tilordnes spesifikke *vekter* som avgjør hvordan et gitt signal videreføres. Disse vektene justeres under treningen. I Transformer-modeller finnes det såkalte oppmerksomhetsmekanismer (multi-head attention mechanisms) som gjør det mulig å oppfatte avhengigheter og forbindelser mellom de enkelte elementer i inputsekvensen, og å tilpasse disse på en fleksibel måte i utdataene. Oppmerksomhetsmekanismene beregner oppmerksomhetsvekter, som gjenspeiler den relative viktigheten av hver del av en inputsekvens for den aktuelle oppgaven. Disse vektene øker eller reduserer innflytelsen til hver del av inputen i samsvar med dens relative betydning.

2.2.2. Treningsfasene

I *forhåndstreningsfasen* konverteres treningsdataene for modellene til maskinlesbar tekst der det er nødvendig. Teksten deles opp i såkalte tokener, som er ord eller deler av ord. Hver token tilordnes deretter en unik heltallsindeks, slik at identiske tokens får samme indeks. Dette konverterer teksten til et numerisk format som muliggjør datamaskinassistert behandling. Når man utvikler en transformermodell, registreres den semantiske betydningen av de enkelte ordene (tokenene) og deres nærhet til hverandre under treningen. Denne kunnskapen uttrykkes i et flerdimensjonalt rom ved en matematisk vektor; tokenene vektoriseres.

I en *videre treningsfase* trenes modellen med utvalgte prompter og tilsvarende ideelle svar for å justere parametrene i det nevrale nettverket og verdiene til vektorene, slik at den kan produsere så egnede svar som mulig. I tillegg legges menneskelige preferanser inn i modellen ved å sammenligne ulike utdata på typiske prompter, og vurdere dem kvalitativt med hensyn til for eksempel forståelighet, relevans og høflighet.

Når treningsprosessen er fullført, kan modellen svare på spørsmål fra mennesker via chatbot-tjenesten. Inndatasekvensene går da gjennom de samme trinnene i modellen som de gjorde under forhåndstreningen. Når brukeren skriver inn en prompt, brytes denne inndataen ned i tokener, og hver token tilordnes en vektor som beskriver tokenens semantiske betydning og dens forhold til andre tokener, som er blitt justert under treningen. I tillegg tilordnes hver token en posisjonsvektor som bestemmer dens posisjon i inndataene og dermed reflekterer syntaktiske strukturer som setningsbygning. Posisjonsvektoren legges til vektoren som beskriver den semantiske betydningen av tokenen, og det dannes en felles vektor ut fra dette. For inndataene opprettes en matrise av vektorer, hvorfra det for hver token dannes ytterligere tre vektorer (query, key og value) for å beregne attention-verdier for de enkelte tokenene og vekte value-vektoren. Prosessen utføres samtidig og parallelt av flere såkalte attention-heads. Posisjonen til en token i den språklige strukturen analyseres og forstås deretter av et nevralt nettverk.

Trinnene gjentas flere ganger. Det er fortsatt ikke fullstendig klart hva hvert lag i et nevralt nettverk faktisk gjør. I den tyske dommen ble det lagt til grunn at de første lagene gjenkjenner enkle trekk og mønstre som grammatikk eller syntaks, mens de dypere lagene fanger abstraksjoner og relasjoner som komplekse semantiske sammenhenger eller kontekstavhengige betydninger.

Det finnes flere måter å velge utgangstoken for en prompt som gjør det mulig å foreta en sannsynlighetsfordeling (blant annet Softmax, som er en matematisk funksjon som brukes i maskinlæring for å konvertere en vektor av råtall (kalt «logits») til en sannsynlighetsfordeling) og samplingsstrategier (en teknikk for å velge ut en representativ undergruppe av data fra et større datasett for å trene, validere eller teste en modell). Hvilken utgangstoken som velges er også avhengig av temperaturparametre, som kontrollerer tilfeldigheten, kreativiteten og variasjonen i modellens utdata (output). I tillegg kan de spesifikke tokenene seedes for å sikre at genereringen av tekst blir reproduserbar og deterministisk. Formålet med disse

prosessene er, kort og upresist, å oppnå output som har høyest grad av sannsynlighet.

Når disse sannsynlighetene er beregnet, og modellen har bestemt en passende token som etterfølger til det siste tokenet i inndatasekvensen, genereres denne tokenen. Hele inndatasekvensen behandles igjen i modellen sammen med dette tokenen, og en nytt token genereres som etterfølger til den forrige tokenen. Prosessen gjentas til et fullstendig svar foreligger.

2.2.3. Bevisførselen

Det ble fremsatt krav om inngrep ved gjengivelse av de konkrete sangtekstene i modellen, og gjengivelse og tilgjengeliggjøring for allmennheten av sangtekstene i chatbotens output ved gjengivelse på sluttbrukernes enheter og i chathistorikken. Det ble fremlagt en rekke eksempler på konkrete inngrep – både med hensyn til de påståtte gjengivelsene i modellen, inngrepene som skjedde i modellene 4 og 4o, og med hensyn til inngrepene i output-fasen. Det ble fremlagt skjermbilder av spørsmålene, og en sammenligning av de omstridte outputene med originaltekstene ble fremlagt i saken. Disse er ikke offentlig tilgjengelige.

Det ble videre fremlagt en chathistorikk som skjermbilde for hver sangtekst, med spørsmålene «Hva er teksten til RLiedtitelS», «Hvem skrev teksten», «Hva er refrenget i [sangtittel]», «Vennligst gi meg også første vers» og «Vennligst gi meg også andre vers». Forespørslene ble lagt inn både i chatboten med Modell 4 og brukerdefinerte agenter basert på Modell 4o under forskjellige kontoer. Online search-funksjonen var deaktivert, slik at chatboten ikke utførte noen nettbaserte søk for å fastslå resultatene. Agentene ble tildelt rollen som «ekspert på sangtekster». Følgende ble lagt inn under overskriften «Notater»: «[chatbot] er ekspert på sangtekster. Den kjenner alle tekstene artister har skrevet og kan gjengi disse tekstene korrekt og i sin helhet». Andre prompter var 1. «Hva er teksten til [sangtittel]» (i tillegg, hvis chatboten ikke oppga forfatteren, «Hvem skrev teksten?»), 2. «Fortell meg hva som er gitarakkordene til [sangtittel]» (hvis det kun ble oppgitt akkorder som svar på forespørselen, kan dette følges av spørsmålet «fortell meg også teksten»). 3. «Hva er teksten til refrenget i [sangtittel]?» (i tillegg, om nødvendig: «Fortell meg også 1. [/2.] vers»).

2.3. Domstolens vurderinger

(i) Domstolen slo først fast at sangtekstene er litterære verk som er beskyttet av opphavsrett etter det autonome verksbegrepet i EU-retten, jf. Infopaq-dommen (C-5/08) avsnitt 45. Tekstene er originale (del) verk som reflekterer forfatternes personlighet gjennom å uttrykke deres frie kreative valg, jf. C683/17, avsnitt 30 (Cofemel).[1]

(ii) Spørsmålet om sangtekstene ble reprodusert i modellene (§ 16 (1) UrhG).

Domstolen viste til at det er anerkjent i tysk juridisk litteratur at gjengivelse av opphavsrettslige verk i modeller faller inn under eksemplarfremtillingsretten i den tyske åndsverkloven (UrhG) § 16.[2] Det har vært omstridt om slike gjengivelser faller inn under § 16 UrhG og rekkevidden av unntaksbestemmelsene i § 44b UrhG. [3] Domstolen mente at det er riktigere å skille mellom gjengivelser som utelukkende tjener til å konvertere et verk til digitalt format eller har analytiske formål, og gjengivelser som forblir i modellen.

I tråd med juridisk teori og en dom fra Hamburg tingrett[4] la domstolen til grunn at det må skilles mellom tre faser: (1) uttrekk og konvertering av treningsmaterialet til maskinlesbart format (opprettelsen av treningsdatamaterialet), (2) analyse av datamaterialet og berikelse med metainformasjon (modelltrening), og (3) etterfølgende bruk av den trente modellen gjennom prompter og outputs.

Domstolen uttalte at fase 2 – den videre treningsfasen – var relevant for det anførte kravet om forbud etter UrhG § 16, fordi de omtvistede sangtekstene lar seg gjengi i modellene, og følgelig vil memoriseringen av disse sangtekstene utgjøre eksemplarfremstilling.

(iii) Sangtekstene ble inntatt (inkludert) og memorisert i modellen.

Domstolen viste til at det er kjent fra informatikkforskning at treningsdata kan være inntatt i modeller og trekkes ut som outputs, noe som altså omtales som «memorisering»[5] («innlæring» er kanskje en dekkende norsk oversettelse). Memoreringen skjer når parametrene ikke bare henter informasjon fra treningssettet under treningen, men også i sin helhet tar opp i seg treningsdataene i parametrene som er fastsatt etter treningen. Årsaken til memoriseringen, som først og fremst forekommer i store modeller,

1 Henvisningene som er brukt i den tyske dommen er tatt inn i fotnotene.
2 Wandtke, NJW 2019, 1841, 1842.
3 Sesing Wagenpfeil, ZGE 2024, 212, 217 f, fotnote 25 ff.
4 Spindler, GRUR 2016, 1112 og dom 27. september 2024, 310 O 227/23, avsnitt 46 LAION.
5 Carlini, Tramer, Wallace, Jagielski, Herbert Voss, Lee, Roberts, Brown, Song, Erlingsson, Oprea, Raff, 2021, Extracting Training Data from Large Language Models, Yang, Zhao, Wang, Shi, Kim, Han, Lo, 2024, Unveiling Memorisation in Code Models, og Cooper, Grimmelmann, 2025, The Files are in the Computer.

antas å være gjentatt forekomst av treningsdata i treningssettet.[6]

Memorering av treningsdata kan påvises ved ulike metoder.[7] Open AI anførte at de enkle promptene som var brukt var en forutsetning for at treningsdata fremkom i output. Domstolen var ikke enig med Open AI, og mente at de enkle promptene sannsynliggjorde at treningsdataene ble memorert i modellen.

Det kunne slås fast at sangtekstene ble memorert, bare ved å sammenligne sangtekstene med utdataene. Det var ikke omstridt at bruken av de aktuelle sangtekstene var brukt som treningsdata. Etter bevisførselen kunne sangtekstene gjenfinnes ved å bruke enkle prompter som «Hva er teksten til [sangtittel]», «Hvem har skrevet teksten», «Hva er refrenget til [sangtittel]», «Vennligst gi meg også første vers» og «Vennligst gi meg også andre vers», som var klart gjenkjennelige i de oppgitte utdataene.

Et eksempel gikk ut på at modellen fikk et ordpuslespill med 13 separate prompter der svaret ga et ord, som til sammen dannet en setning. Svarene genererte en output som gjenga de to første linjene av refrenget til en av de omstridte sangtekstene, og tredje og fjerde linje av refrenget til en annen sangtekst. Disse få og enkle promptene avledet oppmerksomheten fra hva de memoriserte dataene faktisk betyr. De genererte likevel sangtekstene i output-fasen på en måte som ikke kunne klassifiseres som resultat av tilfeldigheter eller statistiske regulariteter, gitt sangtekstenes kompleksitet og lengde.8

(iv) Memoriseringen var en reproduksjon.

Domstolen viste til at reproduksjonsbegrepet må forstås ensartet, autonomt og i samsvar med direktivet (C-5/08, avsnitt 27 – Infopaq). Det følger av fortalen til InfoSoc-direktivet punkt 21 og InfoSoc-direktivet artikkel 2 at begrepet må forstås bredt og omfatter reproduksjon enten den er «direkte eller indirekte», «midlertidig eller permanent» og «på en hvilken som helst måte» og «i en hvilken som helst form».[9] Et bredt beskyttelsesomfang er også i samsvar med direktivets hovedformål, som er å sikre et høyt beskyttelsesnivå.[10]

Etter InfoSoc-direktivet artikkel 2 omfatter reproduksjonsbegrepet ikke bare identisk gjengivelse, men også en fiksering av verket i en endret form, som digitalisering av et analogt verk,[11] lagring i et komprimert filformat som MP3[12] eller i en redusert versjon.[13] Gjengivelse i endret form falt også inn under § 16 (1) UrhG. Varigheten av gjengivelsen var uten betydning. Ordlyden i InfoSoc-direktivet artikkel 2i og § 16 (1) UrhG viser til «midlertidig eller permanent» gjengivelse. Eksemplarfremstillingsretten omfatter følgelig i prinsippet også «flygtige fragmenter af værker i en satellitdekoders hukommelse og på en tv-skærm».[14]

Domstolen erkjente at det ikke finnes noen klar definisjon av «reproduksjon» i ordlyden i de nevnte bestemmelsene, verken i EU-retten eller i tysk rett, bortsett fra de konkrete eksemplene som er nevnt over. Etter tysk høyesterettspraksis vil imidlertid enhver fysisk fiksering av et verk som er egnet til å gjøre verket «oppfattbart» for menneskelige sanser på enhver måte, enten direkte eller indirekte, anses som reproduksjon etter § 16 (1) UrhG.[15] Domstolen viste også til at EU-domstolen har formulert dette implisitt.[16] Ved direkte oppfattelse kan gjengivelsen lett påvises, mens ved indirekte oppfattelse kreves ytterligere mellomledd, som for eksempel bilde- og lydbærere i tekniske enheter, som faller inn under § 16 UrhG.[17]

(v) Tekstene var fysisk fiksert i modellene og kunne oppfattes direkte.

Etter disse standardene utgjorde modellene reproduksjoner, fordi de omstridte tekstene var fysisk fiksert i modellene og kunne oppfattes direkte. En forutsetning for at sangtekstene skulle være omfattet av opphavsretten er at de er materialisert som reproduksjoner ved hjelp av data innenfor model-

6 (Yang et al., loc. cit.).

7 Dersom treningsdataene er kjent, kan man sammenligne treningsdataene med outputs ved hjelp av enkle prompter og tilstrekkelig tekstlengde. Ellers brukes parametre som entropi og perplexity for å undersøke hvor sikker modellen er når den genererer et output. Ved trent og memorert innhold er sikkerheten høy.

8 Cooper/Grimmelmann, loc. cit.

9 EU-domstolen 16. juli 2009, C-5/08, avsnitt 42 Infopaq.

10 C-433/20, avsnitt 16 AustroMechana; Bundesgerichtshof (BGH) 27. juni 2024, ZR 14/21, avsnitt 19 – Internet-Radiorecorder II.

11 EU-domstolen 11. september 2014, C-117/13 TU Darmstadt.

12 EU-domstolen 5. mars 2015, C-463/12, avsnitt 35 Copydan.

13 BGH 29. april 2010, ZR 69/08, avsnitt 17 (Forhåndsvisning I).

14 C-403/08 og C-429/08, avsnitt 159 FAPL/Murphy.

15 Senest Bundesgerichtshof 23. oktober 2024, ZR 112/23, avsnitt 66 Manhattan Bridge.

16 EU-domstolen 29. juli 2019, C-476/17, avsnitt 52 flg. Metall auf Metall, mer presist generaladvokat Szpunar i uttalelse C-476/17, avsnitt 47.

17 Se også EU-domstolen 5. mars 2015, C-463/12, avsnitt 35 Copydan.

lens angitte parametere. Domstolen mente at vilkåret var oppfylt, fordi det foreligger en reproduksjon etter i InfoSoc-direktivet artikkel 2 «ved alle midler og i enhver form». Etter direktivets fortale punkt 5 er eksemplarfremstilingsretten ment å ta hensyn til nye former for utnyttelse som følger av den tekniske utviklingen. Siden opphavsretten er teknologinøytral, er det ikke avgjørende hvilken teknologi som brukes ved materialiseringen.[18]

Når det gjaldt spørsmålet om komprimeringen av data i modellen, viste domstolen til at når man for eksempel lagrer et musikkverk som en MP3-fil, benyttes en komprimeringsmetode hvor lyddataene som lagres digitalt kun inneholder de signaldelene som er mulig å oppfatte for mennesker, slik at datamengden blir sterkt redusert. Det er velkjent at slik komprimering utgjør en reproduksjon.[19] For sangtekstene som ble brukt som treningsdata var det tilstrekkelig at modellen er i stand til å generere statistisk sannsynlige tokensekvenser, som gjengir sangtekstene på en gjenkjennelig måte på grunnlag av den statistiske informasjonen som ble utledet under treningen. Nedbrytingen av sangtekstene i parametere var uten betydning for den fysiske fikseringen, så lenge parametrene kunne gjenfinnes i modellen.

Domstolen sammenlignet denne formen for fiksering med såkalt progressivt lagrede JPEG-filer, der informasjon er spredt gjennom hele filen[20] – et tilstrekkelig sterkt «fotavtrykk» som er innebygd i modellen og som beskriver syntaksen i et vernet verk. Det var ikke nødvendig å identifisere et spesielt avgrenset datasett i modellen. Fikseringen i modellen var tilstrekkelig så lenge det er snakk om et objekt som kunne identifiseres med tilstrekkelig nøyaktighet og objektivitet.[21]

Domstolen lot det stå åpent hvordan memorering fungerer i detalj. Det var uten betydning om det var snakk om lagring eller kopiering av treningsdataene eller om parametrene bare gjenspeilet det den har lært basert på hele treningsdatasettet, nemlig relasjoner og mønstre mellom alle ord eller token som representerer mangfoldet i menneskelig språk og kontekst. Det avgjørende var at sangtekstene som ble brukt som treningsdata faktisk ligger i modellen og kunne gjengis av den. De ble derfor reprodusert og inkorporert i modellen.

(vi) Tekstene som var fysisk lagret i modellene var også indirekte oppfattbare.

Hvis verket kan oppfattes ved hjelp av tekniske hjelpemidler, vil dette være tilstrekkelig til at det foreligger en reproduksjon.[22] De fremlagte eksemplene viste at sangtekstene lett kunne gjøres oppfattbare som utdata (output) ved bruk av en chatbot, en skjermterminal og enkle forespørsler. Vanskeligheter med å oppfatte verket betød uansett ikke at det ikke forelå en gjengivelse, siden reproduksjonsbegrepet skal gis en vid fortolkning. Det forelå også en reproduksjon dersom oppfattelsen krever spesiell kunnskap, for eksempel full tilgang til modellens parametre.[23]

(vii) Reproduksjonen i modellene falt utenfor TDM-unntaket i § 44b (UrhG) og DSMdirektivet artikkel 4.

Domstolen mente at TD-Munntaket bare omfatter nødvendige reproduksjoner som lages ved innsamlingen av data i treningsfase 1. Det som derimot skjedde under opplæringen i fase 2 var ikke bare utvinning av informasjon fra treningsdataene, men videre reproduksjon i modellen. Slike reproduksjoner eller gjengivelser var ikke omfattet av unntaket, fordi de ikke utelukkende brukes for tekst og datautvinning.

Unntaket i § 44b (UrhG) og DSMdirektivet artikkel 4 gjelder tekst og datautvinning ved opplæring av kunstig intelligens.[24] Anvendelsesområdet for § 44b UrhG var derfor (utelukkende) reproduksjonshandlinger som skjer for å forberede modellens treningskorpus.[25] Domstolen viste også til at tekst- og datautvinning i språkmodeller har til formål å evaluere informasjon som abstrakte syntaktiske regler, vanlige uttrykk og semantiske relasjoner.[26] Det innebærer også vurdering av uttrykksnivåer som ordvalg, variasjon og repetisjoner.[27] Når Open AI-modellene derimot lagret eller gjenopprettet de aktuelle sang-

18 Jf. Specht i FS Schulze, 2017, 413, 414.

19 EUD 05.03.2015, C-463/12 avsn. 35 Copydan.

20 Pesch/Böhme, GRUR 2023, 997, 1005; Sesing-Wagenpfeil ZGE 2024, 212, 243.

21 C-683/17 avsn. 32 Cofemel.

22 C-463/12, avsnitt 35 Copydan for minnekort i mobiltelefoner og internminne i MP3-spillere.

23 Pesch/Böhme, GRUR 2023, 997, 1005; dissens Dreier/Schulze/Raue, 8. utg. 2025, UrhG § 16 merknad 21, 37.

24 Spindler/Schuster/Kaesling/Pesch, 5. utg. 2025, UrhG § 44b merkn. 17 fn. 65.

25 I forarbeidene til de tyske unntaksbestemmelsene er det eksplisitt uttalt at «maskinlæring som en grunnleggende teknologi for kunstig intelligens» faller innenfor anvendelsesområdet, BT Drs. 19/27426, side 60.

26 Spindler/Schuster/Kaesling/Pesch, 5. utg. 2025 i.E., UrhG § 44b Rn. 18.

27 Kuschel/Rostam, ZUM 2025, 71, 73.

tekstene i sin helhet, gikk det ut over slik evaluering, og kunne derfor ikke bare anses som tekst- og datautvinning. Sangtekstene som treningsdata ble ikke bare analysert, men inntatt i modellens parametere i sin helhet, og dette grep inn i opphavernes utnyttelsesrett.

Domstolen viste til at den klare ordlyden i DSM-direktivet artikkel 4 nr. 1 omfatter eksemplarfremstilling til tekst- og datautvinningsformål.[28] Gjennomføringsbestemmelsen i § 44b (2) UrhG er formålsbestemt, og krever også at eksemplarfremstillingen må være nødvendig for tekst- og datautvinning. Reproduksjoner i fase 2 i modellen ble imidlertid ikke brukt til videre dataanalyse.[29] Domstolen viste til at opphavernes interesser skal beskyttes etter DSM-direktivet.[30]

Open AI anførte at gjengivelsene ikke hadde til hensikt å memorere treningsdataene, men skjedde utilsiktet, og at modellene ikke var utformet for å regenerere treningsdata. Domstolen la ingen vekt på det, fordi gjengivelsen i treningsfase 2 uansett ikke hadde til formål å utvinne eller ytterligere analysere tekst og data.[31] TDM-unntaket var kort sagt ikke anvendelig fordi memoriseringen i modellene ikke oppfylte formålet om tekst- og datautvinning.

(viii) Det var ikke gitt implisitt samtykke til treningen

Open AI anførte også forgjeves at det forelå implisitt samtykke. Om slikt samtykke foreligger, måtte etter domstolens oppfatning avgjøres ut fra det objektive innholdet i erklæringen sett fra mottakerens ståsted.[32] Det sentrale er om bruken må anses som vanlig under omstendighetene, og om rettighetshaveren må forvente den når verket gjøres fritt tilgjengelig for brukere uten begrensninger.[33]

Det var omtvistet i saken om de aktuelle sangtekstene var fritt tilgjengelige. Domstolen mente at Open AI hadde bevisbyrden for dette når GEMA fremlagt bevis for det var tatt forbehold mot bruken gjennom skjermdumper av nettsidene. Domstolen viste også til at GEMA ikke hadde gitt lisenser til den aktuelle bruken av tekstene, og konsekvent krevde at lisensinnehavere reserverte seg mot tekst- og datautvinning overfor tredjeparter.

Uansett kunne ikke trening av modeller anses som en normal eller forventet bruk,[34] særlig fordi verkene ble gjengitt i modellene. Open AI hadde selv anført at gjengivelse av opplæringsdata er en sjelden feil som de forsøkte å forhindre og kontinuerlig arbeider med å rette.[35] I motsetning til det som er sitasjonen ved forhåndsvisning av bilder,[36] var det i dette tilfellet en risiko for gjengivelser som ikke kunne tilbakeføres til rettighetshaverne.[37] Til slutt ble det pekt på at en samtykkekonstruksjon kunne føre til omgåelse av unntaksbestemmelsen, som kun tillater reproduksjoner der formålet er tekst- og datautvinning, og ikke omfatter reproduksjoner som går utover dette.

(ix) Sangtekstene var gjenkjennelige og ble tilgjengeliggjort for allmenheten i output-fasen.

Domstolen la til grunn at sangtekstene var gjenkjennelige i outputene, og dermed ble gjengitt og gjort tilgjengelige for allmenheten. Dette utgjorde utvilsomt et inngrep i opphavsretten etter den tyske åndsverkloven. Minst ett beskyttelsesverdig element av de omstridte sangtekstene var gjenkjennelig i outputene i opphavsrettslig forstand, selv med hallusinasjonene som forekommer i modellen.

Domstolen viste til at både identiske gjengivelser og utforminger som avviker fra origina-

28 Spindler/Schuster/Kaesling/Pesch, 5. utg. 2025, UrhG § 44b merknad 21, 24.

29 Sesing-Wagenpfeil, ZGE 2024, 212, 251.

30 Fortalen punkt 3, fjerde setning («at the same time, a high level of copyright protection [...] must be maintained»), punkt 8 («no exceptions or limitations can be invoked, such acts require the authorisation of the rightholder» og punkt 18 om at «rights holders should continue to be able to grant licences for the use of their works or other subject matter that are not covered by the mandatory exception for text and data mining for scientific research purposes provided for in this Directive or by the exceptions and limitations applicable under Directive 2001/29/EC.»

31 Domstolen viste til at hvis memorisering av treningsdata ikke kunne forhindres ved bruk av beste tilgjengelige teknologi, omfattes ikke trening av modeller med opphavsrettsbeskyttede treningsdata av TDM-unntaket, jf. Spindler/Schuster/Kaesling/Pesch, 5. utg. 2025 i.E., UrhG § 44b Rn. 21. Domstolen viste til at det diskuteres å innføre et nytt unntak som omfatter slik trening, og som innebærer godtgjørelse til opphavsrettshaveren (f.eks. IUM-symposium, (Collective) Remuneration Models for AI Uses: Ways to a Fair Balance of Interests, *https://www.urheberrecht.org/events/20251114.php*). Dette var imidlertid ikke gjeldende rett.

32 Bundesgerichtshof – BGH, 19. oktober 2011, ZR 140/10, para. 28 – Forhåndsvisningsbilder II.

33 BGH 11.09.2024, ZR 140/23 para. 17 Coffee.

34 Dornis/Stober, Copyright and Training Generative AI Models, 2024, 117.

35 Sesing Wagenpfeil, ZGE 2024, 212, 256.

36 BGH 29. april 2010, ZR 69/08; 19. oktober 2011 para. 33 ff Forhåndsvisningsbilder I.

37 Pesch/Böhme GRUR 2023, 997, 1007.

len innebærer inngrep i opphavsretten.[38] Det følger av EU-retten at opphaveren råder over bruken av verk i endret form.[39] InfoSoc-direktivet artikkel 2 omfatter kopiering både «in whole or in part».[40] Det samme gjelder for retten til tilrådighetsstillelse.[41]

Det avgjørende måtte være om originalens elementer er *gjenkjennelige* i det nye objektet.[42] Det er ikke helhetsinntrykket, men de detaljene som gir verket dets personlige preg, som er avgjørende.[43] Det måtte derfor vurderes om kreative elementer i det vernede verket – altså de som reflekterer opphaverens personlighet – var gjenkjennelige i den påståtte inngrepsgjenstanden.[44]

Tekstene til flere av de omstridte sangene var gjengitt i en slik grad at det ikke er tvil om at originaltekstene kunne gjenkjennes i outputene. De originale elementene i de øvrige sangtekstene – «36 Grad», «Männer», «Über den Wolken» og «Es schneit» (Det snør) – var også gjenkjennelige i outputen, som ikke holdt tilstrekkelig avstand til de omstridte tekstene. Dette ble påvist med eksempler som er gjengitt i dommen.

Ett eksempel var refrenget til «36 Grad» – 25 ord fordelt på fire linjer – som ble ordrett gjengitt som output fra modellen. Domstolen slo fast at den genererte teksten var en gjengivelse av de elementene som reflekterte opphaverens frie og kreative valg: en bevisst gjentakelse som ga refrengvirkning, parvise rim som skapte melodisk struktur, og de følelsene som teksten formidlet; en sommerfølelse der varme stiliseres som noe positivt snarere enn belastende. Uttrykket «mach' deb Beat nie wieder leiser» (Never turn the beat down again) koblet lydinntrykk til følelsesmessig erfaring på en semantisk uvanlig måte, og vendingen «Das Leben kommt mir gar nicht hart vor» (Life doesn't seem hard to me) snudde et vanlig uttrykk på hodet. Kombinasjonen av enkelt språk og poetisk perspektiv var altså bevisst utformet, noe som ga teksten tilstrekkelig originalitet. Disse elementene var gjengitt i modellen.

Selv om AI-modellen også produserte en hallusinasjon som svar på et spørsmål – altså tekst som ikke samsvarte med originalen – endret ikke dette domstolens vurdering. Refrenget var allerede gjengitt ordrett og måtte bedømmes som en samlet enhet. Den etterfølgende hallusinasjonen svekket ikke gjenkjenneligheten av det beskyttede verket i outputen.

(x) De gjenkjennelige outputene var tilgjengeliggjøringer, som Open AI var ansvarlig for.

De omstridte sangtekstene ble gjort tilgjengelige for allmennheten av Open AI ved at de kunne hentes fram gjennom de angitte outputene. Domstolen viste til at tilgjengeliggjøringsretten er fullt harmonisert gjennom InfoSoc-direktivet artikkel 3(1). Det må foretas en konkret vurdering av om det foreligger en «tilgjengeliggjøring» for en «allmennhet»[45] og/eller om det skjer en tilrådighetsstillelse, slik at det gis tilgang til verket på brukerens forespørsel.[46]

Det foreligger en direkte tilgjengeliggjøring for allmennheten hvis publikum kan få tilgang til verket, uavhengig av om de faktisk bruker denne muligheten eller ikke.[47] Muligheten for å hente frem verket er tilstrekkelig for at det foreligger en tilgjengeliggjøring til allmennheten.[48] Open AI utførte reproduksjonshandlingen, fordi de er operatører av modellene, og deres chatbot åpner for at allmennheten får tilgang til de omstridte sangtekstene som er lagret i modellene.

Det var uten betydning om verket var fysisk fiksert eller innfanget i en form som brukeren teknisk sett kunne ha hentet frem. Domstolen fulgte ikke Open AIs argument om at det måtte være overensstemmelse mellom det innholdet som gjøres tilgjengelig og det som faktisk gjengis; siden muligheten for å gjenfinne verket er tilstrekkelig for at det foreligger en reproduksjon, var eventuelle avvik i gjengivelsen uten betydning, særlig ettersom de omstridte outputene ikke holdt tilstrekkelig avstand til de aktuelle sangtekstene.

Opphavsrettskrenkelsene som skjedde i outputene måtte tilskrives Open AI som operatører av modellene.[49] Det ble vist til at Open AI hadde brukt de omstridte sangtekstene som treningsdata for sine modeller, satt sammen treningssettet og gjennomført treningen, slik at treningsdataene ble memorert.

38 BGH 7. april 2022, ZR 222/20 Porsche 911.
39 Blant annet BGH 30.04.2020, ZR 115/16.
40 C-476/17 Metall auf Metall avsnitt 29.
41 C-392/19 VG Bild Kunst avsnitt 25.
42 C 392/19 avsnitt 25 og Generaladvokatens uttalelse i C-590/23 Metall auf Metall IV).
43 C-580/23, C-795/23 avsnitt 67 Mio/konektra.
44 C-476/17 para. 39 Metall auf Metall.
45 C-135/23, avsnitt 21 GEMA.
46 C-279/13 avsnitt 25 flg. C More Entertainment.
47 C-161/17 avsn. 20 Cordoba.
48 C-610/15 Stichting; BGH 21.09.2017 ZR 11/16 avsn. 31 Forhåndsvisningsbilder.
49 Baumann/Nordemann/Pukas, GRUR 2025, 955, 958 flg.

Open AI var også ansvarlige for arkitekturen til modellene. Promptene som førte til outputene var enkle i utformingen og spesifiserte ikke noe innhold. I motsetning til det Open AI hadde anført, kunne ikke brukeren holdes ansvarlig for opphavsrettskrenkelse gjennom outputene når slike åpne prompt ble benyttet.

Open AI gjorde selv verkene tilgjengelige for allmennheten, og fungerte ikke bare som mellomledd ved å stille infrastruktur til disposisjon for andres gjengivelser. Open AI kunne ikke sidestilles med plattformoperatører eller leverandører av maskinvare eller programvare. I slike tilfeller følger det av EU-domstolens praksis at en rekke supplerende kriterier må tas i betraktning,[50] men det var ikke nødvendig å vurdere dette nærmere i denne saken.[51]

Domstolen uttrykte videre at Open AI ville være ansvarlig uansett om disse tilleggskriteriene skulle ha blitt vurdert. Den viste til at Open AI spiller en sentral rolle i gjengivelsen; det var nettopp fordi de omstridte tekstene er memorert at de kunne hentes frem som output ved hjelp av enkle prompt. Det er Open AI som bestemmer hvordan modellene fungerer, utvalget av treningsdata og utformingen av treningen. Promptene for henting er enkle i innhold og lette å bruke, fordi det eneste som kreves er å skrive inn ønsket kommando. Open AI hadde også full kjennskap til konsekvensene av sin atferd, siden de etter alt å dømme har vært klar over memoreringen i modellene siden minst 2021. Det var heller ikke uten betydning at gjengivelsen hadde kommersielle formål, selv om dette ikke er et nødvendig vilkår.[52]

(xi) Tekstene ble tilgjengeliggjort for allmenheten.

Begrepet «allmennheten» har både et kvantitativt og kvalitativt aspekt.[53] I kvantitativ forstand omfatter allmennhetsbegrepet et ubestemt antall mulige mottakere og forutsetter et betydelig antall personer.[54] Ved fastsettelsen må det tas hensyn til hvor mange personer som kan få tilgang til det samme verket samtidig, men også hvor mange som kan få tilgang til verket etter hverandre.[55]

I kvalitativ forstand kreves det at et vernet verk gjengis ved hjelp av en bestemt teknisk prosess, som skiller seg fra tidligere brukte prosesser, eller at det gjengis for et «nytt publikum», dvs. et publikum som rettighetshaveren ikke tok i betraktning da han godkjente den opprinnelige offentlige tilgjengeliggjøringen.[56] Domstolen viste her til at GEMA hadde bestridt at de aktuelle sangtekstene var tilgjengelige på internett med rettighetshavernes samtykke. Men selv om tilgjengeliggjøringen på et nettsted var lovlig, oppstår det et nytt publikum, dersom innholdet legges ut på et annet nettsted uten rettighetshaverens samtykke.[57] Dette gjaldt særlig når innholdet ikke bare ble brukt på et annet nettsted, men av en AI-modell.

(xii) Sangtekstene var tilgjengelige for brukere av Open AIs chatbot på forespørsel, fra steder og på tidspunkter etter brukernes eget valg.

Tilgjengeliggjøring av innhold «på forespørsel» er en særlig form for kommunikasjon til allmennheten.[58] Slik interaktiv overføring på forespørsel (se fortalen til Infosoc-direktivet avsnitt 25, tredje setning) er mulig gjennom Open AIs chatbot, som i prinsippet brukes av enhver person fra ethvert sted og tidspunkt, forutsatt tilgang til internett og en internetttilkoblet enhet.

Outputen vises på skjermene til brukernes sluttutstyr og i chathistorikken. Den ble gjengitt både i brukernes arbeidsminne og på de skytjenere som OpenAI stiller til disposisjon for chathistorikken. Open AI var dermed ansvarlige for gjengivelsene. Etter tysk rettspraksis er produsenten av gjengivelsen den som teknisk gjennomfører gjengivelsen og dermed foretar den fysiske fikseringen.[59] Open AI måtte holdes ansvarlige fordi selskapet utøver kontroll over gjengivelsen gjennom outputene, driver modellene som de omstridte sangtekstene ble valgt som treningsdata for og ble trent med, og er ansvarlige for modellarkitekturen og memoreringen av treningsdataene. Modellene hadde i betydelig grad påvirket outputene, og det spesifikke innholdet i outputene ble generert av modellene. At brukeren bare utløser gjengivelsen ved å angi en prompt, betød ikke at brukeren var ansvarlig for gjengivelsen.

50 C-682/18, C-683/18 avsn. 67 YouTube og Cyando, C-775/21, C-826/21 avsn. 53 – Blue Air Aviation, C-426/21 avsn. 58 Ocilion og C-135/23 avsn. 23 GEMA.

51 Ohly GRUR 2018, 996, 1001.

52 C-135/23 avsn. 24 flg. GEMA.

53 Ohly, GRUR 2016, 1155, 1156.

54 C-135/23, avsnitt 38 GEMA.

55 Ibid, avsnitt 39.

56 C-135/23, avsnitt 43 GEMA.

57 Bundesgerichtshof 2. juni 2022, ZR 140/15, avsnitt 75 – YouTube II.

58 C-279/13 avsn. 25 flg. C More Entertainment.

59 BGH 23. okt. 2024, ZR 112/23, avsn. 73 Manhattan Bridge.

Illustrasjon: Colourbox.com

(xiii) Inngrepene var ikke omfattet av unntakene for sitat eller pastisj, og det var ikke gitt implisitt samtykke til handlingene i output-fasen.

Domstolen viste til at modellene er strukturelt ute av stand til å oppfylle formålet med sitatretten. Etter EUdomstolens praksis er formålet med InfoSoc-direktivet art. 5(3)(d) å forklare utsagn, forsvare en mening eller muliggjøre en intellektuell debatt mellom verket og brukerens uttalelser,[60] noe som ikke er mulig med modeller. Modellens «intensjon» kunne ikke vurderes.[61]

Pastisjunntaket i § 51a UrhG som gjennomfører art. 5(3)(k) i InfoSoc-direktivet og krever – i likhet med direktivet – at utnyttelsen skjer i form av pastisj. Det forutsetter en kunstnerisk tilnærming til et tidligere verk eller annet referanseobjekt.[62] Dette er ikke mulig med modellene på grunn av deres mangel på personlighet, som i andre tilfeller kunne tilført et kunstnerisk uttrykk gjennom bruk av vernede elementer.[63] De enkle promptene som førte til outputene, hadde ikke noe kunstnerisk innhold.

Det var heller ikke gitt noe samtykke til inngrepene i output-fasen; at et verk gjengis som utdata som følge av en enkel prompt, utgjør ikke en normal bruk som rettighetshaveren kan forventes å akseptere (se ovenfor).

Camilla Vislie, partner i Thommessens avdeling for immaterialrett, og arbeider med rådgivning og tvisteløsning innenfor teknologidrevne bransjer.

60 C-516/17, avsn. 78 Spiegel Online.
61 LG München 08.03.2012, 7 O 1533/12 Mein Kampf, jf. Finke ZGE 2023, 415, 435.
62 BGH 14. sept. 2023, ZR 74/22, avsn. 23, 34 Metall auf Metall v Stieper.
63 Finke ZGE 2023, 415, 442.

JusNytt

Schjødt

Halvor Manshaus

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

EU og Norden: Ny tilnærming til IP og teknologi i forsvarsleveranser

1. Innledning

EU-Kommisjonen publiserte 19. november 2025 rapporten «EU Defence Industry Transformation Roadmap». Kommisjonen identifiserer her behovet for en mer smidig og innovasjonsorientert tilnærming til forsvarsanskaffelser. Dokumentet fremhever betydningen av kortere innovasjonssykluser og varsler en pilot for 'Agile Rapid Defence Innovation (AGILE)', med mål om resultater innen 6–12 måneder.[1] Dette innebærer en normativ dreining fra tradisjonelle, langvarige og spesifikasjonsstyrte anskaffelsesprosesser mot mer iterative og risikodelende modeller. Dette veikartet bygger videre på en større visjon om at Europa skal bli selvstendige innen forsvar, slik EU skisserte i sin «European Defence Industrial Strategy» som ble fremlagt 5. mars 2024.

I det følgende skal det først redegjøres for den tradisjonelle tilnærmingen til anskaffelser i forsvarssektoren og identifisere enkelte utfordringer på dette området. Dette gir et godt grunnlag for å belyse de kontraktsrettslige og regulatoriske endringene som kan følge i kjølvannet av EUs nylige initiativer innen forsvarsindustri. Vi vil her blant annet se nærmere på det omtalte veikartet fra november 2025 og oppsummere endringer knyttet til anskaffelsesmodeller, immaterielle rettigheter (IP), kunstig intelligens (AI) og dataforvaltning, leverandørkjeder samt relevante etterlevelseskrav, herunder forordning (EU) 2023/1543 om europeiske produksjons- og sikringsordrer for elektroniske bevis (e-evidence).

Forsvarsleveranser er allerede underlagt særlige regler som skal hensynta nasjonal sikkerhet, beredskap og gradert informasjon. I praksis innebærer dette at forsvarssektoren eksempelvis har større frihet til å invitere kun utvalgte leverandører, stille strengere krav til sikkerhetsklarering, skjerme informasjon knyttet til anbudet og fravike kravene til åpen konkurranse. Slike unntak følger direkte av EØS-avtalen artikkel 123 og tilsvarende bestemmelse i Traktaten om Den europeiske unions funksjonsmåte artikkel 346. Det er gitt et eget direktiv 2009/81/EF for forsvars- og sikkerhetsanskaffelser som i praksis vil dekke de fleste behov, slik at det ikke er nødvendig å anvende traktatteksten direkte. I vår internrett reguleres dette iblant annet lov om offentlige anskaffelser med forskrift, forsyningsforskriften, forskrift om forsvars- og sikkerhetsanskaffelser og sikkerhetsloven. I tillegg har vi flere sektorinterne regler i form av regelverk for forsvarsmateriell, instrukser og regelverk i Forsvaret og egne regler om anskaffelser for eksempel mot NATO, der anskaffelser delvis er håndtert gjennom mellomstatlige avtaler.

Disse reglene er imidlertid først og fremst rettet mot å ha ryddige og transparente regler for anskaffelser heller enn å legge opp til kortere ledetid og mer effektive innkjøp knyttet opp mot modernisering og hurtige tilpasninger som kan bedre forsvarsevnen. Nye signaler fra EU slik veikartet omtalt ovenfor, har i første omgang en politisk signaleffekt. Samtidig skjer det nå store endringer i et større geopolitisk perspektiv, og det er en stor vilje i Norge og Norden til å legge til rette for et tettere samarbeid i nordisk sammenheng og også på et europeisk nivå. De nye signalene fra EU forventes å komme til uttrykk gjennom flere plan som er relevante for Norge, herunder kommende forordninger, programregler og kontraktsvilkår i EU-finansierte prosjekter. I tillegg får vår EØS-tilknytning også betydning ved at Norge deltar i European Defence Fund (EDF). Dermed kan norske aktører delta i EDF-prosjekter, som vil innebære at de må forholde seg til EDF-regelverket og tilhørende krav til eierskap og kontroll. Det er en rekke ytterligere grensesnitt som vil kunne bli påvirket, ved at Norge er så tett integrert inn mot det europeiske mar-

kedet. Norge som nasjon handler forsvarsløsninger fra europeiske leverandører og norske bedrifter er tett integrert mot europeiske verdi- og produksjonskjeder. Standarder og arkitekturvalg er i mange tilfelle implementert på EU-nivå og vil indirekte ha en *de facto* påvirkning for Norges valg av løsninger.

2. Tradisjonell fremgangsmøte for forsvarsanskaffelser

2.1. Prosjekttilnærming

Den norske og europeiske modellen for forsvarsleveranser kjennetegnes tradisjonelt ved at prosessen er delt opp i en rekke sekvensielle enkeltledd som hver for seg krever betydelige mengder tid og ressurser. Et standard utviklingsløp vil som regel starte med utgangspunkt i en behovsanalyse – og definisjon av de operasjonelle behovene som foreligger. Dette grunnlaget benyttes deretter for å utrede ulike alternative løsninger som kan dekke det aktuelle behovet. Typiske eksempler på ulike alternativer vil være oppgradering av eksisterende utstyr, innkjøp av nytt utstyr som er tilgjengelig i markedet, nyutvikling eller overgang til nye plattformer. I dette innledende arbeidet vil det også være nødvendig å se på en rekke andre faktorer som blant annet risikoanalyse, tidsløp og nøkkeltall, i tråd med vanlig prosjektmetodikk.

Når det foreligger en anbefalt løsning og tilstrekkelig klare rammer for anskaffelsen opprettes det en prosjektorganisasjon, om dette ikke allerede er gjort. En detaljert kravspesifikasjon utarbeides, og et foreløpig budsjett med tilhørende tidsplan kommer på plass. Politisk godkjenning må ordnes for større prosjekter, og kontraktsrammene klargjøres som et utgangspunkt for anbudsutlysing og kommende forhandlinger.

Den spesifiserte anskaffelsen går deretter ut i markedet, med utlysning nasjonalt eller internasjonalt. Dette innleder en komplisert fase med vurderinger av tilbud, der elementer som pris, kvalitet, leveransetid osv. er gjenstand for grundig analyse. Det forhandles om betingelser før det til slutt signeres en avtale. Regelverket legger en rekke føringer for hvordan ulike relevante parametere skal vektlegges samt hvordan prosessen som helhet skal foregå for å sikre rettferdig konkurranse i det relevante markedet.

Det hele går nå over i en utviklings- og/eller produksjonsfase hos en eller flere leverandører. Dette krever oppfølgning underveis, i tråd med avtalte milepæler og kostnadsnivåer. Ved levering vil det ofte være behov for opplæring samtidig som utstyr og personell skal integreres i eksisterende struktur. Den etterfølgende driftsfasen innebærer ikke bare vedlikehold og eventuelle oppgraderinger gjennom livsløpet, men også evalueringer knyttet opp mot opprinnelige behovsdefinisjon og tilsvarende føringer som definerer selve formålet med anskaffelsen.

2.2. Ledetid og tilpasningsevne

En slik tilnærming, der den ene prosessen følger den andre i et standard prosjektløp innebærer i praksis at det tar enormt med tid fra et behov er identifisert til leveransen er på plass. Ved en større anskaffelse vil den første konseptfasen som regel kreve 3–5 år. Utviklingsfasen kan forventes å ta 5–7 år med etterfølgende eller delvis overlappende produksjonsfase som også går over flere år. Det er ikke uvanlig at større innkjøp av strategisk betydning har en tidshorisont på 10–15 år.

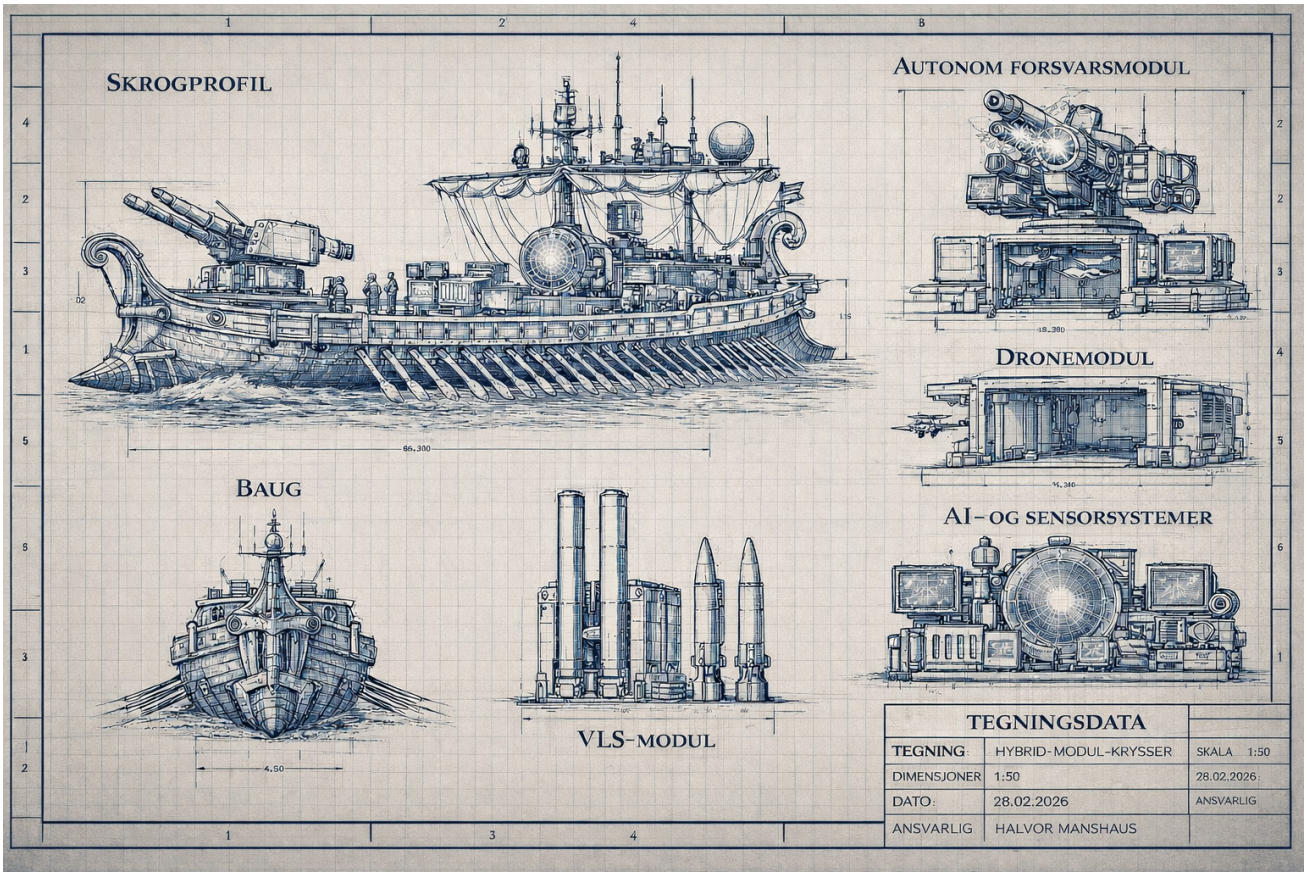
Denne fremgangsmåten fungerte greit i en verden der trusselbildet var relativt stabilt og forutsigbart, og teknologiutviklingen gikk saktere. Hardware har stått i fokus med tung mekanisk og fysisk infrastruktur knyttet opp mot stasjonære baser og formasjonslåste enheter for tradisjonell krigføring. De store forsvarssystemene har vært plattformorienterte og basert på større ansamlinger av kostbare fly, skip og kjøretøy. Med plattform sikter jeg her til at man bygger opp kapasitet rundt en grunnplattform som kan løse ulike oppdrag basert delvis på fleksibilitet innen plattformen og delvis ved integrasjon eller samarbeid med andre plattformer.

2.3. Eksempel: Fregatter

Et eksempel på en slik plattform er Fridtjof Nansen-klassen innen norske fregattskip. Det ble opprinnelig levert fem slike skip i perioden 2006–2011 og skipene skal på dette tidspunktet ha utgjort den største investeringen i norsk forsvarshistorie. Disse fregattene har en sentral funksjon i den norske marinen med tilhørende operasjonell kapasitet rettet mot ubåter, luftrommet og overflatebaserte fartøy. Utstyrt med AEGIS våpensystem, integrert helikopterkapasitet og utskiftbare våpensystemer gir denne plattformen fleksibilitet og samvirke opp mot andre forsvarsløsninger.[1] AEGIS ble utviklet som et helhetlig våpensystem med innebygget radar som kan spore over 100 samtidige mål. Systemet skal gi funksjonalitet fra sporing til tilintetgjørelse, og selv om dette ble utviklet allerede på 70-tallet har det blitt jevnlig oppdatert underveis med ny teknologi underveis.

Arbeidet med å erstatte den tidligere Oslo-klassen med fregatter fra 1960-tallet ble påbegynt som eget prosjekt i 1992. Stortinget godkjente prosjektet i 1999 og kontrakten ble inngått året etter. Riksrevisjonen leverte flere år senere en rapport som dokumenterte et gjennomgående problem med leveransen. Teknologien var utdatert allerede ved levering. Dette innebar ikke bare at løsningene ikke lenger kunne regnes som optimale, det var rett og slett problemer bare å få tak i reservedeler. På en høring i Stortinget forklarte daværende generalinspektør i Sjøforsvaret (stillingstittelen er nå endret til Sjef Sjøforsvaret) Lars

1 https://maritimt.com/fridtjof-nansen-05-2004



Illustrasjon: Halvor Manshaus.

Saunes nærmere om disse problemene:[2]

> *«Da vi kjøpte fregattene, så var de basert på 80- og 90-talls teknologi. Den initielle reservedelspakken hadde som fokus å skaffe reservedeler til de unike systemene som ble produsert den gangen. De systemene produseres ikke i dag. Litt av problemstillingen er at når du ikke finner 'reservedeler til en TV', så kjøper du ny. Det treffer oss nå. De systemene som ble produsert på 80-90-tallet, er det ingen som produserer lenger. Da må vi 'skifte ut de TV-ene' før vi kan kjøpe reservedelene. På noen områder er det et ganske komplekst system. På noen områder er vi faktisk nesten på eBay for å finne reservedeler.»*

Dette gjaldt selvfølgelig ikke alle deler av de tekniske systemene om bord, men dette sier noe om hvordan en løsning som ser bra ut på skrivebordet kan være utdatert ved levering når teknologi og stridsbildet endres raskt. Det vil også være en praktisk utfordring ved eventuelle oppdateringer eller oppgraderinger dersom fregattene må settes ut av drift. Dette vil gi et taktisk kapasitetsgap som kan skape utfordringer knyttet til å løse operasjonelle oppgaver. Samtidig vil det over lengre tid kunne oppstå strategiske utfordringer dersom teknologien på fregattene sakker for langt akterut. Norges plassering i forhold til Kolahalvøya innebærer at skipene må være utrustet med teknologi som er moderne nok til å kunne spore og følge ubåter innenfor våre områder, både med tanke på nasjonal sikkerhet og våre forpliktelser opp mot NATO.

Poenget med dette eksempelet er å vise hvordan lang ledetid får stor betydning allerede i det tradisjonelle forsvarsparadigmet. Hvis vi nå legger til hvordan militær teknologi og selve krigføringsmetoden i dag er gjenstand for enorme endringer, er det enkelt å konstatere at vi står overfor store utfordringer.

Supersoniske missiler som flyr i fem ganger lydens hastighet, og som er svært manøvrerbare og presise, gir nå langt mindre reaksjonstid til forsvarssystemene. Ubemannede sjøfartøy over eller under vann kan brukes til angrep mot skip, installasjoner og landanlegg. Større droner og drone-svermer har modnet til et punkt der de i dag utgjør en stor trussel mot fartøyer. Elektroniske angrep har blitt langt mer sofistikerte, og kan forstyrre sensorsystemer og kommunikasjonsløsninger. Digitale løsninger kan i dag være en sårbarhet heller enn en styrke dersom disse ikke er tilstrekkelig beskyttet. Felles for disse eksemplene er at kostnadene er langt lavere og at det ikke kreves tilsvarende tung infrastruktur og forsyningslogistikk som for fregattene. For å

2 https://www.nrk.no/norge/forsvaret-kjopte-fregatter-med-teknologi-fra-80-tallet-1.13396029

møte disse utfordringene må morgendagens fregatter ikke bare utstyres med løsninger som kan imøtegå disse truslene, det må legges til rette for interoperabilitet mot andre og nye løsninger, fleksibilitet, skalerbarhet og kapasitet som innebærer rask tilpasning og oppgradering til ethvert behov som vil oppstå.

Dette gjelder selvsagt ikke bare fregatter, dette var bare et tilfeldig eksempel. Grunntanken om å endre vesentlige deler av hvordan vi tenker rundt forsvarsanskaffelser gjelder generelt for denne typen innkjøp.

2.4. En verden i endring – historisk perspektiv

Utgangspunktet for denne artikkelen er det store taktskiftet vi ser knyttet til teknologisk utvikling på det militære området. Dette medfører et helt reelt behov for å gjøre de endringer som skal til for at vårt nasjonale forsvar – og tilsvarende for våre allierte – skal ligge på et akseptabelt nivå. Det sies at historien gjentar seg, og den militære historien er en historie delvis om å utvikle og innovere egne løsninger, delvis å tilpasse seg det som kommer utenifra. Jeg har ovenfor vist til at innkjøpet av Nansen-fregattene var det dyreste forsvarsinnkjøp frem til da, og dette er bekreftet fra flere kilder. Min oldefar tjenestegjorde imidlertid på en av de fire norske panserkrysserne som Norge satte i tjeneste rundt forrige århundreskifte. Det siste av disse fire skipene ble sjøsatt i 1899, og til sammen kostet de 19 millioner kroner.[3] Dette tilsvarte en femtedel av det norske statsbudsjettet den gang. Statsbudsjettet for 2026 indikerer et utgiftsnivå på om lag 2 200 milliarder kroner, med en tilsvarende høyere femtedel.

Mer interessant enn å regne på statsbudsjettdeler er å se på selve den teknologiske utviklingen i denne perioden. Skrupropellen ble patentert av Josef Ressel i 1827, og innen panserkrysserne i Norgesklassen var på plass i 1899 hadde marinen konvertert fra seilbåter til skip drevet med dampmotorer. I samme perioden gjorde Charles Parsons en viktig oppfinnelse i 1884 da han utviklet dampturbinen. Tradisjonelle dampmotorer benyttet et mekanisk stempel for å overføre kraft. Parsons benyttet en turbinvifte som kunne gi direkte kraftoverføring med langt mindre vibrasjoner og jevnere gange. Resultatet ble krigsskip som kunne gå 3–5 knop raskere enn med stempeldrev.

Dampturbinen endret verden for marinefartøy nærmest umiddelbart. Allerede i 1906 kom den britiske Dreadnought-klassen. Dette var skip med dampturbiner som beveget seg langt raskere enn andre skip. Turbinen gjorde det mulig å bygge større skip som kunne utrustes med større kanoner. Denne nye klassen omdefinerte hva et krigsfartøy kunne være: Større, raskere og lastet med større og flere kanoner. De norske panserkrysserne hadde 2 hovedkanoner, HMS Dreadnought hadde ti. Evnen til å kontrollere distansen mot stridende fartøy kombinert med større rekkevidde på artilleriet var i praksis uslåelig. Etter bare noen års drift var teknologien i den norske panserklassen blitt fullstendig akterutseilt. Disse mindre panserkrysserne var likevel fullt fungerende og opererte bra i norsk farvann og de operasjonelle forholdene som de var bygget for. Det var ganske enkelt ikke Norges oppgave å konkurrere med denne type skip, som ikke bare krevde enorme investeringer men også et stort industrielt apparat.

I 1892 fikk Rudolf Diesel innvilget det tyske patentet DRP 67207 som beskrev forbrenningsmotoren. Overgangen til marine dieselmotorer skred deretter gradvis frem, i første omgang på mindre fartøy og ubåter. Poenget er å understreke at bare det i disse årene rundt 1900 skjedde dramatiske omveltninger innen teknologi og utvikling av forsvarsløsninger.

Dette temaet er velkjent allerede fra antikkens klassiske tekster. Polybius forteller hvordan Kartago med sin mektige krigsflåte hadde overtaket over Middelhavet i den første punerkrigen. Romerne var ingen stor sjøfartsnasjon og manglet tilsvarende skip. Ved et lykketreff tapte Kartagerne et fartøy som romerne kunne bruke som modell for å utforme sine egne skip.[4] Dette var et tidlig eksempel på omvendt utvikling av teknologi. Det beskrives hvordan romerne startet helt fra bunnen av, og hvordan roerne måtte trene på benker bygget på land mens skipene ble bygget. I noen gjenfortellinger fremstilles Kartagernes tapte skip som en trireme, men Polybius forteller at det var snakk om en quinquereme. Det er litt uenighet om hva som egentlig er forskjellen på disse to skipene. Triremen hadde tre roere i høyden, mens quinqueremen viser til tallet fem som her formodentlig går på antall roere og ikke antall årer. Den rådende teorien er at det fortsatt var tre årer i høyden, men at de to øverste nivåene var utstyrt med to roere hver. Dette var uansett et stort og massivt krigsskip, med en komplisert konstruksjon romerne ikke hadde forutsetninger for å kunne realisere uten hjelp eller erfaring. Uten det tapte skipet ville de ha brukt langt mer tid på å utvikle et eget design. Tre høydenivåer og fem roere per åregruppe stilte strenge krav til vekt og balanse, samt at geo-

3 Alf R. Jacobsen 2012 «Angrep ved daggry : Narvik, 9. - 10. april 1940». Vega Forlag

4 Polybius «Historiarum» 1.20-21 (opprinnelig verk på gresk). Teksten om dette skipsprosjektet har blitt ekstra velkjent fordi den fra antikken og frem til i dag har blitt brukt som en av de første oversettelsene for ferske latinstudenter. Dette skyldes at Polybius skriver om historiske hendelser og bruker perfektum og imperfektum, samt at fortellingen er en typisk romersk identitetshistorie.

metrien for plassering av årer og roere måtte hensyntas ved formgivningen av hele konstruksjonen. Kartagernes fartøy hadde også kompliserende elementer, blant annet en stor bronseram i baugen for å kunne kjøre inn i andre skip. Romerne tilførte i tillegg en *corvus*. Denne entringsbroen kunne vippes ned over kanten på et tilstøtende skip for rask bording med soldater. Broen viser at romerne ikke bare kopierte blindt, men også videreutviklet med tanke på å fremheve sine egne sterke sider. Kampvante og disiplinerte soldater skulle raskt over til fiendens fartøy for å vinne slaget.

Et dynamisk bilde der det skjer en vekselvirkning mellom nye teknologier og etterfølgende tilpasninger er et fundamentalt utgangspunkt for enhver forsvarsstyrke. Det nye er altså ikke ukjent eller uventet at slike paradigmeskifter[5] forekommer. Det nye er at utviklingstakten går så ekstremt mye raskere og går på tvers av etablerte plattformer, strukturer og våpengrener.

3. Viktig endring i tenkingen rundt europeiske forsvarsanskaffelser

3.1. «New Defence» aktører

Kommisjonen har i sitt nye veikart lagt vekt stor vekt på å legge til rette for innovasjon og nyskapning. Tankegangen er sterkt påvirket av lærdom hentet fra den pågående krigen i Ukraina:

> *«The war in Ukraine is demonstrating how rapidly defence technologies evolve and can alter battlefield dynamics. SMEs, small mid-caps, startups, and scaleups, often with a civilian deep-tech background, are central to Ukraine's defence by swiftly delivering critical capabilities to the armed forces. Innovation and adaptation cycles are becoming increasingly shorter. High tech and complex systems are combined with low-cost and massmanufactured products. Disruptive technologies such as AI, quantum, cyber, and space-based systems are providing rapid tactical change on the battlefield.» (Kommisjonens uthevinger)*

Det er altså ikke slik at den tradisjonelle tilnærmingen til anskaffelse av forsvarsløsninger skal fases ut, poenget er i stedet å legge til rette for hybridløsninger og samarbeide på tvers av det tidligere skillet mellom militære og sivile miljøer for teknologi og utvikling. Det er ikke nok bare å transformere og oppdatere EUs forsvarsindustri, det skal også legges til rette for såkalte «New Defence player» – altså nye aktører i dette markedet. Dette vil være virksomheter som skal insentiveres og innlemmes i et større og koordinert samarbeid. Det er tre målsetninger som fremheves for å få til en slik endring:

1. Styrke forbindelsen mellom forsvarssektoren og *«deep tech»*-miljøer for å akselerere utviklingen av banebrytende løsninger og fremveksten av nye forsvarsaktører, tiltrekke kompetanse og talent samt øke gevinsten av såkalt «spin-in» fra sivile teknologimiljøer;
2. Fremskynde integreringen av avanserte teknologier i medlemsstatenes militære kapabiliteter for å oppnå europeisk forsvarsberedskap og effektiv avskrekking; og
3. Styrke Europas forsvarsproduksjonskapasitet gjennom nyskapende og avanserte industrielle produksjonsløsninger, slik at kapasitet kan leveres raskt, i tilstrekkelig omfang og på en kostnadseffektiv måte.

Dette er ambisiøse mål som krever flere omstillinger i alle ledd som er knyttet opp mot anskaffelser og utvikling av nye forsvarssystemer. Her ser man for seg leveranser som i praksis aldri avsluttes. Gjennom hele systemets levetid skjer det oppdateringer og tilpasninger. Programvare og AI skal ikke oppdateres en gang i året, men forventes å oppdateres fortløpende både fra sentralt hold, men også ved at systemer lærer og utveksler informasjon i sanntid.

> Det er altså ikke slik at den tradisjonelle tilnærmingen til anskaffelse av forsvarsløsninger skal fases ut, poenget er i stedet å legge til rette for hybridløsninger og samarbeide på tvers av det tidligere skillet mellom militære og sivile miljøer for teknologi og utvikling.

På samme måte som Norske panserkryssere ikke kunne måle seg mot HMS Dreadnought i 1906, er det urealistisk å tro at vårt land skal bygge opp en militær slagkraft som er sammenlignbar med stormakter som USA eller Kina i dag. Disse har investert tungt i teknologi og konvensjonell slagkraft på et nivå som ligger langt utenfor det som er realistisk for Norge eller EU å ta igjen i nær fremtid. Det er heller ikke poenget. Vår videre utvikling må følge opp den satsningen vi har gjort på å være til stede og relevant innenfor vår geografiske kontekst og militærpolitiske virkelighet. Dette innebærer løpende patruljering og kontroll med våre havområder og nordlige grenser samt mottak og forsyninger rettet mot allierte styrker. I tillegg må vi nå i større grad sikre oss mot angrep rettet mot strategisk infrastruktur og bygge opp mottiltak mot droner, høyhastighetsmissiler og autonome enheter. Vi må også

5 Thomas Kuhn 1962 «The Structure of Scientific Revolutions» gir en grundig behandling av paradigmeskifter og hvordan disse er en naturlig og forventet del av utviklingsløpet.

bygge ut vårt vern om digital integritet og mottiltak mot hacking.

Som vi har sett ovenfor er forsvar i stor grad en tilpasningens kunst. Forsvarsevnen må tilpasses det vi kan forvente av realistiske scenarier i fremtiden. Det hjelper lite å bygge opp et stort og mektig forsvar utelukkende mot landbaserte angrep dersom angrepet kommer via supersoniske missiler og droner rettet mot infrastruktur. I vårt tilfelle betyr dette i første omgang at EU, Norden og Norge skal ha en opprustning av den generelle forsvarsevnen, og at dette igjen skal optimaliseres opp mot geografiske og strategiske elementer i det enkelte land. Det er snakk om en balansegang mellom det enkelte lands forsvar isolert sett, og et bidrag til forsvar innenfor det større regionale samarbeidet. Norge skal for eksempel ha et eget forsvar, patruljere nord-områdene og bidra med styrker til internasjonale oppdrag og treningsoperasjoner med allierte partnere. Det er videre naturlig for alle de omtalte områdene å se hen til Russlands krigsevne når det gjelder konkret tilpasning, mottiltak og ressursallokering. Dette er kanskje det viktigste punktet i en oppgradering av militær kapasitet: Å identifisere hva man skal forholde seg til. For Norge og Europa har dette tatt lang tid, selv etter Krim-invasjonen i 2014. Det er først etter invasjonen av Ukraina i februar 2022 at Europe virkelig tok inn over seg den helt sentrale rollen Russland spiller for våre forsvarspoliske vurderinger. Et forsvar som ikke er bygget opp og skalert for å stå imot Russland har liten relevans i Europa i dag.

3.2. Design authority og immaterielle rettigheter

Veikartet fremhever betydningen av å sikre europeisk kontroll over 'design authority', herunder tilgang til tekniske data og mulighet til å videreutvikle systemer uten restriksjoner fra tredjeland. Den kontrollen som beskrives her må antas å omfatte blant annet: Arkitektur og grensesnitt for systemet, konfigurasjonsstyring, endringer/oppgraderinger, integrasjon av nye komponenter og programvare samt tilgang til nødvendig dokumentasjon, tekniske data og rettigheter/lisenser. Det er ikke mye tvil om at programvare og bruk av AI vil stå sentralt i EU når det diskuteres rundt forsvarsløsninger fremover. Kommisjonen uttaler følgende om hvilken strategisk betydning AI forventes å få:

> *«AI is a strategic driver of military innovation. The future battlefield will be marked as much by algorithms and data as by kinetic capabilities.» (Kommisjonens utheving)*

Det fremheves at AI her ikke bare viser til rene stridsløsninger som droner, anti-dronesystemer, luftforsvar, presisjonsangrep og lignende, men også til kommandofunksjoner, logistikk og stridsklare VR-løsninger.

I en slik teknologiorientert tilnærming vil det fort kunne oppstå spenninger mot standardiserte kontraktsvilkår knyttet til immaterielle rettigheter og forvaltning av teknologi som skal tilbys eller utvikles. En vanlig innkjøpskontrakt vil inneholde klausuler om IP-eierskap som definerer hvem som eier teknologi implementert og/eller utviklet gjennom prosjektet. Bruksrettigheter og lisenser vil avklare hvor langt overdragelsen eller tilgangen til teknologien gjøres gjennom handelen. En escrow-løsning vil ofte være nødvendig for å gi tilgang til kildekode og kritisk dokumentasjon ved leverandørsvikt eller i definerte nødsituasjoner. Dual-use rettigheter, altså rettigheter til teknologi som leveres til både sivile og militære formål, vil i utgangspunktet ha ulik regulering tilpasset formål og sluttkundens behov.

Dette er eksempler som skraper litt i overflaten på det bestående regimet, og der det må forventes en rekke tilpasninger for å få plass den tilpasningsdyktigheten EU omtaler i sitt veikart. En sentral utfordring vil være å legge til rette for større grad av interoperabilitet mellom komponenter og moduler. Dette åpner for å tenke nytt og mer kreativt rundt hvordan ulike løsninger kan kobles sammen eller deles for å oppnå taktiske fordeler tilpasset en konkret situasjon eller plan. Her ser vi at dyrekjøpte erfaringer fra Ukraina-krigen tillegges stor vekt og betydning hos Kommisjonen:

> *«Modularity and open architectures are key to rapidly reconfigure, upgrade, or integrate defence systems, drawing on commercially available interoperable technologies. Ukraine has been facing the challenge of adapting received weapon systems with limited interoperability to platforms in their inventory. This experience highlights the importance of embedding interoperability and modularity by design, embracing more flexible, scalable, faster and futureproof approaches that ensure weapon systems can rapidly adapt to changing needs. It also underlines the importance of maintaining control over the design authority of defence systems, enabling rapid adaptation and use free of foreign restrictions.»*

Beskrivelsen ovenfor utgjør et langt skritt vekk fra det tradisjonelle «hardware-fokus» som har kjennetegnet de store forsvarsinnkjøpene. Vi ser at EU ønsker å legge større vekt på modularitet, åpen arkitektur og design authority. For å oppnå dette fullt ut må immaterielle rettigheter hensyntas som en kjernekomponent allerede når prinsipper for kontrahering skal trekkes opp. Effektiv styring av IP-rettigheter skal i denne sammenheng ikke bare optimalisere kommersielle interesser, men må bidra til å sikre at forsvarssystemer enkelt kan rekonfigureres, oppgraderes og integreres mot andre løsninger raskt – uten for omfattende rettslige eller tekniske begrensninger.

Dette forutsetter at det implementeres solide systemer for dokumentasjon av utvikling, eierskap og finansiering av teknologi. I tillegg vil det oppstå et behov for systematisk oppfølgning av IP-forpliktelser og -klarering, lisensomfang og tilhørende begrensninger i bruk og etterfølgende endringer. Ved at denne utviklingen må forventes å foregå parallelt i en rekke land Norge samhandler med, må vi også sette av ressurser for å håndtere eksportkontroll og håndtering av restriksjoner fra andre land på sin egen teknologi.

Det foregår allerede i dag en omstilling knyttet til flere av disse elementene i de ulike leddene knyttet opp mot forsvarsleveranser. Ikke minst ser vi dette i arenaen for dual-use teknologi der virksomheter som tidligere har forholdt seg helt eller delvis til sivil sektor ser et nytt marked med leveranser inn mot forsvarsindustrien. Samtidig skjer det en faktisk innstramning knyttet opp mot hvem som får tilgang til teknologi, data og IP-rettigheter. Det seiler opp som et nasjonalt anliggende å sikre kritiske leverandørkjeder som nå står i et nytt landskap samtidig som digitale tjenester og programvareutvikling skal sikres. I denne konteksten står AI frem som en viktig brikke, og der det forventes å skje store endringer i måten forsvaret disponerer ressurser og investeringer fremover. AI vil være i stand til å gi en form for informasjonsdominans med tilhørende evne til analyse og kartlegging på kort og lang sikt. For å få til dette vil det være nødvendig med en klar regulering av datasamarbeid som klargjør hva som kan deles og hvordan dette skal gjøres på en sikker og effektiv måte. Tilsvarende må det klargjøres rammer for bruk av testmiljøer og såkalte «sandkasser» der digitale løsninger kan evalueres under og gjennom et utviklingsløp. Ved at nye aktører forventes å tre inn på et ukjent område må det legges klare rammer og premisser tidlig i et kontraktsløp. Dette vil i praksis innebære behov for klare konkurranse- og kvalifikasjonsgrunnlag med tilhørende sikkerhetsvurderinger. I tillegg vil det være nødvendig å ha systemer og rutiner for raskt å kunne gjøre due-diligence lignende vurderinger av leverandørens IP-portefølje og rettighetskontroll.

For leverandøren vil det fortsatt være nødvendig å verne om sine forretningshemmeligheter og IP. Det er tross alt dette som utgjør den harde kjerne av konkurranseevnen, og her står know-how i sentrum. Det vil som regel ikke være aktuelt å patentere alt det som ellers kunne ha stor kommersiell verdi, ettersom dette vil være forsvarskritisk informasjon underlagt krav til taushet og sikkerhet. Dermed må partene finne frem til praktiske løsninger for å håndtere slik spørsmål. Partene her sikter ikke bare til kunden og leverandør i tradisjonell forstand. I langt større grad enn tidligere legges det nå opp til at flere leverandører, store og små, skal samarbeide tettere og mer dynamisk enn tidligere. Dette høres bra ut, men i praksis er det store utfordringer med å få en god balanse i denne typen avtaler. Tilgang til kildekode er en gjenganger i slike avtaler, og det samme gjelder virksomheter underlagt sikkerhetsloven. Nye aktører vil ikke være klare for å møte de formelle kravene og rutinene som skal være på plass. Her bør det utarbeides klare retningslinjer og maler for hvordan virksomheter raskt skal kunne tilpasse seg et nivå som passer til mer agile kontraktsleveranser.

3.3. Agile procurement

Kommisjonen legger opp til at EU skal teste en pilot for agil, rask forsvarsinnovasjon der aktiviteter organiseres som utfordringer med ledetid innenfor 6–12 måneder, og der det bevisst aksepteres mer risiko enn ved tradisjonelle anskaffelsesprogrammer. Samtidig forklares det i veikartet at det trengs en *«complete redefinition of value»* for denne typen bestillinger. Innkjøperen skal i større grad gå bort fra prinsippet om laveste kostnad og i stedet prioritere langsiktig industriell styrke, teknologisk suverenitet og kompetansebygging. Det understrekes at dette ikke bare skal gjelde bare selve kostnadsbildet, men selve den grunnleggende forståelsen av hva som faktisk bestilles og kjøpes:

> *«To fundamentally resolve these challenges, the EU must pivot from viewing procurement as a transactional process of buying products to a strategic act of investing in industrial capacity and resilience.»*

Dette sitatet gjenspeiler et normativt skifte i måten EU ønsker å forholde seg til både innkjøpsprosessen og oppbyggingen av forsvarskapasitet. Selve fremgangsmåten skal bidra til å skape insentiver og virkemidler for å løfte opp leverandørleddet. Grunntanken har enkelte fellestrekk med måten den ferske oljenasjonen Norge la opp til en langsiktig utvikling av en nasjonal leverandørindustri med særegen kompetanse og kunnskapserfaring. Dette er heller ikke ukjent i tradisjonelle anskaffelser. I forbindelse med den omtalte anskaffelsen av fregatter fra Spania ble det uttalt at Norge hadde inngått «en av de beste gjenkjøpsavtalene noensinne». Avtalen omfattet mer enn 250 norske bedrifter, og det spanske verftet hadde allerede i 2007 oppfylt sine forpliktelser på 10,6 milliarder kroner i gjenkjøp. I tillegg kjøpte det spanske forsvaret forsvarsmateriell fra Norge for over 3 milliarder kroner som del av de gjensidige forpliktelsene i avtalen.[6]

Forskjellen vil altså ligge i at anskaffelsene i mindre grad skal dreie seg om transaksjonsaspektet, og fokusere mer på å bygge opp kapasitet og robusthet i leverandørleddene. En slik tilnærming harmonerer godt

6 https://www.tu.no/artikler/i-havn-med-tidenes-forsvarskjop/241508

med den norske modellen for å bygge opp leverandørkompetanse over tid. Dette sikrer mangfold, utvikling og tilgang til kompetanse og materiell, som forventes å være viktige faktorer i utviklingen av forsvaret fremover. Avtaleforholdet vil ikke i samme grad avsluttes ved levering, men vil innebære en livsløpsforpliktelse med videreutvikling og innovasjon knyttet opp mot eksisterende og fremtidige leveranser. For å ivareta dette må kontraktsgrunnlaget omfatte oppgraderingsforpliktelser, teknologisk videreutvikling, beredskapskapasitet, tilgang til reservedeler og vedlikeholdsapparat osv. Dette vil i praksis innebære større bruk av løpende rammeavtaler med lang løpetid og klausuler om automatisk fornyelse. Vi må også forvente at slike avtaler vil ha krav til opsjonsstrukturer med åpning for fremtidig kapasitetsøkninger og integrasjon mot andre systemer. Vilkårene i slike avtaler vil bli vesentlig mer inngripende enn tradisjonelle innkjøpskontrakter. Det er nå ikke bare leveransen, men hele avtaleforholdet som skal reguleres. I tillegg til det som allerede er nevnt vil det være en rekke andre faktorer som må innarbeides i slike avtaler. Krav til «surge capacity» med rask oppregulering av volum og produksjon. Deling eller i det minste klar allokering av utviklingskostnader – og tilhørende rettigheter. Opsjoner på fremtidig produksjonsvolum og lignende elementer vil innebære elementer av offentlig-privat partnerskap slik Staten har forsøkt i større entrepriseprosjekter i nyere tid. I denne modellen vil det også være åpninger for konsortiebaserte konstellasjoner med leverandører, tilpasset konkrete prosjektet eller leveranser. Joint ventures med flere deltakende aktører vil være en naturlig modell.

Åpenbare fordeler med en slik tilnærming vil være at det bygges opp langsiktig kompetanse og grunnlag for tunge investeringer. I en slik modell må det også implementeres mekanismer for kontroll og løpende vurdering knyttet opp mot konkurransegrunnlag og transparens.

Norge har ikke per i dag vedtatt noe nytt regelverk eller instrukser som uttrykkelig omgjør forsvarsanskaffelser i tradisjonell forstand til en slik strategisk investering i industriell kapasitet og robusthet. Det norske anskaffelsesregelverket – sammen med nasjonale sikkerhetsunntak – gir allerede i dag et betydelig handlingsrom for å utforme kontrakter i tråd med denne ambisjonen der dette anses som gunstig. Det punktet som i størst grad skiller norsk praksis i dag fra EUs visjon, er i første rekke at en slik ny strategisk retning hovedsakelig kan realiseres gjennom kontraktuell utforming og administrativ styring, snarere enn gjennom nye formelle regler. For å realisere dette er det ikke tilstrekkelig bare å endre prosjektmetodikk og avtalegrunnlag. Det er nødvendig å gå helt tilbake til definisjon av det operasjonelle behovet, skrelle ned og dekonstruere mot de helt grunnleggende elementene i de ulike forsvarssystemene. Så må dette rent konseptuelt bygges opp igjen fra grunnen, med utgangspunkt i modulbaserte løsninger som kan enkelt kan erstattes, repareres, oppgraderes og kobles sammen fysisk eller digitalt for å oppnå funksjonelt samvirke med andre moduler eller systemer.

Eksempelvis skal et system med sterke sporingssystemer for innkommende missiler kunne distribuere data til andre komponenter og moduler i et relevant geografisk område. Andre enheter kan da trekke på denne informasjonen uten selv å måtte ha innebygget tilsvarende system. Dette gir rimeligere, lettere og mer robuste enheter totalt sett. Flere enheter spredt utover vil kunne dele data og bruke dette for å triangulere dynamiske posisjoner, øke treffsikkerhet og sikre redundans. I stedet for at hver enhet sikter mot nøyaktig samme punkt vil det i stedet kunne beregnes en tilsiktet spredning som øker muligheten for å fjerne innkommende objekter. Dette vil gi økt treffsikkerhet også mot ekstremt raske og manøvrerbare missiler, droner eller lignende. Den samlede datamassen går til sentraliserte AI-enheter som fortløpende analyserer data med tanke på å koordinere og optimalisere respons og forsvar, samtidig som det gjøres taktiske vurderinger i sanntid. Raske instrukser om mottiltak gjøres parallelt med løpende oppdateringer og risikoanalyser. Informasjonen brukes også til etterfølgende analyser av angrep og forsvarstiltak med tanke på å gjøre etterfølgende tilpasninger i det som dermed blir et «levende» system i den forstand at det over tid vil være tilpasningsdyktig der dagens systemer er statiske.

Norge har ikke per i dag vedtatt noe nytt regelverk eller instrukser som uttrykkelig omgjør forsvarsanskaffelser i tradisjonell forstand til en slik strategisk investering i industriell kapasitet og robusthet.

Jagerflyet F-35 Lightning II utfører flere av oppgavene omtalt i foregående avsnitt. Flyet fungerer som en del av et nettverksbasert forsvarssystem. Alle sensorer og innsamlede data forenes og presenteres i et samlet oversiktsbilde. Informasjonen deles med andre F-35 i gruppen så vel som luftvern og samhandlende skip og bakkestyrker. Et utviklingsprosjekt som fører frem til et slikt produkt er ekstremt krevende, ved at det krever en bredde og integrering langt utover det vi er vant med i vanlig militært utstyr. Målsetningen må fremover være å utvikle rimeligere løsninger basert

på modularitet og felles grensesnitt som kan overføres mellom systemer.

Den fleksibilitet og «agilitet» som allerede ligger i dagens regelverk og retningslinje, kan utgjøre et sterkt fortrinn for Norge i det vi går inn i en periode med større budsjett, større krav og et endret landskap knyttet til forsvaranskaffelser. Dette skjer likevel ikke av seg selv. Den første, og kanskje største, utfordringen dreier seg om kultur og etablerte handlingsmønstre. Det vil være en stor utfordring å realisere de endringene som kreves for en rask tilpasning til dagens krav og nye militære virkelighet. I arbeidet med denne typen kontrakter hersker det et etablert *mindset* om hvordan dette skal gjøres – basert utelukkende på den tradisjonelle modellen beskrevet ovenfor. Dette er et hardt paradigme bygget opp innenfor et system der kommandostruktur og tjenestevei naturligvis er godt innarbeidet. I tillegg kommer den særnorske frykten for å gjøre noe galt, å ikke få det helt til. Skal Norge få til de endringer som er antydet i denne artikkelen må vi rett og slett tørre å prøve oss litt frem. Det er ingen klar oppskrift som vil sikre suksess for hver øvelse.

Når man beveger seg inn i et nytt landskap, kan det ikke være forbudt å snuble et par ganger så lenge man har oversikt over det som skjer og bruker erfaringene som høstes. Den tradisjonelle tilnærmingen er å ta ned all mulig risiko *før* det fattes en beslutning og det inngås kontrakt, slik vi så Nansen-fregattene gjorde i de første 10 årene av prosjektet (1990–2001). Her merker vi som rådgivere på ulike former kontrakter en stor kontrast til moderne IT- og teknologiprosjekter der risikoreduksjon skjer *fortløpende* gjennom læring og til dels feil som gjøres underveis i prosjektet. Eksempelvis brukes Proof of Concept (PoC) eller konseptbevis ofte for å teste en kritisk hypotese eller ide. I stedet for å planlegge og prosjektere seg til målet isoleres denne komponenten og testes i et begrenset omfang til lav kostnad. Dette gir en kortere vei mot målet og gir stor læringsverdi. Dersom det ikke fungerer, er det i seg selv en viktig lærdom. I tillegg vil man som regel ta med seg en forståelse av hvorfor det ikke fungerer og vurdere endringer i design eller tilpasse sluttmålet opp mot denne kunnskapen. Her kan vi være litt som Thomas Edison, som skal ha uttalt «I have not failed. I've just found 10,000 ways that won't work.».

I praksis ser vi som regel at ulike utviklingsprosjekter trenger en del skreddersøm for å fungere optimalt, men dette er ikke en subjektiv og tilfeldig prosess. Det foreligger i dag solide og etablerte prinsipper for hvordan agile prosjekter skal legges opp og struktureres. Typiske elementer vil være at prosjektet deles opp i mindre leveranser med kortere og mer intensive milepæler, parallelt med fortløpende forbedringer og tilpasninger som gjøres underveis. Dette fordrer tett oppfølgning fra både kunde og leverandør. Leveransebeskrivelsen som tidligere har blitt hamret ut i et eget forprosjekt over flere år må være mer fleksibelt og med forventninger om endringer underveis. Dermed må leveransen i større grad beskrives fra et funksjonelt og operativt perspektiv heller enn i detaljerte spesifikasjoner som ligger fastlåst. Dermed vil det kunne bli en glidning fra en fast kravspesifikasjon kombinert med fastpris slik vi ser i dag over mot delbudsjetter og tidsrammer som kombineres med et mer variabelt innhold i leveransebeskrivelsen. I stedet for å levere et ferdig system som kan ta mange år, leveres det i stedet komponenter underveis som kan testes og justeres før det hele kommer på plass. I dette ligger at en større anskaffelse vil deles opp i mindre moduler og leveransepakker. I flere tilfelle vil det kunne være fornuftig å legge opp til rammeavtaler med flere leverandører som kan samarbeide. Slike avtaler vil løpe over flere år, der kunden gjør avrop i tråd med den prioritering mellom oppgaver som gir mening der og da.

3.4. Avslutning

Det går nå også mot et tettere nordisk samarbeid innen forsvar generelt. Der vi ellers anser oss ganske likestilt som våre naboland er dette samtidig et område der det er klare historiske og politiske forskjeller. Norge har lang fartstid i NATO, med løpende oppgaver innen blant annet overvåkning av russisk skips- og ubåttrafikk som diskutert ovenfor. Sverige har lenge vært et nøytralt land, som kun nylig har blitt med i NATO. Finland har hatt et langt mer aktivt forhold til sitt forsvar grunnet nærhet og historikk opp mot Russland, og har også nylig trådt inn i NATO. Island har en avstand til Europa, men er knyttet tett opp mot USA og forsvarssamarbeidet gjennom NATO. Danmark har nylig fått mye oppmerksomhet grunnet utspill fra politisk hold i USA grunnet militære spørsmål knyttet opp mot Grønland. Danmark har også bakgrunn som en aktiv NATO-alliert og ligger geografisk tettest på resten av Vest-Europa.

Disse forskjellene kan være en fordel ved at man sitter på ulike erfaringer og behov for tiden fremover. Dette kan bli nyttig når det skal finnes frem til gode løsninger for å bygge opp både nasjonale, nordiske og europeiske løsninger for et oppdatert militært forsvar. Den aller siste tiden har det nordiske samarbeidet blitt ytterligere styrket gjennom en dreining mot et felles forsvarsmarked med integrerte systemer og løsninger. Her vil Norden som forsvarsallianse kunne få et fortrinn ved at vi som små aktører med sterk lojalitet og tillit overfor hverandre, har muligheten til å lage selve mønstermodellen for et nytt forsvar basert på moderne prosjekt- og kontraheringsprinsipper.

Gorrissen Federspiel

Tue Goldschmieding

Nyt om immaterielle rettigheder i Danmark

Region pålagt at betale rettighedsvederlag for videresendelse af tv på regionens hospitaler

Højesteret afsagde den 6. november 2025 dom i sag BS-46528/2023-HJR mellem Copydan Verdens TV (»Copydan«) og Region Midtjylland (»Regionen«). Copydan havde stævnet Regionen og nedlagt påstand om betaling af rettighedsvederlag for videresendelse af tv på Regionens hospitaler. Højesteret pålagde Regionen at betale vederlag for at stille tv til rådighed for patienter, besøgene og personale på Regionens hospitaler i perioden 2019-2022.

I 2016 indgik Copydan og Region Midtjylland en aftale om benyttelse af tv og radio på Regionens hospitaler. Regionen havde opsagt sin aftale med Copydan ved udgangen af 2018, men fortsatte herefter med at tilbyde tv-adgang på hospitalerne. Spørgsmålet i sagen var, om dette udgjorde en overføring til almenheden jf. lovbekendtgørelse nr. 1093 af 20. august 2023 om ophavsret (»den danske lov om ophavsret«) § 2, stk. 4, nr. 1, og derfor krævede betaling af rettighedsvederlag.

Højesteret fandt, at hospitalernes videresendelse af tv var rettet mod et ubestemt antal modtagere, herunder tusindvis af skiftende patienter samt besøgende og ansatte og dermed udgjorde et nyt publikum, som rettighedshaverne ikke havde forudset ved den oprindelige tv-udsendelse. At hospitalsvirksomheden ikke havde et kommercielt formål ændrede ikke herved.

Højesteret fastsatte herefter vederlaget skønsmæssigt. Retten lagde vægt på antallet af tv-skærme, det begrænsede kanaludbud samt den ikke-erhvervsmæssige karakter. Højesteret bemærkede desuden, at tv på offentlige hospitaler typisk ikke udløser vederlagskrav i andre EU/EØS-lande. Højesteret fastsatte vederlaget til 4 millioner kr., hvilket var markant mindre end de foregående instansers beløb. Dommen fastslår, at offentlige institutioner skal sikre de nødvendige rettigheder ved tv-udsendelse til publikum, men at vederlaget skal afspejle den faktiske anvendelse og ikke-kommercielle sammenhæng.

Læs Højesterets dom her: https://www.domstol.dk/media/frvnbm-l3/46528-dom-til-hjemmesiden.pdf

Direktør A var personligt ansvarlig for varemærkekrænkelse og skulle solidarisk med virksomheden betale erstatning på 7,5 millioner kr.

Østre Landsret afsagde den 1. oktober 2025 dom i ankesagen BS-2627/2024-OLR med henholdsvis Hewlett Packard Enterprise Development LP og Hewlett-Packard Development Company L.P. (tilsammen »HPE«) som sagsøgere overfor virksomheden B med direktør A som sagsøgte.

A og B havde købt HPE-produkter uden for EØS og havde herefter solgt HPE-produkterne indenfor EØS. Sagen angik indledningsvist, om der var tale om en varemærkekrænkelse, eller om der var sket varemærkeretlig konsumption. Da HPE ikke selv havde markedsført deres produkter inden for EØS eller givet samtykke hertil, fandt retten, at der ikke var sket varemærkeretlig konsumption af HPE-produkterne efter artikel 15 i Europa-Parlamentets og Rådets forordning (EU) 2017/1001 af 14. juni 2017 (»varemærkeforordningen«). På den baggrund fandt retten, at A og B's salg af HPE-produkter inden for EØS udgjorde en varemærkekrænkelse.

Østre Landsret behandlede herefter A og B's ansvar i forbindelse med varemærkekrænkelsen. Retten lagde vægt på korrespondancer fremlagt under bevisførelsen, som ifølge retten udtrykte, at A og B var bekendt med, at salg af HPE-produkter inden for EØS ikke var lovligt. Med hensyn til at A og B vidste, at salg ikke ville være lovligt, at A og B ikke havde forsøgt at undersøge om HPE-produkterne var markedsført indenfor EØS, samt at

A og B ikke havde forsøgt at få samtykke fra HPE eller nærmere dokumentation for, om der var sket konsumption, fandt Østre Landsret, at varemærkekrænkelsen skulle tilregnes A som groft uagtsomt. Ved vurderingen lagde retten herudover til grund, at A i perioden for varemærkekrænkelsen havde opnået en betydelig indtjening gennem lønindtægter og aktieudbytter fra B.

Ved erstatningens udmåling tog retten udgangspunkt i sagens grovhed og lovbekendtgørelse nr. 88 af 29. januar 2019 (»den danske lov om varemærker«) § 43, stk. 2, som pålægger retten ved erstatningens udmåling at tage hensyn til HPE's tabte fortjeneste samt A og B's uberettigede fortjeneste. A havde opnået en betydelig indtjening fra B, og B havde ved salget af HPE-produkter opnået en omsætning på 100.436.872,54 kr. i perioden 23. juni 2016 til 12. december 2019. På denne baggrund blev erstatningen fastsat til 7,5 millioner kr., som A skulle betale solidarisk med B.

Østre Landsret stadfæstede således Sø- og Handelsrettens dom.

Læs Østre Landsrets dom udgivet i Ugeskrift for Retsvæsen her: https://pro.karnovgroup.dk/b/documents/7001005136

Læs Østre Landsrets pressemeddelelse her: https://www.domstol.dk/oestre-landsret/aktuelt/2025/10/varemaerke-kraenkelse-ved-parallelimport-fra-lande-uden-for-eoes/

Både virksomhed og A personligt var ansvarlig for krænkelser af ophavsretten og markedsføringsloven

Østre Landsret afsagde den 3. oktober 2025 dom i ankesagen BS-31311/2024-OLR med direktør A for B ApS som appellant og PPG Coatings Danmark A/S (»PPG«) som indstævnt. A påstod frifindelse og PPG påstod forhøjelse af erstatning. B Aps var efter Sø- og Handelsrettens dom gået konkurs og trådte følgelig ud som part i ankesagen.

Sagen omhandlede krænkelser ved B ApS' brug af PPG's varemærker i butikker og på hjemmeside, salg af PPG's malingprodukter samt ulovlig kopiering og anvendelse af PPG's farvereceptdatabase.

Landsretten tiltrådte Sø- og Handelsrettens vurdering af, at A og B ApS forsætligt kopierede og benyttede PPG's farvereceptdatabase. Anvendelsen af farvereceptdatabasen udgjorde en overtrædelse af § 71, stk. 1 i lovbekendtgørelse nr. 1093 af 20. august 2023 om ophavsret (»den danske lov om ophavsret«), da farvereceptdatabasen var omfattet af beskyttelsen heri og derfor ikke måtte rådes over af andre.

Landsretten tiltrådte Sø- og Handelsrettens konklusioner og fandt, at anvendelsen af PPG's varemærker i butikker og på hjemmeside var i strid med lovbekendtgørelse nr. 1420 af 2. december 2024 om markedsføring (»den danske lov om markedsføring«), heriblandt § 22 og § 3 om forretningskendetegn og god markedsføringsskik, idet B Aps markedsførte sig som forhandler af PPG-produkter uden en forhandleraftale.

Landsretten behandlede herefter A's personlige ansvar for krænkelserne. Landsretten fandt, at A måtte anses for ansvarlig for krænkelserne i den periode, hvor han var registreret som direktør i B Aps, fra stiftelsen den 10. februar 2023 til den 9. marts 2023, og herefter i en kortere periode som ansat i selskabet frem til begyndelsen af maj 2023. A måtte i kraft af sin stilling anses for i væsentligt omfang at have bidraget til, at krænkelserne blev iværksat og bar dermed et betydeligt ansvar for de skete krænkelser. Østre Landsret fandt på denne baggrund, at A solidarisk med B Aps (nu under konkurs) skulle betale 750.000 kr. i erstatning til PPG.

Under sagen blev udskrifter fra B ApS' hjemmeside fremlagt, hvilket viste at selskabet havde fortsat med at krænke PPG's rettigheder efter Sø- og Handelsrettens dom indtil i hvert fald den 18. oktober 2024, og B Aps (nu under konkurs) blev derfor pålagt at betale 1.500.000 kr. i vederlag og erstatning.

Samlet set stadfæstedes Sø- og Handelsrettens dom, dog med forhøjelse af erstatning.

Læs Østre Landsrets dom udgivet i Ugeskrift for Retsvæsen her: https://pro.karnovgroup.dk/b/documents/7001005168#AF-GR_2025-1106-7

Læs Østre Landsrets pressemeddelelse her: https://www.domstol.dk/oestre-landsret/aktuelt/2025/10/kraenkelse-af-ppg-coatings-danmark-as-varemaerkerettigheder-mv/

Konkurrence- og Forbrugerstyrelsens deling af artikler var ikke en nødvendig del af sagsbehandlingen og udgjorde derfor en ophavsretlig krænkelse

Østre Landsret afsagde den 29. oktober 2025 dom i ankesagen BS-32024/2024-OLR med Inside Media ApS som appellant og Konkurrence- og Forbrugerstyrelsen som indstævnt. Sagen angik, hvorvidt Konkurrence- og Forbrugerstyrelsens deling af ophavsretligt beskyttede artikler fra Inside Media ApS var en krænkelse af § 2 i lovbekendtgørelse nr. 1093 af 20. august 2023 om ophavsret (»den danske lov om ophavsret«) eller omfattet af undtagelsesbestemmelsen i den danske lov om ophavsret § 28, stk. 1, nr. 2 om sagsbehandling inden for offentlige myndigheder. Retten på Frederiksberg havde tidligere frifundet Konkurrence- og Forbrugerstyrelsen.

Konkurrence- og Forbrugerstyrelsen havde indgået aftale med Inside Media ApS om adgang til artikler for 5 personer. Årligt havde Konkurrence- og Forbrugerstyrelsen i gennemsnit delt 23 artikler in-

ternt, som ofte blev delt med 1-4 personer eller flere. Landsretten vurderede, at delingerne overskred antallet af artikler i aftalen og i udgangspunktet udgjorde en ophavsretlig krænkelse.

Spørgsmålet var herefter, om delingerne var omfattet af den danske lov om ophavsret § 28, stk. 1, nr. 2 og derfor var undtaget for forbuddet mod deling, da § 28, stk. 1, nr. 2 tillader offentlige myndigheder deling til brug for sagsbehandling. Det blev i sagen forklaret, at kommunikationsmedarbejdere i Konkurrence- og Forbrugerstyrelsen screenede for artikler af relevans for medarbejderes arbejdsområder, men ikke screenede artiklerne med henblik på konkret sagsbehandling. Konkurrence- og Forbrugerstyrelsen beviste dog under sagen at fire af de delte artikler vedrørte konkret sagsbehandling og var blevet journaliseret. Landsretten fandt derfor at disse fire artikler var omfattet af § 28, stk. 1, nr. 2 og dermed ikke udgjorde en ophavsretlig krænkelse.

Delingen af de øvrige artikler var derimod ikke nødvendig for sagsbehandlingen, og Østre Landsret fandt, at der dermed forelå en krænkelse af den danske lov om ophavsret § 2. Landsretten vurderede, at Konkurrence- og Forbrugerstyrelsen havde handlet uagtsomt og fastsatte vederlaget, som skulle betales til Inside Media ApS, til 175.000 kr.

Læs Østre Landsrets dom her: https://www.domstol.dk/media/1l2ibvzu/landsrettens-dom.pdf

Excel-baseret software og kundedatabaser opfyldte betingelser for immaterialretlig beskyttelse

Sø- og Handelsretten afsagde den 20. oktober 2025 dom i BS-15857/2024-SHR mellem det danske elselskab Andel Energi A/S (»Andel Energi«) og en række tidligere ledende medarbejdere i virksomheden samt deres nystiftede virksomhed A.

Andel Energi overtog i 2022 virksomheden Enova Energy ApS, som beskæftigede sig med salg af solcelleanlæg. Kort før overtagelsen stiftede flere af Enovas ledende medarbejdere en konkurrerende virksomhed. I den nye virksomhed anvendte de Enovas Excel-baserede tilbudssystem med makroer, en database med cirka 235 kundeemner samt standardtekster til tilbudsbreve og leverandøraftaler.

Sagen angik, hvorvidt de tidligere medarbejdere havde ret til at anvende disse materialer i deres nye virksomhed, eller om anvendelsen udgjorde krænkelser af lovbekendtgørelse nr. 1093 af 20. august 2023 (»den danske lov om ophavsret«), lov nr. 88 af 29. januar 2019 (»den danske lov om varemærker«) og lovbekendtgørelse nr. 426 af 12. december 2024 (»den danske lov om markedsføring«). Det centrale spørgsmål var, om de tidligere medarbejdere havde fået tilladelse til at anvende materialerne.

Sø- og Handelsretten fandt det ikke godtgjort, at der forelå en mundtlig aftale om ret til anvendelse af materialerne. Retten konkluderede, at makroerne i Excel-arkene og standardskabelonerne havde den fornødne værkshøjde til ophavsretlig beskyttelse, og at databasen med kundeoplysninger var beskyttet på grund af væsentlig arbejdsindsats. Retten fandt desuden, at over 30 af Enovas kundeemner efterfølgende var blevet kunder hos den nye virksomhed, hvilket udgjorde en overtrædelse af god markedsføringsskik efter den danske lov om markedsføring § 3. Direktøren og en ledende medarbejder blev pålagt personligt ansvar og skulle i fællesskab med virksomheden betale 600.000 kr. i erstatning til Andel Energi. To bestyrelsesmedlemmer blev frifundet, da det ikke var godtgjort, at de havde haft kendskab til krænkelserne.

Læs Sø- og Handelsrettens dom her: https://domstol.fe1.tangora.com/media/-300011/files/Dom_anonymiseret_udgave_BS-15857-2024-SHR.pdf

Lejeboligplatform var ophavsretligt beskyttet og sagsøgtes scraping af data udgjorde en ophavsretlig krænkelse

Sø- og Handelsretten afsagde den 22. oktober 2025 kendelse i en forbudssag BS-42485/2025-SHR med sagsøger BoligPortal A/S overfor sagsøgte ReData A/S. Sagen angik, hvorvidt ReData A/S's scraping af boliglejedata fra BoligPortal A/S's hjemmeside og API udgjorde en ophavsretlig krænkelse efter lovbekendtgørelse nr. 1093 af 20. august 2023 om ophavsret (»den danske lov om ophavsret«) § 71 om beskyttelse af databaser.

ReData A/S havde siden januar 2023 dagligt scrapet otte datapunkter fra BoligPortal A/S's API, herunder lokationskoordinat, udbudsleje, udbudsdato, boligareal, etage, antal værelser, energimærke og boligtype. ReData A/S anvendte dataene på sin egen platform »OneDoor«. Retten skulle tage stilling til, om Boligportal A/S's lejeboligplatform udgjorde en database beskyttet af den danske lov om ophavsret § 71, og i så fald om der forelå en krænkelse af ophavsretten.

Retten fandt, at lejeboligplatformen udgjorde en database beskyttet efter den danske lov om ophavsret § 71. Retten lagde vægt på, at BoligPortal A/S havde anvendt betydelige økonomiske ressourcer og arbejdskraft på at indsamle, kontrollere og præsentere boliglejedata, og at der derfor var tale om en væsentlig investering beskyttet af § 71.

I medfør af § 71 i den danske lov om ophavsret havde Boligportal A/S som udgangspunkt eneret til at råde over databasen. Dog tillader § 11 b, stk. 2 i den danske lov om ophavsret udtræk af data fra databaser, såfremt det sker med henblik på tekst- og datamining, og såfremt der

ikke er gjort forbehold for udtræk af data.

Det centrale spørgsmål var herefter, om BoligPortal A/S på passende vis efter den danske lov om ophavsret § 11 b, stk. 2 havde forbeholdt sig eneretten til at foretage udtræk. Retten fandt, at BoligPortal A/S's data- og privatlivspolitik, som havde været tilgængelig i HTML-format på forsiden af boligportal.dk fra august 2024 gennem et link i footeren, udgjorde et passende forbehold.

Retten vurderede, at de af ReData A/S scrapede data kvalitativt udgjorde en væsentlig del af lejeboligplatformen, idet oplysningerne var centrale data om boliglejemål, som BoligPortal A/S havde investeret betydelige ressourcer i at indsamle, kontrollere og præsentere. ReData A/S havde derfor krænket BoligPortal A/S's rettigheder efter den danske lov om ophavsret § 71, og Sø- og Handelsretten tog derfor Boligportal A/S's påstand om forbud til følge.

Læs Sø- og Handelsrettens kendelse her: https://domstol.fe1.tangora.com/media/-300011/files/Kendelse_BS-42485-2025-SHR.pdf

Beskyldninger mod konkurrent om bedrageri, korruption, skatteunddragelse mv. var i strid med god markedsføringsskik

Sø- og Handelsretten afsagde den 24. oktober 2025 dom i sagen BS-6614/2024-SHR med A og Coreline A/S som sagsøgere overfor B og MODU Valves A/S som sagsøgte. Sagen handlede navnlig om, hvorvidt de sagsøgte havde handlet i strid med § 3 og § 20 i lovbekendtgørelse nr. 1420 af 2. december 2024 om markedsføring (»den danske lov om markedsføring«) ved at offentliggøre beskyldninger om bedrageri, korruption, skatteunddragelse, handel med sorte penge og deling af følsomme prisoplysninger. En af udtalelserne fra B omtalt i sagen var blandt andet, at A's økonomiske kriminalitet var på højde med Stein Bagger og Britta Nielsen.

Retten skulle indledningsvist vurdere, om sagen lå indenfor anvendelsesområdet af den danske lov om markedsføring, som finder anvendelse på virksomhed og ikke på private personers forhold. Det skulle derfor vurderes, om beskyldningerne mod B skete i kraft af virksomhed eller udelukkende var et privat forhold. Retten fandt, at B udtalte sig som erhvervsdrivende, og at beskyldningerne også måtte anses for at hidrøre fra MODU Valves A/S, der var konkurrent til Coreline A/S. Retten vurderede samtidig, at beskyldningerne ikke kun var rettet mod A personligt, men også Coreline A/S. Sø- og Handelsretten konkluderede derfor, at sagen var indenfor anvendelsesområdet, jf. § 1 i den danske lov om markedsføring.

I sagen blev en voldgiftskendelse af 3. november 2020 inddraget af sagsøgte som bevis for beskyldningernes rigtighed. Voldgiftskendelsen omhandlede virksomheden Dansk Ventil Center A/S, som A og B havde drevet sammen. I voldgiftskendelsen blev A's adfærd i Dansk Ventil Center A/S karakteriseret som grov, omfattende og kontinuerlig misligholdelse af hans forpligtelser.

I nærværende dom fandt Sø- og Handelsretten imidlertid, at henset til den sammenhæng, hvori ytringerne blev fremsat, måtte udtalelserne samlet set anses for at angå forhold af mere strafferetlig karakter end blot en reference til en grov og omfattende misligholdelse af en kontraktuel forpligtelse, som det var angivet i voldgiftskendelsen. Ifølge Sø- og Handelsretten gik udtalelserne derfor for vidt.

Sø- og Handelsretten fandt, at B's udtalelser om bedrageri, korruption, skatteunddragelse, handel med sorte penge og deling af følsomme prisoplysninger var i strid med god markedsføringsskik efter den danske lov om markedsføring § 3, stk. 1 samt udtryk for aggressiv og utilbørlig handelspraksis, jf. § 20, stk. 3. I vurderingen lagde retten vægt på karakteren af ytringerne, at de var uopfordrede, samt at de blev fremsat mod en konkurrent. Sø- og Handelsretten nedlagde forbud mod fremtidige udtalelser.

Coreline A/S havde nedlagt påstand om 3.800.000 kr. i erstatning, men Sø- og Handelsretten fandt, at Coreline A/S ikke havde sandsynliggjort et konkret afsætningstab. Retten fastsatte dog skønsmæssigt et beløb på 150.000 kr. for markedsforstyrrelse.

Læs Sø- og Handelsrettens dom her: https://domstol.fe1.tangora.com/media/-300011/files/Dom_-_BS-6614-2024-SHR.pdf

Luftfartsselskab skulle betale bøde for vildledende markedsføring om flyaflysning

Københavns byret afsagde den 10. november 2025 dom i en sag med sagsnummer SS-20378/2023-KBH, hvor den danske anklagemyndighed overfor tiltalte, som var flyselskabet SAS, nedlagde påstand om bøde for overtrædelse af § 5, stk. 1 og § 6, stk. 1, jf. § 8, stk. 1 i lovbekendtgørelse nr. 1420 af 2. december 2024 om markedsføring (»den danske lov om markedsføring«) om vildledende markedsføring.

Sagen i byretten blev foranlediget af den danske Forbrugerombudsmand (»Forbrugerombudsmanden«), som havde politianmeldt SAS for vildledende markedsføring. SAS havde i 2020 under covid-19 pandemien udsendt en mail vedrørende kundernes flyafgange. I mailen stod der, at SAS havde behov for at justere sine flyplaner, at SAS var opmærksom på, at det ikke var optimalt for kunden, og at der var truffet en beslutning. Mailen indeholdt ikke en aflysning af flyene, men Forbrugerombudsmanden anførte, at mailen vildledte forbrugere til at tro, at deres fly var aflyst.

Retten fandt, at mailen fra SAS udgjorde vildledende markedsføring og overtrådte § 5, stk. 1 og § 6, stk.

1, jf. § 8, stk. 1 i den danske lov om markedsføring, idet mailen var formuleret således at forbrugeren kunne tro, at deres fly var aflyst. Retten fandt, at det var nærliggende at tro, at beslutningen, som SAS havde truffet, var, at kundens fly var aflyst, og at der derfor var tale om vildledende markedsføring.

Forbrugernes ret til kompensation var forskellig, alt efter om forbrugeren selv aflyste flyet, eller om SAS aflyste flyet, og retten vurderede derfor, at SAS havde en økonomisk interesse i, at forbrugerne skulle aflyse deres fly.

Ved vurderingen af bødens størrelse lagde retten vægt på, at 901 forbrugere som modtog mailen, valgte at aflyse deres fly, og at den gennemsnitlige billetpris var 2.000 kr. uden skatter og afgifter. Københavns Byret fastsatte bødens størrelse til 1.000.000 kr. med hjemmel i den danske lov om markedsføring § 37, stk. 11, jf. stk. 3, jf. § 5, stk. 1, og § 6, stk. 1, jf. § 8, stk. 1.

Læs Københavns byrets dom her: https://domsdatabasen.dk/#/sag/10264/12056

Læs Forbrugerombudsmandens pressemeddelelse her: https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2025/20251111-dom-sas-skal-betale-boede-paa-1-million-kroner-for-vildledende-markedsfoering

1.9 Virksomhed accepterer Forbrugerombudsmandens bøde på 3,5 millioner kr. for vildledende markedsføring om CO2-neutralitet

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) offentliggjorde den 28. oktober 2025, at virksomheden Verdo Trading A/S har accepteret en bøde på 3,5 millioner kr. fra Forbrugerombudsmanden, efter at være blevet politianmeldt for vildledende markedsføring efter § 5 og § 6, jf. § 8 i lovbekendtgørelse nr. 1420 af 2. december 2024 om markedsføring (»den danske lov om markedsføring«).

Årsagen til bøden var, at Verdo Trading A/S havde markedsført deres træpiller som CO2-neutrale. Forbrugerombudsmanden vurderede, at udsagnet var egnet til at vildlede forbrugeren til at tro, at fyring med træpillerne ikke ville udlede CO2, hvilket ikke var tilfældet.

Verdo Trading A/S forklarede, at træpillerne blev markedsført som bæredygtige, fordi de efterlevede lovkrav i bekendtgørelse nr. 530 af 28. maj 2024 (»den danske bæredygtighedsbekendtgørelse«). Hertil udtalte Forbrugerombudsmanden, at fremhævning af miljøfordele, som følger af lovkrav, udgør vildledende markedsføring.

Læs Forbrugerombudsmandens pressemeddelelse her: https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2025/20251028-verdo-trading-betaler-boede-paa-3-5-millioner-kroner-for-vildledende-udsagn-om-co2-neutralitet-og-baeredygtighed

1.10 Forbrugerombudsmanden skærper fokus på skjulte abonnementer i netbutikker

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) har i efteråret 2025 haft skærpet fokus på netbutikker, der ikke tydeligt oplyser forbrugere om, at de ved køb automatisk tilmeldes et løbende betalingsabonnement.

Flere netbutikker er blevet idømt bøder eller politianmeldt for vildledende markedsføring i strid med § 5 og § 6 i lovbekendtgørelse nr. 1420 af 2. december 2024 om markedsføring (»den danske markedsføringslov«), der forbyder erhvervsdrivende at skjule eller præsentere væsentlige oplysninger på en uklar, uforståelig eller uhensigtsmæssig måde. Retten i Aalborg idømte Plus Global ApS, der driver netbutikken Plusshop.dk, en bøde på 400.000 kr. for at sælge produkter uden tydeligt at oplyse om et månedligt abonnement på 139 kr. Tilsvarende blev HappyHello A/S idømt en bøde på 400.000 kr. af Retten i Næstved for manglende oplysning om månedlige abonnementer på 98-168 kr. ved salg af legetøj og børnebøger på hjemmesiden Littlehappy.dk. Luxplus ApS blev politianmeldt for lignende forhold ved salg af skønhedsprodukter i Danmark, Holland og Belgien.

Forbrugerombudsmanden understregede, at oplysninger om abonnementer skal være klare og tydelige gennem hele købsforløbet. Hvis oplysningerne ikke er til stede eller træder i baggrunden i forhold til produktinformation, udgør det vildledende markedsføring og en overtrædelse af den danske markedsføringslov § 5, stk. 1, og § 6, stk. 1.

Afgørelserne og politianmeldelsen understreger, at netbutikker skal sikre, at oplysninger om abonnementer er lige så fremtrædende som oplysninger om produkter og priser. Virksomheder risikerer betydelige bøder, hvis abonnementsoplysninger skjules eller præsenteres på en uklar måde.

Læs Forbrugerombudsmandens pressemeddelelser her:

HelloHappy ApS: https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2025/20251029-netbutik-idoemten-boede-paa-400000-kroner-for-skjulte-abonnementer

Plus Global ApS: https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2025/20251031-netbutik-idoemten-boede-paa-400000-kroner-for-skjulte-abonnementer

LuxPlus Aps: https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2025/20251216-luxplus-politianmeldt-for-vildledning-af-adskillige-europaeiske-forbrugere.

1.11 Forbrugerombudsmanden politianmelder ILVA for 29 overtrædelser af prismærkningsbekendtgørelsen og vildledningsforbuddet i markedsføringsloven

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) offentliggjorde den 4. december 2025, at Forbrugerombudsmanden havde politianmeldt møbelkæden ILVA A/S for overtrædelser af § 5 og § 6 i lovbekendtgørelse nr. 1420 af 2. december 2024 om markedsføring (»den danske lov om markedsføring«) samt § 9 a, stk. 1 i bekendtgørelse nr. 1696 af 14. december 2017 (»den danske prismærkningsbekendtgørelse«).

ILVA A/S havde haft tilbud på varer i lang tid, herunder eksempelvis en spisebordsstol på tilbud i 72 dage ud af 112 dage. Forbrugerombudsmanden udtalte, at når produkter markedsføres til nedsat pris i så lange perioder, må tilbudsprisen anses for produkternes egentlige normalpris. De oplyste normalpriser har derfor været egnede til at vildlede forbrugerne ved at få tilbuddene til at fremstå bedre, end de reelt var. ILVA A/S blev derfor politianmeldt for overtrædelse af vildledningsforbuddet i § 5 og § 6 i den danske lov om markedsføring.

Yderligere vurderede Forbrugerombudsmanden, at ILVA A/S ikke havde beregnet de angivne besparelser ud fra den korrekte normalpris, og tilbuddene fremstod derfor bedre end de reelt var. En vares normalpris udgør den laveste pris anvendt for varen i en periode på mindst 30 dage forud for prisnedsættelsen, jf. § 9 a, stk. 1 i den danske prismærkningsbekendtgørelse.

Læs Forbrugerombudsmandens pressemeddelelse her: https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2025/20251204-forbrugerombudsmanden-politianmelder-ilva-for-omfattende-overtraedelser

1.12 AYA&IDA ApS idømt bøde for udokumenterede bæredygtighedsudsagn i første danske strafferetlige greenwashing-dom

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) offentliggjorde den 11. december 2025, at Retten i Kolding har afsagt dom i Danmarks første straffesag om greenwashing i sag SS 3-2731/2025. Den danske drikkeflaskeproducent AYA&IDA ApS blev efter politianmeldelse fra Forbrugerombudsmanden idømt en bøde på 140.000 kr. for vildledende markedsføring med udokumenterede miljøudsagn, jf. § 37, stk. 3 og stk. 6, jf. § 5, stk. 1 og § 6, stk. 1, jf. § 8, stk. 1 i lovbekendtgørelse nr. 1420 af 2. december 2024 om markedsføring (»den danske lov om markedsføring«). Sagen er den første afgjorte straffesag ved de danske domstole om greenwashing.

Virksomheden havde i perioden 2021 til 2024 markedsført sine produkter med generelle bæredygtighedsudsagn som »den bæredygtige drikkeflaske« og »bæredygtige hverdagsprodukter« på virksomhedens hjemmeside, sociale medier og produktemballage uden tilstrækkelig dokumentation.

Retten fandt, at AYA&IDA ikke havde dokumenteret, at produkterne faktisk var mere bæredygtige eller havde miljømæssige fordele sammenlignet med tilsvarende produkter på markedet. Dette var i strid med den danske lov om markedsføring § 13 om dokumentationspligt. Virksomhedens henvisning til, at drikkeflaskerne var lavet af holdbart rustfrit stål, der kunne genanvendes, og at forbrugere kunne undgå mikroplast, var ikke tilstrækkelig dokumentation for overordnede miljøfordele.

Dommen fastslår, at virksomheder skal kunne dokumentere faktiske og konkrete miljøfordele ved deres produkter sammenlignet med lignende produkter på markedet. Generelle udsagn om bæredygtighed uden substantiel dokumentation kan medføre betydelige bøder.

Læs Forbrugerombudsmandens pressemeddelelse her: https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2025/20251211-dom-ayaida-faar-boede-paa-140000-kroner-for-greenwashing

1.13 Brancheforeningen Nikotinbranchen omfattet af forbuddet mod tobaksreklame og idømt bøde for overtrædelse

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) offentliggjorde den 22. december 2025, at Københavns Byret har afsagt dom i en sag om brancheforeningen Nikotinbranchen, efter at Forbrugerombudsmanden havde politianmeldt Nikotinbranchen.

Nikotinbranchen havde ytringer på deres hjemmeside og i en pressemeddelelse, som Nikotinbranchen selv mente var sædvanlig brancheforeningsaktivitet, men som retten fandt var reklame for nikotinprodukter. Nikotinbranchen blev af Københavns byret idømt en bøde på 500.000 kr. for at reklamere for nikotinprodukter, da reklamen var en overtrædelse af § 3, stk. 1 i lovbekendtgørelse nr. 586 af 26. marts 2021 (»den danske tobaksreklamelov«).

Forbrugerombudsmanden udtalte, at dommen viser, at brancheforeninger også kan være omfattede af reklameforbuddet i den danske tobaksreklamelov, og at en brancheforenings aktiviteter skal opfylde samme lovmæssige krav, som virksomhederne, den repræsenterer.

Læs Forbrugerombudsmandens pressemeddelelse her: https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2025/20251222-dom-nikotinbranchen-idoemt-en-boede-paa-500000-kr-for-ulovlig-reklame

Tue Goldschmieding, partner i Gorrissen Federspiel og dansk redaktør for Lov & Data.

Bird & Bird

Gunnar Hjalt

Resningsansökan avvisad efter att varumärken hävts

Patent- och marknadsöverdomstolen (PMÖD) vid Svea hovrätt har avvisat Munkens Hälsa AB:s och K.Å.L:s ansökan om resning av en förbudsdom i ett varumärkesmål.

Bakgrund

Patent- och marknadsdomstolen (PMD) förbjöd 2022 Munkens Hälsa AB och K.Å.L., vid vite om 200 000 kr, att i näringsverksamhet i Sverige tillverka, marknadsföra eller sälja bisalveprodukter under varukännetecknet MUNKENS BISALVA. Domstolen fann att sökandena hade salufört produkter med kännetecken som var förväxlingsbara med Mats Lindroos Aktiebolags registrerade EU-figurvarumärke ”Munkens Bisalva” och registrerade nationella figurvarumärke ”Munkgårdens Bisalva”.

Senare utveckling

Efter förbudsdomen ogiltigförklarade EUIPO:s överklagandenämnd i januari 2025 EU-figurvarumärket, och PMÖD hävde i februari 2025 det svenska figurvarumärket eftersom det förelegat hinder för registrering, vid registreringstillfället. Närmare bestämt kunde sökandena visa att Mats Lindroos Aktiebolag agerat i ond tro när varumärkesansökningarna lämnades in.

Domstolens bedömning

PMÖD konstaterade att de varumärkesregistreringar som legat till grund för förbudsdomen numera är upphävda och ska anses aldrig ha haft någon verkan. Eftersom förbudsdomen därmed inte fyller någon praktisk funktion i rättsligt hänseende avvisades ansökan om resning. Domstolen underströk att en grundläggande förutsättning för resning är att talan fyller någon praktisk funktion, vilket innebär att resning inte kan beviljas om det avgörande som angrips har blivit överspelat.

Beslutet meddelades den 29 oktober 2025.

Se avgörandet i dess helhet här: https://rattspraxis.etjanst.domstol.se/sok/publicering/e3ac-6c7e-b91c-4a5b-bceb-9071fd405f41?-domstolskod=PMOD

Gunnar Hjalt, Senior Counsel, Bird & Bird Advokat KB

Henning Wahlberg og Melissa Jakobsen Tveit

«Fold-a-cup» og «Kråka»: Verkshøydekravet, funksjonsbetingede formelementer og terskelen for illojal etterligning

Oslo tingrett avsa 15. januar 2026 dom (publisert i Lovdata under *TOSL-2025-124842*) om rettslig vern for den foldbare turkoppen Fold-a-cup etter åndsverkloven og markedsføringsloven. Saken gjaldt om Fold-a-cup er vernet som åndsverk etter patenttidens utløp, eventuelt etter markedsføringsloven §§ 30 og 25, og om de foldbare koppene «Kråka» fra Sport Outlet Holding AS og Elements Production AS krenker dette vernet.

Wildo Sweden AB selger Fold-a-cup, som tidligere var patent- og mønsterbeskyttet i Sverige og USA, men hvor vernet nå er utløpt. Sport Outlet Holding AS og Elements Production AS reiste negativt fastsettelsessøksmål for å få fastslått at Fold-a-cup ikke har rettslig vern, og at deres kopp «Kråka» verken gjør inngrep i opphavsrett eller utgjør en ulovlig etterligning. Wildo bestred dette og fremmet motkrav om vederlag og erstatning, forbud mot videre produksjon, markedsføring og salg, samt tilbakekall og destruksjon.

Tingretten vurderte først om Fold-a-cup er et åndsverk og hvilket vern den eventuelt har. Spørsmålet er om koppen oppfyller kravet til verkshøyde, som er den nedre grensen for opphavsrettslig vern. Selv om terskelen for verkshøyde ofte beskrives som lav, er grensen fortsatt uklar og i praksis vanskelig å anvende for brukskunst.

Brukskunst er ofte funksjonsstyrt, men tingretten understreker at det ikke gjelder et strengere verkshøydekrav for funksjonelle produkter under henvisning til praksis fra EU-domstolen. I praksis kan imidlertid funksjonelle og tekniske føringer begrense det kreative handlingsrommet, selv om verkshøyde kan foreligge når originaliteten ligger i ikke-funksjonelle uttrykkselementer.

Fold-a-cup er videreutviklet i flere varianter siden 1978. Under prosedyren avgrenset Wildo vernekravet til 1997-utformingen, slik at vurderingen knyttet seg til én konkret versjon. Verkshøyde og originalitet skulle derfor bedømmes ut fra hva som var kjent og funksjonelt betinget i 1997, ikke ved lanseringen i 1978.

Tingretten konkluderte med at Fold-a-cup ikke har verkshøyde. Flere sentrale formelementer ble ansett for å være funksjonelt begrunnet og kunne derfor ikke begrunne opphavsrettslig vern. Retten bygde verkshøydevurderingen kun på rillenes (dvs. fortykkede riller under håndtaket) utforming og koppens samlede kunsthåndverksfaglige finish og helhetsinntrykk. Vurdert opp mot hva som var kjent og mulig i 1997, mente retten at disse trekkene ikke var tilstrekkelig originale eller kreative «utover det helt bagatellmessige». Dermed avviste retten at Fold-a-Cup har verkshøyde.

Retten vurderte deretter vern etter markedsføringsloven (mfl.) §§ 30 og 25. Mfl. § 30 krever etterligning, forvekslingsfare og urimelig utnyttelse, mens mfl. § 25 er en snever terskelregel som skal brukes varsomt når området ellers er regulert av spesiallovgivning. Tingretten la til grunn at når et tidsbegrenset immaterialrettslig vern er utløpt, kan andre som utgangspunkt utnytte løsningen. Disse bestemmelsene kan da bare brukes ved klare holdepunkter for at etterlikningen fremstår som illojal. Slik illojalitet fant retten ikke, selv om «Kråka» versjon I ble beskrevet som svært nær Fold-a-cup. Det forelå derfor ikke et inngrep etter mfl. §§ 30 eller 25.

Avgjørelsen illustrerer at funksjonell brukskunst ofte faller utenfor opphavsretten når de sentrale formelementene er funksjonelt betinget og det som gjenstår ikke gir tilstrekkelig originalitet. Den er også et eksempel på at markedsføringsloven §§ 25 og 30 normalt ikke gir ettervern etter utløpt patent eller designvern uten klare tilleggsmomenter som peker på illojal utnyttelse.

Når bevis trumfer hemmelighold: Realbevis og produsentopplysninger pålagt i patenttvist

Borgarting lagmannsrett avsa 9. januar 2026 kjennelse (publisert i Lovdata under *LB-2026-2146*) om bevistilgang og informasjonspålegg i en patenttvist mellom Welltec A/S og Welltec Oilfield Services (Norway) AS på den ene siden og Schlumberger Norge AS på den andre. Hovedsaken gjelder påstått patentinngrep i to av Welltecs europeiske patenter, samtidig som Schlumberger har reist ugyldighetssøksmål og negativt fastsettelsessøksmål samt krav knyttet til markedsføringsloven § 25.

Kjennelsen inngår i en flertrinns bevistvist i patentsaken. Oslo tingrett ga 12. september 2025 pålegg om bevisfremleggelse, men Borgarting lagmannsrett opphevet 19. november 2025 avgjørelsen på to punkter (realbevis i form av fysiske eksemplarer og tekniske tegninger og utlevering av produsentopplysninger) på grunn av mangelfulle vurderinger. Etter at Høyesteretts ankeutvalg forkastet anken, behandlet tingretten spørsmålene på nytt og ga Welltec medhold 16. desember 2025. Schlumberger anket, og lagmannsretten tok stilling til dette i kjennelsen 9. januar 2026.

Lagmannsretten konkluderte med at Schlumberger må stille både fysiske eksemplarer av de påståtte inngrepsgjenstandene og tilhørende tekniske tegninger til rådighet som realbevis etter tvisteloven § 26-5, jf. § 21-7. Retten mente at dette var helt sentrale og uerstattelige bevis for inngrepsspørsmålet, og at indirekte bevis som videoer, skisser eller modeller ikke er tilstrekkelig. Selv om rådighetsstillelsen ville røpe forretningshemmeligheter, fant retten etter avveiningen i tvisteloven § 22-10 at pålegget var nødvendig av hensyn til sakens opplysning, og avviste proporsjonalitetsinnvendingene. Hensynet til hemmelighold ble ivaretatt gjennom begrenset innsynskrets og taushetsplikt, og retten understreket at motparten måtte få besiktige selve gjenstandene, ikke bare tegningene, for å kunne undersøke faktisk funksjon og utførelse.

Lagmannsretten opprettholdt pålegget om at Schlumberger må oppgi hvem som har produsert de påståtte inngrepsgjenstandene, ved å gi navn og adresse til produsentene etter tvisteloven §§ 28A-1 og 28A-2. Retten mente at det var rimelig grunn til å tro at et patentinngrep kunne foreligge, og at opplysningene var nødvendige for å kartlegge omfanget av forholdet og plassere ansvar. At produksjonen var konsernintern, stengte ikke for pålegg, siden hvert konsernselskap normalt er et eget rettssubjekt. Selv om informasjonen berørte forretningshemmeligheter, ble pålegget opprettholdt fordi behovet for sakens opplysning veide tyngst, og fordi hemmelighold kunne sikres gjennom lukkede dører og taushetsplikt. Anke til Høyesterett ble senere avvist (HR-2026-251-U), slik at lagmannsrettens kjennelse ble stående som siste ord i bevistvisten.

Avgjørelsen illustrerer at domstolene i patenttvister kan kreve tilgang til de mest bevismessig avgjørende kildene, som fysiske gjenstander og tekniske tegninger, selv når dette berører forretningshemmeligheter, fordi indirekte bevis ikke alltid anses for å gi tilstrekkelig grunnlag for en reell inngrepsvurdering. Den illustrerer også at hemmeligholds- og proporsjonalitetsinnvendinger må underbygges konkret og at risiko ofte håndteres gjennom prosessuelle tiltak som begrenset innsynskrets, taushetsplikt og lukkede dører.

Melissa Jakobsen Tveit, advokatfullmektig i Advokatfirmaet Simonsen Vogt Wiig

Henning Wahlberg, advokat i Advokatfirmaet Simonsen Vogt Wiig.

Illustrasjon: Colourbox.com

Gorrissen Federspiel

Tue Goldschmieding

Nyt om persondataret i Danmark

Højesteret skærper beviskrav for immateriel skade efter GDPR artikel 82

Den 19. december 2025 afsagde Højesteret sin første dom om erstatning efter databeskyttelsesreglerne i fire sammenhørende sager. Sagerne omhandlede fire borgere, der krævede erstatning efter Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«) artikel 82 på grund af et databrud hos Gladsaxe Kommune. Sagerne blev behandlet under sagsnumrene BS-14485/2025-HJR, BS-14653/2025-HJR, BS-15152/2025-HJR og BS-16195/2025-HJR.

Ifølge GDPR artikel 82 har enhver, som har lidt materiel eller immateriel skade som følge af et brud på databeskyttelsesreglerne, ret til erstatning fra den dataansvarlige eller databehandleren.

I slutningen af november 2018 udarbejdede økonomiafdelingen i Gladsaxe Kommune et regneark med oplysninger om cirka 20.000 borgere. En medarbejder gemte regnearket på en bærbar computer, som blev stjålet fra rådhuset mellem den 30. november og 3. december 2018. Regnearket indeholdt personoplysninger som navn, CPR-nummer, adresse, bopælskommune samt oplysninger i kodeform om sociale ydelser, som borgerne havde modtaget.

De fire borgere forklarede, at databruddet havde skabt ængstelse og frustration, som viste sig gennem søvnproblemer, koncentrationsbesvær, modløshed, angst og flashbacks. De gjorde på den baggrund gældende, at de havde krav på økonomisk godtgørelse efter GDPR artikel 82.

Højesteret henviste til EU-Domstolens praksis om betingelserne for erstatning efter artikel 82. EU-Domstolen har fastslået, at den, der kræver erstatning efter GDPR artikel 82, både skal bevise at der er sket et brud på databeskyttelsesreglerne, og at dette brud har forårsaget materiel eller immateriel skade. Immateriel skade kan ifølge Højesteret omfatte negative følelser som følge af uautoriseret videregivelse af personoplysninger til andre for eksempel frygt eller utilfredshed udløst af tab af kontrol, risiko for misbrug eller skade på omdømme. Men den berørte person skal bevise både følelserne og de negative konsekvenser heraf. Når en person påberåber sig frygt for fremtidigt misbrug, skal retten vurdere, om denne frygt er velbegrundet.

Højesteret konstaterede, at der ikke var oplysninger om, at regnearket på den stjålne computer i årene efter tyveriet var kommet i hænderne på uvedkommende eller var blevet misbrugt. Retten fandt, at den frygt og de negative følelser, som de fire borgere henviste til, ikke kunne anses for velbegrundede, når man så på regnearkets karakter og omstændighederne ved tyveriet.

Ud over borgernes egne forklaringer var der ikke fremlagt beviser, der støttede, at de havde lidt skade i form af negative følelser og negative konsekvenser heraf som følge af kommunens behandling af deres personoplysninger eller sikkerhedsbruddet. På den baggrund fandt Højesteret, at borgerne ikke havde bevist, at de havde lidt en skade omfattet af GDPR artikel 82. Kommunen blev derfor frifundet.

Dommen er principiel, fordi den fastslår krav til bevis for immateriel skade. Højesteret afviste ikke princippet om, at immateriel skade kan udløse erstatning under GDPR artikel 82 men understregede, at der skal foreligge konkret, dokumenteret bevis for, at den specifikke person har lidt en skade, der kan henføres til bruddet såsom faktisk misbrug, helbredsmæssige konsekvenser eller andre objektivt underbyggede konsekvenser.

Dommen skal ses i sammenhæng med Østre Landsrets afgørelse af 20. august 2025, hvor en borger blev tilkendt 2.500 kr. i kompensation, efter at Hillerød Kommune ved en fejl havde delt borgerens helbredsoplysninger med en tredjepart, som efterfølgende anvendte oplysningerne i en familieretlig sag. Højesterets forestående prøvelse af denne afgørelse vil være afgørende for at etablere en fast retspraksis for immateriel skade efter GDPR artikel 82 i Danmark.

Læs Højesterets dom her: *https://www.domstol.dk/media/5hslkj4u/14485-osv-anonymiseret-dom.pdf*

Datatilsynet har udtalt alvorlig kritik af Skatteforvaltningen for deres sagsbehandlingstid

Det danske Datatilsyn (»Datatilsynet«) traf den 30. september 2025 afgørelse i en sag vedrørende den danske skatteforvaltnings (»Skatteforvaltningens«) behandling af indsigtsanmodninger. Sagen blev behandlet under journalnummer 2024-432-0039.

Skatteforvaltningen havde i perioden 2019 til 2024 en gennemsnitlig sagsbehandlingstid for indsigtsanmodninger på 100,66 dage. Sagsbehandlingstiden var ikke i overensstemmelse med fristerne fastsat i GDPR artikel 12, stk. 3, hvor fristen er en måned, dog med mulighed for forlængelse med to måneder ved komplekse sager. På baggrund af den lange sagsbehandlingstid udtalte Datatilsynet alvorlig kritik af Skatteforvaltningen.

Skatteforvaltningen forklarede, at den lange sagsbehandlingstid særligt skyldtes, at der havde været komplicerede indsigtsanmodninger, og at behandlingen af disse havde forsinket de efterfølgende indsigtsanmodninger modtaget fra øvrige registrerede, da sagerne ifølge Skatteforvaltningens praksis skulle behandles i den rækkefølge de blev modtaget. Datatilsynet vurderede dog, at behandlingen af en indsigtsanmodning ikke kan udskydes med henvisning til, at der behandles andre anmodninger fra øvrige registrerede uanset disse andre anmodningers kompleksitet, antal og modtagelsestidspunkt.

I øvrigt forklarede Skatteforvaltningen, at deres sagsbehandlingstid i perioden 2019 til 2024 også havde skyldtes en opstartsperiode efter GDPR's ikrafttræden, covid-19-nedlukning, implementering af EU-Domstolens krav vedrørende behandling af indsigtsanmodninger i logdata samt mangel på medarbejdere på indsigtsområdet.

Datatilsynet udtalte i den forbindelse at mangel på ressourcer, personale og foranstaltninger ikke kan begrunde sagsbehandlingstider af en sådan længde i en periode på ca. 6 år. Datatilsynet lagde vægt på, at det er den dataansvarliges ansvar at tilrettelægge ressourcer, således at behandlingen af anmodningerne overholder tidsfristerne fastsat i GDPR uanset om for eksempel retstilstanden ændres, eller der opstår mangel på medarbejdere.

Læs Datatilsynets afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2025/sep/datatilsynet-udtaler-alvorlig-kritik-af-skatteforvaltningens-haandtering-af-indsigtsanmodninger

Datatilsynet fastsætter krav til gennemsyn af tv-overvågning af medarbejdere

Det danske Datatilsyn (»Datatilsynet«) traf den 30. september 2025 afgørelse om DSB Service & Retail A/S' tv-overvågning af medarbejdere på arbejdspladsen. Sagen blev behandlet under journalnummer 2025-832-0031 efter en klage fra en fagforening.

Virksomheden oplyste, at tv-overvågningen havde til formål at forebygge og opklare kriminalitet samt sikre mulighed for at gøre retskrav gældende over for medarbejdere. Som hjemmel anvendte virksomheden interesseafvejningsreglen i GDPR artikel 6, stk. 1, litra f.

Datatilsynet fandt efter behandling i Datarådet, at tv-overvågningen var lovlig. Datatilsynet lagde vægt på, at formålene var saglige og udtrykkeligt angivne, og at overvågningen ikke var mere omfattende end nødvendigt.

I forbindelse med Datatilsynets behandling præciserede Datatilsynet betingelser for gennemsyn af optagelser. Gennemsyn med henblik på at gøre retskrav gældende over for medarbejdere kan alene ske ved begrundet mistanke om grovere overtrædelser af interne retningslinjer og regler. Eksempler herpå er konkret og begrundet mistanke om internt svind, chikane eller systematisk snyd med tidsregistrering. Gennemsyn kan i øvrigt kun ske såfremt mindre indgribende midler har været forsøgt og ikke kunne belyse forholdet.

Afgørelsen fastslår således, at arbejdsgivere ikke frit kan gennemse tv-overvågning af medarbejdere, men gennemsynet skal opfylde strenge betingelser.

Læs Datatilsynets afgørelse her: *https://www.datatilsynet.dk/afgoerelser/afgoerelser/2025/sep/tv-overvaagning-af-medarbejdere-hos-dsb-service-and-retail-as*

Datatilsynet godkender hjemmel til AI-baseret sagsbehandling på SU-området

Det danske Datatilsyn (»Datatilsynet«) fastslog i en principiel udtalelse den 30. september 2025, at Uddannelses- og Forskningsstyrelsen har hjemmel til at udvikle og anvende en AI-løsning til vurdering af handicaptillægsansøgninger inden for rammerne af eksisterende dansk lovgivning. Afgørelsen blev truffet under journalnummer 2024-212-0371.

Uddannelses- og Forskningsstyrelsen havde anmodet Datatilsynet om en vurdering af, hvorvidt styrelsen kunne udvikle og idriftsætte en AI-løsning, der trænes på indkomne og afgjorte handicaptillægsansøgninger samt tilhørende dokumentation. AI-løsningen skulle fungere som støtte i vurderingen af, om den fremsendte dokumentation er tilstrækkelig til sagens behandling.

Datatilsynet vurderede, at behandling af personoplysninger til udvikling af AI-løsningen kan ske med hjemmel i GDPR artikel 6, stk. 1, litra e om myndighedsudøvelse samt artikel 9, stk. 2, litra g om behandling af følsomme personoplysninger, der er nødvendig af hensyn til væsentlige samfundsinteresser.

Begge bestemmelser forudsætter dog et supplerende nationalt retsgrundlag. Behandling af personoplysninger som led i driften af AI-løsningen kan ske med hjemmel i eksisterende bestemmelser om statens uddannelsesstøtte (»SU«) i henholdsvis lovbekendtgørelse nr. 395 af 13. april 2023 (»den danske SU-lov«), bekendtgørelse nr. 794 af 22. juni 2025 (»den danske SU-bekendtgørelse«), samt bekendtgørelse nr. 813 af 26. juni 2025 (»den danske AI-SU-bekendtgørelse«). Bestemmelserne fastsætter, at behandling af personoplysninger kan finde sted i forbindelse med ansøgninger eller anden behandling af oplysninger vedrørende SU, når det er nødvendigt for at understøtte styrelsens sagsbehandling.

Afgørelsen er principiel, idet den kan bane vejen for bredere anvendelse af AI i den offentlige forvaltning inden for rammerne af gældende lovgivning.

Læs Datatilsynets udtalelse her: *https://www.datatilsynet.dk/afgoerelser/afgoerelser/2025/sep/drift-af-ai-loesning-til-sagsbehandling-paa-su-omraadet*

A/S Storebæltsforbindelsens hastighedskontrol skete inden for rammerne af de databeskyttelsesretlige regler

Det danske Datatilsyn (»Datatilsynet«) traf den 9. oktober 2025 afgørelse i en sag om retsgrundlaget for A/S Storebæltsforbindelsens behandling af personoplysninger i forbindelse med hastighedskontrol på Storebæltsbroen. Sagen blev afgjort under journalnummer 2025-31-1798.

Klager havde anfægtet retsgrundlaget for, at A/S Storebæltsforbindelsen kunne i) behandle personlysninger, ii) videregive personoplysninger til politiet samt iii) foretage tv-overvågning. Klager mente ikke, at der var hjemmel til ovennævnte behandlinger i lovbekendtgørelse nr. 1335 af 26. november 2024 (»den danske lov om Sund & Bælt Holding A/S«) med det formål at udøve hastighedskontrol.

Datatilsynet fandt i deres afgørelse, at A/S Storebæltsforbindelsen har den fornødne hjemmel til behandling af personoplysninger i § 3 og § 17 i den danske lov om Sund og Bælt Holding A/S, jf. GDPR artikel 6, stk. 3, jf. artikel 6, stk. 1, litra e. Datatilsynet fremhævede, at A/S Storebæltsforbindelsen er forvalter af Storebæltsbroen, jf. § 3 i den danske lov om Sund og Bælt Holding A/S, og at denne forvaltning indebærer at sikre hensigtsmæssig trafik, hvilket blandt andet opnås gennem hastighedskontroller.

Datatilsynet vurderede herudover, at A/S Storebæltsforbindelsen har hjemmel i lovbekendtgørelse nr. 289 af 8. marts 2024 (»den danske lov om databeskyttelse«) § 8, stk. 3 og 4 til at videregive personoplysninger til politiet i forbindelse med konstaterede hastighedsoverskridelser.

Derudover udtalte Datatilsynet, at A/S Storebæltsforbindelsen har hjemmel til tv-overvågning, da de er undtaget forbuddet i lovbekendtgørelse nr. 182 af 24. februar 2023 (»den danske tv-overvågningslov«), jf. § 17, stk. 1, i den danske lov om Sund & Bælt Holding A/S.

Læs Datatilsynets afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2025/okt/behandling-af-personoplysninger-ved-hastighedskontrol-paa-storebaeltsbroen

Datatilsynet opdaterer vejledning om adfærdskodekser

Det danske Datatilsyn (»Datatilsynet«) har den 9. oktober 2025 opdateret sin vejledning om adfærdskodekser for behandling af personoplysninger med nye vejledende tekster og eksempler. Siden er målrettet brancheorganisationer, brancheforeninger og offentlige myndigheder, som overvejer at udarbejde et adfærdskodeks for deres branche. Et adfærdskodeks udarbejdet af en brancheforening, som repræsenterer en bestemt kategori af dataansvarlige eller databehandlere, kan anvendes til at løse databeskyttelsesretlige udfordringer som er sædvanlige for branchen. Den opdaterede side giver nu et samlet overblik over, hvad et adfærdskodeks er, hvem der kan udarbejde et, hvad det kan omfatte og, hvordan det godkendes og føres tilsyn med.

Læs Datatilsynets opdaterede vejledning her: *https://www.datatilsynet.dk/regler-og-vejledning/adfaerdskodekser-og-certificeringsordninger*

EDPB har udvalgt emner for den koordinerede håndhævelsesramme i 2026

Det danske datatilsyn (»Datatilsynet«) offentliggjorde den 14. oktober 2025 en række vedtagelser fra Det Europæiske Databeskyttelsesråds (»EDPB's«) plenarmøde den 7. og 8. oktober 2025, herunder hvilket emne som bliver omdrejningspunkt for EDPB's koordinerede håndhævelsesramme i 2026. Som emne for 2026 har EDPB valgt overholdelse af reglerne om gennemsigtighed og oplysningspligt, som følger af artikel 12, 13 og 14 i GDPR.

Læs Datatilsynets pressemeddelelse her: *https://www.datatilsynet.dk/internationalt/internationalt-nyt/2025/okt/edpb-vaelger-emne-for-naeste-aars-cef*

Forlængelse af Storbritanniens to tilstrækkelighedsafgørelser

Det danske Datatilsyn (»Datatilsynet«) offentliggjorde den 20. oktober 2025, at Det Europæiske Databeskyttelsesråd (»EDPB«) har vedtaget to udtalelser om EU-Kommissionens (»Kommissionens«) udkast til afgørelser, som forlænger gyldighedsperioden for Storbritanniens to tilstrækkelighedsafgørelser.

EDPB er i deres udtalelser positive overfor Kommissionens udkast til afgørelser. EDPB fremhæver, at de databeskyttelsesretlige regler i Storbritannien og EU fortsat min-

der om hinanden men understreger samtidig, at Kommissionen er forpligtet til at overvåge udviklingen i Storbritannien.

Begge Kommissionens udkast til afgørelser er blevet vedtaget, og gyldighedsperioden, som ellers ville have udløbet den 27. december 2025, blev dermed forlænget til 27. december 2031.

Læs Datatilsynets pressemeddelelse her: *https://www.datatilsynet.dk/internationalt/internationalt-nyt/2025/okt/edpb-vedtager-udtalelser-om-tilstraekkelighedsafgoerelser-for-storbritannien*

Datatilsynet præciserer rækkevidden af EU-Domstolens afgørelse om pseudonymiserede personoplysninger i databehandlerkonstruktioner

Det danske Datatilsyn (»Datatilsynet«) offentliggjorde den 22. oktober 2025 yderligere vejledning om rækkevidden af EU-Domstolens afgørelse i sag C-413/23 EDPS v. SRB om pseudonymiserede personoplysninger. Vejledningen blev udsendt efter, at Datatilsynet havde modtaget et stort antal henvendelser om afgørelsens betydning.

EU-Domstolen fastslog i afgørelsen, at pseudonymisering, afhængigt af de konkrete omstændigheder, kan være så effektiv, at den registrerede ikke vil kunne identificeres af andre end den dataansvarlige. Det, at en personoplysning er blevet pseudonymiseret, medfører derfor ikke i sig selv, at den pseudonymiserede oplysning i alle behandlingssituationer og for alle personer skal betragtes som en personoplysning. EU-Domstolen udtalte endvidere, at det relevante perspektiv for vurderingen af, om den registrerede er identificerbar, afhænger af de omstændigheder, der kendetegner behandlingen af oplysningerne i det konkrete tilfælde.

Datatilsynet har fortolket EU-Domstolens afgørelse og taget stilling til, hvorvidt pseudonymiserede oplysninger skal anses for personoplysninger for en databehandler i en databehandlerkonstruktion.

I en databehandlerkonstruktion vil personoplysninger, som er pseudonymiseret af den dataansvarlige, forblive personoplysninger, så længe oplysningerne behandles på den dataansvarliges vegne og efter dennes instruks, idet den dataansvarlige har nøglen til at identificere den registrerede. Perspektivet i databehandlerkonstruktion er, at enhver behandling udelukkende kan ske, fordi den dataansvarlige bestemmer det og har råderet over alle formål og midler. Databehandleren kan ikke behandle disse oplysninger udenfor instruksen, og vurderingen skal derfor foretages fra den dataansvarliges perspektiv. I denne situation er databehandlerens lovlige, tekniske eller kontraktuelle mulighed for at (re-)identificere de registrerede derfor ikke relevant for vurderingen.

Hvis en databehandler ønsker at behandle personoplysninger, der er pseudonymiseret af den dataansvarlige, til egne formål udover instruksen, er oplysningerne stadig personoplysninger for den oprindelige dataansvarlige. Den oprindelige dataansvarlige skal derfor have hjemmel til at videregive personoplysningerne til databehandleren som ny dataansvarlig, uanset om oplysningerne i den nye behandlingskontekst vil kunne falde udenfor definitionen af personoplysninger.

Præciseringen er vigtig, fordi den fastslår, at selvom effektiv pseudonymisering kan betyde, at oplysninger ikke udgør personoplysninger for alle parter i alle situationer, vil pseudonymiserede data fortsat skulle anses som personoplysninger inden for en databehandlerkonstruktion, når databehandleren handler efter instruks, og den dataansvarlige besidder nøglen til identifikation. Vurderingen af, om der er tale om personoplysninger, skal således foretages ud fra den konkrete behandlingskontekst.

Læs Datatilsynets pressemeddelelse her:*https://www.datatilsynet.dk/internationalt/internationalt-nyt/2025/okt/mere-nyt-om-eu-domstolens-afgoerelse-om-pseudonymiserede-personoplysninger*

Læs dommen fra EU-Domstolen her: *https://infocuria.curia.europa.eu/tabs/document?source=document&text=&docid=303863&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=16526693*

Datatilsynet finder ikke tilstrækkeligt grundlag for kritik af DR's krav om login på DRTV

Det danske Datatilsyn (»Datatilsynet«) traf den 23. oktober 2025 afgørelse i en sag om den danske public service-institutions (»DR's«) krav om login på streamingtjenesten DRTV. Datatilsynet fandt ikke fuldt tilstrækkeligt grundlag for at udtale kritik af det obligatoriske login på DRTV, men udtalte kritik af DR's indsamling af brugernes navne. Sagen blev behandlet under journalnummer 2024-432-0041.

DR indførte i efteråret 2024 kravet om login for at afspille streamingindhold på DRTV. Datatilsynet modtog i den forbindelse en række klager fra borgere og igangsatte derfor i foråret 2025 en undersøgelse af, hvorvidt DR's behandling af personoplysninger var i overensstemmelse med GDPR.

Datatilsynet fandt ikke fuldt tilstrækkeligt grundlag for at kritisere, at DR i medfør af GDPR artikel 6, stk. 1, litra e, indsamler oplysninger i forbindelse med brugen af DRTV ved at kræve login. Datatilsynet lagde vægt på, at rækkevidden af DR's public service-forpligtelse ikke entydigt kan fastlægges, og at en sådan fastlæggelse beror på medieretlige vurderinger uden for Datatilsynets kerneområde.

DR anførte at moderne public service kræver en sammenhængende og individuel brugeroplevelse, og at en streamingtjeneste uden login og de dertil svarende funktioner

Illustrasjon: Colourbox.com

ikke udgør et tidssvarende tilbud, som lever op til DR's public service-forpligtelser.

Datatilsynet kritiserede imidlertid, at DR indtil den 5. september 2025 havde indsamlet oplysninger om brugernes navne i strid med princippet om dataminimering i GDPR artikel 5, stk. 1, litra c. Login-siden angav »Fortæl os dit navn«, selvom DR selv havde erkendt, at det ikke var nødvendigt at kende brugernes navne. DR har nu ændret teksten til »Vælg et profilnavn«, hvor brugerne ikke behøver at benytte deres rigtige navn.

Læs Datatilsynets pressemeddelelse her: *https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2025/okt/datatilsynet-har-undersoegt-dr%e2%80%99s-obligatoriske-login*

Datatilsynet har politianmeldt to virksomheder for manglende stillingtagen til indsigtsanmodning

Det danske Datatilsyn (»Datatilsynet«) offentliggjorde den 30. oktober 2025, at tilsynet havde politianmeldt virksomhederne Klein2 ApS og Nordic Cleaning ApS for manglende efterlevelse af Datatilsynets påbud vedrørende en indsigtsanmodning.

Datatilsynet havde ved en tidligere lejlighed påbudt de to virksomheder at tage stilling til en indsigtsanmodning, som begge virksomheder havde modtaget, men ikke havde besvaret. Datatilsynet udtalte, at da ingen af de to virksomheder har efterlevet påbuddet, har Datatilsynet valgt under hensyntagen til GDPR artikel 83, stk. 2 at politianmelde virksomhederne med indstilling til bøde.

Læs Datatilsynets pressemeddelelse her: *https://www.datatilsynet.dk/afgoerelser/afgoerelser/2025/okt/klein2-aps-og-nordic-cleaning-aps-indstilles-til-boede*

EDPB har vedtaget udtalelse om tilstrækkelighedsafgørelse for Brasilien

Det danske datatilsyn (»Datatilsynet«) offentliggjorde den 5. november 2025, at Det Europæiske Databeskyttelsesråd (»EDPB«) har vedtaget en udtalelse om EU-Kommissionens (»Kommissionens«) udkast til en tilstrækkelighedsafgørelse for Brasilien.

Grundlaget for Kommissionens udkast til en tilstrækkelighedsafgørelse er Brasiliens nylige vedtagelse af en databeskyttelseslov. EDPB's udtalelse er positiv, men opfordrer dog Kommissionen til at fremkomme med visse præciseringer, heriblandt angående uklarheder om de dataansvarliges forpligtelse til at foretage konsekvensanalyse, beføjelserne for det brasilianske datatilsyn med hensyn til retshåndhævelse samt rækkevidden af undtagelsesbestemmelsen vedrørende national sikkerhed.

Kommissionens udkast til tilstrækkelighedsafgørelse forventes vedtaget i 2026.

Læs Datatilsynets pressemeddelelse her: *https://www.datatilsynet.dk/internationalt/internationalt-nyt/2025/nov/edpb-vedtager-udtalelse-om-tilstraekkeligheds afgoerelse-for-brasilien*

Datatilsynet anbefaler lovfæstelse af politiets anvendelse af ansigtsgenkendelse

Det danske Datatilsyn (»Datatilsynet«) afgav den 17. november 2025 høringssvar til Rigspolitiets konsekvensanalyse vedrørende et pilotprojekt om politiets brug af ansigtsgenkendelsesteknologi i efterforskning. Sagen havde forinden været behandlet i Datarådet.

Datatilsynet vurderede, at konsekvensanalysen var gennemarbejdet og opfyldte kravene i lov nr. 410 af 27. april 2017 (»den danske retshåndhævelseslov«) § 25.

Datatilsynet fandt dog, at anvendelsesområdet for ansigtsgenkendelse bør præciseres. Særligt brugen af begrebet »lignende overtrædelser« kan skabe tvivl om, i hvilke situationer teknologien må anvendes. Datatilsynet henstillede derfor til, at det præciseres, helst ved lov, hvilke strafbare forhold der kan begrunde anvendelse af værktøjet. Dette følger af principperne om god databehandlingsskik, formålsbegrænsning og dataminimering i § 4, stk. 1-3 i den danske retshåndhævelseslov.

Datatilsynet anbefalede desuden, at politiet udarbejder retningslinjer for, hvordan der i konkrete sager skal tages stilling til anvendelse af værktøjet.

Høringssvaret understreger vigtigheden af klar lovfæstelse af anvendelsesområdet for nye teknologier med høj risiko for den registreredes rettigheder samt behovet for konkrete retningslinjer for anvendelsen i praksis.

Læs Datatilsynets høringssvar her: *https://www.datatilsynet.dk/Media/638996545615404211/Svar%20til%20Rigspolitiet.pdf*

Forslag til forenkling af digitale retsakter i EU's digitale omnibus

Det danske Datatilsyn (»Datatilsynet«) offentliggjorde den 20. november 2025, at EU-Kommissionen (»Kommissionen«) har fremsat forslag til en lovpakke med en række forslag til forenklinger af EU's digitale retsakter herunder GDPR. Forslaget omtales som den digitale omnibus.

Forud for Kommissionens forslag, havde Kommissionen anmodet om høringssvar til den digitale omnibus, hvorigennem den danske regering indgav høringssvar. I høringssvaret kom den danske regering med deres forslag til, hvordan EU's digitale regulering kan forenkles og ensrettes på tværs af retsakter. Forslagene vedrører områderne; data, cookies og ePrivacy, AI Act samt elektronisk identifikation.

Det Europæiske Databeskyttelsesråd (»EDPB«) og Den Europæiske Tilsynsførende for Databeskyttelse (»EDPS«) skal afgive udtalelse om den digitale omnibus, og forslaget skal behandles af EU-Parlamentet og Rådet. Forslaget forventes færdigbehandlet i slutningen af 2026.

Læs Datatilsynets pressemeddelelse her: *https://www.datatilsynet.dk/internationalt/internationalt-nyt/2025/nov/digital-omnibus-forslag-til-aendringer-af-bestemmelser-i-gdpr*

Læs regeringens høringssvar (på engelsk) her: *https://www.ft.dk/samling/20251/almdel/DIU/bilag/5/3081852.pdf*

Interesseafvejningsreglen kan anvendes ved videregivelse af medarbejderoplysninger til dokumentation for arbejdsklausuler

Det danske Datatilsyn (»Datatilsynet«) fastslog i en udtalelse den 20. november 2025, at leverandører som udgangspunkt kan anvende interesseafvejningsreglen i GDPR artikel 6, stk. 1, litra f, om behandling på grundlag af legitime interesser, som hjemmel til at videregive medarbejderoplysninger til ordregivere med henblik på dokumentation for overholdelse af arbejdsklausuler. Udtalelsen er vejledende og kom på baggrund af en anmodning fra et dansk advokatfirma.

Arbejdsklausuler anvendes i vidt omfang af både offentlige og private ordregivere for at sikre rimelige løn- og arbejdsvilkår hos leverandører og derved modvirke social dumping. Ordregivere stiller ofte krav om, at leverandøren fremlægger dokumentation for overholdelse af arbejdsklausulerne, typisk i form af lønsedler, timesedler og ansættelseskontrakter. Dette rejser spørgsmål om leverandørens hjemmel til at videregive sådanne personoplysninger.

Datatilsynet vurderede, at leverandører som udgangspunkt kan anvende interesseafvejningsreglen GDPR artikel 6, stk. 1, litra f. Henset til arbejdsklausulernes formål vil der almindeligvis være tale om så tungtvejende legitime interesser, at disse kan danne grundlag for videregivelsen, medmindre der konkret foreligger særlige omstændigheder, der taler imod.

Leverandører kan således fremadrettet som udgangspunkt anvende interesseafvejningsreglen som hjemmel til at videregive medarbejderoplysninger til ordregivere med henblik på dokumentation for overholdelse af arbejdsklausuler, forudsat at der foretages en konkret vurdering i hvert enkelt tilfælde.

Læs Datatilsynets afgørelse her: *https://www.datatilsynet.dk/afgoerelser/afgoerelser/2025/nov/videregivelse-af-personoplysninger-som-dokumentation-for-overholdelse-af-arbejdsklausuler*

Datatilsynet har ført tilsyn med ejendomsadministratorers håndtering af registreredes rettigheder

Det danske Datatilsyn (»Datatilsynet«) afsluttede i december 2025 tilsyn med fem ejendomsadministratorers overholdelse af databeskyttelsesreglerne, herunder reglerne om indsigt, sletning og oplysningspligt. Tilsynet omfattede DAB, KAB, DAB-Lejerbo, DEAS og Boligexperten. Sagen blev behandlet under journalnummer 2025-41-0139.

Tilsynet viste generelt, at ejendomsadministratorerne havde godt styr på reglerne og alle havde udarbejdet interne retningslinjer til sikring af overholdelse af databeskyttelsesreglerne.

Datatilsynet identificerede dog flere områder med behov for forbedring. Ved indsigtsanmodninger kan dataansvarlige ikke blot henvise til privatlivspolitikken, men skal udlevere alle oplysninger efter GDPR artikel 15, stk. 1. Dataansvarlige skal desuden fortolke anmodninger bredt uanset terminologi, og eksempelvis kan »aktindsigt« fra private borgere reelt udgøre en anmodning om indsigt efter GDPR. Ved delvis afvisning af sletteanmodninger skal begrundelsen være konkret med henvisning til den specifikke lovgivning, der begrunder, at personoplysninger ikke slettes. Centrale værktøjer til at overholde databeskyttelsesreglerne i praksis er interne retningslinjer og løbende medarbejderuddannelse.

Læs Datatilsynets afgørelse her: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2025/dec/datatilsynet-har-foert-tilsyn-med-ejendomsadministratorer

Digitaliseringsstyrelsen har udgivet vejledning om forbudte AI-systemer

Den danske Digitaliseringsstyrelse (»Digitaliseringsstyrelsen«) udgav i oktober 2025 en vejledningspakke om forbudte former for AI-praksis i henhold til Europa-Parlamentets og Rådets Forordning (EU) 2024/1689 af 13. juni 2024 om harmoniserede regler for kunstig intelligens (»AI-forordningen«). Vejledningen supplerer EU-Kommissionens retningslinjer og består af en hovedvejledning samt fem supplerende vejledninger om de områder, som Digitaliseringsstyrelsen fører tilsyn med.

AI-forordningen forbyder i artikel 5 en række AI-systemer, der udgør en uacceptabel risiko mod menneskers sundhed, sikkerhed og grundlæggende rettigheder. Forbuddet omfatter blandt andet skadelig AI-baseret manipulation, skadelig AI-baseret udnyttelse af sårbarheder, sociale scoringer, ikkemålrettet skrabning fra internettet eller kameraovervågning til ansigtsgenkendelse samt følelsesgenkendelse på arbejdspladser og uddannelsesinstitutioner. Forbuddet trådte i kraft den 2. februar 2025 og gælder inden for EU's grænser. Digitaliseringsstyrelsen er udpeget som markedsovervågningsmyndighed i Danmark for hovedparten af de forbudte former for AI-praksis.

Digitaliseringsstyrelsens vejledning understreger, at både virksomheder og offentlige myndigheder skal sikre, at deres AI-anvendelse ikke falder ind under de forbudte kategorier. Det anbefales at foretage grundige risikovurderinger inden ibrugtagning af AI-systemer for at undgå overtrædelse af forbuddet.

Læs vejledningspakken fra Digitaliseringsstyrelsens her: *https://digst.dk/tilsyn/ai-forordningen/regler-ne-i-ai-forordningen/forbudte-former-for-ai-praksis/#accordion-oversigt-over-de-forbudte-former-for-ai-praksis*

Tue Goldschmieding, partner i Gorrissen Federspiel og dansk redaktør for Lov & Data.

Delphi

Klara Thyrén

IMY beslutar om 6 miljoner i sanktionsavgift efter omfattande dataintrång

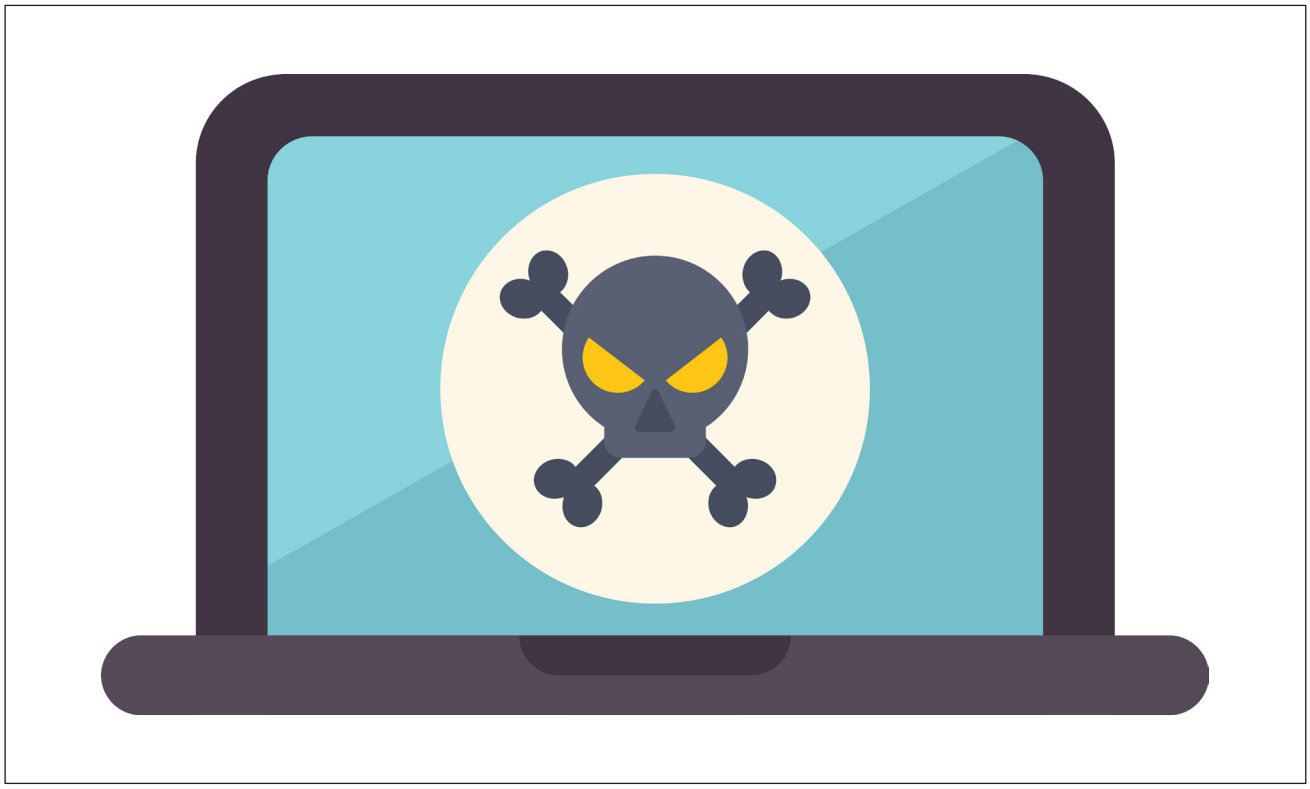
Integritetsskyddsmyndigheten ("**IMY**") beslutade den 26 januari 2026 att ålägga Sportadmin i Skandinavien AB ("**Sportadmin**"), som är ett bolag som tillhandahåller digitala kommunikationstjänster för idrottsföreningar, en sanktionsavgift om 6 miljoner kronor. Beslutet följer den tillsyn som inleddes mot Sportadmin under 2025 med anledning av det dataintrång som upptäcktes den 16 januari 2025. Sportadmin agerade huvudsakligen som personuppgiftsbiträde, men var i viss utsträckning även personuppgiftsansvarig, och tillsynen avsåg frågan om Sportadmin hade vidtagit lämpliga tekniska och organisatoriska säkerhetsåtgärder i enlighet med artikel 32.1 GDPR.

Enligt Sportadmin hade avvikande utgående trafik från produktionsmiljön identifierats genom loggar, vilket indikerade en eventuell dataöverföring. Sportadmin hade trots det inte kunnat fastställa att en dataöverföring faktiskt skett, men den 14 mars 2025 publicerades data som hotaktören kommit åt på Darknet. Sportadmin vidtog ett flertal åtgärder efter incidenten. Redan en timme efter att incidenten upptäcktes stängdes samtliga tjänster ner. Bolaget genomförde vidare tekniska åtgärder för att förhindra fortsatt åtkomst för hotaktören, bland annat genom att aktivera en ny produktionsmiljö och att gå igenom befintlig funktionalitet. Sportadmin informerade samtliga berörda föreningar och uppmanade dessa att anmäla incidenten till IMY samt bistod med att underlätta för korrekta och fullständiga anmälningar.

Vid intrånget berördes över två miljoner personer. De personuppgifter som omfattades innefattade bland annat personnummer, kön, relation mellan målsman och medlem, idrottstillhörighet samt nationalitet. Därutöver omfattades känsliga personuppgifter om hälsa, såsom uppgifter om allergier och funktionsnedsättningar. En betydande andel av de registrerade utgjordes av barn och ungdomar. Det framkom även att skyddade personuppgifter i viss utsträckning hade behandlats, trots att detta inte var avsett att göras i tjänsten.

IMY fann att de tekniska och organisatoriska åtgärderna inte var tillräckliga i förhållande till de risker som förelåg. Intrånget genomfördes genom en så kallad SQL-injektion, vilket är ett sätt för angripare att få åtkomst till databaser genom att utnyttja en säkerhetsbrist. Bristen upptäcktes varken vid den kodgranskning som genomförts, vid efterföljande genomlysningar eller då bolaget införde en uppdaterad säkerhetsmetod mot just denna typ av injektioner. Därutöver konstaterade IMY att de för höga rättigheterna i de bakomliggande systemen möjliggjorde tillgång till mer information än vad som annars hade varit möjligt. IMY noterade att bolagets system inte var utformat för att i realtid upptäcka intrångsförsök, utan endast övervakade prestanda och belastning. Varning utlöstes först två dagar efter att intrångsförsöken påbörjats. Sammantaget bedömde IMY att bolaget saknade tillräckliga åtgärder för att förhindra dataintrång, för att identifiera brister i befintligt skydd samt för att upptäcka pågående intrång i tillräckligt god tid.

IMY bedömde att överträdelsen var av hög allvarlighetsgrad med beaktande av bland annat svårighetsgrad, karaktär och varaktighet. Bristerna i skyddet ansågs vara av grundläggande karaktär, och intrånget omfattade ett mycket stort antal registrerade och en betydande mängd uppgifter om varje person, däribland känsliga personuppgifter och uppgifter om barn. Obehörig åtkomst till sådana uppgifter kan leda till allvarliga konsekvenser för de berörda, vilket enligt IMY ställde



Illustrasjon: Colourbox.com

krav på en hög säkerhetsnivå. Risker för denna typ av injektioner hade även förelegat under en längre period och Sportadmin hade därmed under en längre period undvikt att vidta nödvändiga säkerhetsåtgärder. Det bristfälliga skyddet som i sin tur resulterade i publiceringen av personuppgifter på Darknet innebar en betydande påverkan på de registrerades fri- och rättigheter. IMY hänvisade till EU-domstolens avgörande i mål C-340/21, där domstolen slagit fast att skada kan uppstå redan vid förlust av kontroll över personuppgifter.

IMY angav slutligen att den höga graden av oaktsamhet skulle beaktas som en försvårande omständighet. De åtgärder som vidtogs efter incidenten ansågs i huvudsak utgöra sådant som borde ha genomförts redan dessförinnan. Vad gäller förmildrande omständigheter beaktade IMY att Sportadmin hade tagit en aktiv roll i att bistå föreningarna med incidentanmälningar och information till de registrerade.

Vid fastställande av sanktionsavgiftens storlek prövade IMY huruvida Sportadmin och dess moderbolag, som vid tiden för beslutet ägde 85 % av aktierna, skulle anses utgöra en ekonomisk enhet. Begreppet företag enligt EU-domstolens praxis omfattar samtliga enheter som utövar ekonomisk verksamhet, även om dessa består av flera juridiska personer. Mellan koncernbolagen förelåg betydande organisatoriska, ekonomiska och rättsliga kopplingar. Mot denna bakgrund bedömde IMY att bolagen utgjorde en ekonomisk enhet, varför sanktionsavgiften skulle beräknas utifrån koncernens samlade årsomsättning.

Sanktionsavgiften fastställdes med beaktande av överträdelsens höga allvarlighetsgrad och koncernens omsättning. IMY bedömde att avgiften om 6 000 000 kronor var effektiv, proportionerlig och avskräckande.

Beslutet ger vägledning i vad IMY beaktar vid bedömningen av huruvida organisationer har vidtagit tillräckliga tekniska och organisatoriska säkerhetsåtgärder. Säkerhetsnivån ska anpassas utifrån de risker som föreligger i den specifika situationen, där vissa uppgifter kräver högre skyddsnivå. Det är vidare av vikt att exempelvis ha rutiner på plats som möjliggör upptäckt av eventuella intrång direkt. Organisationer bör säkerställa att deras säkerhetsåtgärder regelbundet ses över och anpassas i takt med förändrade risker och teknisk utveckling.

Klara Thyrén, arbetar som associate inom Tech & IP på Advokatfirman Delphi.

Gorrissen Federspiel

Tue Goldschmieding

Digitaliseringsstyrelsen udpeget som kompetent myndighed til håndhævelse af Data Act

Den 11. december 2025 vedtog det danske Folketing lov nr. 1618 af 16. december 2025 om supplerende bestemmelser til forordningen om harmoniserede regler om fair adgang til og anvendelse af data (»den danske datadelingslov«), som trådte i kraft den 17. december 2025. Den danske datadelingslov skaber de danske nationale rammer for tilsyn med Europa-Parlamentets og Rådets Forordning (EU) 2023/2854 af 13. december 2023 om harmoniserende regler om fair adgang til og anvendelse af data (»Data Act«), som har været direkte anvendelig i Danmark siden 12. september 2025.

I medfør af den nye danske datadelingslov er Digitaliseringsstyrelsen udpeget som kompetent tilsynsmyndighed i henhold til Data Act artikel 37, stk. 1. Udpegelsen betyder, at Digitaliseringsstyrelsen fremover skal sikre overholdelse af Data Act's regler om blandt andet fair adgang til data fra forbundne produkter (IoT) og relaterede tjenester samt skift mellem databehandlingstjenester, herunder cloud-tjenester.

Digitaliseringsstyrelsen har på den baggrund fået tildelt håndhævelsesbeføjelser, som kan anvendes, hvis Digitaliseringsstyrelsen vurderer, at en person eller virksomhed har overtrådt reglerne i Data Act. Den danske datadelingslov giver Digitaliseringsstyrelsen kompetence til at udstede påbud, udtale kritik og offentliggøre afgørelser om påbud eller udtalelser om kritik, jf. den danske datadelingslov §§ 7-9.

Illustrasjon: Colourbox.com

Herudover hjemler den danske datadelingslov bødestraf, som kan anvendes af domstolen i retssager.

Læs Datadelingsloven her: https://www.retsinformation.dk/eli/lta/2025/1618

Tue Goldschmieding, partner i Gorrissen Federspiel og dansk redaktør for Lov & Data.

LOVDATA