

Lov & Data

September 2026

Nr. 167 3/2026

Innhold

Leder	2
Viveca Still	
Upphovsmännens krav på skydd mot AI-användning ökar – men hur hitta en bra och balanserad modell?	

Artikler

Erik Janzon, Fredrik Qvist och Ann Sofie Silversved	
Modern datadelning med integritetsfrämjande teknik.	4
Jalmari Männistö	
Freedom of personal data business – conflict of commercial practice and authority review	7
Hanne P. Gulbrandsen	
Innsynsrettens rekkevidde – logginnsyn og identitetsinformasjon.	12
Emil Piva	
Finjustering av AI-modeller och AI-system När en tillhandahållare kan bli leverantör enligt AI-förordningen.	17
Ove A. Vanebo	
«Pay or consent»: Hva er tillatt innenfor rammene av GDPR?	22
Jakub Skórczynski	
How stakeholder pressure and institutional priorities can shape AI legislation – The case of AI Act Annex I under the Digital Omnibus on AI	28
Håvard Sveier Ottemo og Line Helen Haukalid	
Når er opplysninger anonyme? EDPB foreslår nye retningslinjer om anonymisering	33
Viveca Still	
Licensing works for AI – Do the licensing practices of Nordic copyright management organisations comply with the CRM Directive?	36
JusNytt	41
Halvor Manshaus	
Tysk avgjørelse om trening av AI på musikkverk: GEMA vs Suno	
Rettsinformatisk litteratur med mer.	44
Nytt om personvern	45
Nytt om immaterialrett.	50
Nytt om IT-kontrakter.	56
Annet nytt	60



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.

Lov
& Data

Layout: Aksell AS

Leder

Upphovsmännens krav på skydd mot AI-användning ökar – men hur hitta en bra och balanserad modell?

Många rättsinnehavare menar att EU:s regelverk, särskilt undantagen för text- och datautvinning i EU:s upphovsrättsdirektiv från år 2019, det sk DSM-direktivet, har skapat en situation där stora teknikföretag kan bygga kommersiella AI-system med stöd av kreativa verk utan att inhämta tillstånd eller betala ersättning till dem som skapat innehållet.

Ur upphovsmännens perspektiv är kritiken lätt att förstå. Dagens generativa AI-system tränas på enorma mängder texter, bilder, musik och annat material som skapats genom mänskligt arbete och ofta skyddas av upphovsrätt. När värdet av detta material omsätts i AI-tjänster som genererar miljardintäkter uppstår en berättigad fråga om vem som egentligen får del av den ekonomiska nyttan.

Därför växer kraven på en tillståndsbaserad modell. Upphovsmännen menar att användning baserad på ett undantag i upphovsrätten inte är hållbart, inte är rättvist mot upphovsmännen och inte medför tillräcklig rättssäkerhet för användarna.

Men frågan är mer komplicerad än så.

Dels är det mycket möjligt att ett flertal av de AI-system som finns idag strider mot nuvarande regelverk och därmed uttryckligen redan kräver tillstånd från upphovsmännen. Det är till exempel helt uppenbart att AI-system inte kan tränas utan licens från upphovsmännen med material som framställts och spridits till all-



Viveca Still

mänheten utan upphovsmännens tillstånd. Upphovsrättslicenser krävs också för AI-system att generera resultat som återger rättsligt skyddat material.

Det finns också andra situationer där en licens helt klart behövs enligt gällande rätt. Den exakta omfattningen och tillämpningen av undantagen för text- och datautvinning kommer dessutom att påverkas av EU-domstolen avgöranden, även om det idag finns gråområden. Domstolens första avgöranden är redan på väg; Då denna tidning utkommer har kanske generaladvokatens utlåtande i Like Company-fallet (C-250/25) redan publicerats.

Den kompromiss som antogs i DSM-direktivet innebär att text- och datautvinning särskilt för forskningsändamål har ett särskilt skydd. Då det gäller andra användningsändamål har man försökt nå en balans genom

att erbjuda en opt-out-möjlighet som är avsedd att skydda rättsinnehavarnas kommersiella intressen. Förbättringar av de praktiska förutsättningarna för att göra en opt-out har de senaste åren aktivt befrämjats som en del av arbetet med upphovsrättens infrastruktur, ett arbete som startade under Finlands EU-förmanstidsperiod år 2019. EU:s reglering innebär alltså ingen obegränsad nyttjandemöjlighet för AI-industrin, och även om nuvarande reglering inte fungerar perfekt, finns det ännu mycket som sker på praktiskt plan.

Dels måste man kunna svara på behoven för och förväntningarna på en licens- eller ersättningsordning. Ur AI-utvecklarnas synvinkel behöver en lösning täcka alla skeden av träning och finjustering av AI-modeller, inklusive även partiell inkludering av skyddat material i innehåll som genereras och spridning av AI-modeller. Ett betydande problem är att AI-modeller av hög kvalitet kan kräva tillgång till material med vilket AI inte kan tränas idag, i första hand sådant material som tillgängliggörs inom ramen för digitala innehållstjänster som i sina användningsvillkor eller genom tekniska åtgärder exkluderar möjligheten att använda materialet för text- och datautvinning. Är upphovsmännen villiga att frångå nuvarande modell som till den här delen baserar sig på individuella eller kollektiva licenslösningar?

Hur ser upphovsmännen att regelverket och licensmodellerna borde se ut? Tänker man sig att tillhandahållaren av en sökmotor innan den indexerar och producerar svar till användaren ska utreda innehållet på varje webbsida för att detektera upphovsrättsligt skyddat material, leta upp och förhandla om tillstånd av alla potentiella rättsinnehavare? Det fungerar knappast i praktiken.

Hur skulle upphovsmännen förhålla sig till en ny uppgörelse i upphovsrätten som med säkerhet skulle täcka alla former av reproduktion och tillgängliggörande för träning av AI-modeller, agenter och all använd-

ning i generativ AI och som täcker allt upphovsrättsligt skyddat material? Det är ju endast en sådan modell som skulle öka rättssäkerheten också för teknikbolagen och användarna. Men med tanke på den enorma mängden skyddat material det är frågan om kunde en sådan lösning väl knappast vara något annat än någon form av allmän ersättningsordning. Det är svårt att se att det skulle gillas av upphovsmännen.

En avtalslicenslösning är troligtvis en modell som upphovsmännen själva gärna ser och för fram som en ”kompromisslösning”. En koncentring av rättigheterna på rättsinnehavarsidan garanterar en stark förhandlingsposition i förhållande till de globala jättarna – men hur garanterar man att avtalen är skäliga och förhandlingspositionen är jämbördig för mindre aktörer och att inte avtalsvillkoren innebär att man ändå är tvungen att utlösa individuella licenser? Och hur når man enighet om gränsoverskridande verkan av sådana licenser, vilket skulle vara en förutsättning för att modellen skulle fungera i en global miljö?

Det är också nödvändigt att titta på vad en lösning skulle innebära med tanke på upphovsrättens allmänna läror. Vad är den ”användning” som skall anses vara upphovsrättsligt relevant, och förespråkar man teknologineutrala eller teknologibundna regler?

DSM-direktivets regler om text- och datautvinning berör en aktivitet, inte en viss teknologi. Vill man binda reglerna till en viss teknologi, såsom generativ AI, så finns det en stor risk att regelverket snabbt blir föråldrat.

DSM-direktivet utgår ifrån att det är den exemplarframställning som är nödvändig för att kunna analysera upphovsrättsligt skyddat material som är den upphovsrättsligt relevanta användning som undantaget tillåter. Själva analysen är inte upphovsrättsligt relevant. Det finns ingen rätt för upphovsmännen att kontrollera hur information generas från upphovsrättsligt skyddat material, såsom att

identifiera mönster, trender och samband. Om sådan analys i sig kräver tillstånd riskerar upphovsrätten att flytta sitt fokus från uttrycket till informationen i verket. Då skyddas inte längre bara det som skapats, utan även möjligheten att lära sig av det och att skapa nytt.

Vill man ändra nuvarande regelverk så att det anses vara ett upphovsrättsligt relevant nyttjande som kräver licens om man laddar upp material för att få det sammanfattat, analyserat eller jämfört med annat material? Om svaret är ja närmar vi oss ett system där själva läsningen och analysen av ett verk blir tillståndspliktig. Det vore ett betydande steg bort från den upphovsrättsliga tradition som hittills präglat Europa.

Även om det är rimligt att de som bidrar med det kreativa råmaterialet också får del av de ekonomiska värden som AI genererar, så är det viktigt att se till att lösningen också medför en samhällsnytta. Det får inte innebära att upphovsrätten omvandlas till en rätt att kontrollera informationsanalys och informations-spridning.

Den verkliga utmaningen ligger därför i att hitta en balans och praktiska lösningar. Upphovsmän ska kunna få ersättning när deras verk skapar mervärde för AI-industrin. Men framtida licensordning måste också garantera att den är ändamålsenlig och möjliggör utveckling och användning av generativ AI och framtida teknologi. Dessutom måste samhället bevara en grundläggande frihet att läsa, analysera och lära av information och skapa nytt. Om den balansen går förlorad riskerar vi inte bara att förändra reglerna för AI. Vi riskerar att förändra själva idén om vad upphovsrätten är till för.

Viveca Still, juris doktor, lagstiftningsråd. Finsk redaktör.



Modern datadelning med integritetsfrämjande teknik

Av Erik Janzon, Fredrik Qvist och Ann Sofie Silversved



Erik Janzon



Fredrik Qvist



Ann Sofie Silversved

Tänk om en myndighet kunde identifiera vilka personer som har rätt till ett bidrag, eller vilka personer som inte har rätt till det, utan att få tillgång till uppgifter om deras faktiska inkomster. Eller om flera vårdgivare kunde träna en gemensam AI-modell utan att patientuppgifter behövde lämna respektive organisation. Eller om det gick att på ett tillförlitligt sätt fastställa risken för att enskilda personer identifieras i en datamängd som ska tillgängliggöras som öppen data. Detta är inte längre enbart teoretiska resonemang utan faktiska möjligheter med hjälp av integritetsfrämjande teknik – *Privacy Enhancing Technologies*, PET.

I den statliga utredningen *En stärkt förmåga till modern datadelning – integritetsfrämjande teknik i offentlig förvaltning* (SOU 2026:44) analyserar vi ett antal sådana tekniker och deras rättsliga och praktiska förutsättningar. Utredningen behandlar bland annat moderna tekniker för anonymisering såsom differentiell integritet (*differential privacy*) och syntetiska data. Därutöver behandlas nya tekniker

som möjliggör analys och kunskapsdelning utan att de underliggande uppgifterna behöver delas mellan aktörerna. Exempel på sådana tekniker är federerad inläring, säker flerpartsberäkning (*secure multi-party computation*) och homomorf kryptering (*homomorphic encryption*).

I det följande redogör vi kort för utredningens slutsatser kring integritetsfrämjande tekniks nytta och potential, rättsliga förutsättningar och framtidens moderna datadelning.

Från datadelning till kunskapsdelning

Traditionell datadelning innebär ofta att en aktör lämnar över uppgifter till en annan. För offentlig förvaltning kan detta vara problematiskt när uppgifterna är känsliga, omfattas av sekretess eller medför betydande integritetsrisker. Integritetsfrämjande teknik möjliggör ett annat angreppssätt. I stället för att dela själva uppgifterna kan aktörerna dela den kunskap eller det resultat som behövs. Säker flerpartsberäkning gör det exempelvis möjligt

för flera aktörer att genomföra gemensamma beräkningar på sina respektive datamängder under kryptering, utan att datamängderna behöver delas i klartext. I det enklaste exemplet kan två aktörer jämföra listor över personer med varandra och komma fram till hur många personer som finns på båda listorna, utan att exponera vilka personer som finns på respektive lista för varandra. Vid behov kan även uppgiften om vilka personer som finns med på båda listorna delas mellan aktörerna. Ett annat exempel på integritetsfrämjande teknik som möjliggör kunskapsdelning är federerad inläring. Genom tekniken kan en AI-modell tränas gemensamt av flera aktörer, utan att det träningsdata som respektive aktör använder behöver delas med andra.

En ökad användning av integritetsfrämjande teknik kan innebära ett skifte i synen på datadelning. I stället för att utgå från att data måste överföras mellan aktörer kan uppgifterna i fler situationer lämnas kvar hos den som innehar datat och



Illustrasjon: Conolorbox

endast kunskap och insikter från datamängden delas. Rätt utformad och använd kan integritetsfrämjande teknik göra det möjligt att tillgodogöra sig kunskap från data utan att de underliggande uppgifterna behöver exponeras. Integritetsskydd och datadelning behöver således inte vara motstående intressen utan förenas i modern datadelning.

Integritetsfrämjande teknik som teknisk skyddsåtgärd

Integritetsfrämjande teknik kan inte bara göra datadelning möjlig i situationer där det annars skulle vara svårt eller olagligt att dela uppgifter. Teknikerna kan också vara en del av de skyddsåtgärder som krävs enligt dataskyddsförordningen. Pseudonymisering och kryptering nämns uttryckligen som exempel på sådana åtgärder, och vid valet av åtgärder ska även den senaste utvecklingen (*state of the art*) beaktas. Vad som utgör den senaste utvecklingen är inte statistiskt utan behöver bedömas kontinuerligt och i förhållande till vilka tekniska möjligheter som faktiskt finns.

I utredningen har vi bedömt att integritetsfrämjande tekniker kan utgöra lämpliga tekniska skyddsåtgärder, en bedömning som stöds av uttalanden från IMY och EDPB.¹

Flera av de tekniker som berörs i utredningen kan dessutom anses ligga inom ramen för vad som är *state of the art*. Det gäller särskilt differentiell integritet, syntetiska data och säker flerpartsberäkning. Teknikerna har funnits inom forskning och akademi under en längre tid men är ännu inte allmänt etablerade i praktisk användning.

Det innebär att aktörer som ska dela eller bearbeta data som innehåller personuppgifter bör överväga om det är lämpligt att använda integritetsfrämjande teknik som ett ytterligare skyddslager för sin personuppgiftsbehandling. Det innebär vidare att det inte krävs någon egen rättlig grund eller något eget ändamål för att använda integritetsfrämjande teknik. Användningen av integritetsfrämjande teknik har till syfte att stärka säkerheten i samband med en personuppgiftsbehandling, på samma sätt som behörighetsstyrning, loggning och andra skyddsåtgärder.

Omfattande potential för offentlig datadelning

Betydelsen av integritetsfrämjande teknik är inte begränsad till skyddet för personuppgifter. Användningen vid datadelning kan även bidra till ökad effektivitet, säkerhet, kvalitet och service samt till bättre beslutsunderlag och ökad innovation inom den offentliga förvaltningen. Den samhällsekonomiska potentialen för användning av integritetsfrämjande teknik i samband med datadelning inom offentlig förvaltning är också betydande. En analys som RISE har

genomfört på uppdrag av utredningen uppskattar nyttan av ökad och förbättrad datadelning till mellan 30 och 80 miljarder kronor per år. Av detta bedöms mellan 10 och 40 miljarder kronor vara direkt beroende av att integritetsfrämjande teknik används.

I utredningen beskriver vi flera användningsområden för integritetsfrämjande teknik. Dessa spänner över stora delar av den offentliga förvaltningen. Ett sådant område är hälso- och sjukvård, där stora mängder känsliga personuppgifter hantearas. Det finns samtidigt ett stort behov av att dela och använda data för vård, forskning och verksamhetsutveckling. Federerad inlärning och syntetiska data kan till exempel användas för att minska behovet av att dela patientuppgifter, vilket bland annat ett svenskt projekt visar där gemensamma AI-modeller för att förutsäga vårdtider har utforskats.²

Ett annat område är brottsförebyggande och brottsbekämpande verksamhet, där stora mängder data behöver samlas in och analyseras. Integritetsfrämjande teknik kan bidra till att begränsa både vilken information som behöver behandlas och vem som får tillgång till den. I internationella pilotprojekt har det bland annat undersökts hur federerad inlärning och homomorf kryptering kan användas för att motverka penning-

¹ Europeiska dataskyddsstyrelsen (EDPB), Guidelines 1/2026 on processing of personal data for scientific research purposes, adopted version for public consultation, s. 65 och Integritetsskyddsmyndigheten (IMY), IMY-2025-5444, Betrodda exekveringsmiljöer för uppkopplade fordon, s. 5, 13 och 23.

² AI Sweden, Syntetiska data inom intensivvård

” En utveckling mot kryptering som regel, där data endast dekrypteras i undantagsfall, skulle kunna förena två till synes motstående intressen – ett ökat nyttjande av data och ett starkare skydd för den enskilde

Även inom andra områden av den offentliga förvaltningen finns det stor potential med användningen av integritetsfrämjande teknik. Internationellt finns det flera exempel på användning av teknikerna. Säker flerpartsberäkning och homomorf kryptering används för att identifiera pensionärer som har rätt till ett underutnyttjat bidrag i Nederländerna.⁴ Differentiell integritet och syntetiska data har använts för att offentliggöra uppgifter ur Israels födelseregister som kan användas som underlag för framtida politiska beslut.⁵ Federerad inlärning och betrodda exekveringsmiljöer (trusted execution environments) har använts för att samla in känsliga data och möjliggöra analys och träning av en gemensam AI-modell som ska ge bättre beslutsunderlag om bland annat bevattning och

skadedjursbekämpning för vinodlare i Spanien och Italien.⁶

Datadelning i framtiden

Trots potentialen används moderna integritetsfrämjande tekniker fortfarande i begränsad omfattning inom den offentliga förvaltningen. Vi har i utredningen konstaterat att många myndigheter saknar kunskap, erfarenhet och teknisk kompetens, vilket kan leda till överdriven försiktighet och att möjligheterna till datadelning inte tas till vara. Det finns inte heller någon tydlig nationell styrning av användningen av integritetsfrämjande teknik i Sverige, och det saknas även i Norge, Finland och Danmark. För att öka användningen av teknikerna vid datadelning inom den offentliga förvaltningen har vi föreslagit åtgärder som ska höja kunskapsnivån och underlätta den tekniska användningen. I korthet innebär förslagen att Myndigheten för digital förvaltning (som slås ihop med Post- och telestyrelsen 1 januari 2027) ska få i uppdrag att ge stöd och vägledning om integritetsfrämjande teknik till offentlig förvaltning. Vi har också föreslagit att Skatteverket ska tillhandahålla förvaltningsgemensamma tjänster som gör vissa tekniker lättare att använda. En förvaltningsgemensam tjänst för säker flerpartsberäkning pekas ut som en första sådan tjänst. Vi har även föreslagit uppdrag till vissa myndigheter för att stimulera användningen av teknikerna, bland annat att Socialstyrelsen ska utforska användningen av differentiell integritet inom hälso- och sjukvården.

Mot bakgrund av den tekniska utvecklingen och de ökande kraven på skydd för personuppgifter och andra känsliga uppgifter framstår det som sannolikt att kryptering på längre sikt kommer att få en alltmer cen-

tral roll i samhällets informationshantering. Utvecklingen går från att data huvudsakligen skyddas vid överföring och lagring till att skyddet även omfattar själva bearbetningen. Genom så kallad krypterad databehandling (*encrypted computation*) kan beräkningar utföras på krypterade data, bland annat genom säker flerpartsberäkning. På motsvarande sätt utvecklas inom integritetsbevarande maskininlärning (*privacy-preserving machine learning*) metoder för att träna AI-modeller på krypterade eller på annat sätt skyddade data. Att kryptering väntas få en större betydelse vid all informationshantering ligger även i linje med den moderna cybersäkerhetsmodellen Zero Trust, där säkerheten utgår från kontrollmekanismer som auktorisering och kryptering istället för systemgränser och organisatoriska avgränsningar.⁷ Sammantaget framstår det därför som sannolikt att kryptering successivt utvecklas från att utgöra en kompletterande skyddsåtgärd till att bli till regel i all datahantering.

En utveckling mot kryptering som regel, där data endast dekrypteras i undantagsfall, skulle kunna förena två till synes motstående intressen – ett ökat nyttjande av data och ett starkare skydd för den enskilde. Fler insikter kan då utvinnas och delas, vilket skapar stora nyttor samtidigt som mindre data behöver göras tillgängliga i läsbar form. Genom de förslag som utredningen har lämnat kan den offentliga förvaltningen ta de första stegen mot en modernare datadelning.

Erik Janzon var särskild utredare, Fredrik Qvist huvudsekreterare och Ann Sofie Silversved sekreterare i Utredningen om integritetsfrämjande teknik i förvaltningen.

3 Infocomm Media Development Authority, Preventing financial fraud across different jurisdictions with secure collaborations IMDA PET sandbox – Mastercard case study.

4 <https://www.tno.nl/en/newsroom/insights/2021/09/targeted-yet-privacy-friendly-approach/> (hämtad 2026-08-25).

5 S. Hod & R. Canettis, 2025, Differentially Private Release of Israel's National Registry of Live Births.

6 <https://cordis.europa.eu/project/id/101129822> (hämtad 2026-08-25) och <https://titan-cosc.eu/> (hämtad 2026-08-25).

7 Z. Adahman, A. W. Malik & Z. Anwar, 2022, "An analysis of zero-trust architecture and its cost-effectiveness for organizational security", Computers & Security, Volume 122.

Freedom of personal data business – conflict of commercial practice and authority review

By Jalmari Männistö

Personal data processing and conducting business in an IT environment are high inseparable concepts. The GDPR and limited national statutory instruments create a walled garden in which such enterprises are free to operate within clear boundaries – or do they? A rising theme in Nordic authority and court jurisprudence is the role and weight given to a business's freedom to choose its methods of operation in relation to how they affect the protection of personal data. The question essentially is to what extent a commercial choice can justify or undermine related personal data processing.

This short article explores the topic via two recent Finnish court decisions (the Posti/OmaPosti case and the data protection fine imposed on [Verkkokauppa.com](https://www.verkkokauppa.com)), wherein the respective companies defended themselves against data protection fines on the basis that the allegedly breaching data processing was the result of legitimate commercial choices.

Legal background

While the GDPR does *not* set out to which extent a data controller's commercial choices dictate the scope of processing, this autonomy is indirectly protected through general legal principles and the broader regulatory context. Recital 4 of the GDPR explicitly recognises (in line with the broader EU fundamental rights regime) that “*the right to protection of personal data is not an absolute right*”, underlying the fact that it

must be balanced according to the principle of proportionality against other rights, such as the freedom to conduct a business. In line with later analysis, both the Finnish Constitution (Section 18) and the EU Charter of Fundamental Rights (Article 16) contain express recognitions of the freedom to conduct a business, requiring a proportionality assessment when these rights conflict. In practice, this conflict assessment is generally baked into the more clear-cut application of data protection regulation, but the broader statutes require an additional balancing exercise.

While the GDPR utilizes a risk-based approach for managing data processing, this framework focuses primarily on implementing security measures and mitigation strategies for established activities. It is not, however, a substitute for the substantive requirement of lawfulness which the controller has primary responsibility to demonstrate compliance with.¹ A risk assessment cannot retroactively validate a processing activity that fundamentally lacks a valid legal basis or fails to



Jalmari Männistö

satisfy core statutory obligations, such as proportionality and data minimization.² The ongoing gauging of proportionality – established in cases such as Digital Rights Ireland and Schrems II – underscores a positive obligation to uphold fundamental rights. This demonstrates that when norms conflict, the necessity and proportionality test acts as a constitutional filter that cannot be bypassed by a controller's internal risk management processes.³ As

1 European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law* (2018 edn, Publications Office of the European Union 2018); Raphaël Gellert, ‘Understanding the notion of risk in the General Data Protection Regulation’ (2018) 34 *Computer Law & Security Review* 279; see e.g. Case C-60/22, *UZ v. Bundesrepublik Deutschland* (ECLI:EU:C:2023:373), para. 53

2 Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020); Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679* (17/EN WP 248 rev.01, 2017).

3 Brkan M, ‘The essence of the fundamental rights to privacy and data protection: Finding the way through the maze of the CJEU’s constitutional reasoning’ (2019) 20 *German Law Journal* 864

lawfulness itself concerns the choice of the most correct legal basis for the chosen activity, the question increasingly concerns the specific limits found in the wording of these legal bases.

” In practice, this conflict assessment is generally baked into the more clear-cut application of data protection regulation, but the broader statutes require an additional balancing exercise.

The primary avenues for accommodating commercial interests appear to lie in determining processing necessity under contract (Article 6(1)(b) GDPR) – where central questions relate to which contractual obligations are strictly necessary for the performance of a contract which the data subject has willingly entered into⁴ – and legitimate interest (Article 6(1)(f) GDPR) – where the inquiry focuses on which commercial interests are balanced against and do not override fundamental rights.⁵ Whilst legitimate interest has received some love in jurisprudence via recognising commercial interests as simply existing,

the fundamental open question underpinning Art. 6(1)(b) on what obligations and processing are deemed “necessary” under GDPR framework, or *what kind of contracts and related processing would be infringing as-is* is an evergreen topic.

The relevance of supervisory authority guidance done by the European Data Protection Board (EDPB) is integral to the application of data protection regulatory standard to commercial practices. Recently the EDPB has taken a proactive stance in issuing guidelines on edge-cases where there is not as established jurisprudence⁶ – this should be considered as a major theme in the two case studies discussed below especially as EDPB does not merely offer soft law documents but binding guidelines to supervisory authority enforcement.

Recent Finnish cases on data protection and commercial freedom

Case study 1: Verkkokauppa.com Background

Verkkokauppa.com (aptly translating to “onlineshop.com”) is a prominent Finnish e-commerce and retail company listed on Nasdaq Helsinki. Operating a major online retail store alongside physical store locations in Finland the company focuses on consumer electronics, home appliances and related services.

The Finnish Data Protection Ombudsman (“SA”) initiated an inquiry on April 13, 2021, following a complaint regarding a mandatory requirement to register a user account on the company’s portal in order to complete a one-off purchase – preventing the complainant, who declined to register, from making a purchase. The inquiry encom-

passed two main issues: first, the mandatory registration requirement for all online purchases, and second, the practice of retaining customer data “for as long as necessary.”

To the company, these two issues were interlinked: it had made a deliberate commercial decision to adopt an online sales model requiring user account registration, under which personal data was retained for the duration of the underlying customer contract that was in force for the time being and in practice until the customer requested account deletion. In its submissions to the SA, the company stated that the purpose of maintaining continuous user accounts was to provide customers with historical purchase records, warranty tracking, and ongoing service support. The company argued that under the freedom to conduct a business, it had the right to offer a bundled service package requiring user registration to fulfill the contract’s purpose, asserting that “*data protection regulation does not explicitly or implicitly require an undertaking to offer potential customers the option to purchase from an online store without registration*”.

The SA decision

On March 6, 2024, the Data Protection Ombudsman’s Sanctions Board (Tietosuojavaltuutetun seuraamuskollegio) issued decision TSV/26/2020⁷, issuing a formal reprimand under Article 58(2)(b) GDPR and imposing an administrative fine of €856,000 on Verkkokauppa.com Oyj. Additionally, under Article 58(2)(d) GDPR, the supervisory authority issued an order mandating the company to bring its data processing operations into compliance with data protection laws. Specifically, Verkkokaup-

4 *Meta Platforms Inc and Others v Bundeskartellamt* (C-252/21) EU:C:2023:537; Irish Data Protection Commission, decision of 31 December 2022 on Meta Platforms Ireland Ltd’s Facebook service, as affirmed by EDPB, Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR)

5 *Koninklijke Nederlandse Lawn Tennis-bond v Autoriteit Persoonsgegevens* (C-621/22), judgment of 4 October 2024, confirming that a purely commercial interest is not categorically excluded from being a legitimate interest under art. 6(1)(f) GDPR.

6 EDPB, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms (adopted 17 April 2024)

7 tietosuojavaltuutettu (Finland), Decision TSV/26/2020 (6 March 2024) <<https://www.finlex.fi/fi/viranomaiset/tietosuojavaltuutettu/2024/2163>>>

pa.com was ordered to define a compliant retention period for customer personal data, cease its practice of requiring mandatory account creation for one-off online purchases, and delete or anonymize all personal data older than the defined retention period without undue delay.

The Data Protection Ombudsman (“SA”) decision involves two primary legal issues, both touching upon the company’s defense based on the freedom to conduct a business:

First, the SA outlines that the case concerns the legality of personal data retention as a whole, which it combines with the commercial choice of having a persistent user account and contract upon. Throughout the decision SA argumentation (and final decision on fines) heavily relies on general principle of storage limitation and the fact that in practice this commercial choice could result in retention period of decades.⁸ The conclusion of a breach is essentially derived from the point that the company had not in fact (due to choice of contracts valid under further notice) determined a storage period (which then could not have been informed). This argumentation is easy to swallow as relying on the primacy of Article 5(1)(e) GDPR (storage limitation) but still essentially establishing that while Article 6(1)(b) GDPR contract processing can be lawful - its proportionality assessment is essentially done on assessing the processing against ultimate fulfillment of Article 5 GDPR general principles.

Second, and more interestingly, the SA assessed the legality (i.e. correct applicability of Art. 6(1)(b)

GDPR) of requiring users to register for one-off online purchases at length as separate from retention time issue.⁹ In its assessment, SA outlined that “*the personal data processing was done in the interest of business*” and “*the main object of the contract could be done without personal data processing*”.¹⁰ The SA’s analysis then relied on an analysis¹¹ of the company’s disclaimed purpose (fulfillment of online purchase) against its assessment of what was possible and necessary for that purpose.

This is a challenging interpretation as the SA relied on the standard of “objectively necessary”, as flowing from EDPB dispute mechanism decision,¹² and standard-setting Bundeskartellamt CJEU-decision¹³ which set out a strict fundamentality test on Art. 6(1)(b) GDPR which was used to distinguish targeted advertising as not belonging to the scope of social media’s contract legal basis (and as provided by unrelated third parties). However in this case, the argumentation leads to a point where not just a partial commercial activity but the whole framework of requiring registration would be prohibited as being *possible* to conduct in a more limited manner, and thus not fulfilling the legality requirement of Article

5(1)(a) GDPR. The SA decision underlines the issues concerning application of this objective necessity standard as

- a. the objectivity can essentially disregard the original intention and goal sought by the company in establishing a service containing multiple different processing activities; and
- b. result in the wholesale infringement of the processing if one of these processing activities can be distinguished as not strictly necessary for a narrow goal of the contract.

Following strictly *this* interpretation of objective necessity – as one without necessarily taking into account the service as a whole under Article 6(1)(b) GDPR assessment - the use of contract-based data processing would essentially need to identify the simplest form of service performance (for which there is no explicit legal standard for determination) and compare each personal data processing against that purpose.

Administrative court decisions and final analysis

As typical of GDPR fines of sufficient size, the company appealed the decision to the administrative court. The administrative court decision¹⁴ (Dnro 2096/03.04.04.04.01/2024) is rather uneventful¹⁵ in its content and basically repeats assessment in the SA decision focusing on the issue with data minimisation and retention

⁸ relying on e.g. European Data Protection Board (EDPB), ‘Guidelines 4/2019 on Article 25 Data Protection by Design and by Default’ (Version 2.0, adopted 20 October 2020).

⁹

¹⁰ Paras 64-65 of the decision

¹¹ See, for example, the justification provided in European Data Protection Board (EDPB), ‘Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects’ (Version 2.0, adopted 8 October 2019).

¹² European Data Protection Board (EDPB), ‘Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR)’ (adopted 5 December 2022).

¹³ Case C-252/21 *Meta Platforms Inc. and Others v Bundeskartellamt* ECLI:EU:C:2023:537.

¹⁴ Helsingin hallinto-oikeus (Helsinki administrative court) Decision 2096/03.04.04.04.01/2024

¹⁵ There is a salient procedural question for another text of at which part of the SA consultancy becomes and infringement procedure requiring sufficient hearings, and before which the company should be given possibility to rectify its infringement.

times – and upholding the fine while lowering its amount (792 639 EUR). While the SA decision (or the attached sanctions board decision) does not clearly distinguish whether the fine is issued on the basis of merely infringement of minimisation and retention times as resulting from commercial decision to require registration, or as that mandatory registration forming a partial basis of infringement independently, the administrative court’s decision streamlines this by assessing the fine’s validity and amount solely on the context of retention times (as a result of commercial decision). The distinction is quite material as then the administrative court, nor the supreme administrative court in the following appeal¹⁶, did not assess the legality of mandatory registrations *an sich* similarly as in the SA decision. On the contrary, both the administrative court and supreme administrative court separately stated that the SA decision should not be interpreted as ruling mandatory registration as unlawful, but rather only on its resulting data retention.¹⁷ While I somewhat disagree on this assess-



Illustrasjon: Coulorbox

ment of the SA decision¹⁸ this assessment results in an interesting what-if:

1. As the only issue by which the courts upheld the fine concerned the failure to establish and communicate retention times¹⁹ – this assumes that the issue of mandatory registrations and its legal basis did not act as a basis of the fine;
2. Then the interesting question is whether the fine would have been upheld (or even issued at all) if the retention time infringement had been lesser or non-existent. In other words, it seems that the company could justify its mandatory registration with freedom of commerce.

Contrary to this recognition, the SA position against mandatory registrations has also been since enshrined in the EDPB Recommendation 2/2025 where it is still maintained

18 Paras 62-67 clearly outline the argument for missing legal basis of mandatory requirements - same sentiment which the EDPB reiterated in its following guidance Recommendations 2/2025 on the legal basis for requiring the creation of user accounts on e-commerce websites

19 Also important to note that the administrative court lessened the amount of the fine following the company’s efforts to already rectify the infringement

that “*necessity test required [...] is unlikely to be met*”.

Scenario 2: Posti (OmaPosti)

Background

In many ways similar to the [Verkkokauppa.com](#) case discussed above, another case concerning freedom of commerce defence concerns online services and its necessity test. Continuing on the theme of aptly named companies and services, Finnish postal company Posti Jakelu Oy was issued a €2.4 million fine for their “OmaPosti-postilaatikko”-service (again aptly named eng: “OwnPost-postbox”) bundling together multiple different online services with registration to just one.²⁰ This OmaPosti-service combines together multiple different online services, such as postal address changes, parcel tracking, rerouting mail and e-post which multiple Finnish authorities use by default. Posti’s service design maintained that in order to use the online services you had to a) register to the service, and b) by default take the service into use in full. Meaning that if you wanted to conduct an address change, this automatically opened up an e-post inbox for you.

On July 7, 2020, the Finnish SA opened an investigation following customer complaints regarding the mandatory activation of the digital inbox. The inquiry addressed two main issues: transparency shortcomings during account onboarding, and the mandatory bundling of all OmaPosti service features upon registration. The fine imposed by the SA was based specifically on the mandatory service bundling, while the transparency failures received a formal reprimand.

SA decision

Similarly to the case in [Verkkokauppa.com](#) above, Posti claimed

16 *Korkein hallinto-oikeus* (Supreme Administrative Court of Finland), Decision KHO 2026/1604

17 KHO 12.6.2026/1604 para 10 “According to the Administrative Court’s decision, it does not appear from the Data Protection Ombudsman’s decision that the company’s practice – requiring customer registration to make a single purchase in the online store – was considered in itself to be in violation of the General Data Protection Regulation or other data protection regulations. Therefore, the Administrative Court has assessed the legality of the company’s practice only insofar as whether it has resulted in an unlawful situation regarding the retention period of personal data.”

20 Tietosuojavaltuutettu (Finland), Decision of 13 November 2024 (Finlex 2024/2363).

throughout the consultancy that it had the right under freedom of commerce to design its service offering how it sees fit and combine different functionalities in its service as one unified service and offer that by default to all its users without possibility to opt-out of single functionalities. Similarly to Verkkokauppa.com Posti argued that applicable data protection regulation lacks general principles which would determine which specific parts of a service are allowed to function under the same legal basis and which would need to be distinguished - and thus neither the SA would have the authority to determine this.

The SA relied generally on the exact same legal sources and argumentation²¹ as in the case concerning Verkkokauppa.com (concerning legal basis of mandatory registration) and maintained that specifically the e-post inbox (OmaPosti-postilaatikko) can be separated from the performance of post rerouting and cannot thus be considered objectively necessary for the performance of contract which the user might seek by entering into a contract. The personal data processing related to e-post inbox was then outside of the contractual legal basis and its data processing unlawful.

Due to Posti relying multiple times on freedom of commerce defence, the SA addressed this shortly stating that the decision is not about the evaluation of a specific business practice, or a part of a service, but rather on whether a data controller has a valid legal basis for its processing. A legal chicken-and-egg.

Administrative court decision and final analysis

Following Posti's appeal of the SA decision, on 3 November 2025, the Helsinki administrative court gave a shock decision on the matter – the €2.4 million fine was overturned in its entirety.²² The court's decision addressed both streams of inquiry and validated the first concerning lack of sufficient information to the inbound users of the OmaPosti-service – however the fine was solely based on the invalidity of Posti's contractual legal basis in which the court disagreed with the SA.

In a well argued decision the court compared the Posti-processing with the processing and standard set out in Bundeskartellamt-decision: whereas the personalisation of marketing content on a social media platform cannot be justified as necessary or otherwise “important” to the processing which the underlying contract concerns (even if it would be “useful” for the user) because the user can be offered the same service in an equivalent manner without that processing and importantly without sharing the personal data to third parties for this purpose. The court recognised that the situation with Posti differs from Meta's advertising personalisation in a material manner as OmaPosti was solely Posti's own service and the processing was result of its own commercial choices and not that of third parties. In reference to EDPB Guidelines 2/2019 the court recognised that OmaPosti-service had internal service justifications to bundling the services together instead of solely the company's ancillary commercial gain or resulting in additional personal data processing unnecessary for that service-purpose. Bundling the e-post inbox to the other services was justified in

the same legal basis and contractual freedom - the fine was overturned.²³

From an immediate viewpoint it might seem that the [Verkkokauppa.com](https://www.verkkokauppa.com) and Posti -cases might have very different building blocks as one fine maintained and the other overturned, but when we disregard Posti's information obligation failures and [Verkkokauppa.com](https://www.verkkokauppa.com)'s lack of retention times, the cases have very similar grounding. In both cases the company acted on the basis of Article 6(1) (b) GDPR, bundling multiple service functionalities together, and were challenged on the necessity of some of those functionalities. In both cases the administrative courts confirmed (against the SA) that the controller had the commercial freedom to determine the scope of their data processing on contractual basis (provided that the functionality was necessary).

From this point of view, it would seem that the objectivity and necessity standard set out in Bundeskartellamt and relevant EDPB guidelines gives more leeway to commercial actors to offer service packages on the objective they have contractually defined, as long as the parties to the processing are the same and it contributes to the service's functionality instead of just independent commercial interest.

In conclusion:

Jurisprudence addressing the intersection of contractual necessity and commercial discretion under the GDPR continues to evolve. Recent judicial decisions in Finland indicate a balanced approach that protects consumer data rights while respecting controllers' constitutional freedom to conduct a business.

Jalmari Männistö, Secretary of Finnish IT-law association (IT-oikeuden Yhdistys ry), Legal counsel (technology & contracting) - Epassi Group.

²¹ To be clear the SA employed a more deep analysis of CJEU case C-252/21 para 98 wherein it relied on the controller's obligation to be able to show why each processing is necessary for the main purpose of the contract.

²² Helsingin hallinto-oikeus (Helsinki administrative court) 2096/03.04.04.04.01/2024

²³ For clarity, the matter is still pending on the Finnish Supreme Administrative Court

Innsynsrettens rekkevidde – logginnsyn og identitetsinformasjon

Av Hanne P. Gulbrandsen

1. Innledning

Personopplysninger behandles i dag nesten utelukkende elektronisk. For å sikre lovlig og forsvarlig tilgang til systemene, krever personvernforordningen (GDPR) artikkel 32 at den behandlingsansvarlige iverksetter tekniske og organisatoriske sikkerhetstiltak. Logging av oppslag og andre aktiviteter er et slikt tiltak. Loggene kan for eksempel inneholde informasjon om hvilken aktivitet som er gjort, dato, tidspunkt, formål og identiteten til den som gjennomførte aktiviteten.

Aktivitetslogger er et viktig verktøy ved mistanke om uautorisert tilgang. Loggene gjør det mulig å avdekke hvem som har hatt tilgang på et gitt tidspunkt, og gir slik et godt utgangspunkt for å vurdere om det forelå tjenstlig behov. For den registrerte kan logginnsyn derfor bidra til å oppklare om noen uvedkommende har vært inne i opplysningene.

Når arbeidsgiver innfører detaljerte logger og gjennomgår disse, er dette et utslag av plikten til å sikre forsvarlig behandling, og hensynet til de registrerte vil som hovedregel veie tyngre enn de ansattes interesse i å ikke bli registrert og kontrollert. Men kan det samme hensynet begrunne at den registrerte via logginnsyn alltid skal få kunnskap om identiteten til de ansatte, eller vil ansattes rett til personvern i noen tilfeller kunne tillegges mer vekt?

Dette spenningsfeltet har vært behandlet av både EU-domstolen og norsk Høyesterett.

I artikkelen vil jeg gjennomgå gjeldende rett med vekt på EU-domstolens avgjørelse i Pankki S

(C-579/21), Høyesteretts dom HR-2026-372-A og sektorspesifikk regulering i helsesektoren. Avslutningsvis drøftes om fullt identitetsinnsyn i tilgangslogger som standardpraksis kan ha rettslig forankring, og alternative mekanismer som kan ivareta den registrertes kontrollbehov.¹

2. De rettslige rammene

2.1. Krav til logger som sikkerhetstiltak

GDPR artikkel 32 pålegger behandlingsansvarlige og databehandlere å gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå tilpasset risikoen. Kravet skal blant annet forebygge uautorisert tilgang til personopplysninger. Logging er et sentralt tiltak under denne bestemmelsen.

EDPB beskriver aktivitets- og tilgangslogger som et verktøy for å spore hvem som har hatt tilgang til personopplysninger, gjennom oppslag, lesing, utskrift, kopiering, endring eller sletting, og for å kontrollere at opplysningene ikke har vært gjenstand for uautorisert tilgang.² Slike logger kan inneholde personopplysninger om ulike registrerte. De dokumenterer at den registrertes opplysninger har vært gjenstand for en bestemt behandlingsaktivitet. De inneholder også opplysninger om den ansatte som utfører aktiviteten som deres identitet, organisatoriske tilhørighet og eventuelt rolle eller



Hanne P. Gulbrandsen

autorisasjonsnivå. I tillegg registreres dato og tidspunkt for oppslaget, hvilken handling som ble utført (lesing, utskrift, kopiering, endring eller sletting), og begrunnelsen for tilgangen dersom dette registreres.

I norsk rett er kravet til logging tydeliggjort i flere lover. Pasientjournalloven § 22 pålegger både den dataansvarlige og databehandleren å sørge for tilgangsstyring, logging og etterfølgende kontroll, med uttrykkelig henvisning til GDPR artikkel 32. Tilsvarende følger av helseregisterloven § 21.

Forarbeidene til politiregisterloven begrunner behovet for logging både i muligheten til å forebygge og til å kontrollere regelverksbrudd og til å «sanksjonere urettmessig bruk». Datatilsynet fremhevet i sin høringsuttalelse i forkant av politiregisterlovens vedtakelse, at logging er viktig for kontrollen med de registrertes personvern, men samtidig at utstrakt bruk kan utgjøre en trussel mot polititjenestepersonells eget personvern. Loggene bør derfor kun brukes til å kontrollere om krav

- 1 Det avgrenses mot innsynsrett som ikke er regulert i GDPR, som partsinnsyn etter forvaltningsloven.
- 2 EDPB, Guidelines 01/2022 on data subject rights – Right of access, Version 2.1, vedtatt 28. mars 2023.

til sikkerhet og tilgang overholdes.³ Dette underbygger at loggkontroll primært er en intern funksjon i kraft av rollen som behandlingsansvarlig/dataansvarlig.

2.2 Retten til innsyn

GDPR artikkel 15 gir den registrerte rett til innsyn i egne personopplysninger. Fortalepunkt 39 fremhever at behandling bør være transparent overfor de registrerte.

Innsynsretten omfatter også en rekke tilleggsopplysninger. Etter artikkel 15 nr. 1 bokstav c har den registrerte rett til informasjon om «mottakerne eller kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til». Begrepet «mottaker» er definert i artikkel 4 nr. 9 som en fysisk eller juridisk person, offentlig myndighet, institusjon eller annet organ som personopplysninger utleveres til, uavhengig av om det dreier seg om en tredjepart. I konteksten av logginnsyn oppstår dermed spørsmålet om ansatte som har gjort oppslag i, eller på annen måte konsultert, en registrerts personopplysninger er «mottakere» i denne forstand.

Den registrerte har også rett til kopi av personopplysningene som behandles, jf. GDPR artikkel 15 nr. 3. Kopiretten er imidlertid begrenset av artikkel 15 nr. 4, som fastslår at retten til kopi ikke skal ha negativ innvirkning på andres rettigheter og friheter⁴. Denne reguleringen viser at lovgiver har lagt til grunn at også andre enn den som ber om innsyn kan ha behov for beskyttelse. Det er

viktig å merke seg at begrensningen i artikkel 15 nr. 4 kun gjelder retten til å få en kopi, og ikke retten til informasjon etter artikkel 15 nr. 1 bokstav a) til h) som sådan.

Begrensningen i GDPR artikkel 15 nr. 4 får ikke automatisk anvendelse. Ifølge EDPB kreves det en konkret vurdering av om andres rettigheter faktisk berøres av at en kopi utleveres, en avveining mellom de kolliderende interessene, og en vurdering av om konflikten kan løses med mindre inngripende tiltak, som sladding fremfor full avvisning av innsynsbegjæringen.⁵ EDPB understreker at generelle antakelser om at ansattes rettigheter kan bli påvirket ikke er tilstrekkelig. Virksomheten må konkret begrunne hvorfor ansattes rettigheter og friheter vil bli negativt påvirket dersom innsynsretten skal begrenses. Hovedregelen er at mest mulig innsyn skal gis, for eksempel ved sladding av identifiserende opplysninger fremfor å nekte innsyn helt.

Fortalepunkt 63 bekrefter dette utgangspunktet der det fremgår at «...[a]lle registrerte bør derfor ha rett til å kjenne til og bli informert om formålene med behandlingen av personopplysninger, om mulig om perioden som personopplysningene behandles i, hvem mottakerne av personopplysningene er...». Samtidig presiseres det at «denne retten bør ikke ha negativ innvirkning på andres rettigheter eller friheter, berunder forretningshemmeligheter eller immaterialretten, særlig opphavsretten som programvaren er beskyttet av. Disse hensynene bør imidlertid ikke føre til at den registrerte nektes innsyn i alle opplysninger. Dersom den behandlingsansvarlige behandler en stor mengde opplysninger om den registrerte, bør den behandlingsansvarlige for informasjonen gis, kunne anmode om at den registrerte presiserer hvilke opplysninger eller behandlingsaktiviteter anmodningen gjelder».

2.3. Når innsyn er i strid med åpenbare og grunnleggende interesser

Personopplysningsloven § 16 første ledd bokstav f gjør unntak fra retten til informasjon og innsyn for opplysninger som det vil være i strid med «åpenbare og grunnleggende private eller offentlige interesser» å informere om. I Prop. 56 LS (2017–2018) punkt 10.3.4 beskriver departementet bestemmelsen som en videreføring av personopplysningsloven 2000 § 23 første ledd bokstav f, og viser til at den fungerer som en sikkerhetsventil for interesser som ikke dekkes av de øvrige unntakene. Departementet legger samtidig til grunn at unntaket må anvendes innenfor rammene av GDPR artikkel 23, slik at begrensningen må respektere det vesentlige innholdet i de grunnleggende rettighetene og være et nødvendig og forholdsmessig tiltak i et demokratisk samfunn. Formuleringen «åpenbare og grunnleggende» tilsier derfor at ikke enhver privat eller offentlig interesse er tilstrekkelig; det må påvises tungtveiende hensyn i den konkrete saken.

Bestemmelsen har et annet nedslagsfelt enn GDPR artikkel 15 nr. 4. Mens artikkel 15 nr. 4 kun begrenser kopiretten, rammer personopplysningsloven § 16 informasjonsretten etter artikkel 15 nr. 1 som sådan. Terskelen er imidlertid høyere enn etter artikkel 15 nr. 4, og bestemmelsen gir et nasjonalt hjemmelsgrunnlag for å nekte innsyn når tungtveiende mothensyn foreligger. Avveiningen må i begge tilfeller være konkret, og hensynet til den ansattes personvern og sikkerhet må vurderes mot den registrertes interesse i kontroll og etterprøvbarehet.

2.4. EU-domstolens praksis

2.4.1. Innledning

Spørsmålet om innsynsrettens rekkevidde overfor mottakere og interne ansatte har vært gjenstand for flere avgjørelser fra EU-domstolen.

3 Ot.prp. nr. 108 (2008–2009) Om lov om behandling av opplysninger i politiet og påtalemyndigheten (politi-registerloven), punkt 10.3.3, s. 116–117.

4 For en generell fremstilling av innsynsretten og mottakerbegrepet, se Skullerud m.fl., Personvernforordningen (GDPR) – Kommentartutgave, Juridika (løpende revidert), kommentarer til artikkel 15 og artikkel 4 nr. 9.

5 Guidelines 01/2022 on data subject rights - Right of access, Version 2.1, Adopted on 28 March 2023

2.4.2. Österreichische Post (C-154/21, dom 12. januar 2023)

Saken gjaldt en østerriksk borger, RW, som ba postoperatøren Österreichische Post om innsyn etter GDPR artikkel 15 nr. 1 bokstav c i hvem som hadde mottatt hans personopplysninger. Postoperatøren hadde brukt opplysningene til markedsføring og videresendt dem til tredjeparter, blant andre annonsører, IT-selskaper og politiske partier. Innsynsbegjæringen ble besvart med kun kategorier av mottakere, uten å oppgi konkrete navn.

Domstolen kom til at artikkel 15 nr. 1 bokstav c i utgangspunktet gir den registrerte rett til å få oppgitt identiteten til de konkrete mottakerne som personopplysninger faktisk er utlevert til, og ikke bare kategorier av mottakere. Bare slik kan den registrerte gjøre sine rettigheter gjeldende overfor disse mottakerne. Det klare utgangspunktet etter denne avgjørelsen er at innsynsretten omfatter retten til å få oppgitt de konkrete mottakernes identitet. Om interne ansatte er «mottakere» etter artikkel 15 nr. 1 bokstav c var imidlertid ikke omfattet av avgjørelsen.

2.4.3. Pankki S (C-579/21, dom 22. juni 2023)

Saken gjaldt J.M., som var både kunde og ansatt i den finske banken Suur-Savon Osuuspankki (Pankki S). J.M. oppdaget i 2014 at hans kundeopplysninger hadde vært gjenstand for interne oppslag i perioden november til desember 2013. Etter å ha blitt oppsagt ba han om innsyn, herunder identiteten til de ansatte som hadde slått opp i hans data, de nøyaktige datoene for oppslagene og formålet med behandlingen. Innsynsbegjæringen ble opprettholdt etter at GDPR trådte i kraft 25. mai 2018, og saken ble deretter behandlet etter artikkel 15. Banken nektet å utlevere de ansattes identitet og begrunnet dette med at innsynsretten ikke omfatter loggdata om hvilke ansatte som har hatt tilgang. Det finske datatilsynet av-

viste J.M.s klage, og saken ble forelagt EU-domstolen.

EU-domstolen fastslo at ansatte som behandler personopplysninger «under den behandlingsansvarliges myndighet og i samsvar med instruks» ikke er «mottakere» etter artikkel 15 nr. 1 bokstav c⁶, og at bestemmelsen som hovedregel ikke gir rett til å få oppgitt identiteten til ansatte som har gjort oppslag. Domstolen slo samtidig fast at loggopplysninger om oppslag i den registrertes personopplysninger, herunder datoer og formål, er informasjon den registrerte har rett på etter artikkel 15 nr. 1.

Domstolen åpner likevel for at ansattes identitet kan måtte utleveres dersom opplysningen er nødvendig («essential») for at den registrerte effektivt skal kunne utøve sine rettigheter etter GDPR. Unntaket forutsetter etter sin ordlyd en konkret vurdering i den enkelte sak, der de ansattes rettigheter og friheter veies opp mot den registrertes behov. Begrunnelsen er at identiteten i visse tilfeller kan være avgjørende for at den registrerte skal kunne vurdere om behandlingen var lovlig.

Rettspraksisen etter Pankki S er presisert i en nyere avgjørelse. I WS v. European Commission⁷ slo EU-retten fast at det ikke kan utledes av Pankki S at GDPR artikkel 15 krever at behandlingsansvarlige etablerer en loggingsmekanisme som identifiserer ansatte som har konsultert den registrertes personopplysninger. Avgjørelsen gjentar at der en slik logg faktisk eksisterer og inneholder ansattes identitet, må det vurderes konkret om den registrerte har rett til denne informasjonen basert på nødvendighetskriteriet fra Pankki S.

6 EU-domstolen, sak C-579/21, Pankki S, dom 22. juni 2023, ECLI:EU:C:2023:501.

7 Retten (General Court) T-318/24 og T-362/24, WS v. European Commission, dom 3. desember 2025, ECLI:EU:T:2025:1052.

2.5. Norsk rettspraksis og et knippe eksempler fra særlovgivningen

2.5.1. Innledning

I norsk rett kan det se ut til at spørsmålet om logginnsyn omfatter identiteten til ansatte har fått en særegen utvikling. Stortinget har slått fast at retten til innsyn i egen logg skal være et bærende prinsipp for større offentlige og private registre. På helseområdet har lovgiver gått lenger enn GDPR og uttrykkelig lovfestet at innsynsretten også omfatter identiteten til den som har hatt tilgang til pasientopplysninger.

2.5.2. Stortingets prinsipputtalelse om logginnsyn

Under Stortingets behandling av EUs datalagringsdirektiv uttalte et flertall i Innst. 275 L (2010–2011), punkt 12, at «et grunnleggende prinsipp er at enhver har rett til innsyn i hvem som får tilgang til opplysninger om en selv», og at «plikten til logging og retten til innsyn i egen logg skal være det bærende prinsipp for alle større offentlige og private registre». Uttalelsen må leses i kontekst. Den inngikk i avtalen mellom Arbeiderpartiet og Høyre om innføring av datalagringsdirektivet, der logging og logginnsyn ble fremhevet som kompenserende personverntiltak for den utvidede lagringsplikten. Spenningsforholdet mellom den registrertes innsynsrett og behovet for å ivareta personvernet til den som er identifisert i loggen ble ikke drøftet.⁸ Stortingsflertallet forutsatte videre at det i stortingsmeldingen om personvern skulle drøftes «avgrensninger som bør gjøres i loggplikten, innsynsretten, omfanget av innsynet i det enkelte forhold og framdriften i arbeidet med å virkeliggjøre prinsippet». Prinsippet

8 Innst. 275 L (2010–2011) Innstilling fra transport- og kommunikasjonskomiteen om endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett), punkt 12 «Styrking av det generelle personvernet».

ser likevel ut til å ha fått betydning som normativ målsetting i norsk personvernpolitikk, og særlig i helsesektoren der det er operasjonalisert gjennom uttrykkelig lovfesting av innsynsrett i logger.

2.5.3. Særregulering av innsynsretten

2.5.3.1. Helsesektoren

I helsesektoren er det særskilt regulert at innsynsretten også omfatter informasjon om hvem som har hatt tilgang til pasientopplysninger. Den strengere reguleringen har en klar begrunnelse. Et sentralt formål er avdekking av ulovlig snoking, og det fremgår av forarbeidene at departementet mener at de grovere tilfellene av illegitime oppslag ofte er knyttet til nære relasjoner, som familie- og nabokonflikter, sosial kontroll, barnefordelingssaker, samlivsbrudd og stalking. Slike oppslag avdekkes ofte nettopp av den registrerte selv gjennom logginnsyn, ved at vedkommende gjenkjenner hvem som har fått opplysningene tilgjengeliggjort.⁹

Helseregisterloven § 24 gir innsynsrett etter GDPR artikkel 13–15, men fastslår i tillegg at den registrerte «også [har] rett til innsyn i hvem som har hatt tilgang til eller fått utlevert helseopplysninger knyttet til den registrertes navn eller fødselsnummer». Bestemmelsen går dermed lenger enn det som følger av GDPR artikkel 15 alene.

Pasientjournalloven § 18 slår fast at pasienten eller brukeren har rett til informasjon og innsyn etter pasient- og brukerrettighetsloven og GDPR artiklene 13 og 15. Det er videre presisert i pasientjournalloven § 22a at innsynsretten omfatter blant annet «...identiteten og den organisatoriske tilhørigheten til den som får helseopplysningene».

2.5.3.2. Politiet

Etter politiregisterloven § 49 har den registrerte utenfor den enkelte straffesak rett til å få opplyst hvilke opplysninger som er registrert, og hvorvidt opplysninger er utlevert, til hvem og hvilke opplysninger det dreier seg om. Innsyn kan nektes av hensyn til blant annet kriminalitetsbekjempelse, nasjonal og offentlig sikkerhet, eller vern av andre personer. Forarbeidene viser at departementet la opp til utvidet innsynsrett, men med vidtgående unntaksmuligheter av hensyn til politiets virksomhet.

2.5.4. Norsk rettspraksis

Høyesteretts dom av 13. februar 2026, *HR-2026-372-A*, gjelder retten til å vite hvem som har ført et journalnotat i en pasientjournal, altså avgrenset identitetsinformasjon knyttet til innholdet i den registrertes journal. Saken hadde sin bakgrunn i at en familie ble gjenstand for en bekymringsmelding til barnevernstjenesten på grunnlag av et journalnotat ved den lokale legevakten. Familien ba om innsyn i journalen, herunder hvem som hadde skrevet notatet. Kommunen avslo. Sivilombudet anførte at retten til innsyn i pasientjournal også omfatter retten til å vite hvem som har skrevet det aktuelle journalnotatet, og at eventuelle unntak må begrunnes i personopplysningsloven § 16.

Høyesterett mente at GDPR artikkel 15 nr. 1 bokstav g, som ved indirekte innsamling gir rett til «all tilgjengelig informasjon» om opplysningenes opprinnelse, var «nærliggende» å forstå slik at det kan omfatte informasjon om hvem som har skrevet den aktuelle teksten. Høyesterett la vekt på at helsepersonelloven § 40 annet ledd fastslår at det skal fremgå hvem som har ført opplysningene i journalen, og konkluderte med at fullt navn i utgangspunktet skal fremgå. Selv om initialer kan brukes av praktiske grunner, må innsyn praktiseres slik at pasienten ved behov får opplyst hvem som har ført journalen.

Dommen legger betydelig vekt på at et av formålene med pasientjournalen er at pasienten skal kunne utøve kontroll og ivareta sine rettigheter, herunder vurdere om helsehjelpen er forsvarlig. Førstvoterende viser til Pankki S, men mener at avveiningen av personverninteresser som der ble lagt til grunn ikke kan være til hinder for at det legges vesentlig vekt på pasientens interesse i å få vite hvem som har skrevet notatet. Førstvoterende fremhever at dette uansett må være en del av vurderingen etter personopplysningsloven § 16 bokstav f, som åpner for unntak der det «vil være i strid med åpenbare og grunnleggende private eller offentlige interesser å informere om» opplysningene.

I den konkrete saken fant Høyesterett at belastningene for sykepleieren, herunder plager og sykmeldinger, ikke var tilstrekkelige til å nekte innsyn. Formålet med innsynskravet, å vurdere forsvarlig behandling, habilitet og faglig kompetanse, lå innenfor de grunnleggende hensynene bak innsynsretten. Saken gjaldt identiteten til den som hadde forfattet et konkret journalnotat, altså en avgrenset og innholdsnaer opplysning som den registrerte trengte for å vurdere helsehjelpen. Overføringsverdien til spørsmålet om direkte utlevering av samtlige ansattes identitet fra en fullstendig tilgangsslogg, der flertallet av de ansatte kan ha konsultert opplysningene som ledd i ordinært tjenstlig arbeid, anses begrenset.

3. Identitetsopplysninger skal ikke utleveres automatisk ved logginnsyn

Informasjon om identiteten til en ansatt som har hatt tilgang til en registrerts personopplysninger er ikke nevnt som en av informasjonstypene den registrerte har krav på etter GDPR artikkel 15 nr. 1. Utgangspunktet etter Pankki S er at den registrerte har rett til å vite at oppslag er foretatt, og til informasjon om dato, formål og organisato-

⁹ Prop. 154 L. (2024–2025) Endringer i helsepersonelloven og pasientjournalloven mv. (taushetsplikt og tilgjengeliggjøring av pasientopplysninger), punkt 4.3.7 «Tilgangsstyring, logg og etterfølgende kontroll».

risk tilhørighet, men ikke automatisk rett til informasjon om den ansattes identitet. WS v. European Commission bekrefter at GDPR heller ikke pålegger behandlingsansvarlige å opprette identifiserende logger. Regelverket etablerer med andre ord ingen presumsjon for at kunnskap om identitet er omfattet av logginnsyn. Det at lovgiver har funnet det nødvendig å vedta egne bestemmelser om identitetsinnsyn i helseregisterloven § 24 og pasientjournalloven § 22a, er videre et sterkt argument som taler mot at identitetsopplysninger alltid skal omfattes ved logginnsyn. Dersom GDPR artikkel 15 allerede etablerte en slik rett, ville disse bestemmelsene vært overflødige.

Høyesterett tolker i *HR-2026-372-A* informasjon om den ansattes identitet inn i punktet «all tilgjengelig informasjon» om opplysningenes opprinnelse, mens EU-domstolen åpner i *Pankki S* for at ansattes identitet kan måtte utleveres kun når dette er «nødvendig» for at den registrerte effektivt skal kunne utøve sine rettigheter. Dette forutsetter at det må gjøres en konkret vurdering. Dersom man gjennom den konkrete vurderingen møter på andre personer hvis rettigheter og friheter bør beskyttes, må det hensyntas. Dette må gjelde uavhengig av om man anvender kopiretten eller ikke, gitt at utgangspunktet er at informasjon om ansattes identitet i utgangspunktet ikke er omfattet av innsynsretten etter GDPR artikkel 15.

Nødvendighetskriteriet er trolig oppfylt der den registrerte har en konkret og begrunnet mistanke om at en bestemt person har foretatt et uberettiget oppslag, og der identiteten er nødvendig for å vurdere behandlingens lovlighet eller for å gjøre andre rettigheter gjeldende. Kriteriet er derimot ikke nødvendigvis oppfylt for de deler av loggen som inneholder oppslag fra de mange andre ansatte med dokumentert tjenstlig behov. Dersom innsynskravet ikke er knyttet til noen bestemt uregelmess-

sighet, vil kriteriet neppe være oppfylt. Proporsjonalitetsprinsippet understøtter en slik forståelse. I mange virksomheter kan en tilgangslogg omfatte titalls eller hundrevis av oppslag fra ansatte som har konsultert opplysningene som ledd i ordinært arbeid. Rutinemessig utlevering av samtlige navn vil innebære et inngrep overfor en bred krets av ansatte som på ingen måte har vært gjenstand for den registrertes mistanke.

” Gjennomgangen har vist at å praktisere fullt identitetsinnsyn i tilgangsligger som standard, ikke har rettslig forankring i GDPR artikkel 15.

I sektorer der ansatte er utsatt for trusler og sjikane, slik som barnevern, Nav og kriminalomsorgen, kan utlevering av navn også reise spørsmål om de ansattes sikkerhet.¹⁰ De ansattes personvern bør derfor også vektes tungt og det bør her særlig sees hen til at andres rettigheter og friheter også skal vernes.

Gjennom å innføre en trinnvis innsynsmodell vil den behandlingsansvarlige bedre kunne svare ut den registrertes kontrollbehov og samtidig ivareta de ansattes personvern bedre sammenlignet med full identitetsutlevering som standard.

I en trinnvis innsynsmodell gjøres det en løpende vurdering av nødvendigheten. Innsynsbegjæringen besvares innledningsvis ved at den behandlingsansvarlige gir innsyn i anonymiserte eller pseudonymiserte loggdata. Det vil si dato, tidspunkt, formål, type handling og organisatorisk enhet, men uten at den enkelte ansattes identitet fremgår. Dersom den registrerte på grunnlag av de anonymiserte loggdataene har en konkret og begrunnet mistanke om at et bestemt oppslag var uberettiget,

går vurderingen over i neste trinn. Her må den behandlingsansvarlige ta stilling til om det foreligger et reelt behov for identitetsopplysninger. Vurderingen bør ta hensyn til om mistanken knytter seg til et avgrenset oppslag eller til loggen som helhet, om den registrerte har angitt konkrete holdepunkter for at oppslaget manglet tjenstlig begrunnelse, og om identiteten til en ansatt eller alle ansatte er nødvendig for at den registrerte effektivt skal kunne utøve sine rettigheter etter GDPR. Dersom den behandlingsansvarlige kommer til at informasjon om en eller flere identiteter skal utleveres, bør dette begrenses til det aktuelle oppslaget, og utleveringen bør dokumenteres med en kort begrunnelse.

Den behandlingsansvarlige kan også vurdere å håndtere mistanken gjennom intern oppfølging i stedet for utlevering, gitt at dette gir den registrerte tilstrekkelig informasjon. Arbeidsgivers egen kontrollplikt og tilsynsmyndighetenes kompetanse etter GDPR artiklene 58 og 77 er mekanismer som kan avdekke uregelmessigheter uten at den registrerte selv får tilgang til identifiserende loggdata. En trinnvis tilnærming vil både ivareta hovedregelen om mest mulig innsyn for den registrerte og nødvendighetskriteriet i *Pankki S*, fordi innsyn gis, men identitetsopplysninger utleveres kun der den registrerte har vist at det foreligger et konkret behov.

Gjennomgangen har vist at å praktisere fullt identitetsinnsyn i tilgangsligger som standard, ikke har rettslig forankring i GDPR artikkel 15. Utlevering av den enkelte ansattes identitet forutsetter en konkret nødvendighetsvurdering. Virksomheter som i dag utleverer alle navn som standard, uten en slik vurdering, bør derfor innrette sin praksis etter den rettslige rammen som følger av EU-domstolens praksis og for eksempel tilpasse innsynsrutinene til en trinnvis modell.

Hanne Pernille Gulbrandsen partner og advokat i Deloitte Advokatfirma AS.

¹⁰ Dette oppleves også i helsesektoren.

Finjustering av AI-modeller och AI-system

När en tillhandahållare kan bli leverantör enligt AI-förordningen

Av Emil Piva

Inledning

En verksamhet som rättar ett fel i ett inköpt AI-system kan under vissa förutsättningar ta över den rättsliga roll som den ursprungliga leverantören hade. Det kan framstå som oväntat. Det fel som ändringen var avsedd att rätta har minskat och systemet används fortfarande för samma uppgift, men verksamheten kan ändå behöva uppfylla leverantörens skyldigheter för den ändrade versionen. För att förstå hur detta kan ske behöver några grunddrag i förordningen först hållas isär.¹

” En ändring av modellen kan därför få olika rättslig betydelse beroende på vilket system som modellen används i och vad systemet är avsett att göra.

AI-förordningen reglerar framför allt AI-system, men innehåller också särskilda regler för AI-modeller för allmänna ändamål. En AI-modell kan förenklat beskrivas som resultatet av en träningsprocess. Den bearbetar indata och tar fram utdata, exempelvis en rekommendation. När modellen kombineras med an-

dra delar för en bestämd användning kan den ingå i ett AI-system. Systemet omfattar då även exempelvis regler för in- och utdata, ett gränssnitt och andra funktioner. Samma modell kan byggas in i flera olika system. En ändring av modellen kan därför få olika rättslig betydelse beroende på vilket system som modellen används i och vad systemet är avsett att göra.²

Förordningen skiljer också mellan olika aktörsroller. Den som utvecklar ett AI-system, eller låter utveckla det, och släpper ut systemet på marknaden eller tar det i bruk under eget namn är leverantör (*provider*). Den som använder ett AI-system i sin verksamhet är normalt tillhandahållare (*deployer*). Skillnaden är särskilt betydelsefull för system som förordningen klassificerar som AI-system med hög risk. Det är en rättslig kategori som medför mer långtgående skyldigheter för leverantören. Leverantören av ett sådant system ska bland annat hantera risker, upprätta teknisk dokumentation och säkerställa att kraven på data, mänsklig kontroll, riktighet och robusthet är uppfyllda. Leverantören ska också genomföra en bedömning av överensstämmelse (*conformity assessment*), alltså den process genom



Emil Piva

vilken det visas att systemet uppfyller kraven.³

Det avsedda ändamålet kan avgöra om ett AI-system har hög risk. Bilaga III till AI-förordningen räknar upp användningar som enligt huvudregeln hör till högriskkategorin. Listan omfattar bland annat AI-system som används för att bedöma nödsamtal och prioritera utsändningen av larmtjänster. Artikel 6.3 innehåller ett begränsat undantag för vissa system som visserligen omfattas av bilaga III men som inte medför någon betydande risk för skada på fysiska personers hälsa, säkerhet eller grundläggande rättigheter.⁴

Aktörsrollerna kan förändras under systemets livstid. Artikel 25 reglerar vad som händer när någon annan än den ursprungliga

1 Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens (AI-förordningen), EUT L, 2024/1689, 12.7.2024, artiklarna 3.23, 25.1, 25.2 och 43.4.

2 AI-förordningen, artiklarna 1.2 c, 1.2 e, 3.1 och 3.63. Martin Ebers och Emmanuel Vargas Penagos, 'Upstream, downstream, and in between: navigating the GPAI value chain under EU law', *Information & Communications Technology Law* (2026), s. 3–4, doi: 10.1080/13600834.2026.2624923.

3 AI-förordningen, artiklarna 3.3, 3.4, 3.20, 9–16 och 43.

4 AI-förordningen, artiklarna 6.2 och 6.3 samt bilaga III punkt 5 d.

leverantören ändrar ett system som redan har släppts ut på marknaden eller tagits i bruk. En tillhandahållare kan bli leverantör om den gör en väsentlig ändring av ett befintligt AI-system med hög risk och systemet fortsatt har hög risk. Samma följd kan inträda om tillhandahållaren ändrar det avsedda ändamålet för ett system som inte har klassificerats som högrisk, så att systemet efter ändringen hör till högriskskategorin. Med leverantörsansvar avses i den här artikeln de skyldigheter som följer av leverantörsrollen enligt AI-förordningen. Frågan om civilrättsligt skadeståndsansvar är en annan.⁵

Finjustering (*fine-tuning*) innebär att en redan tränad modell tränas vidare på utvalt material för att påverka hur den utför en uppgift. AI-förordningen nämner finjustering i anslutning till reglerna om modeller för allmänna ändamål, men metoden i sig innebär inte en övergång från en tillhandahållarroll till en leverantörsroll för ett AI-system. På systemnivå beror bedömningen på vad finjusteringen medför. Har den ändrade versionen kvar samma avsedda ändamål? Påverkar ändringen systemets uppfyllelse av högriskkraven? Eller ges systemet i samband med finjusteringen en ny uppgift som gör att det klassificeras som ett AI-system med hög risk? De frågorna kan belysas genom två versioner av samma larmcentralsfall.⁶

Två finjusteringar, två rättsliga vägar

Föreställ dig att en larmcentral använder ett inköpt AI-system som

rekommenderar hur inkommande nödsamtal ska prioriteras. Efter en tids användning upptäcks ett återkommande fel. Korta men brådskande samtal får ibland för låg prioritet. Larmcentralen tränar därför den AI-modell som ingår i systemet vidare på fler granskade samtal för att minska just den felbedömningen.

Finjusteringen ger resultat. Färre brådskande samtal får för låg prioritet. Samtidigt visar testerna att fler samtal än tidigare får en obefogat hög prioritet, en förändring som den ursprungliga dokumentationen inte behandlar. Det kan innebära att larmcentralen går från att vara tillhandahållare till att bli leverantör av den ändrade versionen. Med leverantörsrollen följer ansvaret för att högriskkraven är uppfyllda.⁷

Anta i stället att larmcentralen använder ett inköpt AI-system för att transkribera och sammanfatta samtal. Systemet är inte avsett att vare sig bedöma eller prioritera nödsamtal, och exemplet utgår därför från att det inte har klassificerats som ett AI-system med hög risk. Larmcentralen ändrar samma system genom att finjustera modellen och ger samtidigt systemet ett nytt avsett ändamål. Den ändrade systemversionen ska rekommendera hur nödsamtal prioriteras. Larmcentralen kan därför komma att bli leverantör genom en annan bestämmelse än i det första fallet.

De två fallen utgår från samma tekniska metod, men aktualiserar olika bestämmelser. I det första är frågan om ett befintligt AI-system med hög risk har ändrats väsentligt enligt artikel 25.1 b. I det andra har systemets avsedda ändamål ändrats så att det blir ett AI-system med hög risk enligt artikel 25.1 c. Vilken bestämmelse som ska tillämpas av-

görs därför av hur systemet har förändrats.⁸

Från modelländring till systembedömning

Det som ändras under träningen är modellens parametrar, de numeriska värden som påverkar hur modellen bearbetar indata och tar fram resultat. Vid en fullständig finjustering uppdateras samtliga parametrar. Vid andra former av finjustering uppdateras bara en mindre del av parametrarna eller särskilda tillägg till modellen. Metodens namn och antalet ändrade parametrar visar emellertid inte hur den färdiga systemversionen fungerar i sin avsedda användning. Den ändrade systemversionens funktion måste därför undersökas genom tester efter ändringen.⁹

Artikel 3.23 och artikel 25.1 b gäller AI-systemet, inte modellen betraktad för sig. Den rättsliga prövningen gäller därför vad finjusteringen innebär för systemet som helhet.¹⁰

Systemets avsedda ändamål är den användning som leverantören har angett, tillsammans med det sammanhang och de villkor som

8 AI-förordningen, artiklarna 3.12, 3.23 och 25.1 b och c.

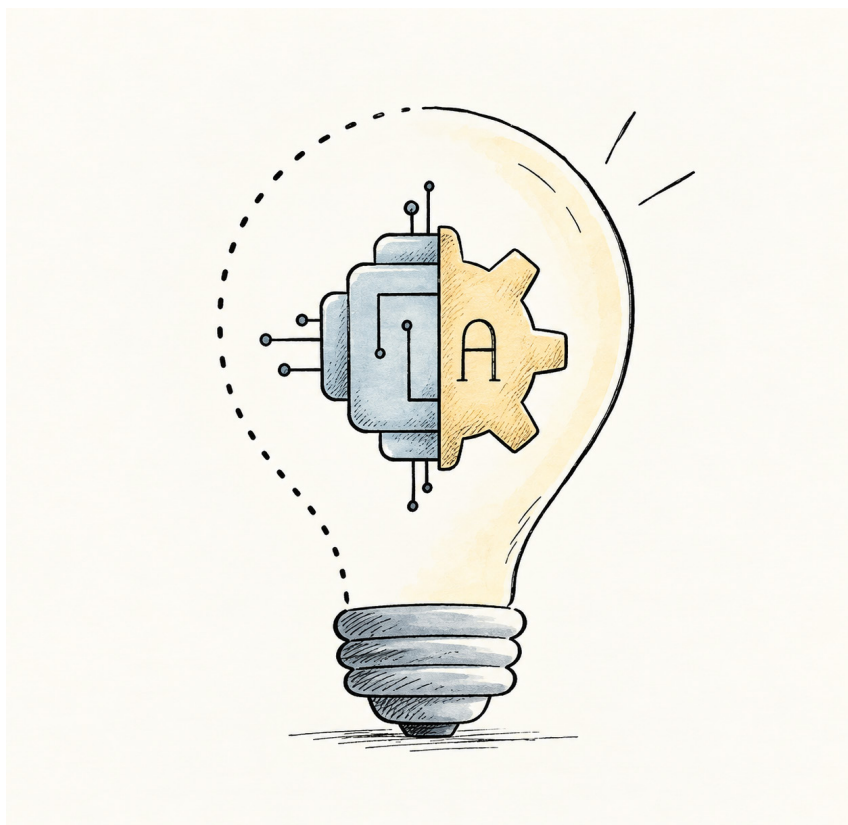
9 Lorenzo Pacchiardi m.fl., *A Framework to Categorise Modified General-Purpose AI Models as New Models Based on Behavioural Changes*, JRC143257, Europeiska unionens publikationsbyrå 2025, s. 16–19. Jämförelsen på systemnivå följer av AI-förordningen, artiklarna 3.23, 9 och 15.

10 Martin Ebers och Emmanuel Vargas Penagos, 'Upstream, downstream, and in between: navigating the GPAI value chain under EU law', *Information & Communications Technology Law* (2026), s. 3–4, doi: 10.1080/13600834.2026.2624923. AI-förordningen, artiklarna 3.1, 3.23 och 25.1 b samt skäl 97. Se även Philipp Hacker och Matthias Holweg, 'The regulation of fine-tuning: Federated compliance for modified general-purpose AI models', *Computer Law & Security Review* 60 (2026) 106234, s. 6, doi: 10.1016/j.clsr.2025.106234.

5 AI-förordningen, artikel 25.1 b och c.

6 Lorenzo Pacchiardi m.fl., *A Framework to Categorise Modified General-Purpose AI Models as New Models Based on Behavioural Changes*, JRC143257, Europeiska unionens publikationsbyrå 2025, s. 16–19. AI-förordningen, artiklarna 3.23 och 25.1 samt skäl 109.

7 AI-förordningen, artiklarna 3.3, 3.4, 3.23, 16 och 25.1.



Illustrasjon: Coulorbox/ChatGPT

framgår av bland annat bruksanvisningen och den tekniska dokumentationen. I det första fallet är oppgiften att prioritera nödsamtal densamma före och efter finjusteringen. I det andra förändras oppgiften från transkribering och sammanfattning till prioritering.¹¹

När systemet redan har hög risk

Klassificeringen måste provas innan artikel 25.1 b kan tillämpas. För system som bedöms enligt artikel 6.2 anges användningsfallen i bilaga III. I punkt 5 d nämns uttryckligen system som är avsedda att utvärdera och klassificera nödsamtal eller att sända ut eller bestämma prioriteringsordningen för larmtjänster. I det första exemplet används syste-

met för just en sådan uppgift både före och efter finjusteringen.¹² Att en användning finns i bilaga III avgör inte alltid klassificeringen. Artikel 6.3 kan undanta ett system om det inte medför någon betydande risk för skada på fysiska personers hälsa, säkerhet eller grundläggande rättigheter och minst ett av bestämmelsens fyra ytterligare villkor är uppfyllt. Larmcentralens rekommendation ingår i operatörens beslutsunderlag och kan påverka vilken hjälp som skickas och hur snabbt den kommer fram. En felaktigt låg prioritet kan därför medföra en betydande risk för hälsa eller säkerhet. Undantaget är därför inte tillämpligt i det första exemplet.

12 AI-förordningen, artikel 6.2 och bilaga III punkt 5 d. Europeiska kommissionen, *Draft Commission Guidelines on the classification of high-risk AI systems*, 19.5.2026, avsnitt IV.3.5.6, 'Analysing calls and prioritising interventions'. Riktlinjerna är vid artikelns färdigställande inte antagna eller bindande.

11 AI-förordningen, artiklarna 3.12, 3.23 och 25.1 b och c.

Systemet har hög risk både före och efter finjusteringen.¹³

Därmed blir artikel 25.1 b relevant. Bestämmelsen gör en tillhandahållare till leverantör om tre förutsättningar är uppfyllda: systemet har redan släppts ut på marknaden eller tagits i bruk, ändringen är väsentlig och systemet förblir ett AI-system med hög risk. Den första och den tredje förutsättningen är givna i exemplet. Nästa steg är därför att avgöra om ändringen är väsentlig.¹⁴

När ändringen är väsentlig

Artikel 3.23 definierar väsentlig ändring. Utöver att ändringen ska ha skett efter att systemet släpptes ut på marknaden eller togs i bruk innehåller definitionen två led som måste vara uppfyllda. Ändringen får inte ha förutsetts eller planerats i leverantörens ursprungliga bedömning av överensstämmelse. Ändringen ska dessutom påverka systemets uppfyllelse av högriskkraven i kapitel III avsnitt 2 eller leda till att det avsedda ändamål som låg till grund för bedömningen ändras.¹⁵

Artikel 43.4 visar hur definitionens första led fungerar för AI-system med hög risk som fortsätter att lära sig efter att de har släppts ut på marknaden eller tagits i bruk. För sådana system är en förändring av systemet eller dess prestanda inte väsentlig om leverantören har fastställt den på förhand vid den ursprungliga bedömningen och beskrivit den i den tekniska dokumentationen. Den särskilda regeln är inte direkt tillämplig på exemplet, eftersom finjusteringen görs vid ett enda tillfälle. Regelen visar ändå varför den ursprungliga bedömningen är central. Larmcentralens finjustering antas dock ligga utanför det som den ursprungliga

13 AI-förordningen, artikel 6.3. Tillämpningen på det hypotetiska fallet är artikelns bedömning.

14 AI-förordningen, artiklarna 3.23 och 25.1 b.

15 AI-förordningen, artikel 3.23 samt artiklarna 9, 10, 14 och 15.

leverantören dokumenterade. Efter-
som systemets avsedda ändamål är
oförändrat återstår då att bedöma
om finjusteringen påverkar uppfyl-
lsen av högriskkraven.¹⁶

Vad betyder det då att ändringen
”påverkar” uppfyllelsen av kraven?
Här förstås rekvisitet så att en rent
redaktionell uppdatering av doku-
mentationen inte är tillräcklig. Änd-
ringen måste ha faktisk betydelse
för bedömningen av minst ett krav i
kapitel III avsnitt 2, exempelvis
riskhantering, datakvalitet eller rik-
tighet. Det behöver däremot inte
redan vara visat att den ändrade ver-
sionen bryter mot ett krav. Frågan
är om förändringen rubbar den fak-
tiska eller dokumenterade grund på
vilken systemets överensstämmelse
tidigare visades, så att den ur-
sprungliga bedömningen inte utan
vidare kan läggas till grund för den
ändrade versionen.¹⁷

En ändring kan därför vara vä-
sentlig även om den minskar det fel
som den var avsedd att avhjälpa.
Finjusteringen kan minska antalet
brådskande samtal som får för låg
prioritet och samtidigt leda till fler
obefogat höga prioriteringar. För att
avgöra om systemets beteende har
förändrats bör versionerna jämföras
på samma oberoende testmaterial,
representativt för den avsedda an-
vändningen. Felaktigt låga och höga
prioriteringar bör redovisas var för
sig och tillsammans med resultatens
osäkerhet. AI-förordningen före-
skriver inte ett visst testupplägg.
Testerna får rättslig betydelse först
när resultaten kopplas till ett eller
flera av förordningens krav, i detta

fall främst riskhantering, datakvali-
tet och riktighet.¹⁸

I det första exemplet ligger
finjusteringen utanför de föränd-
ringar som den ursprungliga leve-
rantören planerade och dokumente-
rade. Det första ledet i artikel 3.23
är därför uppfyllt. De nya testerna
kan dessutom antas visa en tydlig
förändring av felmönstret, något
som har betydelse för systemets ris-
ker och riktighet. Förändringen rub-
bar därmed den faktiska och doku-
menterade grund på vilken
systemets risker och riktighet tidiga-
re bedömdes. Det talar för att uppfyllelsen av högriskkraven har på-
verkats i den mening som avses i
artikel 3.23. Under dessa förutsätt-
ningar innebär finjusteringen en vä-
sentlig ändring och larmcentralen
blir leverantör enligt artikel 25.1 b.
Om variationerna däremot saknar
betydelse för något av kraven, eller
om den ursprungliga bedömningen
redan omfattar förändringen, är vill-
koren i artikel 3.23 inte uppfyllda.

När systemet får ett nytt högriskändamål

Det andra exemplet börjar i ett an-
nat rättsligt läge. Systemet används
först för transkribering och sam-
manfattning och är inte klassificerat
som ett AI-system med hög risk.
Efter ändringen är systemversionen
avsedd att rekommendera hur nöds-
amtal ska prioriteras. Det avsedda
ändamålet har därmed ändrats till
en användning som anges i bilaga
III punkt 5 d. På samma grunder
som i det första fallet är undantaget
i artikel 6.3 inte tillämpligt. Den
ändrade systemversionen omfattas
därför av högriskreglerna.

Artikel 25.1 c reglerar just denna
situation. Den aktör som ändrar det
avsedda ändamålet så att ett system

som inte har klassificerats som hög-
risk blir ett AI-system med hög risk
ska betraktas som leverantör. I ex-
emplet är det larmcentralen som har
gett systemet den nya uppgiften.
Artikel 25.1 c hänvisar, till skillnad
från artikel 25.1 b, inte till definitio-
nen av väsentlig ändring i artikel
3.23. Bestämmelsens ordalydelse
innehåller därför inget separat krav
på att finjusteringen ska vara väsent-
lig. Det nya avsedda ändamålet och
den följande högriskklassificeringen
är den rättsliga grunden för ansvars-
skiftet.¹⁹

En separat fråga på modellnivå

Analysen hittills gäller leverantörs-
ansvaret för AI-systemet. Om syste-
met innehåller en AI-modell för all-
männa ändamål kan samma
finjustering dessutom väcka en se-
parat fråga om leverantörsansvaret
för modellen. Den frågan aktualise-
ras om den ändrade modellen
släpps ut på marknaden. Enligt
kommissionens icke-bindande rikt-
linjer blir en aktör i ett senare led
leverantör av den ändrade modellen
endast om finjusteringen leder till
en betydande förändring av model-
lens generalitet, alltså hur brett den
kan användas, dess kapacitet eller
dess systemrisker. Som vägledande
indikator används att beräkningsin-
satsen för ändringen överstiger en

16 AI-förordningen, artiklarna 3.23 och 43.4, bilaga IV punkt 2 f samt skäl 128.

17 AI-förordningen, artikel 3.23 och skäl 128. Tolkningen av rekvisitet ”påverkar” är artikelns egen och följer den bevisinriktade läsning som utvecklas i det examensarbete som artikeln bygger på.

18 AI-förordningen, artikel 3 punkterna 29–32 samt artiklarna 9, 10, 14 och 15. Pacchiardi m.fl., *A Framework to Categorise Modified General-Purpose AI Models*, s. 11–13 och 18–20. De konkreta riskerna och testupplägget är artikelns analys.

19 AI-förordningen, artiklarna 3.12 och 25.1 c. Ebers och Vargas Penagos, ‘Upstream, downstream, and in between’, s. 14–15. Att artikel 25.1 c saknar en hänvisning till artikel 3.23 framgår av en jämförelse med ordalydelsen i artikel 25.1 b.

tredjedel av beräkningsinsatsen för den ursprungliga träningen.²⁰

Kommissionens riktlinjer gäller modellreglerna och anger inte hur artikel 3.23 ska tillämpas på AI-system. Här görs därför bedömningen att tredjedelsindikatorn inte sätter någon nedre gräns för systemprovningen enligt artiklarna 3.23 och 25.1 b. Larmcentralen kan därmed bli leverantör av den ändrade systemversionen även när den beräkningsinsats som använts för finjusteringen ligger långt under indikatorn.²¹

Vad leverantörsrollen innebär

När larmcentralen blir leverantör ansvarar den för att den ändrade systemversionen uppfyller högriskkraven. Innan versionen tas i bruk måste larmcentralen upprätta den tekniska dokumentation som krävs och genomföra en bedömning av överensstämmelse. För ett system som omfattas av bilaga III punkt 5 d sker bedömningen genom intern kontroll enligt bilaga VI. Intern kontroll betyder här att larmcentralen själv granskar och dokumenterar överensstämmelsen. Det är ett rätts-

ligt kontrollförfarande, och inte bara verksamhetens vanliga kvalitetsarbete. Bedömningen sker utan medverkan av något anmält organ. Kraven börjar tillämpas på dessa system den 2 december 2027. Exempelen i texten avser tiden därefter.²²

Den ursprungliga leverantören upphör samtidigt att vara leverantör av just den ändrade versionen. Artikel 25.2 kräver dock att den ursprungliga leverantören samarbetar med den nya. Den digitala omnibusförordningen om AI trädde i kraft 2026 och preciserar vad samarbetet ska omfatta när det är relevant. Det gäller bland annat teknisk dokumentation, uppgifter om kända begränsningar och feltillstånd samt riktad teknisk tillgång för testning och validering. Ändringen gör samarbetsplikten mer konkret, men ändrar inte förutsättningarna för att leverantörsrollen ska övergå.²³

Slutsats: systemets förändring avgör

Finjustering är en teknisk metod. På systemnivå utlöser metoden ingen

rättsföljd enbart genom sitt namn eller sin omfattning. Om ett system redan har hög risk och behåller samma avsedda ändamål blir frågan om finjusteringen är en väsentlig ändring enligt artiklarna 3.23 och 25.1 b. Om finjusteringen i stället används för att ge ett tidigare icke-högrisksystem ett nytt ändamål som omfattas av högriskreglerna aktualiseras artikel 25.1 c. I båda fallen måste bedömningen göras på systemnivå och innan den ändrade versionen tas i bruk. Det avgörande är om finjusteringen medför en förändring som påverkar systemets uppfyllelse av högriskkraven eller ger systemet ett nytt avsett ändamål som gör det till ett AI-system med hög risk.

Emil Piva är juriststudent vid Uppsala universitet. Artikeln bygger på författarens examensarbete vid Uppsala universitet, Substantial Modification under Article 3(23) of the EU Artificial Intelligence Act: An Interpretive Analysis within the New Legislative Framework.

20 AI-förordningen, artiklarna 3.63 och 3.65. Europeiska kommissionen, *Commission Guidelines on the scope of the obligations for providers of general-purpose AI models established by Regulation (EU) 2024/1689 (AI Act)*, C(2025) 7719 final, 19.11.2025, punkterna 9, 47, 51 och 57–64. Kommissionen räknar enligt punkt 51 även vissa interna användningar som utsläppande på marknaden, bland annat när de påverkar fysiska personers rättigheter i unionen.

21 Ebers och Vargas Penagos, 'Upstream, downstream, and in between', s. 13–15. Skillnaden mellan modell- och systemprovningen följer även av AI-förordningen, artikel 1.2 c och e samt skäl 97. Se däremot Hacker och Holweg, 'The regulation of fine-tuning', s. 7–10, som föreslår att tredjedelsindikatorn tillämpas analogt tillsammans med en konsekvensanalys.

22 AI-förordningen, artiklarna 11, 16, 43.2 och 43.4 samt bilaga VI. För tillämpningsdatumet för kapitel III avsnitten 1–3, se Europaparlamentets och rådets förordning (EU) 2026/1744 (digital omnibusförordning om AI), EUT L, 2026/1744, 24.7.2026, artikel 1 led 40 b.

23 AI-förordningen, artikel 25.2 i dess ursprungliga lydelse. Förordning (EU) 2026/1744, artikel 1 led 12 a. Omnibusändringen behåller den grundläggande samarbetsplikten, preciserar vad den ska omfatta och behåller undantaget när den ursprungliga leverantören tydligt har angett att systemet inte får omvandlas till ett AI-system med hög risk.

«Pay or consent»: Hva er tillatt innenfor rammene av GDPR?

Av Ove A. Vanebo

1. Innledning

Konseptet «betaling eller samtykke» (ofte omtalt som «pay or consent» eller «pay or OK») har fått betydelig oppmerksomhet i Norge etter at Schibsted og andre eiere av nettaviser har valgt denne løsningen i forbindelse med tilgang til nettaviser. Spørsmålet er om det er forenlig med GDPR at brukere gis valget mellom å samtykke til behandling av personopplysninger eller betale for tjenesten – og i så fall hvor stort handlingsrommet er.

Kort sagt innebærer modellen at en digital tjeneste tilbys, men der «betalingen» kan skje på to måter: Enten aksepterer brukeren en reklamefinansiert versjon som er gratis for brukeren, eller så velges en betalt versjon uten annonser. I den reklamefinansierte løsningen må brukeren samtykke til behandling av sine personopplysninger for å muliggjøre visning av personlig tilpasset reklame fra tredjeparter i tjenesten. En beslektet forretningsmodell er det som noen ganger kalles «freemium»; en kombinasjon av ordene «gratis» og «premium». Et karakteristisk trekk ved freemium-modellen er at gratisversjonen utgjør en basisversjon av tjenesten (og det må gis samtykke til opplysningsinnsamling og -bruk), mens den betalte versjonen tilbyr bedre funksjoner eller andre fordeler (og har ingen eller mer beskjeden bruk av personopplysninger).

I EU ble modellen særlig kjent etter at det amerikanske selskapet Meta introduserte modellen på sine sosiale medieplattformer Facebook og Instagram – som igjen skapte mye støy. Det kan kanskje virke

pussig at det blir så mye oppmerksomhet rundt en tjeneste som er frivillig å velge, og der man jo selv kan ta stilling til om man vil gi fra seg personopplysninger. Reaksjonene må sees i lys av at sosiale medier spiller en stor rolle i folks daglige liv, og muliggjør kontakt med venner og kjente på en helt annen måte enn da papirbrev og fasttelefoner var de vanligste kommunikasjonsmidlene. Ulike rettighetsorganisasjoner og europeiske datatilsyn hevder at modellen tvinger brukere til å betale for å ivareta retten til privatliv og kontroll på egne personopplysninger.

Denne artikkelen vil belyse handlingsrommet for å kunne be om samtykke til behandling av personopplysninger som et alternativ til ordinær betaling med tradisjonelle pengeytelser eller andre pekuniære midler. Det vil særlig innebære en analyse av vilkårene for et gyldig samtykke etter EUs personvernforordning («GDPR»), som er gjennomført i norsk rett via personopplysningsloven.

For å belyse vilkårene for samtykke vil jeg særlig ta utgangspunkt i den såkalte *Bundeskartellamt*-dommen fra EU-domstolen, som gjaldt det tyske konkurransetilsynets (Bundeskartellamt) vurdering av om Facebook-eieren Meta misbrakte sin markedsrett.¹ Sentralt i dommen stod blant annet spørsmålet om Bundeskartellamt kunne ta hensyn til brudd på personvernregler ved interesseavveining i avgjørelser under konkurranseretten. Bundes-



Ove A. Vanebo

kartellamt forbød Meta å kombinere brukerdata fra flere kilder uten brukernes samtykke. Meta anket denne avgjørelsen til den høyere regionale domstolen i Düsseldorf. Domstolen i Düsseldorf ba EU-domstolen om å avklare hvordan visse bestemmelser i personvernforordningen (GDPR) skal tolkes, og om Bundeskartellamt også kan ta hensyn til GDPR-normer ved interesseavveining i avgjørelser under konkurranseretten. I sin anvendelse av konkurranseretten kan konkurransemyndighetene også ta hensyn til personvernreglene. EU-domstolen drøftet derfor om samtykke til personopplysningsbehandling kunne aksepteres som et alternativ til betaling for Metas tjenester.

2. Kan personopplysninger brukes som betaling?

Forordningen utelukker ikke prinsipielt sett at det kan samtykkes til opplysningsbehandling som «counter-performance» eller motytelse i et avtaleforhold, slik at personopplysninger blir en form for vederlag.

¹ C-252/21, *Meta Platforms Inc. v Bundeskartellamt*, EU:C:2023:537.

Selv om GDPR naturligvis skal ivareta personvern og kontroll på personopplysninger, har forståelsen støtte i GDPRs overordnede systematikk og de hensynene forordningen er ment å ivareta. Forordningen bygger på en forutsetning om at personvern ikke er en absolutt rettighet, men må balanseres mot andre interesser, slik som fornuftig bruk av personopplysninger for å ivareta en sunn markedsøkonomi.

Fortalepunkt 4 illustrerer dette ved å fastslå at: «*Retten til vern av personopplysninger er ikke en absolutt rettighet; den må ses i sammenheng med den funksjon den har i samfunnet, og veies mot andre grunnleggende rettigheter i samsvar med forholdsmessighetsprinsippet.*» Videre er følgende påpekt i samme fortepunkt: «*Før å sikre et velfungerende indre marked kreves det at den frie utvekslingen av personopplysninger i Unionen ikke begrenses eller forbyr av årsaker knyttet til vern av fysiske personer i forbindelse med behandling av personopplysninger.*»

” Forordningen utelukker ikke prinsipielt sett at det kan samtykkes til opplysningsbehandling som «counter-performance» eller motytelse i et avtaleforhold, slik at personopplysninger blir en form for vederlag.

Dette belyses også i EUs pakt om grunnleggende rettigheter, som skal ivareta og balansere brukernes rett til beskyttelse av personopplysninger i henhold til artikkel 8 opp mot næringsdrivendes frihet til å drive virksomhet i henhold til artikkel 16 i samme pakt. GDPR forutsettes å bli tolket og praktisert i lys av pakten, ved at forordningen «overholder alle grunnleggende rettigheter og de friheter og prinsipper som er anerkjent i pakten, slik de er nedfelt i trakta-

tene, særlig med hensyn til privatliv og familieliv, hjem og kommunikasjon, vern av personopplysninger, ... [og] frihet til å drive næringsvirksomhet ...».

EUs øvrige aktiviteter for å utforme hensiktsmessig regulering av personvern trekker heller ikke i retning av at personopplysninger skal avskjæres som betalingsmiddel. Tvert imot har EU initiert ulike planer, reguleringer og strategier for at personopplysninger skal kunne brukes som «betalingsmiddel», ved å etablere et «indre marked for data».²

Et eksempel på at personopplysninger anerkjennes som betalingsmiddel kan sees i digitalytelsesdirektivet.³ Direktivet ble vedtatt som en del av strategien for det digitale indre marked i Europa (Digital Single Market Strategy). I direktivets artikkel 3 nr. 1 annet avsnitt er det fastsatt at direktivet gjelder for avtaler der den næringsdrivende leverer en digital ytelse til en forbruker, og forbrukeren betaler en pris som vederlag for ytelsen. Vederlagsbegrepet i direktivet favner vidt, og vil omfatte både betaling med penger, digitale uttrykk for verdi og andre motytelser. Fortalepunkt 24 uttrykker en viss ambivalens og skepsis til personopplysninger som en ren vare, men presiserer samtidig at direktivet skal sørge for at forbrukere har rettigheter når de tilbyr personopplysninger som en motytelse:

«*Digitalt innhold eller digitale tjenester leveres ofte også når forbrukeren ikke betaler en pris, men gir den næringsdrivende personopplysninger. Slike forretningsmodeller brukes i forskjellige former i en betydelig del av markedet. Selv om dette direktivet fullt ut anerkjenner at vern av personopplysninger er en grunnleggende rettighet, og at personopplysnin-*

ger derfor ikke kan anses som en vare, bør det sikre at forbrukerne i forbindelse med slike forretningsmodeller har rett til avtalefestede beføyelser. Dette direktivet bør derfor få anvendelse på avtaler der den næringsdrivende leverer eller påtar seg å levere digitalt innhold eller en digital tjeneste til forbrukeren, og der forbrukeren gir eller påtar seg å gi personopplysninger.»

Digitalytelsesloven gjennomfører digitalytelsesdirektivet, og lovens § 1 fjerde ledd slår derfor fast at:

«*Med vederlag menes betaling i penger eller annen motytelse. Som vederlag regnes også at forbrukeren oppgir personopplysninger, med mindre leverandøren behandler personopplysningene utelukkende for å kunne levere den digitale ytelsen eller overholde lønpålagte plikter. Personopplysningsloven går ved motstrid foran reglene i denne loven.*»

3. Kan et samtykke til opplysningsbehandling som motytelse være «frivillig»?

3.1 Innledning

GDPR har som nevnt i punkt 2 ingen eksplisitte bestemmelser som forbyr bruk av personopplysninger som en motytelse for ulike tjenester. GDPR oppstiller imidlertid et grunnleggende vilkår om rettslig grunnlag, dvs. at bruk av personopplysninger som utgangspunkt er forbudt og at det må finnes en hjemmel for å behandle personopplysninger, se artikkel 6 nr. 1 bokstaven a til f. Her er det altså grunnlaget at «den registrerte har samtykket til behandling av sine personopplysninger for ett eller flere spesifikke formål», jf. bokstav a.

Spørsmålet blir derfor om vilkårene for et gyldig samtykke kan være oppfylt når det gis i en slik sammenheng. Et samtykke er «enhver frivillig, spesifikk, informert og utvetydig viljesytring fra den registrerte der vedkommende ved en erklæring eller en tydelig bekreftelse gir sitt samtykke til behandling av

2 EU-kommisjonens dokument COM(2020) 66 final, 2020-02-19A European strategy for data.

3 Europaparlaments- og rådsdirektiv (EU) 2019/770 av 20. mai 2019 om visse aspekter ved avtaler om levering av digitalt innhold og digitale tjenester

personopplysninger som gjelder vedkommende», jf. art. 4 nr. 11.

I forbindelse med samtykke for opplysningsbruk knyttet til bruk av tjenester, er det særlig kriteriet «frivillighet» som står sentralt. Generelt sett skal det lite til før et samtykke anses for ikke å være tilstrekkelig frivillig. Situasjonen med at samtykke gis i forbindelse med inngåelse eller oppfyllelse av en tjenestavtale, er særlig behandlet i GDPR art. 7 nr. 4:

«Ved vurdering av om et samtykke er gitt frivillig skal det tas størst mulig hensyn til blant annet om oppfyllelse av en avtale, herunder om yting av en tjeneste, er gjort betinget av samtykke til behandling av personopplysninger som ikke er nødvendig for å oppfylle nevnte avtale.»

Tvert imot synes artikkel 7 nr. 4 å forutsette at det kan skje, siden det kun skal «tas størst mulig hensyn til» om avtale er betinget av samtykke, og ikke er nedfelt et absolutt forbud mot samtykke i slike tilfeller. Jeg går nærmere inn på denne bestemmelsen i punkt 3.2 under.

Problemstillingen kom på spissen i *Bundeskartellamt-dommen* (se punkt 1 for nærmere redegjørelse for dommens innhold), der det i gjennomgangen av spørsmål 6 ble berørt om det er mulig å samtykke til opplysningsbehandling når aktøren som mottar samtykke har en dominerende posisjon. Dette mer spesifikke spørsmålet berøres i punkt 5 under, men dommen klargjør altså at det i prinsippet er mulig å samtykke til en tjenesteleverandør som en slags motytelse for å kunne bruke en digital tjeneste.

Dette var for øvrig også antatt i juridisk teori før EU-domstolen tok stilling til spørsmålet, noe som understreker at det er naturlig å lese GDPR som at forordningen tillater slike betingelser.⁴ Eksempelvis skrev

Hajo Michael Holtz følgende om frivillighetskravet i 2017:⁵ «*Detta krav kan sannolikt oppfylles endast om sådana tjänster erbjuder användarna rikliga valmöjligheter, exempelvis valet mellan ett gratis- och ett betalalternativ.*»

I den videre fremstillingen vil jeg gå gjennom ulike aspekter ved frivillighetskravet. Først vil jeg i punkt 3.2 drøfte om det er mulig å samtykke til opplysningsinnhenting og -bruk i forbindelse med avtaleinngåelse. Deretter vil jeg gå inn på hva man kan samtykke til i forbindelse med en avtale – om det samtykkes til «alb» fra tjenesteleverandøren, eller om det må avgrenses til den konkrete tjenesten, jf. punkt 3.3. I punkt 4 analyserer jeg om en dominerende posisjon i markedet påvirker frivilligheten, samt hvordan aktører med mye markedsaktører med mye markedsaktører kan ivareta frivillighet. Til sist vil jeg i punkt 5 berøre hva som kan være en passende betaling som alternativ til samtykke.

3.2 Adgangen til å «bunte sammen» avtale om tjeneste og samtykke

Som nevnt slår GDPR artikkel 7 nr. 4 fast at vurderingen av om et samtykke er gitt frivillig, skal ta «størst mulig hensyn til blant annet om oppfyllelse av en avtale, herunder om yting av en tjeneste, er gjort betinget av samtykke til behandling av personopplysninger som ikke er nødvendig for å oppfylle nevnte avtale.»

Bestemmelsen må anses som en utdypning av hva som utgjør et gyldig samtykke, særlig i lys av kravet til frivillighet. Artikkel 7 nr. 4 er ment å sørge for å motvirke bestemmelser som på urimelig vis innebærer at noen må samtykke til å gi fra seg personopplysninger i forbindelse med et avtaleforhold. I utgangspunktet kan personopplysninger som det er nødvendig å behand-

le benyttes, jf. også artikkel 6 nr. 1 bokstav b. Det er imidlertid når en registrert person må samtykke til behandling av personopplysninger som *ikke er nødvendige* for kontraktsforholdet det kan være problematisk.

Ofte vil krav om å samtykke legges frem som en «take it or leave it»-situasjon, der man må samtykke til opplysningsbehandlingen for overhodet å inngå avtalen, eller der viktige ytelser «suspenderes» uten samtykke. Samtykke kan også «buntes sammen» med andre forhold eller vilkår det samtykkes til. Det kan f.eks. hende at samtykke knyttes til behandlingsaktiviteter som er mer fjerntliggende fra hva som skal presteres under avtalen. Dersom samtykke innebærer en «avhengighet», dvs. at brukeren må akseptere opplysningsbehandling for å få en yttelse, er det trolig en presumpsjon (som kan utfordres) for at samtykket neppe er frivillig.⁶

Her tror jeg at den norske oversettelsen av GDPR har skapt et inntrykk av at adgangen til «sammenbunting» er noe snevrere enn den faktisk er. Fortalepunkt 43 i norsk språkdrakt, uttrykker at: «*Samtykket antas å ikke være gitt frivillig dersom det ikke er mulig å gi separat samtykke for forskjellige behandlingsaktiviteter, selv om det er hensiktsmessig i det enkelte tilfellet, eller dersom oppfyllelsen av en avtale, herunder yting av en tjeneste, avhenger av samtykket, til tross for at et slikt samtykke ikke er nødvendig for å oppfylle avtalen.*» Dette synes å uttrykke et mer ubetinget brudd på frivillighetskriteriet dersom samtykke «buntes sammen» med en avtale eller omfatter flere behandlingsaktiviteter. Den engelskspråklige versjonen tydeliggjør at det kun er tale om en presumpsjon: «*Consent is presumed not to be freely given if it does not allow sepa-*

4 Jan Philipp Albrecht og Florian Jotzo, *Das neue Datenschutzrecht der EU*, 2017, s. 72.

5 Hajo Michael Holtz, «*Den nya allmänna dataskyddsförordningen — några anmärkningar*». I: Svensk Juristtidning, 2018, s. 250.

6 Judith Rauhofer og Burkhard Schaffer, «*Art. 7: Conditions for consent*». I: Spiecker et al. (red.), *General Data Protection Regulation*, 2023, s. 389.

rate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.»

Selv om det er diskutabelt hvor stort handlingsrommet er, må artikkel 7 nr. 4 ikke anses som et forbud mot å «bunte sammen» samtykke og kontraktsoppfyllelse.⁷ Ordlyden er det skal «*tas størst mulig hensyn til*» blant annet om oppfyllelse av en avtale [...], er gjort betinget av samtykke til behandling av personopplysninger». At det skal tas hensyn til må indikere at det kun er et sentralt moment, og ikke noe avgjørende argument mot, om avtale er frivillig inngått.

Denne forståelsen er også i samsvar med GDPRs forhistorie. Opprinnelig foreslo Europaparlamentet at det skulle inntas et forbud mot å gjøre avtaler eller tjenesteytelser «conditional of the consent on the processing or use of data that is not necessary for the execution of that contract or the provision of the service».⁸ Forslaget ble avvist. Sett i lys av foralepunkt 43 og formålet med art. 7 nr. 4 må det likevel legges til grunn at adgangen til sammenbunting av samtykker er betydelig begrenset.⁹ Bestemmelsen er uansett nokså skjønnsmessig og uklar, og rekkevidden må kartlegges og utvikles gjennom praksis.¹⁰

3.3 Samtykket må gjelde nærmere avgrensede behandlingsoperasjoner

Tidlige reguleringsmekanismer for personvern fokuserte på selve reguleringsgjenstanden, særlig datafilen eller lignende, og bruk av data.¹¹ I denne sammenheng kan det nevnes at Norge hadde personregisterloven av 1979, som gjaldt personregistre og «annen bruk av personopplysninger i visse typer virksomhet», jf. lovens § 1. Også Europarådets personvernkonvensjon hadde en slik objektsentrert tilnærming, og viste til pliktsubjektet som «controller of the file».¹²

Bruddet med fokuset på objektet eller gjenstanden som brukes, kom med personverndirektivet av 1995, som innebar en «justering» av personvernregulering: Fra å fokusere på objektet eller gjenstanden, ble formål og behandlinger mer sentralt.

Endringen ser man også eksplisitt i Bundeskartellamt-dommen, som ifølge teoretikeren Seiichi Igaya gjenspeiler et prinsipp om «operation-first».¹³ Prinsippet innebærer at samtykke må knyttes til behandlingsoperasjoner, og ikke den behandlingsansvarlige. Det betyr at det er problematisk å knytte samtykke til en bestemt behandlingsansvarlig eller dennes (ofte svært om-

fattende) økosystem.¹⁴ EU-domstolen påpekte derfor I Bundeskartellamt-dommen at «*given the scale of the processing of the data in question and the significant impact of that processing on the users*», var det «*appropriate, within the meaning of recital 43, to have the possibility of giving separate consent for the processing of the latter data [on-Facebook data], on the one hand, and the off-Facebook data, on the other*».¹⁵

3.4 Hva slags alternativ må det være til samtykke?

Virksomheten har ifølge Bundeskartellamt-dommen et ansvar for å sikre at forbrukerne står fritt til å nekte samtykke, uten å bli forhindret fra å bruke tjenesten i sin helhet, dvs. «*an equivalent alternative not accompanied by such data processing operations*».¹⁶ Dette må oppfattes som at det er tilstrekkelig å ha ett alternativ til samtykke.¹⁷

Et særlig spørsmål er om det må eksistere et tredje alternativ til samtykke eller betaling. I april 2024 publiserte Personvernrådet en uttalelse som spesifikt vurderte «betaling eller samtykke». Rådet konkluderte med at det i de fleste tilfeller ikke vil være mulig for store nettplattformer å oppfylle kravene til gyldig samtykke hvis de bare gir brukerne et valg mellom å samtykke til behand-

7 Kristian Korfits Nielsen og Anders Lotterup, *Databeskyttelsesforordningen og databeskyttelsesloven*, 2020, s. 413.

8 Gjengitt i fotnote 61 i Rauhofer og Schafer (2023) s. 389.

9 Rauhofer og Schafer (2023) s. 389 og Inge Graef, «*Meta platforms: How the CJEU leaves competition and data protection authorities with an assignment*». I: Maastricht Journal of European and Comparative Law 2023, Vol. 30(3) 325–334, s. 331.

10 Nielsen og Lotterup (2020) s. 413–414.

11 Seiichi Igaya, «*Operator-first versus operation-first: regulatory architectures in data protection law and the Meta Platforms judgment*». I: International Data Privacy Law, Volume 16, Issue 2, 2026, s. 6.

12 Konvensjon om personvern i forbindelse med elektronisk databehandling av personopplysninger av 1981, ETS nr. 108, artikkel 2 bokstav d.

13 Igaya (2026) s. 6.

14 Inge Graef, «The European Court of Justice in Meta Platforms leaves competition and data protection authorities with an assignment». I: European Law Blog, side 4: «*This clarification by the Court considerably restricts the ability of providers of digital ecosystems like Meta to combine personal data from different sources and between different services*» Lest 10. september 2026: <https://europeanlawblog.eu/the-european-court-of-justice-in-meta-platforms-leaves-competition-and-data-protection-authorities-with-an-assignment/pdf/>

15 Avsnitt 151.

16 Avsnitt 150.

17 Martin Nettesheim, *GDPR Overreach? The Challenges of Regulating Pay-or-Consent Models through Data Protection Law*. Lest 7. September 2026: <https://verfassungsblog.de/gdpr-overreach/>

ling av personopplysninger (med det formål å benytte adferdsbasert markedsføring) eller å betale for tjenesten. Rådet uttrykte at tilbydere av sosiale tjenester bør («should») tilby brukerne et tredje alternativ, dvs. en gratisløsning basert på reklamefinansiering uten profilering.¹⁸ Denne løsningen synes vanskelig å forankre i GDPR eller *Bundeskartellamt*-dommen, og det kunne være fristende å vise til Hajo Michael Holtz, som påpeker at: «Denna tolkning av GDPR kan anses som ekstrem, eftersom den inte har ett tydligt stöd i varken lagtexten eller EU-domstolens rättspraxis.»¹⁹ Holtz nevner også at det strengt tatt også er et alternativ å avstå fra å bruke tjenesten overhodet.

På den annen side kan det nok være et moment i en helhetsvurdering om det tilbys ytterligere et tilbud, utover det obligatoriske ene alternativet. Dette er imidlertid mer basert på «best practice», og kan neppe anses som en rettslig forpliktelse.

4. Vil en dominerende markedsposisjon ha betydning?

GDPR tydeliggjør i fortalepunkt 43 at maktubalanse kan medføre at et samtykke ikke er gitt «frivillig»: «For å sikre at et samtykke gis frivillig bør det ikke utgjøre et gyldig rettslig grunnlag for behandling av personopplysninger i et bestemt tilfelle dersom det er en klar skjevhet mellom den registrerte og den behandlingsansvarlige, særlig dersom den behandlingsansvarlige er en offentlig myndighet og det derfor er usannsynlig at samtykket er gitt frivillig med hensyn til alle omstendigheter som kjennetegner den bestemte situasjonen.»

Lignende betraktninger må også legges til grunn ved samtykke i for



Illustrasjon: Coulorbox/ChatGPT

eksempel arbeidsforhold, dvs. at et samtykke til arbeidsgiver mer unnaksvis vil være «frivillig».²⁰

Facebooks dominerende stilling på markedet for sosiale medier er imidlertid ifølge EU-domstolen ikke nødvendigvis et hinder at gyldig samtykke kan gis; markedsmakten «does not, as such, preclude the users of such a network from being able validly to consent, within the meaning of Article 4(11) of [the GDPR], to the processing of their personal data by that operator», jf. *Bundeskartellamt*-dommen avsnitt 154. Samtykke kan altså fortsatt være frivillig selv til et dominerende foretak.²¹ Et selskaps dominans kan likevel føre til en «klar ubalanse» mellom forbrukeren og selskapet, noe som i henhold til fortalepunkt 43 kan gjøre samtykket ugyldig.²² Jeg oppfatter at det må være en høy terskel for ubalansen fører til ufrivillighet, jf. ordlyden «klar».

Det må trolig antas at betydningen av tjenesten også vil ha betydning, som uttrykt i Sören Ömans lovkommentar til GDPR:²³

«Är varan eller tjänsten inte mer eller mindre nödvändig i dagens samhälle eller för den enskilde, har den enskilde fortfarande ett fritt val mellan att samtycka och att avstå från varan eller tjänsten. Ett exempel kan vara en tjänst som gör det ännu enklare än vanligt att surfa på internet. Behöver å andra sidan den enskilde, t.ex. en synskadad, tjänsten för att över huvud taget kunna surfa på internet, får däremot tjänsten anses nödvändig för just honom eller henne (eftersom det i dagens samhälle i Sverige får anses mer eller mindre nödvändigt att ha möjlighet att surfa på internet.)»

Jeg antar at dette må være en konkret og dynamisk vurdering. Det er ingen tvil om at svært mange bruker f.eks. det sosiale mediumet Facebook. Mediumet betyr mye for folks nett-

18 Personvernrådet, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, s. 20-21.

19 Hajo Michael Holtz, «Affärsmodellen "pay or consent" – Olaglig eller innovativ?»: I: Europarättslig tidskrift, 2025, nr. 2 s. 208.

20 Personvernrådet, *Guidelines 05/2020 on consent under Regulation 2016/679; Version 1.1*, s. 9.

21 Se avsnittene 144-145. Se også Graef (2023) 328.

22 Avsnitt 149

23 Öman, Sören, *Dataskyddsförordningen (GDPR) m.m. – En kommentar*, 2025, digital oppdatering i Karnov forlag, jf. punktet «Frivilligt samtykke»

verksbygging og sosiale liv. Samtidig vil mediernes oppslutning og bruk variere, og det vil etter mitt skjønn også være relevant å ta hensyn til at færre bruker Facebook nå enn tidligere, slik at det i det minste prinsipielt kan argumenteres for at behovet/nødvendigheten er redusert.

5. Hva er et «passende gebyr»?

EU-domstolen nevner i *Bundeskartellamt*-saken at det en betalingsløsning kan være et hensiktsmessig alternativ til samtykkebasert tilbud, som «om nødvendig» innebærer å betale «et passende gebyr» for tjenesten.²⁴ EU-domstolen tar likevel ikke stilling til hva som kan være et «passende gebyr». En rekke kilder har gått gjennom ulike modeller for å fastsette størrelsen på gebyret, uten å komme til en klar konklusjon.

Heller ikke Personvernrådet har kommet med klar veiledning. Rådet påpeker at gebyret ikke skal hindre registrerte fra å nekte samtykke, og dessuten ikke få dem til å føle seg tvunget til å samtykke. Selv om Personvernrådet nevner at det skal tas hensyn til hva som synes rimelig, synes det også som at utgangspunktet er at: «*Businesses are free to set their own prices and choose how their revenue models are structured ...*».²⁵

Behandlingsansvarlige bør også ifølge rådet dokumentere sine valg og vurdering av om et gitt gebyr er passende i det spesifikke tilfellet for å demonstrere at det å pålegge gebyret ikke effektivt undergraver muligheten for fritt gitt samtykke i den aktuelle situasjonen. Ut fra Personvernrådets (uklare) råd, synes det som om det sentrale er å velge en løsning som ikke er klart urimelig eller upassende, og at man bør forklare hvorfor prisen er akseptabel. Rådet synes lite interessert i å være en pådriver for priskontroll.

I juridisk teori er det først og fremst vist til at prisen ikke skal være uforholdsmessig høy. Professor Martin Nettesheim har vært innom en tanke om at betaling ikke må bli et svært ufordelaktig valg, som undergraver det frie valget.²⁶ I annen teori er det foreslått at det er hensiktsmessig å ta utgangspunkt i at prisen ikke skal vesentlig overstige den som kreves av sammenlignbare tjenester.²⁷ Eksistensen av et marked for sammenlignbare tjenester til sammenlignbare priser tyder derfor på at prisnivået ikke overstiger kundenes økonomiske kapasitet.²⁸ Det er derfor trolig hensiktsmessig å se nærmere på hva som anses som markedspris.

Det må uansett være på det rene at det ikke er meningen å ha en beskjedne «kostpris» eller «kostnad(pluss)»-tilnærming der bedrifter rettferdiggjør prisene sine med henvisning til kostnadene og en viss fortjenestemargin. Både GDPR og EU-pakten om grunnleggende rettigheter skal underbygge vellykkede, harmoniserte markeder med relativt fri prisfastsettelse, og er ikke ment å være instrumenter for prisregulering eller maksimalpriser.²⁹

Det danske Datatilsynet traff derfor, etter mitt skjønn, spikeren på hodet da det i forbindelse med en eldre veileder om cookie walls påpekte at: «*Datatilsynet bemærker, at det ikke tilkommer tilsynet at gå nærmere ind i prisfastsettelsen af indhold, tjenester mv. Virksomheder har derfor et vidt skøn ved vurderingen og fastsettelsen af det specifikke beløb, der skal udgøre et betalingsalternativ til den besøgendes samtykke til behandling af personoplysninger.*»³⁰

6. Avsluttende merknader

GDPR er ikke ment å være et hinder for innovative forretningsmodeller, men balanserer hensynet til personvern opp mot hensynet til å fremme velfungerende markeder. GDPR er også ment å omfatte behandlingsaktivitetene som er knyttet til tilbud av varer eller tjenester, uansett om det kreves tradisjonell betaling eller ikke.³¹

Målsettingen med artikkelen er ikke å argumentere for at personopplysninger i større grad enn gjeldende rett bør kunne brukes som et vederlag, men å nyansere forenklete utgangspunkter – som f.eks. at muligheten nær sagt er avskåret uansett. Sett i lys av punkt 2 over om at personopplysninger kan være en form for vederlag, samt gjennomgangen over i punktene 2 til 6, er det ikke grunnlag for en altfor restriktiv tilnærming til å bruke personopplysninger som «betaling» for digitale ytelser. Muligheten til å samtykke til behandling av personopplysninger må derfor vurderes konkret, og bør ikke avvises på autopilot.

Ove A. Vanebo, advokat og assosiert partner i CMS Kluge Advokatfirma. Vanebo har arbeidet med personvern og tilgrensende IKT-rettslige spørsmål i over 10 år.

²⁴ Avsnitt 150.

²⁵ Personvernrådet, *Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms*, s. 30.

²⁶ Martin Nettesheim, EU Data Protection Law and Pay-or-Consent Business Models, 2024. Lest 8. september 2024: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4768419

²⁷ Eric Benjamin Seufert og Mikołaj Barczentewicz, *Podcast: What's happening with DMA enforcement?* Lest/hørt 8. september 2026: <https://mobiledevmemo.com/podcast-whats-happening-with-dma-enforcement-with-mikolaj-barzentewicz/>

²⁸ Mikołaj Barczentewicz, Pay or OK: what is an «appropriate fee»? 2024. Lest 8. september 2026: <https://eutechreg.com/p/pay-or-ok-what-is-an-appropriate>

²⁹ Martin Nettesheim, GDPR Overreach? The Challenges of Regulating Pay-or-Consent Models through Data Protection Law, 2024. Lest 7. september 2026: <https://verfassungsblog.de/gdpr-overreach/> Se også: Holtz (2024) side 211.

³⁰ Datatilsynet, *Cookie walls. Ukjent dato*. Lest 8. september 2026: <https://web.archive.org/web/20240206013918/https://www.datatilsynet.dk/bvad-siger-reglerne/vejledning/cookies/cookie-walls>

³¹ Jf. Fortalepunkt 23. Se også Laura Drechsler, *Data As Counter-Performance: A New Way Forward Or A Step Back For The Fundamental Right Of Data Protection?*, 2018.

How stakeholder pressure and institutional priorities can shape AI legislation – The case of AI Act Annex I under the Digital Omnibus on AI

By Jakub Skórczynski

When the AI Act entered into force in August 2024, not many could have foreseen that it would be subject to reform in 2026. The reform was part of EU's broader revisiting of recent legislative initiatives in the digital domain as part of EU's Digital Package.¹ With "simplification" as a key driver for the Digital Omnibus on AI, the European Commission proposed to change the AI Act.² The proposed changes encompassed, for example, the revision of the requirement on AI literacy and the postponement of the requirements on high-risk AI systems. Among these changes, and amid the trilogue, a push towards a bigger focus on sectoral exemptions from the AI Act could be observed.

Behind amendments to the AI Act lies a question: who ultimately influences the direction of EU AI legislation? This article presents two

distinct ways in which external and internal policy objectives have had and can have an influence on the reform of AI Act.

” Behind amendments to the AI Act lies a question: who ultimately influences the direction of EU AI legislation?

The structure of the article

The article is structured by firstly addressing input from external stakeholders as an example of how they can influence the trilogue. Thereafter, the article considers internal policy objectives within the European Commission as drivers of change and the interaction between different entities within the Commission. Lastly, the article is concluded by giving an insight to why legal professionals dealing with digital legislation can have a benefit from considering the above matters.

The external aspect – When stakeholders influence the member states in trilogue.

In the beginning of May 2026, news outlets specialised in EU policy affairs reported on the fierce negotiations on the role of sectoral legislation in relation to the subsequent publication of the political agree-



Jakub Skórczynski

ment between the European Parliament and the Council of the EU on the Digital Omnibus on AI.³

In the late stages of the negotiations of the Digital Omnibus on AI a push towards a sectoral outlook on AI was strongly supported by

1 European Commission, 'Simpler EU digital rules and new digital wallets to save billions for businesses and boost innovation*' (2025) <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2718> accessed 31-08-2026

2 Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), 2025/0404 (COD)

3 See for example: Pieter Haack, 'Germany set to secure win for industry in AI talks' *Politico* (06-05-2026) <<https://www.politico.eu/article/germany-eu-ai-law-machinery-exemption-industrial-rewrite/>>, Maximilian Henning, 'EU clinches AI reform deal centring on machinery cuts' *Euractiv* (07-05-2026) <<https://www.euractiv.com/news/eu-clinches-ai-reform-deal-centring-on-machinery-cuts/>> or Jedidiah Bracy, 'EU agrees to amend AI Act, clarifies overlap with machinery rules' *IAPP* (07-05-2026) <<https://iapp.org/news/a/eu-agrees-to-amend-ai-act-clarifies-overlap-with-machinery-rules>>

Germany, despite the sight of the provisional agreement being just beyond the horizon. In early April 2026, Chancellor Friedrich Merz made a statement at an industrial fair in Hannover, where he voiced his support of a “[...] *push to ease the regulatory burden in the EU on AI and, where possible, to exempt industrial AI from the current regulatory straitjacket*”.⁴ The commitment aligned with the arguments of several German industrial giants and, later, with a plea from seven leading EU industry actors.⁵ As reported by Politico, the initiative encompassed a broader push to prioritise sectoral regulation of AI rather than the horizontal regulation of the AI Act. The reasoning behind such approach was to minimise the risk of “*double obligations, overlapping requirements and legal uncertainty*”.⁶ It was suggested that the sectoral legislation should be moved from Section A of the Annex I to the Section B, which would significantly impact the scope of the AI Act. In a practical perspective, this would mean that legislation encompassed by the dual conformity assessment, including inter alia legislation on manufacturing, toys, and medical devices, would be moved to solely be covered by the sectoral legislation.⁷ A very similar approach was seen in a study com-

missioned by Bertelsmann Stiftung in November 2025.⁸ The authors argued that the ‘*bifurcation*’ between Annex I, Section A and Section B led to ‘*significant implementation challenges*’.⁹ It was highlighted that products regulated in Section A, and thus already subject to New Legislative Framework (NLF) were placed under direct application of AI Act. At the same time, products subject to Annex I, Section B, such as, for example, automotive, aviation and transportation products, were not subject to the NLF, whereby the AI Act governance principles were meant to be incorporated into existing sectoral legislation, but the AI Act would not be directly applicable in this context. This approach could thus indicate a high level of complexity, arising from the diverging scopes of applications, particularly relevant for undertakings working with both types of products.

The final version of the Digital Omnibus on AI has implemented the suggested change related to the Machinery Regulation in Annex I, Section B. The recitals refer to the “specific nature”¹⁰ of machinery and its corresponding sector. However, this change shows that even a late push made by the stakeholders can effectively affect the outcome of the legislative act, such as the AI Act.

The internal aspect – Diverging interests within the Commission or “Turf battles”?

The above changes were, however, not the sole efforts to alter parts of the AI Act in favour of sectoral legislation. In December 2025, as the legal community continued to assess the ramifications of the recently published Digital Omnibus on AI, an interesting development arose.

The Directorate-General for Health and Food Safety (DG SANTE) presented the proposal for a regulation to simplify rules on medical and in vitro diagnostic devices.¹¹ The proposal presented somewhat of a “backdoor” alteration of the AI Act, by proposing to move Medical Devices Regulation (MDR) and In Vitro Diagnostics Regulations (IVDR) from the AI Act, Annex I, Section A to AI Act, Annex I, Section B. Similarly, to the recent developments of Machinery Regulation, it was indicated that the status quo led to uncertainty. Representatives of European trade associations indicated inter alia that “*The AI Act created significant interplay issues with the MDR and IVDR, with different definitions and concepts applying to the same product (how to assess risk, substantial modification, etc.), which would have created friction*”.¹² This argument was however disputed by AI professionals such as Adam Leon Smith, who argued that it is common for NLF legislation to overlap “*In such a case, the issue of overlap might be resolved by giving preference to the more specific Union harmonisation act. For example, the Machinery and Low Voltage regulations often both apply to the*

4 ‘Germany’s Merz says industrial AI needs less stringent EU regulation’ *Reuters* (31–08–2026) <<https://www.reuters.com/business/germanys-merz-says-industrial-ai-needs-less-stringent-eu-regulation-2026-04-19/>>

5 ASML, *ASML CEO Christophe Fouquet co-signed opinion piece with European technology companies* (2026)

6 Pieter Haeck, ‘Germany faces resistance in push to weaken AI rules’ (21–04–2026) <<https://www.politico.eu/article/germany-stronger-ai-deregulation-brussels-eu-opposition/>>

7 Luca Bertuzzi, *EU policymakers fall short of agreeing on AI Act amendments* (2026) or see the same authors LinkedIn post about the topic <<https://lnkd.in/p/eukFRUKC>> (29-04-2026)

8 Philip Hacker, Robert Kilian and Jana Costas, “*Simplifying*” *European AI Regulation - An Evidence-based Study*, 2025)

9 Ibid, p. 39

10 Regulation (EU) 2026/1744, Digital Omnibus on AI, recital 42

11 Proposal for a regulation amending Regulations (EU) 2017/745 and (EU) 2017/746 as regards simplifying and reducing the burden of the rules on medical devices and in vitro diagnostic medical devices, and amending Regulation (EU) 2022/123 as regards the support of the European Medicines Agency for the expert panels on medical devices and Regulation (EU) 2024/1689 as regards the list of Union harmonisation legislation referred to in its Annex I, 2025/0404 (COD)

12 Julien Chasserieu, *Barely a month after the AI omnibus was presented, another major AI Act amendment just got proposed through the revision of the MDR and IVDR, changing the way the EU AI regulation will apply to medical devices with AI capabilities*. (2026) published on LinkedIn <<https://lnkd.in/p/e9Z-d9r9x>>



Illustration: Coulorbox/ChatGPT

same product’.¹³ The author not only criticised the approach but also highlighted that alterations to the existing framework could have significant implications, for example for the process of developing harmonised standards, due to the potential withdrawal of stakeholders in medical devices.

However, this can lead to another question, which is: How can it be that DG SANTE tried to reform the AI Act by presenting its own proposal for a different legislative act, while the negotiations on the AI Omnibus were ongoing? The answer to this question will remain unresolved in the article, but it leads us to considering a broader question of cooperation within the European Commission.

The internal cooperation within the European Commission.

The tasks within the European Commission are split among com-

missioners and the administrative apparatus consisting of more than 30 Directorates-General (DG) and 20-service departments.¹⁴ As argued by Blom-Hansen, Finke and Senninger, the sheer size of the organisation leads to an unavoidable fragmentation due to a further division to separate departments and ministries with the aim to solve tasks at a specialised level.¹⁵ The different DGs within the European Commission are responsible for different policy areas, by pursuing a number of tasks encompassing implementation and management of EU policy and legislation.¹⁶ To exemplify, the Directorate-General for Communications Networks, Content and

Technology (DG Connect) was the DG responsible for a significant part of the work on the AI Act, and the Directorate itself consists of number of sublevel departments.¹⁷ The political responsibilities of the DG Connect encompasses among others pursuing the goals of promoting digitalisation of the EU, promoting technological sovereignty and enforcement of the rulebook for online platforms and AI.¹⁸ It is relevant to highlight that, the European Commission has formalised

13 Adam Leon Smith, *DG SANTE proposal threatens to undermine both the EU AI Act, and the New Legislative Framework itself* (2025)

14 Jens Blom-Hansen, Daniel Finke and Roman Senninger, ‘Coordination in European Commission’ in Gijs Jan Brandsma (ed), *Handbook on European Union Public Administration*, (Edward Elgar Publishing 2024), p. 239

15 Ibid

16 European Commission Directorate-General for Communication, ‘Organisation of the European Commission’ (2026) <https://commission.europa.eu/about/organisation_en> accessed 31-08-2026

17 Publications Office of the European Union, ‘Directorate-General for Communications Networks, Content and Technology (CNECT)’ (2026) <<https://op.europa.eu/en/web/who-is-who/organization/-/organization/CNECT/CNECT>> accessed 31-08-2026

18 European Commission Directorate-General for Communication, ‘Communications Networks, Content and Technology’ (2026) <https://commission.europa.eu/about/departments-and-executive-agencies/communications-networks-content-and-technology_en> accessed 31-08-2026

rules of procedure¹⁹ and that if a DG submits a proposal, it is usually followed by an inter-service consultation process, giving other relevant DG's the possibilities to comment.²⁰ However, as highlighted in scientific literature, there are examples questioning whether this coordination is always effective.²¹ Several articles have illustrated the conflictual tendencies within the Commission, for example when the DG's work in "silos" which affects the effectiveness of work due to lacks in coordination²², or the legislative process within Commission is occasionally subject to internal frictions, due to diverging interdepartmental interests.²³ With such instances in mind, it is possible that DG SANTE, in the case of the suggested changes to the AI Act, pursued its own ambitions for legislative change by placing medical devices in the AI Act, Annex I, Section B.

Conclusion: What's in it for legal practitioners?

This article briefly illustrates two of many ways in which policy objectives and politics affected the dialogue regarding the Digital Omnibus on AI. On the one hand, negotiations can be significantly affected by pursuing policy goals promoted by stakeholders in the industry or interest groups, for example within civil society or business, as illustrated by the German example.

On the other hand, there are also policy goals within the EU institutions. The example of DG SANTE and its suggested changes to the AI Act can serve as an illustrate example of diverging priorities within the EU Commission itself. This peculiarity often goes unnoticed by legal practitioners, since it is not as evident as the influence of external actors, and the EU is generally a highly capable and well-functioning organisation given its size, influence and power.²⁴

However, raising awareness on the potential tensions when regulating AI or other digital technologies, can have an impact on legal professionals within the field. The legal practitioners must navigate a complex landscape in which both horizontal (cross-sectoral) and sector-specific regulatory frameworks coexist. Each framework is driven by distinct policy objectives, and it is important to remember that EU is not a monolith. A perspective limited to horizontal IT legislation may not adequately address the legal elements and policy of sectoral legislation, such as within the medical technology sector. Similarly, an undue emphasis on sector-specific sources may lead to a distorted per-

ception of overarching regulatory frameworks in cross-sectoral legislation. A holistic approach that considers the contextual elements of policy and legal objectives can be essential, particularly for legal professionals seeking to better predict the overall development of digital legislation.

Chassericau J, *Barely a month after the AI omnibus was presented, another major AI Act amendment just got proposed through the revision of the MDR and IVDR, changing the way the EU AI regulation will apply to medical devices with AI capabilities.* (2026)

Smith AL, *DG SANTE proposal threatens to undermine both the EU AI Act, and the New Legislative Framework itself* (2025)

Hartlapp M, Metz J and Rauh C, *Which Policy for Europe?: Power and Conflict inside the European Commission* (Oxford University Press 2014)

Blom-Hansen J, Finke D and Senninger R, 'Coordination in European Commission' in Brandsma GJ (ed), *Handbook on European Union Public Administration* (Edward Elgar Publishing 2024)

Chatzopoulou S, 'Resilience of the Silo Organizational Structure in the European Commission' (2023) 61 JCMS: Journal of Common Market Studies

Rauh C, 'One agenda-setter or many? The varying success of policy initiatives by individual Directorates-General of the European Commission 1994–2016' (2021) 22 European Union Politics, 'Germany's Merz says industrial AI needs less stringent EU regulation' *Reuters* (31–08–2026) <<https://www.reuters.com/business/germanys-merz-says-industrial-ai-needs-less-stringent-eu-regulation-2026-04-19/>>

19 Rules of Procedure of the Commission [C(2000) 3614], L 308

20 Blom-Hansen, Finke and Senninger, 'Coordination in European Commission', p. 245

21 The chapter 'Coordination in European Commission' by Blom-Hansen, Finke and Senninger in the "Handbook on European Public Administration" presented a nuanced list of different research articles both indicating that the work within the EU Commission is effective but also examples on articles stating the opposite, see p. 246 – 249.

22 Sevasti Chatzopoulou, 'Resilience of the Silo Organizational Structure in the European Commission' (2023) 61 JCMS: Journal of Common Market Studies

23 Miriam Hartlapp, Julia Metz and Christian Rauh, *Which Policy for Europe?: Power and Conflict inside the European Commission*, (Oxford University Press 2014) and Christian Rauh, 'One agenda-setter or many? The varying success of policy initiatives by individual Directorates-General of the European Commission 1994–2016' (2021) 22 European Union Politics

24 Just to illustrate the European Commission alone, employs around 32.000 permanent and contract employees: European Commission Directorate-General for Communication, 'Commission staff' (2026) <https://commission.europa.eu/about/organisation/commission-staff_en> accessed 31-08-2026

Bracy J, 'EU agrees to amend AI Act, clarifies overlap with machinery rules' *LAPP* (07-05-2026) <<https://iapp.org/news/a/eu-agrees-to-amend-ai-act-clarifies-overlap-with-machinery-rules>>

Haeck P, 'Germany faces resistance in push to weaken AI rules' (21-04-2026) <<https://www.politico.eu/article/germany-stronger-ai-deregulation-brussels-eu-opposition/>>

Haeck P, 'Germany set to secure win for industry in AI talks' *Politico* (06-05-2026) <<https://www.politico.eu/article/germany-eu-ai-law-machinery-exemption-industrial-rewrite/>>

Henning M, 'EU clinches AI reform deal centring on machinery cuts' *Euractiv* (07-05-2026) <<https://www.euractiv.com/news/eu-clinches-ai-reform-deal-centring-on-machinery-cuts/>>

ASML, *ASML CEO Christophe Fouquet co-signed opinion piece with European technology companies* (2026)

Bertuzzi L, *EU policymakers fall short of agreeing on AI Act amendments* (2026)

Hacker P, Kilian R and Costas J, *"Simplifying" European AI Regulation - An Evidence-based Study*, (2025)

Rules of Procedure of the Commission [C(2000) 3614], L 308

Proposal for a regulation amending Regulations (EU) 2017/745 and (EU) 2017/746 as regards simplifying and reducing the burden of the rules on medical devices and in vitro diagnostic medical devices, and amending Regulation (EU) 2022/123 as regards the support of the European Medicines Agency for the expert panels on medical devices and Regulation (EU) 2024/1689 as regards the list of Union harmonisation legislation referred to in its Annex I, 2025/0404 (COD)

Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), 2025/0404 (COD)

Commission E, 'Simpler EU digital rules and new digital wallets to save billions for businesses and boost innovation*' (2025) <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2718> accessed 31-08-2026

Directorate-General for Communication EC, 'Commission staff' (2026) <https://commission.europa.eu/about/organisation/commission-staff_en> accessed 31-08-2026

Directorate-General for Communication EC, 'Communications Networks, Content and Technology' (2026) <https://commission.europa.eu/about/departments-and-executive-agencies/communications-networks-content-and-technology_en> accessed 31-08-2026

Directorate-General for Communication EC, 'Organisation of the European Commission' (2026) <https://commission.europa.eu/about/organisation_en> accessed 31-08-2026

Union POotE, 'Directorate-General for Communications Networks, Content and Technology (CNECT)' (2026) <<https://op.europa.eu/en/web/who-is-who/organization/-/organization/CNECT/CNECT>> accessed 31-08-2026

Jakub Skórczynski, PhD candidate at the University of Southern Denmark, Department of Law, Esbjerg, with research focusing on the relationship between the EU's horizontal data regulation and sector-specific data rules in the energy sector, particularly complex data-sharing arrangements such as data spaces.

Når er opplysninger anonyme? EDPB foreslår nye retningslinjer om anonymisering

Av Håvard Sveier Ottemo og Line Helen Haukalid

I en ny veileder klargjør EDPB at anonymitet ikke bare avhenger av datasettet, men også av hvem som har tilgang til opplysningene, hvilke identifikasjonsmidler som er tilgjengelige, og hvor sannsynlig det er at disse vil bli brukt. Veilederen presiserer også hvilke GDPR-forpliktelser som gjelder under anonymiseringsprosessen, og hvordan virksomheter bør vurdere, teste og dokumentere at opplysningene faktisk er anonyme.

Den 7. juli 2026 sendte EDPB *Guidelines 02/2026 on Anonymisation* for offentlig høring. Veilederen oppdaterer Artikkel 29-gruppens uttalelse 05/2014 om anonymisering i lys av nyere rettspraksis og den rettslige og teknologiske utviklingen. Den bygger særlig på EU-domstolens dom i sak C-413/23 P, EDPS mot SRB, og innebærer en tydelig presisering og videreutvikling av EDPBs syn på anonymitet. Høringsfristen er 30. oktober 2026.

EDPS mot SRB gjaldt personvernreglene for EUs institusjoner, men EDPB anvender dommens *resonnement* i sin analyse av anonymitet etter GDPR. I saken skulle opplysningsplikten vurderes på innstillingstidspunktet og fra den behandlingsansvarliges perspektiv. Fordi opplysningene da var personopplysninger for den behandlingsansvarlige, måtte de registrerte informeres om mottakerne. Dette gjaldt selv om opplysningene senere kunne være anonyme for mottakeren. Et sentralt poeng var altså at anonymitet må vurderes fra det relevante aktørperspektivet.



Håvard Sveier Ottemo

Anonymitet må vurderes fra riktig perspektiv

EDPB tar utgangspunkt i definisjonen av personopplysninger i GDPR artikkel 4 nr. 1 og stiller to spørsmål: (1) Er opplysningene «om» en fysisk person, og (2) er personen «identifisert eller identifiserbar»? Hvis svaret på ett av spørsmålene er nei, skal opplysningene anses som anonyme. Svaret kan variere mellom aktører: De samme opplysningene kan være personopplysninger for én aktør, men anonyme for en annen.

Ved bruk av databehandlere skal vurderingen foretas fra den behandlingsansvarliges perspektiv. Er opplysningene personopplysninger for den behandlingsansvarlige, må databehandleren behandle dem som personopplysninger selv om databehandleren ikke selv kan identifisere de registrerte. Den behandlingsansvarlige kan dermed ikke omgå GDPR ved å overlate behandlingen til en aktør med færre identifikasjonsmidler.



Line Helen Haukalid

Når er opplysninger «om» en identifiserbar person?

Opplysninger kan være «om» en person på grunn av sitt innhold, formål eller sin virkning. Tilknytningen trenger ikke være umiddelbart synlig, men kan avdekkes gjennom videre behandling. Også aggregerte opplysninger kan derfor være personopplysninger dersom de kan brukes til å utlede informasjon om enkeltpersoner.

Det neste spørsmålet er om personen er identifisert eller identifiserbar ved hjelp av midler som med rimelighet kan forventes brukt. Identifikasjon innebærer at personen kan skilles fra andre i en bestemt sammenheng på en måte som gjør det mulig å behandle vedkommende annerledes. Det er ikke nødvendig at én aktør alene råder over alle nødvendige opplysninger eller identifikasjonsmidler. Personen kan også være identifiserbar dersom opplysninger som flere aktører kontrollerer, med



Illustrasjon: Colorbox/ ChatGPT

rimelighet kan forventes kombinert. Ved vurderingen skal det tas hensyn til alle objektive faktorer som påvirker både tilgangen til identifikasjonsmidlene og sannsynligheten for at de faktisk vil bli brukt.

Manglende motivasjon for å identifisere personen er ikke i seg selv avgjørende. Et lovforbud kan tale for at et identifikasjonsmiddel ikke med rimelighet kan forventes brukt, med mindre det foreligger en konkret risiko for lovbrudd. Et kontraktsforbud har ikke samme vekt, men kan inngå i vurderingen.

GDPR gjelder frem til opplysningene er anonyme

At opplysningene er anonyme for mottakeren, fritar ikke avsenderen dersom denne fortsatt kan identifisere personene. Avsenderen må fortsatt behandle dem som personopplysninger og oppfylle sine forpliktelser etter GDPR.

Anonymiseringen må ha behandlingsgrunnlag etter artikkel 6 og eventuelt oppfylle et unntak etter

artikkel 9 nr. 2. Anonymisering kan dessuten være et moment i favør av den behandlingsansvarlige i en interesseavveining.

Den behandlingsansvarlige må også oppfylle åpenhetsforpliktelsene etter GDPR artikkel 5 nr. 1 bokstav a og artikkel 12–15 ved anonymiseringen. EDPB fremhever at de registrerte klart bør informeres om at personopplysningene vil bli behandlet for å fremstille anonyme opplysninger som deretter faller utenfor GDPRs virkeområde.

Anonymiseringsprosessen og testing av resultatet bør dokumenteres på en egnet måte, slik at den behandlingsansvarlige både kan påvise at anonymiseringsprosessen skjer i samsvar med GDPR og at anonymiseringen faktisk er effektiv. Dokumentasjonen bør oppbevares også etter at anonymiseringsprosessen er avsluttet.

To måter å vurdere anonymitet på

EDPB beskriver to tilnærminger til vurderingen av om anonymisering av personopplysninger har vært vellykket:

Den **kontekstuelle tilnærmingen** bygger på den rettslige analysen og tar hensyn til hvilke identifikasjonsmidler hver relevant aktør har eller kan få tilgang til og sannsynligheten for at midlene vil bli brukt.

” Anonymiseringsprosessen og testing av resultatet bør dokumenteres på en egnet måte, slik at den behandlingsansvarlige både kan påvise at anonymiseringsprosessen skjer i samsvar med GDPR og at anonymiseringen faktisk er effektiv.

Den **forenklede tilnærmingen** vurderer muligheten for reidentifikasjon uten å skille mellom aktørenes ulike muligheter til å få tilgang

til datasettet, tilleggsopplysninger og andre nødvendige ressurser. Vurderingen tar dermed utgangspunkt i om opplysningene kan knyttes til enkeltpersoner når alle relevante identifikasjonsmidler tas i betraktning, ikke hva den enkelte aktøren med rimelighet kan forventes å gjøre. Dette er ikke en alternativ rettslig standard, men et frivillig og mer forsiktig analyseverktøy.

Tilnærmingene kan kombineres. Ved begge undersøkes tre forhold: om datasettet inneholder en unik kombinasjon av opplysninger om én person (No Record Isolation), om opplysningene med sikkerhet eller høy sannsynlighet kan kobles til opplysninger om samme person i et annet datasett (No Linkage), og om det kan utledes spesifikke og meningsfulle opplysninger om en identifisert eller identifiserbar person (No Inference).

Eksempelvis kan et datasett inneholde opplysninger om alder, yrke, bosted og bevegelsesmønster:

- En opplysningskombinasjon – 47 år, tannlege og bosatt i en bestemt kommune – er unik i datasettet og gjelder én enkeltperson (brudd på No Record Isolation).
- Opplysningene kan kobles til en navngitt tannlege i et offentlig register (brudd på No Linkage).
- Bevegelsesmønsteret viser regelmessige besøk på en kreftklinikk og kan gi grunnlag for å utlede at personen mottar kreftrelatert behandling (brudd på No Inference).

Dersom ett eller flere kriterier ikke er oppfylt, betyr det ikke automatisk at opplysningene er personopplysninger. Bruddets betydning må vurderes nærmere for å avgjøre om opplysningene likevel kan anses som anonyme. Ved brudd på No Inference er EDPB strengere: Dersom kriteriet ikke er oppfylt under den kontekstuelle tilnærmingen, bør opplysningene ikke anses som anonyme fra minst ett relevant perspektiv.

EDPB går i veilederen særlig detaljert gjennom begge tilnærmingene og kriteriene, og gjennomgangen bør leses i sin helhet.

Hva betyr veilederen i praksis?

Veilederen innebærer neppe nye plikter, men tydeliggjør hva virksomheter må vurdere og dokumentere ved anonymisering.

For det første må virksomheten vurdere anonymitet i den konkrete sammenhengen. Det er ikke tilstrekkelig å undersøke datasettet isolert. Virksomheten bør også kartlegge hvem som kan få tilgang til opplysningene, hvilke tilleggsopplysninger

de har eller kan få tilgang til, og hvilke metoder de med rimelighet kan forventes å bruke for å identifisere enkeltpersoner.

For det andre må avsenderens og mottakerens perspektiv vurderes separat. Et datasett kan være anonymt for mottakeren, men fortsatt inneholde personopplysninger for avsenderen. Avsenderen må da fortsatt oppfylle sine GDPR-forpliktelser ved anonymiseringen og utleveringen.

For det tredje bør vurderingen dokumenteres og oppdateres dersom teknologien, tilgangen til tilleggsopplysninger eller andre relevante forhold endrer seg. Et datasett som er anonymt i dag, kan senere måtte anses som personopplysninger dersom reidentifikasjon blir tilstrekkelig sannsynlig.

Veilederen er fortsatt på høring, men viser hvordan EDPB tolker dommen i *EDPS mot SRB*, og gir virksomheter mer konkrete holdpunkter for anonymitetsvurderingen.

Håvard Sveier Ottemo, advokatfullmektig, Advokatfirmaet Wiersholms avdeling for teknologi, media, telekom og immateriell rett.

Line Helen Haukalid, Managing Associate, Advokatfirmaet Wiersholm.

Licensing works for AI – Do the licensing practices of Nordic copyright management organisations comply with the CRM Directive?

By Viveca Still

1. Introduction

This article examines whether Nordic collective management organisations (CMOs) license AI-related uses of copyright-protected content in a manner consistent with Directive (EU) 2019/790 (*DSM Directive*) and Directive 2014/26/EU (*CRM Directive*). The focus is not on whether the legislative framework is appropriate, but on whether current licensing practices comply with existing EU law.

While the precise scope of the text and data mining (*TDM*) exceptions in articles 3 and 4 of the DSM directive remains uncertain, in particular in relation to use for the training of generative AI models and the provision of subsequent AI services, some issues must be considered quite clear, such as the need for permission for including works and other subject matter protected by copyright (*protected content*) in the output of AI. On the other hand, it seems equally obvious that permission from rightholders is not required for uses clearly covered by copyright exceptions. The question therefore arises whether CMOs' practice of extending licences to uses covered by copyright exceptions complies with the licensing rules of the CRM Directive, in particular the duty to conduct negotiations in good faith.

2. The text and data mining exceptions in article 3 and 4 of the DSM directive

Before examining the licensing approaches of Nordic CMOs, let us first

look at the TDM exceptions in articles 3 and 4 of the DSM directive. Article 3 concerns TDM for the purpose of scientific research, whereas article 4 concerns TDM for any other purpose.

Article 3 is a mandatory exception that prevents contractual restrictions from undermining the possibility for research organisations and cultural heritage institutions to conduct TDM on content to which they have lawful access¹.

1 Article 3 para 1 states that Member States shall provide for an exception for reproductions and extractions made by research organisations and cultural heritage institutions in order to carry out, for the purposes of scientific research, text and data mining of works or other subject matter to which they have lawful access. The scope of application of article 3 is broad; it concerns all different types of protected subject matter, i.e. works, fixations of performances, phonograms, films, fixations of broadcasts, databases and the new press publishers right, which was introduced through the DSM directive. Article 3 also allows the retention of the copies made for TDM purposes, as it allows copies to be stored as long as necessary and used also for verification of research results. This in fact would also seem to allow giving access to the copies made in order to verify the results of a TDM process. However, such access may not be provided to the public, but must be restricted to persons that need such access in order to verify the research. The concept of "lawful access" is also quite broad, including not only licensed content but any content freely available on the internet (with the exclusion of pirated content).



Viveca Still

Its background lies in conflicts between the research community and publishers regarding the use of computational tools on licensed scientific publications². The purpose was not merely to create a defence against infringement claims, but to provide a genuine right to conduct TDM and prevent publishers from neutralising the exception through contractual or technical restrictions.

Although article 3 allows rightholders to apply measures necessary to protect the security and integrity of their systems, it significantly restricts their freedom to control how lawfully accessible content may be exported, analysed and retained for research purposes.

2 Regarding the background and purpose of article 3, see recital 10 of the DSM directive.

Article 4 follows a different logic. Unlike article 3, it does not prevent contractual arrangements that limit TDM. Most importantly, it allows rightholders to opt out by reserving rights *expressly* and in an *appropriate manner*. The exact requirements for such a reservation remain uncertain and will ultimately require clarification by the European Court of Justice (ECJ).

” The question therefore arises whether CMOs’ practice of extending licences to uses covered by copyright exceptions complies with the licensing rules of the CRM Directive, in particular the duty to conduct negotiations in good faith.

The distinction between Articles 3 and 4 suggests that Article 4 leaves considerably more room for service providers to structure their business models, including the deployment of proprietary TDM tools. Copies made under Article 4 may only be retained for as long as necessary for mining purposes. This prevents the indefinite retention and reuse of protected content. The scope of article 3 is also limited to a very special use case, that of scientific research. Taken together, these differences reflect the application of the three-step test.³

Article 4 was introduced to avoid the possibility of an *e contrario* interpretation of article 3 that reproduction of protected content necessary to perform TDM for other purposes than for research would require permission from the rightholders.

Contrary to the general approach to exceptions and limitations to copyright in the Infosoc-directive,

articles 3 and 4 of the DSM directive are mandatory exceptions that as a starting point provide little room of manoeuvre for Member States.

There are several safeguards in the DSM directive which are aimed at preserving freedom of information. Firstly, it is clarified in the definition of TDM that information retrieval or analysis of works are not in itself copyright relevant, but the exceptions and limitations to copyright in article 3 and 4 only cover reproductions and extractions made with the purpose of making it possible to analyse protected content through computational means. Secondly, regarding the new press publishers right, it is also clarified that copyright does not cover mere facts and that the new right is subject to the exceptions and limitations of the Infosoc directive, including the exception in the case of quotations for purposes such as criticism or review. This also has an impact on the interpretation of the TDM exceptions.

Thirdly, although search engines are not mentioned expressly, it is apparent that one of the main aims of article 4 is to enable search engines to continue to operate, as they are essential to the functioning of the internet. In practice they should be protected from claims of infringement of copyright as long as they fulfill the requirements of the directive, in particular do not index webpages excluded from indexing such as private areas (intranet or other areas with restricted access) and honor robot.txt and similar technical measures.

3. The room for manoeuvre left to Member States in relation to articles 3 and 4

There is little indication that Member States enjoy substantial discretion when implementing Articles 3 and 4. The DSM Directive requires Member States to introduce these exceptions. Although Article 4 is

formally labelled an ‘exception or limitation’, this does not imply freedom to fundamentally alter its operation. Its core structure consists of a TDM exception combined with an opt-out for rightholders⁴.

Recital 17 of the DSM directive states that Member States are not to provide for compensation for rightholders as regards uses under the text and data mining exceptions (in plurals) introduced by the Directive. This also suggests that Member States are expected to transpose the articles without modifying their *modus operandi*.

4. The application of the TDM exceptions to AI

The DSM Directive defines TDM as an automated analytical technique aimed at analysing digital text and data to generate information, including patterns, trends and correlations. TDM itself is not a copyright-relevant activity. Copyright becomes relevant only because reproductions of protected content may be required.

The TDM exceptions express the principle “a right to read is a right to mine”. The basic idea underlying Articles 3 and 4 is that reproductions made solely to analyse protected content should not affect its commercial exploitation.

As explained in recital 9 of the directive, TDM can also be carried out in relation to mere facts or data that are not protected by copyright, and in such instances no authorisation is required under copyright law. There can also be instances of TDM that do not involve acts of reproduction or where the reproductions made fall under the mandatory exception for temporary acts of reproduction provided for in the Infosoc-directive, which should continue to apply to TDM techniques that do not involve the mak-

3 DSM directive article 7.2.

4 Because of the opt-out-possibility, it is a merely a limitation.

ing of copies beyond the scope of that exception.

Text and data mining refers to an activity and shall apply notwithstanding the type of TDM tool or methodology applied. Examples of different TDM methodologies are statistical tools, search engines, machine-learning models and foundation models.

A key question is whether the TDM exceptions apply when analysing protected content with the help of AI, when training foundation models or AI systems and when creating outputs of AI.

It seems quite clear that articles 3 and 4 at least cover the reproduction necessary for providing the input to be analysed in an AI system. It is also very clear that the exceptions in articles 3 and 4 do not cover the output. This means that the reproduction, communication or making available to the public of output that includes protected content requires the authorization of the rightsholders.

The position regarding AI training is more complex. Training foundation models appears to satisfy the definition of TDM because it involves automated analysis of text and data to generate information and capabilities. Recital 18 further acknowledges that TDM supports the development of new applications and technologies. At the same time, copyright concerns may arise where protected content remains incorporated in ways that extend beyond what is necessary for analysis. Whether particular training practices fall inside or outside the TDM framework must therefore be assessed case by case and may ultimately require judicial clarification by the ECJ.

5. Licensing practices of Nordic copyright societies

Nordic CMOs have adopted different approaches to AI-related licensing. Some rely on ordinary collective licensing while others employ

extended collective licensing (ECL) mechanisms. The scope of the licences also varies considerably. Some focus on AI training, others on prompting, and some potentially extend to outputs.

The Swedish CMO for musical works STIM has introduced a licence covering rights required for certain AI models and services, although the repertoire covered remains limited⁵. In Finland, Teosto has not yet introduced comparable licensing but has amended its authorisation framework in preparation for AI-related licensing⁶. It is unclear whether their licensing conditions would also cover outputs generated by AI, although this possibility cannot be entirely excluded.

Kopinor in Norway has concluded an agreement with the National Library concerning the use of news content for training Norwegian and Sami language models⁷. The agreement is designed to facilitate public-interest language technology while excluding specialised services that would compete with media or news publishers. The agreement appears primarily concerned with training, and it is not entirely clear whether it also covers AI outputs to the extent that protected content may incidentally be included in the output.

Kopinor has adopted a cautious approach to licensing reproductions for educational purposes. Its agreement with universities and higher education institutions excludes machine-learning and generative-AI training unless supported by a separate legal basis⁸. A forthcoming pri-

vate-school agreement permits limited prompting of AI systems in closed environments while excluding systematic use for training internal or external AI solutions⁹. Similarly, the Bokhyllan agreement excludes the use of digitised cultural heritage collections as a basis for AI training without a specific licence and prohibits indexing by external search-engines.

In Denmark Tekst & Node has received approval from the Danish Ministry of Culture to provide an addition for prompting purposes to existing extended collective licences for reproduction of reprographic works¹⁰. The licences cover educational establishments and internal use in companies and other organisations. The licence conditions have not been published.

In Finland Kopiosto has added to its licences for reproduction or use for internal purposes in private sector organisations¹¹ as well as for municipalities and well-fare areas¹² a right to use works (text, pictures) for prompting in internal, secure AI systems. The licence does not allow for the use of generated content for external use or for prompting in other than internal, secure AI systems and does not allow, for instance, pictures to be modified with the help of AI.

Kopiosto offers in addition an add-on licence that allows for fine-tuning of AI systems for internal

5 <https://www.stim.se/nyheter/stim-lanserar-varldens-forsta-ai-licens-for-musik>.

6 <https://www.teosto.fi/tekoaly-oikeusluokka/>.

7 <https://kopinor.no/aktuelt/historisk-avtale-om-avisinnhold-til-kunstig-intelligens/>. The conditions of the agreement is found at <https://kopinor.no/wp-content/uploads/2026/02/Trening-ar-norske-sprakmodeller.pdf>.

8 This structure seems to indicate, that the agreement does not preclude the possibility for the TDM exceptions to be applied.

9 § 8 of the agreement, <https://kopinor.no/wp-content/uploads/2026/06/Privatskoler-2027.pdf>.

10 https://kum.dk/fileadmin/_kum/2_Kulturomraader/Ophavsret/Aftalelicens-godkendelser/Generelle/TekstNode_-_OHL_50_stk_4_jf_50_stk_2.pdf

11 <https://kopiosto.fi/lupaannppa/wp-content/uploads/sites/3/2025/10/Kopiointiluvan-lupaebdot-yritykset-ja-muut-yhteisot.pdf>

12 https://kopiosto.fi/wp-content/uploads/2022/06/Kopiointiluvan-lupaebdot_kunnat-ja-hyvinvointialueet.pdf



Illustration: Coulorbox/ChatGPT

use¹³. The licence is confined to protected content to which the organisation has legal access¹⁴ and provided that the finetuned AI system is only used within the organisation. The licence excludes a wide range of protected content such as

13 <https://kopiosto.fi/lupakauppa/wp-content/uploads/sites/3/2025/10/Sisaisen-tekoalyohjelman-bienosaamisen-lupaeh-dot-yritykset-ja-muut-yhteisot.pdf>

14 According to the agreement, “legal access” is based on subscription, agreement or purchase. The concept of legal access is thus more limited than the definition in the DSM directive, which specifically covers any protected content made available on the internet with the rightholders permission.

the collections of cultural heritage institutions, research reports and similar publications and content the use of which is based on a specific agreement or licence. Specifically excluded is the possibility to collect or record works with web scraping or corresponding data collection methods or use data sets collected by a third party for fine tuning. Specifically excluded is also the possibility to use protected content in whole or in part for TDM¹⁵.

15 It seems contradictory to prohibit TDM while licensing AI training. The relationship between these concepts have not been explained in conjunction with the agreement.

As these examples demonstrate, there are substantial differences in licensing strategies of CMOs. Unfortunately many CMOs don’t offer public access to the actual texts of the agreements for an in-depth analysis. Nevertheless, it seems plausible that in most (if not all) cases they do not license the use of protected content for training of general AI models or publicly accessible AI services. Such licensing can instead be expected to emerge

predominantly through direct contractual arrangements¹⁶.

6. Assessment under EU law

When assessing whether some of the agreements offered by the CMOs could be unlawful, an important question is whether a use is covered by an exception and whether that exception is mandatory.

To the extent agreements made by CMOs cover the output of AI, there do not seem to be any particular legal challenges, providing that the authorizations from the rightholders or the ECL arrangement of the country allows for such licences. Such use is not part of the TDM exception.

There might also be agreements that cover uses that are in the grey zone. Even though training of AI appears to fulfill the general requisites and the definition of TDM in the directive, there might be other reasons why the exceptions may not be applied (for instance if a copy is retained for an unlimited period of time).

Making copies necessary to analyse protected content (for example through prompting) seems to be part of the key area of the mandatory exceptions in article 3 and 4; that activity can clearly be considered to fulfill the principle of “a right to read is a right to mine”. But even in that case, the exception in article 4 is not applied if copyright has been reserved expressly and in an appropriate manner¹⁷.

Could a CMO be considered to have the capacity to represent rightholders in expressing an opt-out in accordance with article 4? In principle I don't see why not, provided that the CMO has been duly man-

dated to do so and possesses the practical means to implement it.

However, practical difficulties arise insofar as CMOs don't maintain comprehensive databases of protected content and lack the technical mechanisms that would make work-specific opt-outs readily identifiable. The structure of Article 4 instead seems to assume that the commercial actor placing content on the market is typically best positioned to reserve rights.

Another question is whether Member States may effectively replace TDM exceptions with extended collective licensing arrangements. Article 12 in the DSM directive recognises licensing mechanisms with extended effect but also states that it does not affect other provisions of Union law, including provisions containing exceptions and limitations. In my view, this cannot be interpreted as allowing Member States to transform mandatory exceptions into permission-based licensing schemes.

7. The CRM directive requires CMO's to act responsibly in their licensing activities

The CRM Directive recognises the gatekeeper role of CMOs and therefore requires licensing activities to be conducted on objective, reasonable and non-discriminatory terms. Negotiations must be carried out in good faith and tariffs must reflect the economic value of both the rights and the licensing services provided.

Against this background, concerns arise where CMOs attempt to license activities already covered by mandatory TDM exceptions. Acting in good faith arguably requires in-

forming users when a particular use does not require authorisation. Efforts to present statutory exceptions as licensable rights sit uneasily with the objectives of the CRM Directive.

Particular concerns arise in relation to some prompting licences, where users may effectively be paying for uses that are exempted from copyright. As a minimum CMOs would be wise to cautiously draft the agreements to only complement existing exceptions, thus ensuring that the agreements do not contravene the possibilities to use a work in accordance with a copyright exception.

The current practice may also create difficulties for rightholders. If broad rights-reservation statements by CMOs are assumed to constitute valid opt-outs under Article 4, rightholders wishing to permit TDM may have to withdraw from collective arrangements in order to ensure that their works remain available for TDM. Such an outcome would run counter to the original logic of Article 4.

However, it remains to be seen whether users, rightholders or supervising authorities will intervene in the licensing practices of CMOs, to the extent made possible in the national laws transposing the CRM directive, or if the CMOs themselves correct their current practices to reduce legal risks.

Viveca Still, LL.D., Ministry of Finance, Senior Ministerial Adviser, Legal Affairs. Finnish editor.

¹⁶ In the music sector Spotify is said to negotiate a licensing agreement related to AI with the majors, <https://www.bbc.com/news/articles/cn7emv83edjo>.

¹⁷ Contrary to this, in relation to article 3 it is clear that no room for licensing solutions exist under that TDM exception.



Tysk avgjørelse om trening av AI på musikkverk: GEMA vs Suno

1. Innledning

Den 31. juli 2026 avsa tingretten i München (Landgericht München I) dom i en sak anlagt av den tyske rettighetsorganisasjonen GEMA mot den amerikanske leverandøren Suno Inc (sak 42 O 763/25). Retten fant at komposisjonen til seks angitte sanger var innkodet i Sunos AI-modell og nedla forbud mot fire konkrete handlinger knyttet til disse sangene:

- Reproduksjon gjennom trening av AI-modellen i USA
- Reproduksjon gjennom innkoding i AI-modellen i Tyskland
- Reproduksjon og tilgjengeliggjøring av innhold generert fra AI-modellen
- Tilgjengeliggjøring for allmenheten ved å tilby AI-modellen

Den tyske førsteinstansen tok også stilling til trening av AI-modellen som utelukkende hadde funnet sted i USA. Saken åpner således for en diskusjon om jurisdiksjon ved trening av AI-modeller i andre land slik vi også har sett i tidligere saker diskutert i denne spalten. Den samme underinstansen har tidligere avgjort en lignende sak mellom GEMA og OpenAI i november 2025 som gjaldt et tekst-til-tekst verktøy. Dette er imidlertid den første saken jeg kjenner til i Europa som konkret gjelder et generativt AI-verktøy for musikk.

Dommen er ikke rettskraftig og forventes å bli anket videre til neste instans, Oberlandesgericht München. Dette tilsvarer vår lagmannsrett. Saken reiser også EU-rettslige spørsmål som vi kanskje vil se fremmet for EU-domstolen for uttalelse før saken blir endelig avgjort.

2. partene og tvisten

GEMA er et vederlagsbyrå som kan sammenliknes med vårt norske TONO, men som også behandler såkalte mekaniske rettigheter (eksemplarframstilling). Det fremgår direkte av navnet som GEMA er en forkortelse for: *Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte*. Både TONO og GEMA representerer den praktiske forlengelsen av EUs direktiv om kollektiv forvaltning. Ettersom disse er implementert gjennom sine respektive nasjonale lovverk, er det likevel praktiske og rettslige forskjeller på hvordan disse fungerer. Som det vil fremgå lenger ned i denne saken reiste den tyske saken et spørsmål om jurisdiksjon over AI-trening som ble utført i USA. Dette ble løst under en særlig vernetingsregel i den tyske loven *Gesetz über die Wahrnehmung von Urheberrechten und verwandten Schutzrechten durch Verwertungsgesellschaften*. Det norske motstykket er vår lov om kollektiv forvaltning om opphavsrett. Disse to lovene er ikke

identiske, og det er ikke gitt at utfallet av jurisdiksjonsspørsmålet ville ha blitt det samme under norsk rett.

GEMA har vist både evne og vilje til å ta opp kampen mot større internasjonale aktører tidligere. I Tyskland var YouTube i en lang periode blokkert for filmer som inneholdt musikk uten rettighetsklaring. Bakgrunnen var en lisensavtale med GEMA som utløp i 2009. Partene kom ikke til enighet om en ny lisensavtale, og dette utløste flere juridiske tvister mellom GEMA og YouTube. Brukere i Tyskland fikk etter hvert opp en tekstboks med følgende beskjed "This video is not available in Germany because it may contain music for which GEMA has not granted the respective music rights". Denne meldingen ble i seg selv gjenstand for en tvist, ettersom GEMA mente at skylden for blokkering urettmessig ble tillagt GEMA. Det hele endte med et forlik i 2016 der YouTube fikk gjøre sine videoer tilgjengelig i Tyskland.

Suno Inc. er et amerikansk selskap registrert i Delaware. Suno tilbyr en AI-tjeneste som produserer avspillbare sanger basert på korte tekstinstruksjoner (prompts) fra brukerne. AI-tjenesten har blitt levert i ulike versjoner. Saken for tingretten i München gjaldt tidligere versjoner, mens Suno nå har sluppet en versjon V6. Det er en utfordring

med saker som gjelder trening av AI-modeller at ulike versjoner vil kunne være basert på ulike metoder og kildedata, som igjen innebærer at det kan være vanskelig for rettighetshavere å vite hvordan den ene modellen skiller seg fra den andre. Samtidig ligger det i dette at en rettslig prosess som kan ta flere år gjennom ulike rettsinstanser vil ha kunne ha liten aktualitet når endelig avgjørelse foreligger. Leverandøren vil i mellomtiden kunne ha endret treningsprogrammet eller andre egenskaper ved AI-modellen som innebærer vesentlige endring av situasjonen overfor rettighetshaverne. Suno har vært involvert i flere andre rettstvister, og har sett pågang fra blant annet Sony, Universal, Warner og den danske motparten til TONO og GEMA: Koda.

Saken gjaldt komposisjonene for seks konkrete verk: «Atemlos durch die Nacht», «Daddy Cool», «Rasputin», «Big in Japan», «Forever Young» og refrenget i «Mambo No. 5». GEMA fremmet ikke krav under henvisning til selve sangtekstene, utøver- eller produsentrettigheter. Saksøkers krav i saken var rettet mot fire av de seks angitte verkene, der det ble krevd forføyning, ytterligere opplysninger og erstatning.

Det vesentlige av faktum i saken var ubestridt. Det var slått fast at Suno hadde trent sine modeller i USA på flere millioner ulike innspillinger av ulike musikkverk. De seks verkene som var trukket frem av GEMA inngikk i dette treningsmaterialet. Suno hadde hentet verkene fra YouTube ved bruk av såkalt «streamripping», som innebærer at innholdet lastes ned utenom plattformens nedlastingssperre. YouTube benytter blant annet et såkalt «rolling cipher» som innebærer at hvert enkelt video deles opp i en rekke mindre filer med ulike rullerende URL-adresser som gjør det vanskeligere for alminnelige brukere å laste ned en video.

Suno kodet det enkelte verk med metadata om blant annet tittel, sjan-

ger og sangtekst. Deretter inngikk verket i treningsmaterialet til AI-modellen for Suno versjon 3.5 og versjon 4. Jeg har i en tidligere artikkel i Lov & Data nr. 164 4/2025 «AI på treningsrommet – Getty Images vs. Stability AI Limited» beskrevet hvordan såkalte vekter inngår ved AI-trening. Suno brukte en tilsvarende metode tilpasset for musikkverkene. Det enkelte verk kombinert med metadata blir dekonstruert ned til mindre komponenter eller tokens. Dette omtales gjerne som tokenisering. En del av denne prosessen innebærer en vesentlig grad av komprimering ved det som kalles kvantisering. I praksis avrundes de aktuelle verdiene ned til et begrenset antall nivåer som inneholder mindre informasjon enn utgangspunktet. I dommen sammenligner tingretten dette med koding av musikk fra en CD-plate til MP3-format, der resultatet er en komprimert versjon av originalen. Det er dette materialet AI-modellen trenes på. Gjennom denne treningen dannes såkalte vekter, som innebærer innkoding i AI-modellen. Treningen skjer altså på et bredt grunnlag av komprimerte enheter, og innebærer en form for innlæring og memorering. Som en del av denne prosessen vil AI-modellen innta større eller mindre deler av innholdet av hvert enkelt originalverk.

3. Rettens vurdering

Retten la til grunn at de aktuelle AI-modellene var lagret på servere som rent fysisk var plassert i Tyskland. Når en bruker genererte sanger fra Suno ble disse midlertidig lagret på lokale servere nærmere bruken. Dette skulle gi raskere og mer stabil overføring til brukeren. GEMA hevdet at det genererte materialet viste at de seks påberopte sangene var lagret i selve modellen. Det var for store likheter mellom disse sangene og innholdet som ble publisert av de aktuelle AI-modellene. Suno nektet for at det forelå noen slik lagring, og fremholdt at det kun var snakk om matematiske mønstre som ikke kunne inneholde noen relevant andel av treningsdataene. I den grad det var noen likhet måtte dette ligge på brukeren, ikke på Suno. Suno viste også til flere andre grunnlag for hvorfor det ikke kunne foreligge noen rettslig relevant lagring fra Sunos side.

Dommeren konkluderte med at verkene rent faktisk var fiksert i selve AI-modellen. Med støtte i teknisk litteratur på området konkluderer retten med at en AI-modell memorerer et verk når det ikke bare trekkes ut mønstre og sammenheng, men også en del av selve innholdet fra verket selv (se dommens avsnitt 243 flg). Etter rettens vurdering er det ikke avgjørende hvor mye som la-



Illustrasjon: Coulorbox/ChatGPT

gres, men heller hva som lagres. Det legges altså en kvalitativ heller enn kvantitativ vurdering til grunn. Dette følger også av at det er benyttet en kvantiseringsmodell som beskrevet ovenfor, der verket i praksis komprimeres. Det er verdt å merke seg at i den tidligere omtalte saken mellom GEMA og OpenAI la tingretten til grunn at det var snakk om en fullstendig lagring av tekst, så lempes det altså her tilsynelatende noe på kravet for lydinformasjon.

Retten ser også på sammenhengen mellom brukerens forespørsel (prompt) og innholdet som blir generert fra AI-modellen. Selv om trykksterke stavelser kan forventes på trykksterke taktslag er ikke dette bestemmende for melodiens form. Det vil altså foreligge en stor grad av variasjonsmuligheter for AI-modellen. Eksempler fra GEMA viste imidlertid at melodiene som ble generert så ut til å stamme fra de aktuelle underliggende sangene. Der Suno anførte at eksemplene fra GEMA var tendensiøse og var egnet til å fremprovosere de ønskede resultatene, konkluderte retten i motsatt retning. Det ble vist til at prompts fra GEMA var gjentatt flere ganger, og at dette hang sammen med at forespørsler, parametre og den distribuerte sannsynlighet knyttet opp mot innholdsproduksjonen ville være lik. Dermed holdt det i prinsippet å vise til et enkelt resultat for hvert enkelt verk. Retten avslo i denne sammenheng også Sunos begjæring om å innkalle en sakkyndig som kunne gjennomgå eksemplene. En slik ekspert kunne kanskje ha sagt noe mer om betydningen av de prompts som GEMA hadde benyttet i sine eksempler. Her hadde nemlig GEMA benyttet hele sangtekster, og i tillegg helt konkret bedt om å få musikken fra samme tidsperiode og med stemmer som tilsvarte originalverkene. Det tok da fra 4 til 176 forsøk å fremskape musikk tilsvarende originalverkene. En ekspert på området kunne kanskje ha gått noe dypere inn i spørsmålet om graden av varia-

sjon som gjenstår og hvor ledende et prompt kan være for å avgjøre inngrep i opphavsretten.

Tingretten konkluderte etter dette med at fiksering i denne forstand var å regne som eksemplarframstilling etter InfoSoc-direktivet og tysk nasjonal rett. Retten sammenlignet data lagret i AI-modellen med en progressivt og spredt lagret JPEG-bilde-fil eller de tap av data som skjer med lagring i komprimerte formater som MP3. Selv om slike analogier kan være godt egnet for å beskrive noen av de tekniske prosessene er det likevel ingen av disse som fanger opp den metoden som helt konkret benyttes ved trening av AI-modeller. Her ligger det kanskje en sårbarhet i tingrettens avgjørelse opp mot en potensiell ankeomgang. Jeg har ovenfor vist til artikkel i *Lov & Data* i saken Getty Images mot Stability AI. I denne engelske saken kom High Court til et motsatt resultat basert på omfattende ekspertbevis ført for retten. Her er det riktignok snakk om ulike AI-modeller og ulikheter i faktum. Det tekniske området retten er inne på her er likevel så nytt og komplisert at det kunne ha vært ønskelig å ha fått tilført noe mer teknisk kompetanse til rettens vurderinger.

Saken inneholder flere drøftelser og vurderinger, men jeg velger å løfte frem spørsmålet om treningen av AI-modellen som foregikk i USA. Tysk rett har en bestemmelse i sin lov om kollektive vederlagsbyråer som samordner krenkelser ved en enkelt domstol. Tingretten så hen til denne bestemmelsen i kombinasjon med lovens jurisdiksjonsbestemmelse som åpner for å samle flere krav for en felles domstol. Retten landet deretter på at også treningen som skjedde i USA lå under tingrettens kompetanse i den aktuelle saken. Det ble også lagt vekt på at rettighetshaverne er tyske og at det var en nær sammenheng mellom handlingene i USA og Tyskland.

Det er viktig at det her skilles mellom på den ene siden det som er lagret i AI-modellen og innholdet som

AI-modellen genererer, og på den andre siden selve treningen av AI-modellen. De første to punktene var direkte knyttet opp mot Tyskland. De to versjonene det var snakk om var begge lagret i Tyskland. Innholdet ble i tillegg direkte generert av disse versjonene av AI-modellen mens disse befant seg i Tyskland. Når det gjelder treningen skjedde det imidlertid som beskrevet ovenfor i USA. Dette var handlinger som var utført i USA, og det var ikke åpenbart at det kunne skje noen krenkelse av tysk opphavsrettslov i USA. Der-som saken blir anket vil dette være et spennende punkt å følge videre i ankesaken. Den aktuelle bestemmelsen om å samordne jurisdiksjon for vederlagssakene skyldes nok mer hensynet til prosessøkonomi enn å avklare den internasjonale rekkevidden til GEMA. Dersom denne hjemmelen ikke er dekkende for trening som skjer i USA vil det hjelpe lite å vise til at GEMA er tysk og at dette taler for tysk verneting. Det er grunn til å stille spørsmål om saksøkers nasjonalitet skal tillegges så stor vekt i et spørsmål internasjonal jurisdiksjon for tingretten i München.

Retten forbød fire handlinger knyttet til de seks verkene GEMA hadde vist til:

Eksemplarframstilling for trening (inkludert USA), memorering i AI-modellen i Tyskland, overføring til allmennheten ved å tilby AI-modellen og eksemplarframstilling og overføring gjennom generert innhold.

Suno ble pålagt en egen informasjonsplikt i tråd med GEMAs påstand og erstatningsansvar. Beløpet for erstatningen er p.t. ikke fastsatt. Som nevnt er dommen ikke rettskraftig, og det er forventet at Suno anker til neste instans. Det kan nevnes at saken mellom GEMA og OpenAI omtalt ovenfor allerede er anket til Oberlandesgericht München.

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

CompLex 1/26 – Formålsbegrensningsprinsippets betydning i forbindelse med kontrolltiltak



Illustrasjon: colourbox.com / UiO

Denne utgaven handler om betydningen av formålsbegrensningsprinsippet i personvernforordningen ved arbeidsgivers bruk av kontrolltiltak.

Forfatter: Aleksa Bohlin, 2026

Oslo: Universitetet i Oslo, Juridisk fakultet,

Senter for rettsinformatikk 2026, 1/2026.

ISSN 2703-8777 Complex (online)

Den første delen av fremstillingen inneholder en analyse av hvilke krav som stilles til formålsangivelsen ved innsamling av arbeidstakernes personopplysninger til kontrollformål. Den andre delen inneholder en drøftelse av i hvilken grad arbeidsgi-

vere kan bruke allerede innsamlede personopplysninger til nye kontrollformål som ikke var spesifisert på innsamlingstidspunktet. Fremstillingen er særlig rettet mot problemstillinger i arbeidslivet, men har også overføringsverdi til andre områder hvor spørsmål om formålsangivelse og viderebehandling av personopplysninger kan oppstå.

Les hele utgivelsen på *CompLex* 1/26 ([pdf](#))

Omtalen er hentet fra: <https://www.jus.uio.no/jfp/forskning/publikasjoner/complex/2026/complex-1-26.html>

CompLex 5/25 – Personvern og integrert kunstig intelligens



Illustrasjon: colourbox.com / UiO

En studie av arbeid med etterlevelse av personvernlovet ved implementering av Microsoft 365 Copilot

Forfatter: Aksel Mellingen

Oslo: Universitetet i Oslo, Juridisk fakultet,

Senter for rettsinformatikk 2025, 5/2025.

ISSN 2703-8777 Complex (online)

Denne utgaven av ComLex omhandler det generative KI-verktøyet Microsoft 365 Copilot, og hvordan det kan utfordre personvernet i virksomheter som tar det i bruk. Formålet er å bidra til et kunnskapsgrunnlag som kan sikre tryggere implementering av Copilot og andre lignende systemer. Utgaven tar utgangspunkt i offentlig forvaltning,

og inneholder en casestudie fra Navs implementering av Copilot. Resultatene vil likevel også være relevant for andre virksomheter som er underlagt det europeiske personvernregelverket.

Denne utgaven av CompLex er skrevet som en masteroppgave. Masteroppgaven vant ISACA-prisen for beste masteroppgave i 2025.

Les hele utgivelsen på *CompLex* 5/25 ([pdf](#))

Omtalen er hentet fra: <https://www.jus.uio.no/jfp/forskning/publikasjoner/complex/2025/complex-5-25---personvern-og-integrert-kunstig-int.html>



Delphi

Klara Thyren

EU-domstolen klargör kring svenska undantag från GDPR och Integritetsskyddsmyndigheten vägleder om streaming av barn- och ungdomsidrott

Utgivningsbevis räcker inte för undantag från GDPR

Den 9 juli 2026 meddelade EU-domstolen dom i det så kallade "Lexbase-målet" (C-199/24). Av domen följer att ett utgivningsbevis, och det grundlagsskydd enligt yttrandefrihetsgrundlagen som följer därav, inte i sig är tillräckligt för att undanta personuppgiftsbehandling från GDPR.

Lexbase är en databas som drivs av Legal Newsdesk Sweden AB. Mot betalning kan vem som helst söka på enskilda personer som åtalats i svenska domstolar för att ta del av domar. Käranden, i domen benämnd "ND", dömdes för brott 2011 och begärde att få sina uppgifter raderade – men företaget bakom tjänsten gjorde inte detta omedelbart, utan först senare enligt deras gallringsrutin. ND yrkade skadestånd om 300 000 kronor för överträdelse av dataskyddsförordningen vid Attunda tingsrätt. Företaget bakom tjänsten bestred käromålet med hänvisning till att GDPR inte var tillämpligt, eftersom Lexbase

omfattades av utgivningsbevis. Tingsrätten begärde förhandsavgörande från EU-domstolen för att få klarhet i vad som faktiskt gäller.

Undantagen i GDPR – vad gäller egentligen?

Enligt artikel 85.1 GDPR ska medlemsstaterna, i lag, förena rätten för den personliga integriteten med yttrande- och informationsfriheten. Artikel 85.2 GDPR ger medlemsstaterna en uttrycklig möjlighet att göra undantag från stora delar av förordningen (kapitel II–VII och IX), men bara om det gäller behandling för journalistiska ändamål, alternativt akademiskt, konstnärligt eller litterärt skapande, och bara om undantagen är nödvändiga för att skapa en balans mellan integritet och yttrande- och informationsfriheten. EU-domstolen slår i domen fast att artikel 85.1 GDPR inte i sig ger medlemsstaterna rätt att införa avvikelser utöver det som tillåts i artikel 85.2 GDPR. Till följd av detta kan Sverige inte undanta verksamheter från GDPR enbart med

hänvisning till yttrandefriheten om behandlingen inte sker för något av de ändamål som anges i GDPR – det vill säga för journalistiska, akademiska, konstnärliga eller litterära ändamål.

Vad krävs för att det ska vara av "journalistiska ändamål"?

EU-domstolen anger att begreppet journalistiska ändamål visserligen ska tolkas brett, men att det inte omfattar all spridning av yttranden. Tre förutsättningar måste vara uppfyllda för att behandlingen ska anses ske för journalistiska ändamål:

1. Det aktuella materialet ska vara föremål för visst redigerings- eller bearbetningsarbete innan publicering;
2. Publiceringen ska ske med iakttagande av yrkesetiska och pressetiska regler för journalister, eller åtminstone med utgångspunkt i en redaktionell linje; och
3. Påståenden gällande fakta och omständigheter i det relevanta materialet ska granskas innan publicering.

I Lexbase-fallet saknades de tre förutsättningarna ovan. Att bara lägga ut obearbetade brottmålsdomar räcker alltså inte enligt domstolens bedömning. EU-domstolen förtydligar samtidigt att varken det faktum att tjänsten bedrivs mot betalning på internet, eller att personuppgifterna avser brottmålsdomar, i sig utesluter att behandlingen *kan* ske för journalistiska ändamål.

GDPR:s rättsmedel kan inte uteslutas av grundlagsskyddet

Enligt den svenska ordning som Attunda tingsrätt beskrev i sin begäran om förhandsavgörande har den registrerade, när GDPR till följd av grundlagsskyddet inte varit tillämplig, varit hänvisad till förtalsrättsliga rättsmedel. EU-domstolen klargör att en sådan ordning inte får innebära att de rättsmedel som följer av GDPR sätts ur spel. Kapitel VIII i förordningen – som innehåller rätten att klaga till tillsynsmyndigheten (artikel 77), rätten till domstolsprövning (artiklarna 78 och 79) och rätten till skadestånd (artikel 82) – ingår inte bland de kapitel som får undantas enligt artikel 85.2. Dessa rättsmedel får därför inte uteslutas genom nationell reglering.

Medlemsstaterna får bestämma de processuella formerna för hur rättsmedlen utövas, men de kan inte ställa upp andra materiella villkor än de som följer av GDPR.

Vad innebär domen i praktiken?

Domen innebär ett viktigt klargörande av den rättsliga bedömningen av söktjänster som Lexbase och andra databaser med frivilligt utgivningsbevis. För verksamheter som tillhandahåller likartade tjänster finns det nu i praktiken tre alternativ: anpassa verksamheten så att den uppfyller kraven för journalistiskt ändamål (bearbetning, redaktionell linje och pressetik), säkerställa att behandlingen i övrigt uppfyller GDPR krav, inklusive kraven på rättslig grund och behandling av uppgifter om lagöverträdelse, eller



Illustration: Coulorbox/ChatGPT

upphöra med publiceringen. Att hänvisa till utgivningsbevis eller grundlagsskydd räcker inte.

För enskilda som fått sina brottmålsdomar publicerade på liknande plattformar innebär domen ett förtydligt och i praktiken stärkt skydd. Ett utgivningsbevis är inte i sig tillräckligt för att sätta GDPR ur spel, och den registrerade får inte vara hänvisad enbart till förtalsrättsliga vägar.

Det återstår att se hur målet utvecklas vid Attunda tingsrätt.

Integritetsskyddsmyndigheten ("IMY") publicerar ny vägledning om streaming av barn- och ungdomsidrott

Streaming av barn- och ungdomsidrott har blivit allt vanligare. Streaming kan fylla många praktiska funktioner: familjemedlemmar som bor långt bort kan följa matcher på distans, tränare kan spara klipp för coachning och klubben kan dra in pengar till lagkassan. Samtidigt finns vissa nackdelar och risker. Enligt

vägledningen har barn vittnat om att de känner sig övervakade och att prestationspressen ökar. Barn med skyddad identitet riskerar att exponeras. Därtill har barn ett särskilt starkt skydd för sina personuppgifter enligt GDPR. IMY har därför publicerat en vägledning som behandlar sådant som är viktigt att ta hänsyn till vid en bedömning av vad som är tillåtet.

Vem ansvarar för streamingen?

En central del av vägledningen rör ansvarsfördelningen. IMY understryker att de faktiska förhållandena avgör vem som är personuppgiftsansvarig, inte vad som står i avtalet. Om en förening sköter hela kedjan själv (kameran, sändningen, publiceringen) är den ensam ansvarig. Antas ett produktionsbolag som bara agerar på föreningens instruktioner blir det ett biträdesförhållande. Bestämmer båda aktörer gemensamt om ändamål och medel uppstår i stället ett gemensamt personuppgiftsansvar.

Särskild uppmärksamhet ägnas kommuners roll som arenaägare. Att en kommun tillåter att en kame-
ra monteras i en idrottshall, eller
ställer begränsande villkor för hur
hallen får användas, gör inte i sig
kommunen till personuppgiftsan-
svarig. Kommunen måste aktivt ha
bestämt varför och hur streamingen
ska genomföras för att ansvar ska
uppstå.

Vilka rättsliga grunder är aktuella?

Vägledningen pekar ut tre rättsliga grunder som i praktiken kan kom-
ma i fråga.

Den första är samtycke, som innebär att varje filmad person (eller dess vårdnadshavare) godkänner sändningen. IMY rekommenderar att vårdnadshavarens samtycke alltid inhämtas för barn som inte ännu har fyllt 13 år. Samtycke är dock svårt att använda i lagsporter: om ett enda barns nej innebär att hela matchen inte kan streamas riskerar både barn och föräldrar att känna sig pressade att säga ja, och då är samtycket ogiltigt. Samtycke lämpar sig därför enligt vägledningen bäst för individuella sporter med få deltagare.

Den andra rättsliga grunden är berättigat intresse (intresseavvägning), där aktören visar att dess intresse av att streama väger tyngre än intrånget i barnens integritet. Tre steg krävs: (i) att identifiera ett berättigat intresse, (ii) att visa att streamingen är nödvändig för att uppnå

intresset, och (iii) att väga intresset mot barnens integritetsintresse.

Vägledningen ger inte någon exakt åldersgräns för när streaming är tillåten, men en tydlig skala framträder: yngre ålder, idrott på lägre nivå, obegränsad publik och inspelningar som sparas i efterhand talar för starkare integritetsskydd. Högre ålder, elitnivå och konkreta skyddsåtgärder – såsom åtkomstbegränsningar, fördröjd sändning, utzoomad filmning, eller enbart livesändning – kan skapa större utrymme.

Den tredje grunden är uppgift av allmänt intresse, som framför allt kan bli aktuell för kommuner. Om en kommun får personuppgiftsansvar för streamingen anger IMY att det inte är lämpligt att grunda behandlingen på samtycke eller intresseavvägning. Kommunen måste i stället undersöka om behandlingen är nödvändig för att utföra en uppgift av allmänt intresse. Uppgiften måste ha stöd i lag eller annan författning, och ju större integritetsintrånget är, desto mer preciserat måste det rättsliga stödet vara. IMY pekar bland annat på att kommunallagen ger kommuner rätt att hantera frågor av allmänt intresse, vilket omfattar exempelvis drift av fritids- och idrottsanläggningar. Kommunen måste dessutom bedöma om streamingen är nödvändig för att utföra uppgiften och proportionerlig i förhållande till det mål som eftersträvas. I den bedömningen påverkar bland annat barnens ålder, sändningens utformning och vilka skyddsåtgärder som vidtas.

Undantag – när gäller inte GDPR?

Vägledningen pekar ut tre situationer där GDPR helt eller delvis inte blir tillämplig. Filmning för rent privat bruk, exempelvis en förälder som filmar och skickar till mor- och farföräldrar, kan omfattas av det så kallade privatundantaget, men så fort filmen publiceras för en obegränsad krets gäller GDPR. Vidare kan sändningar med grundlagsskydd, exempelvis via utgivningsbevis, undantas från GDPR i den del som omfattas av grundlagsskyddet. Undantaget för journalistiska ändamål kan aktualiseras om det centrala syftet med sändningen är att sprida information till allmänheten i journalistisk form.

Avslutande kommentar

Vägledningen visar att frågan inte kan reduceras till om barn- och ungdomsidrott ”får” streamas eller inte. Det handlar om en bedömning i varje enskilt fall som omfattar bland annat ansvarsfördelning, rättslig grund och att beakta barnens ålder, idrottens nivå, sändningens räckvidd och de skyddsåtgärder som vidtagits. Vägledningen ger inga generella svar på när streaming är tillåten – men den ger ett ramverk som relevanta aktörer kan ta sig igenom innan streaming inleds.

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



Gorrissen Federspiel

Tue Goldschmieding

Nyt om persondataret i Danmark

Arbejdsgiver videregav personlige oplysninger til tredjemand

Det danske Datatilsyn (»Datatilsynet«) offentliggjorde den 9. april 2026 deres afgørelse om en arbejdsgivers videregivelse af personoplysninger til en tredjepart. Sagen blev behandlet under journalnummer 2025-31-1972.

En medarbejder og arbejdsgiver var i en arbejdsretlig tvist, hvor medarbejderen blev repræsenteret af sin fagforening. I forbindelse med tvisten mellem parterne videregav arbejdsgiveren personoplysninger til en tredjepart, herunder oplysninger om den tidligere medarbejders fagforeningsmæssige tilhørsforhold. Datatilsynet skulle vurdere, om videregivelsen til tredjemand var nødvendig til behandling af den arbejdsretlige tvist.

Efter Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«) artikel 6, stk. 1, litra f, kræves det, at videregivelse af personoplysninger følger en legitim interesse, medmindre den registreredes rettigheder interesser eller grundlæggende rettigheder og frihedsrettigheder går forud herfor. GDPR artikel 9, stk. 2, litra f, foreskriver, at nogle personoplysninger som fagforeningsmæssige tilhold kan behandles, såfremt de behandles til eksempelvis at fastlægge et retskrav.

Datatilsynet fandt, at arbejdsgiverens videregivelse af personoplys-

ninger forfulgte en legitim interesse til behandlingen af den arbejdsretlige tvist. Tredjepart i sagen var en rådgiver, der bistod arbejdsgiver i parternes tvist, herunder med rådgivning om betydningen af den tidligere medarbejders ansættelseskontrakt. Derudover blev tredjeparten kun bekendt med de personoplysninger, der var relevante for tvisten.

Endvidere fandt Datatilsynet, at det var legitimt at dele oplysninger om den tidligere medarbejders fagforeningsmæssige tilhold. De lagde vægt på, at medarbejderen lod sig repræsentere af fagforeningen, og at det generelt var en relevant oplysning at dele med en rådgiver, der blandt andet skulle rådgive om et eventuelt retskrav.

Det centrale i sagen var, at parterne stod i en arbejdsretlig tvist, og at den tidligere medarbejder lod sig repræsentere af sin fagforening. Dermed illustrerer afgørelsen, at i sådanne konkrete tilfælde kan det være legitimt at viderelede personoplysninger til en tredjepart.

Læs Datatilsynets afgørelse her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2026/apr/arbejdsgivers-videregivelse-af-personoplysninger>

Datatilsynet meddeler påbud til Aalborgs Kommune for manglende sletning af personoplysninger

Det danske Datatilsyn (»Datatilsynet«) meddelte den 4. maj 2026 Aal-

borg Kommune (»Kommunen«) påbud om at bringe Kommunens sletning af personoplysninger i overensstemmelse med GDPR. Sagen er behandlet under journalnummer 2026-432-0055.

Datatilsynet indledte den 10. april 2026 en undersøgelse af egen drift på baggrund af presseomtale af Kommunens manglende sletning af personoplysninger. Datatilsynet fandt, at Kommunen overtrådte GDPR artikel 5, stk. 1, litra e, om opbevaringsbegrænsning og artikel 5, stk. 2, om ansvarlighed, og meddelte Kommunen påbud om at kortlægge sine systemer med henblik på sletning, straks slette de personoplysninger, der umiddelbart lod sig slette, og udarbejde en plan for sletning af de resterende i samarbejde med systemleverandørerne. Fristen for opfyldelse blev sat til den 2. oktober 2026. Påbuddet blev meddelt i medfør af GDPR artikel 58, stk. 2, litra d.

Afgørelsen fastslog, at åbne mangler i sletterutiner udgør en selvstændig overtrædelse af GDPR's princip om opbevaringsbegrænsning, og at Datatilsynets tidligere offentliggjorte praksis udgør et minimum, som offentlige dataansvarlige forventes at efterleve.

Læs Datatilsynets afgørelse her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2026/maj/datatilsynet-giver-paabud-til-aalborg-kommune>



Illustration: Coulorbox/ChatGPT

Datatilsynet udtaler alvorlig kritik af Securitas A/S' håndtering af indsigtanmodning

Det danske Datatilsyn (»Datatilsynet«) traf den 25. juni 2026 afgørelse i en sag om Securitas A/S' (»Securitas«) håndtering af en registrerets anmodning om indsigt i optagelser fra en telefonsamtale. Sagen er behandlet under journalnummer 2025-43-0065.

En borger klagede over, at Securitas afslog indsigt i optagelser fra en telefonsamtale og efterfølgende oplyste borgeren, at optagelserne ikke længere eksisterede, selv om dette på daværende tidspunkt var ukorrekt. Optagelserne blev herefter slettet, hvorved borgeren endeligt blev afskåret fra muligheden for indsigt. Datatilsynet fandt,

at Securitas' håndtering ikke var i overensstemmelse med GDPR artikel 15, stk. 1 og 3, om den registreredes ret til indsigt og kopi af egne personoplysninger, da Securitas havde afgivet oplysninger, der hindrede borgerens adgang til optagelserne. Datatilsynet udtalte derfor alvorlig kritik. Datatilsynet fandt derimod ikke grundlag for at kritisere Securitas' generelle håndtering af indsigtanmodninger.

Læs Datatilsynets afgørelse her: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2026/jun/datatilsynet-udtaler-alvorlig-kritik-af-securitas-a/s>

Om forældres ret til indsigt i deres afdøde børns oplysninger

Det danske Datatilsyn (»Datatilsynet«) udkom den 22. juni 2026 med

en pressemeddelelse om forældres muligheder for at få indsigt i deres afdøde børns oplysninger. Datatilsynets vurdering kom efter spørgsmålet var blevet forelagt Datatilsynets øverste organ, det danske Dataråd, henset til spørgsmålets principielle karakter. På den baggrund har Datatilsynet udarbejdet en række vejledende retningslinjer til den dataansvarlige om forældres anmodninger om indsigt i afdøde børns oplysninger.

Datatilsynet bemærkede generelt, at udgangspunktet efter GDPR er, at retten til indsigt er en personlig rettighed, og at indsigtsretten bortfalder ved dødsfald. Datatilsynet fastslog, at det særlige for mindreårige børn er, at deres forældre allerede varetager deres ret til indsigt.

På baggrund heraf kan forældre fortsat udøve denne ret efter barnets død. Datatilsynet fremhævede samtidigt, at der fortsat gælder undtagelser fra udgangspunktet. Den dataansvarlige skal stadig foretage en konkret vurdering, hvor en række kriterier såsom barnets alder, modenhed og oplysningens karakter kan indgå.

Hjemmelsgrundlaget for forældres ret til indsigt i deres afdøde børns oplysninger er GDPR art. 15 sammenholdt med Lovbekendtgørelse nr. 289 af 8. marts 2024 (»den danske databeskyttelseslov«) § 2, stk. 5.

Læs Datatilsynets pressemeddelelse her: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2026/jun/foraeldre-kan-faa-indsigt-i-afdoede-boerns-oplysninger>

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



Bird & Bird

Beatrice Rälg

Nya svenska regler om privatkopieringsersättning från den 1 september 2026

Den 1 september 2026 träder nya regler om privatkopieringsersättning i kraft i Sverige. Riksdagen har antagit regeringens proposition 2025/26:184, som innebär ändringar i den svenska upphovsrättslagen och vissa angränsande lagar. Syftet är att modernisera ersättningsordningen och anpassa den till den tekniska och rättsliga utvecklingen sedan de nuvarande reglerna infördes. De nya reglerna ska ge rättighetshavarna en likvärdig rätt till rimlig kompensation och skapa enklare, mer förutsebara och konkurrensneutrala villkor för företagen.

Bakgrund och centrala ändringar

Privatkopieringsersättningen bygger på principen att rättighetshavare ska kompenseras för den ekonomiska påverkan som uppkommer när upphovsrätten inskränks genom möjligheten till privatkopiering. Den tekniska utvecklingen, bland annat genom digital lagring, multifunktionella konsumentprodukter och nya former av digital användning, har gjort det nödvändigt att anpassa regleringen.

Den nya ersättningsordningen omfattar upphovsmän vars verk har tillgängliggjorts i förvärvssyfte och vars ensamrätt har inskränkts genom reglerna om privatkopiering, under förutsättning att de inte endast påverkas ekonomiskt i obetyd-

lig omfattning. Motsvarande rätt gäller för vissa närstående rättighetshavare, bland annat utövande konstnärer, framställare av ljud- eller bildupptagningar samt radio- och tv-företag. Framställare av fotografiska bilder samt framställare av kataloger och liknande omfattas däremot inte av den nya ersättningsordningen.

” Den nya ersättningsordningen omfattar upphovsmän vars verk har tillgängliggjorts i förvärvssyfte och vars ensamrätt har inskränkts genom reglerna om privatkopiering, under förutsättning att de inte endast påverkas ekonomiskt i obetydlig omfattning.

Regleringen av vilka anordningar som omfattas ändras och blir i princip teknikneutral. Den tidigare begränsningen till anordningar där ljud eller rörliga bilder kan tas upp tas bort. I stället knyts ersättningsskyldigheten till fysiska anordningar som är särskilt ägnade för framställning av exemplar av verk för privat bruk.

Det omfattar bland annat anordningar för digital lagring, andra anordningar där digital lagring kan ske samt anordningar för framställning av exemplar i fysisk eller digital form.

Ersättningsnivåerna regleras direkt i lag. Reglerna innehåller även bestämmelser om hur vissa belopp ska räknas om över tid.

För att ersättningen ska bli rimlig införs regler om nedsättning i vissa situationer. Nedsättning kan bland annat komma i fråga om upphovsmännen kompenseras på annat sätt eller om ersättningen med hänsyn till omständigheter hänförliga till en anordning eller förhållandena på marknaden i övrigt är oskäligt hög.

Den nya lagen innehåller också regler om betalning och redovisning. Huvudregeln är att näringsidkaren ska betala ersättningen vid försäljning av en anordning. Genom avtal med den organisation som kräver in ersättningen kan en annan näringsidkare överta betalnings- och redovisningsskyldigheten. I vissa fall finns även rätt till återbetalning av erlagd ersättning.

För att underlätta avtalsförhandlingar införs dessutom en möjlighet att ansöka hos Patent- och marknadsdomstolen om att få en medlare utsedd. Medlaren ska vara opartisk och lämplig för uppdraget. Parterna behåller sin avtalsfrihet och kan inte tvingas att ingå ett av-

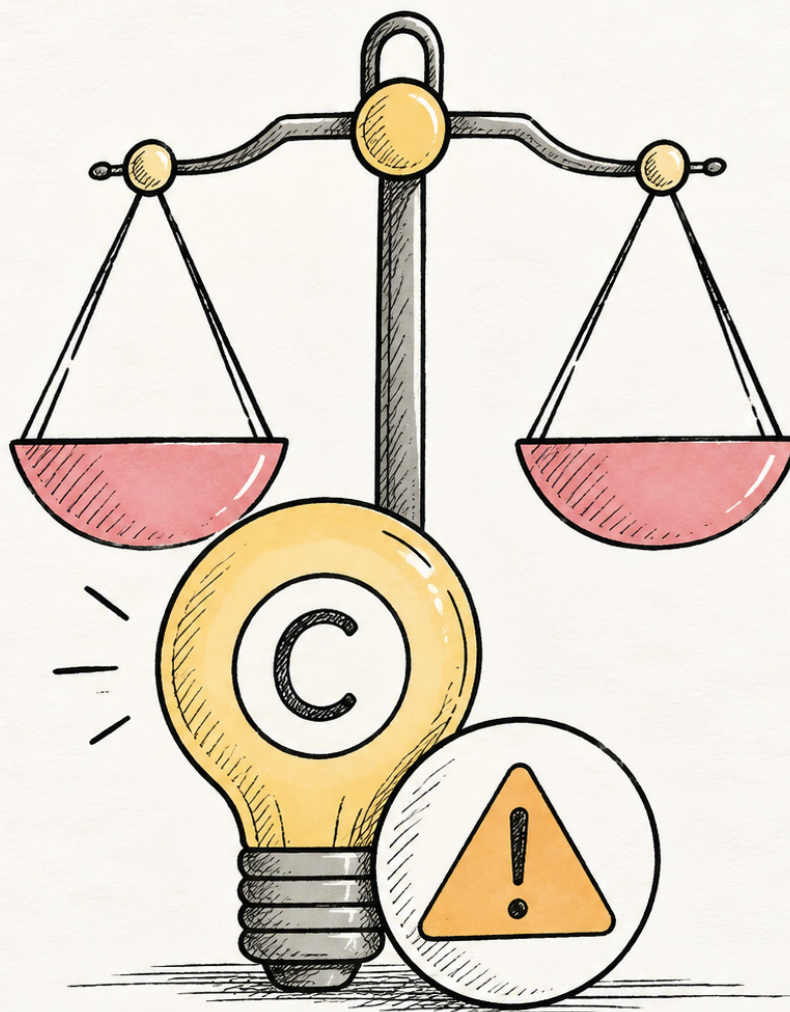


Illustration: Colorbox/ ChatGPT

tal. Om parterna inte har avtalat annat ska kostnaden för medlingen delas lika.

EU-rättslig utveckling

Under lagstiftningsarbetet aktualiserades EU-domstolens praxis om privatkopiering inom betalda strömningstjänster. I dom av den 16 april 2026 i mål C-496/24 prövade EU-domstolen bland annat frågan om kopior för offlineanvändning inom en strömningstjänst omfattas av undantaget för privatkopiering.

Den svenska regleringen har utformats med hänsyn till EU-rättens krav och innehåller mekanismer som gör det möjligt att beakta rele-

vanta omständigheter vid bedömningen av ersättningen. Det är samtidigt viktigt att skilja mellan frågan om en viss kopiering omfattas av privatkopieringsundantaget och frågan om en viss anordning omfattas av ersättningsskyldigheten.

Övergångsbestämmelser

De nya reglerna träder i kraft den 1 september 2026. De ska även tillämpas på verk och prestationer som har tillkommit före ikraftträdandet. Äldre bestämmelser gäller däremot för åtgärder som har vidtagits före ikraftträdandet. Det innebär enligt propositionens författningskommentarer bland annat att

de nya reglerna gäller i förhållande till anordningar som efter ikraftträdandet tillverkas i Sverige eller förs in eller säljs från utlandet.

Sammantaget innebär reformen en modernisering av privatkopieringsersättningen med ett tydligare regelverk för rättighetshavare, ersättningsgrundande anordningar, betalningsskyldighet och medling.

Beatrice Rälg, biträdande jurist på Bird & Bird Advokatbyrå i Stockholm, har en bakgrund inom immaterialrätt och kommersiell tvistlösning och arbetar idag huvudsakligen med IP-rättsliga frågor.



Gorrissen Federspiel

Tue Goldschmieding

Nyt om immaterielle rettigheder i Danmark

LinkedIn opslag var ikke vildledende udsagn

Sø- og Handelsretten afsagde den 1. maj 2026 dom i sag BS-34240/2024-SHR mellem ENERCON Global GmbH og ENERCON GmbH (»Enercon«) som sagsøger og TA Towers ApS, Blue Nordic GmbH og selskabernes direktør (»TA Towers«) som sagsøgte.

Enercon indledte i 2019 ugyldighedssager mod to EF-designs til vindmøletårnssegmenter, som TA Towers ApS havde registreret. Den Europæiske Unions Kontor for Intellectuel Ejendomsrets (»EUIPO«) Appelkammer fandt, at designene manglede individuel karakter, men Den Europæiske Unions Ret (»Retten«) annullerede efterfølgende appelkammerets afgørelser ved domme af 24. januar 2024 i sagerne T-202/22 og T-201/22, dog uden at designenes gyldighed dermed var endeligt afgjort.

Herefter varslede TA Towers henvendelser til Enercons kunder om påståede designkrænkelser, og direktøren offentliggjorde et LinkedIn-opslag, som ifølge Enercon fremstillede designenes gyldighed som endeligt afgjort. Enercon påstod på den baggrund, at opslaget var i strid med § 5 om vildledende markedsføring i lovebekendtgørelse nr. 1420 af 2. december 2024 (»den danske markedsføringslov«), og krævede anerkendelse af den uaf-

klarede status af de pågældende designs, forbud mod kundeforholdene samt korrektion af opslaget.

Sø- og Handelsrettens afgørelse indfinder sig i snitfladen af processretten og markedsføringsretten, eftersom retten afviste de to første påstande, idet designenes status for det første var ubestridt mellem parterne, mens den af Enercon nedlagte påstand om kundeforhold var for bredt formuleret og vedrørte henvendelser, som aldrig var foretaget. For så vidt angik LinkedIn-opslaget fandt retten, at dette var omfattet af markedsføringsloven henset til direktørens tilknytning til TA Towers og LinkedIns karakter af en professionel netværksplatform. Da direktøren efter sagens anlæg havde ændret opslaget, vurderede retten den reviderede formulering som vinklet, men ikke vildledende, og afviste derfor Enercons berigtigelseskrav og frifandt direktøren.

Læs Sø- og Handelsrettens afgørelse her: <https://domstol.fe1.tangora.com/ref.aspx?s=-300011&id=22936&page-id=16692>

Planet Nusa fik udvidet beskyttelsen af sit velkendte varemærke

Sø- og Handelsretten afsagde den 5. maj 2026 dom i sag BS-13239/2025-SHR mellem Planet Nusa ApS (»Planet Nusa«) og Ankenævnet for Patenter og Varemærker

(»Ankenævnet«). Sagen angik en prøvelse af Ankenævnets kendelse af 9. januar 2025 om registrering af varemærket »NUSA PLANET«.

Brix Denmark ApS havde ansøgt om registrering af »NUSA PLANET« for en række varer. Planet Nusa gjorde indsigelse med henvisning til selskabets ældre rettigheder til »NUSA PLANET«. Spørgsmålet var, om registreringen skulle nægtes for »optiske apparater og instrumenter« i klasse 9, der bl.a. omfatter solbriller, efter § 15, stk. 1, nr. 2, om risiko for forveksling eller § 15, stk. 3, nr. 1, om beskyttelse af velkendte varemærker, i lovebekendtgørelse nr. 88 af 29. januar 2019 (»den danske varemærkelov«), i forbindelse med Planet Nusas varemærke »PLANET NUSA«.

Retten fandt, ligesom Ankenævnet, at sportstøj og optiske apparater og instrumenter ikke var lignende varer. Varerne havde forskellige formål, var ikke komplementære og blev overvejende solgt gennem forskellige distributionskanaler. Der forelå derfor ikke risiko for forveksling efter varemærkelovens § 15, stk. 1, nr. 2, selv om varemærkerne havde en høj grad af lighed.

Retten fandt derimod, at »NUSA PLANET« havde en høj grad af iboende særpræg og måtte anses for velkendt. På baggrund af mærkernes lighed, Planet Nusas landsdækkende markedsføring og forbindel-

sen mellem sportstøj og solbriller fandt retten, at omsætningskredsen ville skabe en sammenhæng mellem mærkerne. Brugen af »NUSA PLANET« ville derfor indebære en utilbørlig udnyttelse af »PLANET NUSA«-mærkets særpræg efter varemærkelovens § 15, stk. 3, nr. 1.

Sø og Handelsretten pålagde her efter Ankenævnet at anerkende, at »NUSA PLANET« skulle nægtes registrering for »optiske apparater og instrumenter« i klasse 9, og at betale 30.750 kr. i sagsomkostninger til Planet Nusa.

Læs Sø- og Handelsrettens afgørelse her: <https://domstol.fe1.tangora.com/ref.aspx?s=-300011&id=22929&page-id=16692>

Brugen af billeder af atleter og landsholdstrøjen var sket i kommercielt øjemed og i strid med retten til eget billede

Sø- og Handelsretten afsagde den 23. juni 2026 dom i sag BS-23785/2025-SHR om brugen af billeder af atleter og den danske håndboldlandsholdstrøje.

Medievirksomheden Better Collective A/S var sagsøgt af en række danske håndbold- og badmintonspillere og foreningen Dansk Håndbold for at have brugt billeder af de pågældende atleter og håndboldlandsholdstrøjen i online sport-sindhold på hjemmesiden »SpilXperten.com« samt tilknyttede sociale medie-konti, uden samtykke fra sagsøgerne.

Atleterne og foreningen Dansk Håndbold påstod, at brugen af billederne var sket i kommerciel sammenhæng, og derfor udgjorde en krænkelse af deres rettigheder over billederne. Better Collective A/S påstod derimod, at brugen var sket i redaktionel sammenhæng, og derfor ikke krævede samtykke.

I vurderingen af, om brugen af billederne havde kommerciel eller redaktionel karakter, så retten på den konkrete brug i hvert enkelt tilfælde. Retten lagde vægt på, at SpilXperten artikler indeholdt in-

spiration til sportsvæddemål og henvisninger med affiliate-links til konkrete spiludbydere. Retten lagde også vægt på, at cirka 70% af SpilXperten omsætning bestod af indtægter fra affiliate-markedsføring, samt at hjemmesiden var begrænset til brugere over 18 år, og indeholdt referencer til ROFUS og Center for Ludomani. Retten konkluderede på baggrund heraf, at spil anbefalingerne og affiliate-markedsføringen var så integreret i SpilXperten indhold, at det havde kommerciel, og ikke redaktionel, karakter.

Retten konkluderede derfor, at SpilXperten på forsætlig vis havde krænket rettighederne til billederne, og idømte Better Collective A/S at betale både erstatning og vederlag til atleterne efter § 24, stk. 2 og 3, jf. § 3, stk. 1, i den danske lov om markedsføring, jf. lovbekendtgørelse nr. 1420 af 2. december 2024 (»markedsføringsloven«), og til spillerforeningen og foreningen Dansk Håndbold efter markedsføringslovens § 24, stk. 2 og 3, jf. § 22, stk. 1.

Læs Sø- og Handelsrettens dom her: https://domstol.fe1.tangora.com/media/-300011/files/Dom_TIL_OF-FENTLIGG%C3%98RELSE_BS-23785-2025-SHR.pdf

Forbrugerombudsmanden politianmeldte virksomhed bag boligportal

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) offentliggjorde den 1. maj 2026, at Forbrugerombudsmanden havde politianmeldt virksomheden Reva Group ApS. Virksomheden, der stod bag en række boligportaler i Danmark, Sverige, Norge og flere andre europæiske lande, blev politianmeldt for at vildlede platformens brugere om abonnementer.

På platformen kunne forbrugere søge efter lejeboliger og kollegieværelser mod en mindre intropris. Introprisen var eksempelvis på ni danske kroner eller én euro, og gav en kortvarig adgang til portalen på for-

eksempel fire dage. Efter den kortvarige periode blev forbrugerens abonnement automatisk fornyet til et løbende abonnement til en pris på eksempelvis 299 danske kroner eller 39 euro. Abonnementet blev fornyet hver 28. dag.

Lovbekendtgørelse nr. 1420 af 2. december 2024 (»den danske lov om markedsføring«) § 5, stk. 1 og § 6, stk. 1, foreskriver, at virksomheder ikke må vildlede gennemsnitsforbrugeren i sin markedsføring, herunder ved at udelade eller skjule væsentlige oplysninger på en uklar måde.

Forbrugerombudsmanden var af den opfattelse, at virksomheden vildlede platformens forbrugere ved ikke tilstrækkelig klart og tydeligt at oplyse om, at forbrugerens abonnement automatisk blev fornyet til et markant dyrere periodisk abonnement. Endvidere udtalte Forbrugerombudsmanden, at forbrugere ikke skulle være i tvivl om, hvilken aftale de indgår.

Forbrugermyndigheder i udlandet havde også klaget over Reva Group ApS' boligportaler til Forbrugerombudsmanden, herunder myndigheder i Irland, Belgien og Frankrig.

Læs Forbrugerombudsmandens pressemeddelelse her: <https://forbrugerombudsmanden.dk/menu/nyheder-og-presse/nyhedsarkiv/pressemeddelelser/2026/20260501-virksomhed-bag-boligportaler-politianmeldes-for-at-vildlede-om-abonnementer>

Rejsekort & Rejseplan A/S politianmeldt af Forbrugerombudsmanden

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) offentliggjorde den 2. juni 2026, at den danske virksomhed Rejsekort & Rejseplan A/S var blevet politianmeldt af Forbrugerombudsmanden for vildledende markedsføring. Virksomheden havde i en længere periode kørt en landsdækkende kampagne for deres digitale rejsekort. Det fremgik af kampagnen, at

det fysiske rejsekort lukkede, hvorfor forbrugeren fremadrettet måtte benytte det digitale rejsekort. Budskaber såsom »Rejs med digitalt. Det fysiske rejsekort lukker. Brug i stedet en af disse billet-apps.« fremgik på stationer, i offentlig transport og på sociale medier. Kampagnen indeholdt ikke klar information om, at et fysisk alternativ ville bestå efter indfasningen af det digitale rejsekort. Forbrugerombudsmanden politianmeldte virksomheden for brud på lovbekendtgørelse nr. 1420 af 2. december 2024 (»den danske lov om markedsføring«) § 5, stk. 1, og § 6, stk. 1, om vildledende markedsføring. Det indgik i Forbrugerombudsmandens vurdering, at virksomheden havde udeladt væsentlige oplysninger for at påvirke en bestemt adfærd hos forbrugerne. Omfanget af kampagnen var en skærpende omstændighed. Ydermere var det en skærpende omstændighed, at der var tale om offentlig transport, som mange forbrugere ikke har mulighed for at fravælge.

Forbrugerombudsmanden modtog mere end 35 klager over kampagnen. Rejsekort & Rejseplan A/S oplyste til Forbrugerombudsmanden i forbindelse med Forbrugerombudsmandens undersøgelse, at selskabet var uenige i, at kampagnen var vildledende.

Læs Forbrugerombudsmandens pressemeddelelse her: <https://forbrugerombudsmanden.dk/pressemeddelelser/2026/20260602-forbrugerombudsmanden-politianmelder-rejsekort-rejseplan-for-vildledende-markedsfoering>

CleanFriend politianmeldt for skjult reklame og vildledning

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) oplyste den 15. juni 2026, at have politianmeldt CleanFriend ApS (»CleanFriend«) for skjult reklame og vildledende markedsføring.

CleanFriend havde oprettet hjemmesiden bedsttests.dk, hvor virksomheden rangerede sine egne produkter højest i en række



Illustration: Coulorbox/ ChatGPT

»test«-artikler, uden at oplyse om den kommercielle interesse bag siden. Hjemmesiden fremstod som en uvildig forbrugerportal og anvendte grønne logoer og udsagnet »bedst i test«, som efter Forbrugerombudsmandens vurdering var egnet til at forveksles med Forbrugerrådet Tænks testmærker. CleanFriend anvendte herefter testresultaterne på sin webshop og i 59 annoncer på bl.a. Facebook og Instagram, hvor produkterne blev markedsført som »bedst i test«, »testvinder« og »anbefalet af« bedsttests.dk.

Forbrugerombudsmanden vurderede, at markedsføringen var i strid med § 5 om vildledende handlinger og § 6, stk. 4, om pligten til at oplyse den kommercielle hensigt med en handelspraksis, i lovbekendtgørelse nr. 1420 af 2. december 2024 (»den danske markedsføringslov«).

Forbrugerombudsmanden understregede, at virksomheder alene må anvende udsagn som »bedst i test« og »testvinder«, såfremt disse kan dokumenteres, og at en virksomheds anbefaling af egne produkter tydeligt skal fremgå som reklame.

Læs Forbrugerombudsmandens meddelelse her: <https://forbrugerombudsmanden.dk/menu/nyheder-og-presse/pressemeddelelser/pressemeddelelser/2026/20260615-forbrugerombudsmanden-politianmelder-cleanfriend-for-skjult-reklame-og-vildledning>

Youtuber dømt for indirekte at opfordre til farlig adfærd

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) offentliggjorde den 16. juni 2026, at en youtuber, Forbrugerombudsmanden tidligere havde politianmeldt, var blevet dømt ved Retten i Esbjerg. Youtuber blev ikendt en bøde på 120.000 danske kroner for skjult reklame og for indirekte at opfordre børn og unge til farlig adfærd. Retten i Esbjerg behandlede sagen under journalnummeret 98-1703/2025.

Den erhvervsdrivende youtuber lavede to underholdningsvideoer til sin platform på YouTube. I den ene video smagte youtuber på 100 shots, blev undervejs beruset og kastede op. I den anden smagte vedkommende på 52 energidrikke.

Under begge videoer fremgik et link til youtuberens eget merchandise.

Efter Lovbekendtgørelse nr. 1420 af 2. december 2024 (»den danske lov om markedsføring«) § 11, stk. 1, må markedsføring, der direkte eller indirekte opfordrer til farlig eller hensynsløs adfærd, ikke rettes mod børn og unge. Lov om markedsføring § 11, stk. 2, foreskriver, at alkohol eller energidrikke ikke må markedsføres mod børn og unge under 18 år.

Retten i Esbjerg vurderede, at youtuberens fremviste en farlig situation eller en situation, der tilsidesatte almindelig sikkerhed ved at drikke 100 shots i en video. Derudover fandt retten efter en samlet vurdering af videoens kontekst, at den var rettet mod børn og unge.

Linkene under youtuberens videoer var skjult reklame, da det ikke tilstrækkeligt klart og tydeligt var oplyst, at youtuberens havde en kommerciel hensigt med at linke til sit eget merchandise, jf. § 6, stk. 4, i lov om markedsføring.

Dommen er i overensstemmelse med den hidtidige praksis, hvorefter indhold produceret af erhvervsdrivende influenter også skal overholde markedsføringsloven.

Læs Forbrugerombudsmandens pressemeddelelse her: <https://forbrugerombudsmanden.dk/menu/nyheder-og-presse/pressemeddelelser/pressemeddelelser/2026/20260616-youtuber-ident-boede-for-indirekte-at-opfordre-boern-og-unge-til-farlig-adfaerd-med-alkohol>

Klagenævnet for Domænenavn overfører domænenavnet buyit-shop.dk til tidligere registrant

Det danske Klagenævn for Domænenavne (»Klagenævnet«) traf den 9. april 2026 afgørelse i sagen med journalnummer 2025-10189 og bestemte, at domænenavnet »buyit-shop.dk« skulle overføres til klageren A.

A havde tidligere anvendt »buyit-shop.dk« i forbindelse med sin enkeltmandsvirksomhed »BuyIT« med salg af iPhones. Efter domænets udløb registrerede B domænet den 5. april 2025 og anvendte

A's virksomhedsnavn på en vildledende måde på en hjemmeside, der fremstod autogenereret og uden egentlig forretningsmæssigt indhold. B besvarede ikke Klagenævnets henvendelser i sagen. Klagenævnet fandt herefter, at B ikke havde nogen interesse af betydning i domænet, og at en opretholdelse af registreringen ville udgøre en overtrædelse af god domænenavns-skik, jf. § 25, stk. 1, i lov nr. 164 af 26. februar 2014 om internetdomæner m.v. (»den danske domænelov«). Domænet blev på den baggrund overført til A i medfør af den danske domænelov § 28, stk. 4, nr. 1.

Læs afgørelsen her: https://www.domæneklager.dk/sites/default/files/decision-pdf/2025-10189_buyit-shop.dk_anonym.pdf

Klagenævnet for Domænenavn overfører ikke domænenavnet detvarnemt.dk til tidligere registrant

Det danske Klagenævn for Domænenavne (»Klagenævnet«) traf den 9. april 2026 afgørelse i sagen med journalnummer 2025-10167 og bestemte, at domænenavnet »detvarnemt.dk« ikke skulle overføres til klageren, Det Var Nemt (»Klageren«). Klageren havde i cirka 15 år anvendt »detvarnemt.dk« i forbindelse med sin virksomhed med samme navn. Da klageren ikke fornyede domænet til tiden, registrerede indklagede, LOMAX A/S, domænenavnet. LOMAX A/S havde siden 2006 været indehaver af varemærkeregistreringen »DET VAR NEMT« samt »LOMAX – DET VAR NEMT« siden 2020 og anvender disse konsekvent som en del af virksomhedens branding på tværs af markedsføringskanaler.

Klagenævnet foretog en interesseafvejning i overensstemmelse med § 25, stk. 1, i lov nr. 164 af 26. februar 2014 om internetdomæner m.v. (»den danske domænelov«), der forbyder registranter at registrere og anvende domænenavne i strid med god domænenavns-skik. Klagenæv-

net fandt at klagerens interesse i domænenavnet ikke i væsentlig grad oversteg indklagedes interesse, og at en opretholdelse af registreringen dermed ikke udgjorde en overtrædelse af den danske domænelov.

Læs afgørelsen her: https://www.domæneklager.dk/sites/default/files/decision-pdf/2025-10167_detvarnemt.dk_.pdf

Klagenævnet for Domænenavn overfører domænenavnet danske-natur.dk til tidligere registrant

Det danske Klagenævn for Domænenavne (»Klagenævnet«) traf den 9. april 2026 afgørelse i sagen med journalnummer 2025-10177 og bestemte, at domænenavnet »danske-natur.dk« skal overføres til klageren, A. A's bror havde siden 2006 drevet en hjemmeside om danske sommerfugle og insekter på domænenavnet. Efter brorens død fornyede boet ikke registreringen rettidigt, som følge af manglende opkrævning fra registreringsvirksomheden Punktum.dk og efterfølgende fejlagtig vejledning. Indklagede, B, registrerede herefter domænenavnet. B omdirigerede domænenavnet til en generisk faktaside og lagde først naturrelateret indhold på hjemmesiden, efter at klagen var indbragt.

Klagenævnet fandt, at dette indhold fremstod ufuldstændigt og tilfældigt, og at A's interesse i domænenavnet i væsentlig grad oversteg B's. B's fastholdelse af registreringen udgjorde herefter en overtrædelse af § 25, stk. 1, i lov nr. 164 af 26. februar 2014 om internetdomæner m.v. (»den danske domænelov«) om god domænenavns-skik. Domænet blev på den baggrund overført til A i medfør af den danske domænelov § 28, stk. 4, nr. 1.

Læs afgørelsen her: https://www.domæneklager.dk/sites/default/files/decision-pdf/2025-10177_danske-natur.dk_anonym.pdf

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



Selmer

Amanda Johnson og Jennifer Parmlind

Ny dom om cybersikkerhet og IT-kontrakter (LG-2025-156056)

Gulating lagmannsrett avsa 30. juni 2026 dom i saken mellom Btec AS («Btec») og Nordlo Haugesund AS («Nordlo»). Btec krevde erstatning etter å ha mistet data da Nordlo, leverandør av ASP-tjenester, ble rammet av et cyberangrep. Saken reiser spørsmål om bindende standardvilkår uten signert kontrakt, grensene for force majeure ved løsepengevirus, og hvor mye som skal til før en IT-leverandørs sikkerhetssvikt er grovt uaktsom. Dommen er anket til Høyesterett og derfor ikke rettskraftig.

I mars 2017 inngikk partene avtale om levering av ASP-tjenester, som innebærer at leverandøren drifter, vedlikeholder og tilgjengeliggjør programvare for kunden via internett. Det ble ikke utarbeidet skriftlig kontrakt. Den 22. april 2021 krypterte trusselaktører store deler av Nordlos driftsmiljø med løsepengeviruset «Ryuk» og krevde 50–60 millioner kroner i bitcoin. Nordlo betalte ikke. Av selskapets 255 kunder mistet fire av dem data helt eller delvis, deriblant Btec. For Btec var konsekvensene store: 14 000 produksjonsmodeller og kritiske ERP-data som ordre- og produktinformasjon, fakturaer og varedokumentasjon gikk tapt. Btec beregnet tapet til 57,2–64,2 millioner kroner. Tingretten tilkjente Btec 8 280 kroner i tråd med ansvarsbegrensningen i Nordlos standardvilkår. Btec anket dommen.

Standardvilkårene var bindende

Lagmannsretten fant at Nordlo hadde rimelig grunn til å forvente at Btec hadde akseptert standardvilkårene, herunder en omfattende ansvarsbegrensning, selv uten signert kontrakt.

Avgjørende var at Btecs bestilling bygget på den samme standardiserte ASP-tjenesten som allerede var etablert for Btecs datterselskap Deltapump Maskinering AS («DM»). Da daglig leder ba om administratorrettigheter, ble det vist uttrykkelig til DMs ASP-avtale, og samme dag ble tilsvarende tjeneste bestilt for Btec med et ønske om å «samkjøre» virksomhetene. Prisingen ble også knyttet til det DM betalte. Btec må derfor anses for å ha vært kjent med Nordlos standardvilkår.

Vilkårene var heller ikke overraskende eller ubalanserte. Det gjaldt en standardisert tjeneste til 429 kroner per bruker per måned, og tilsvarende ansvarsbegrensninger var utbredt hos sammenlignbare leverandører av ASP- og skytjenester og i statens standardavtaler for IT-anskaffelser. Nordlo tilbød utvidede sikkerhetsløsninger for kunder med særskilte behov, men Btec bestilte ikke dette. En ASP-avtale uten ansvarsbegrensning ville etter rettens syn påført Nordlo en «ikke ubetydelig risiko» ved levering av en standard abonnementstjeneste til beskjedne pris. I tillegg hadde

Nordlo innkalt Btec til oppstartsmøte og forsøkt å komme i kontakt per e-post, uten at Btec møtte eller svarte. At Btec som profesjonell part ikke fulgte opp møteinnkallelser fra Nordlo eller tok skritt for å avklare hvilke vilkår som gjaldt, måtte selskapet selv bære risikoen for.

Standardvilkårenes ansvarsbegrensning utelukket dekning av indirekte tap og begrenset øvrig erstatning oppad til tre måneders leie.

Kontraktsbrudd, men ikke force majeure

Retten konkluderte med at Nordlos utilstrekkelige sikkerhetskopiering og manglende oppetid utgjorde kontraktsbrudd. Deler av Btecs data lå på en RDS-server og den tilhørende backup-serveren som tok sikkerhetskopier var ikke flyttet til det atskilte managementnett slik resten av backup-infrastrukturen var, men lå i samme produksjonsnett (Prodnett 1). Prodnett 1 ble rammet av angrepet og dataene gikk dermed tapt. Sikkerhetskopieringen var utilstrekkelig, og angrepet medførte én virkedags nedetid, slik at kravene til sikkerhetskopiering, drift, tilgjengeliggjøring av programvare og oppetidsgaranti ikke var oppfylt.

Nordlos innsigelse om force majeure førte ikke frem. Løsepengevirus har vært en kjent risiko siden midten av 2010-tallet, og Nasjonal

sikkerhetsmyndighet pekte allerede i 2017 på økt fare for avanserte cyberangrep. Hendelsen var derfor verken ekstraordinær eller upåregnelig for en profesjonell IT-leverandør.

Nordlo har ikke opptrådt grovt uaktsomt

Siste spørsmål var om ansvarsbegrensningen måtte settes til side, slik at Btec kunne kreve full erstatning fordi Nordlo hadde opptrådt grovt uaktsomt.

Retten presiserte at grov uaktsomhet krever et markert og klart klanderverdig avvik fra forsvarlig handlemåte, vurdert ut fra risikoens størrelse, skadesannsynlighet, tilgjengelige forebyggende tiltak, skadepolders kompetanse og eventuell svikt i grunnleggende rutiner. Vurderingen må også skje i lys av hva partene hadde avtalt om ytelse, pris og risikofordeling. Avtalen gjaldt en standardisert ASP-tjeneste uten tilleggsbestilte sikkerhetstjenester, og spørsmålet var om sikkerhetsnivået representerte et kvalifisert avvik fra det som var bestilt og betalt for. Retten så hen til Nasjonal sikkerhetsmyndighets grunnprinsipper for IKT-sikkerhet (basert på ISO 27001), men presiserte at avvik fra anbefalt standard ikke i seg selv er grovt uaktsomt.

Retten påviste flere konkrete svakheter. Nordlo var i gang med å flytte backup-serverne til et eget, adskilt managementnett, men serveren som tok sikkerhetskopier av Btecs data var ennå ikke flyttet og lå fortsatt i det rammede produksjonsnettet. Konsekvensen var at både data og sikkerhetskopier ble kryptert i angrepet. Retten fant at segmenteringsarbeidet ikke var feilprioritert. Videre var Btec nærmest til å opplyse om at tjenesten lagret virksomhetskritiske data. Retten uttalte generelt at en ASP-leverandør ikke har noen alminnelig plikt til å orientere kundene om interne arkitekturvalg eller mellomstadier i en pågående

segmenteringsprosess. Retten påpekte at dette kan stille seg annerledes dersom leverandøren kjenner til at kunden har spesielle data eller risikoforhold.

I tillegg manglet Nordlo skriftlige rutiner og krav om flerfaktoraутentisering. Retten fant det ikke sannsynliggjort at det i 2021 gjaldt noe bransjekrav om flerfaktoraутentisering for tilsvarende tjenester, og skriftlige rutiner ville uansett ikke avverget datatapet.

Retten pekte også på visse svakheter ved sikkerhetsovervåkingen og oppdateringen av applikasjonsprogramvarer, men fant det ikke sannsynliggjort at disse svakhetene forårsaket datatapet eller utgjorde en så kvalifisert svikt at Nordlo kunne anses å ha opptrådt grovt uaktsomt.

I helhetsvurderingen vektla retten at beskyttelse mot et trusselbilde i kontinuerlig utvikling er krevende, at angrepet var utført av en velorganisert og teknologisk kompetent aktør, og at sikkerhetsnivået måtte måles mot bransjepraksis for tilsvarende ASP-tjenester til små og mellomstore virksomheter i 2021. Avgjørende for lagmannsretten var at Nordlo hadde implementert flere sentrale sikkerhetstiltak som sikret at hoveddelen av selskapets infrastruktur og backup-løsninger sto imot angrepet. Btecs egen håndtering fikk også en viss, om enn begrenset, betydning. Etter standardvilkårene var kunden selv ansvarlig for å forsikre verdien av egne data, men Btec hadde ikke tegnet slik forsikring.

Verken enkeltvis eller samlet utgjorde svakhetene et tilstrekkelig kvalifisert avvik til at grov uaktsomhet forelå, og misligholdet av kjerneytelsen var ikke så gjennomgripende at ansvarsbegrensningen kunne settes til side eller tolkes innskrenkende.

Btec ble, som i tingretten, tilkjent 8 280 kroner i erstatning, tilsvarende tre månedsløyer. Btec ble også pålagt å betale Nordlos sakskostnader på 2 320 647 kroner.

Hva kan vi lære av dommen?

Dommen etterlater et tydelig budskap. Terskelen for grov uaktsomhet er høy, særlig når et profesjonelt utført cyberangrep rammer en standardtjeneste levert til beskjedent vederlag, uten bestilte tilleggsytelser, fra en lokal leverandør til små og mellomstore virksomheter. Kravene til sikkerhet måles mot hva som var påregnelig for den bestilte tjenesten, ikke mot hva som i ettertid kan påvises som mulige forbedringer.

For kunder er lærdommen å være tydelig overfor leverandøren om hvilke data som er virksomhetskritiske, og å forstå at ansvaret for å bestille eller presisere sikkerhetsbehov ligger hos kunden selv. Aller helst bør avtalen si uttrykkelig hvilket sikkerhetsnivå som forventes, men da må kunden også være forberedt på å betale for det. Kunder som forholder seg passive, bærer også risikoen for dette.

For leverandører er det viktig merke seg at en generell force majeure-bestemmelse ikke er et forsvar mot cyberangrep. Løsepengevirus, som var tema i denne saken, anses som en kjent og påregnelig risiko for en profesjonell IT-leverandør.

Avslutningsvis er aktsomhetsnormen dynamisk. Retten bedømte Nordlo etter bransjepraksis i 2021, og fremhevet blant annet at Microsoft først innførte krav om multifaktoraутentisering for eksisterende kunder i januar 2025. Det som var forsvarlig den gang, er ikke nødvendigvis forsvarlig nå, verken for leverandører som vurderer eget sikkerhetsnivå eller for kunder som vurderer et krav.

Amanda Johnson, advokatfullmektig og Jennifer Parmlind, senioradvokat. Begge arbeider særlig med teknologi og immaterielle rettigheter i Advokatfirmaet Selmer.

Les dommen her:

<https://lovdata.no/dokument/LGSIV/avgjorelse/lg-2025-156056?q=LG-2025-156056>



< kahn
> pedersen

Fredrik Sandström, Hanna Bogsjö Österberg
och Staffan Malmgren

Är företagshemligheter på väg att bli mjukvarans viktigaste skydd?

Den svenska patent- och marknadsöverdomstolen (PMÖD) meddelade den 10 juni 2026 dom i ett mål om skyddet för källkod. Bakgrunden var en relativt klassisk avhopparsituation. Tidigare anställda på mjukvarubolaget Phenixid hoppade av och startade ett nytt bolag, Fortifiedid. Efter att Fortifiedid lanserat en konkurrerande lösning gjorde Phenixid gällande att den utvecklats med hjälp av Phenixids källkod, och väckte efter en inträngsundersökning talan på två grunder: dels upphovsrättsintrång, dels angrepp på företagshemligheter.

I upphovsrättsdelen lämnades talan utan bifall. Phenixid gav in ett urval av sin källkod utan att redovisa vare sig urvalskriterierna eller hur delarna förhöll sig till varandra och till mjukvaran i dess helhet. Vilket datorprogram källkoden hörde till, och om det handlade om ett skyddat verk eller flera, gick enligt domstolen inte att avgöra. Källkoden som helhet kunde därmed inte identifieras som ett verk, och under alla förhållanden ansåg domstolen att det inte var visat att valet, dispositionen och kombinationen av beståndsdelar gav uttryck för sådana kreativa val som krävs. Prövningen tvingades därför ned till att bedöma de enskilda källkodsfilerna för sig. Phenixids bevisning tog emellertid sikte på kod-

basen som helhet och räckte därför inte.¹

I frågan om angrepp på företagshemligheter blev utgången den motsatta. Lagen om företagshemligheter skyddar information som är hemlig som helhet eller i den form dess beståndsdelar ordnats och satts samman.² Den sammansättningsregeln saknar motsvarighet i upphovsrätten. PMÖD fann därför, till skillnad från underinstansen,³ att

- 1 Domstolen framhöll samtidigt att kravet på individualiserad bevisning inte hade ställts lika högt om prövningen gällt ett helt datorprogram. Referenten var skiljaktig och ansåg att identitetskravet var uppfyllt så snart alstret lagrats på ett medium och därmed kommit till uttryck i någon form. Han ansåg även att originalitetskravet var uppfyllt och att källkoden alltså utgjorde ett upphovsrättsligt skyddat verk. Att det ingivna materialet var begränsat och ostrukturerat var enligt honom en fråga för originalitetsbedömningen, inte för identifieringen.
- 2 § första stycket 2 lagen (2018:558) om företagshemligheter.
- 3 Underinstansen ansåg att källkoden i och för sig kunde kvalificera sig som företagshemlighet, men att inte samtliga element i den kunde göra det, och att Phenixid därför måste knyta varje påstått angrepp till kod där en företagshemlighet kunde verifieras. PMÖD delade underinstansens bedömning att informationen varit hemlig, att rimliga hemlighållandeåtgärder vidtagits och att ett röjande varit ägnat att medföra skada i konkurrenshänseende.

källkoden i sin sammansatta form varit skyddsvärd även om den delvis bestått av bland annat öppen källkod som var för sig varit allmänt känd. PMÖD sammanfattade saken så att det av allt att döma funnits ”en marknad för källkoden som helhet, inte dess olika enskildheter”. Även angreppet ansågs avse koden i dess helhet.

Fortifiedid förbjöds vid vite att utnyttja eller röja uppgifterna i den ingivna källkoden med undantag för vissa filer, och förpliktades även att betala skadestånd.

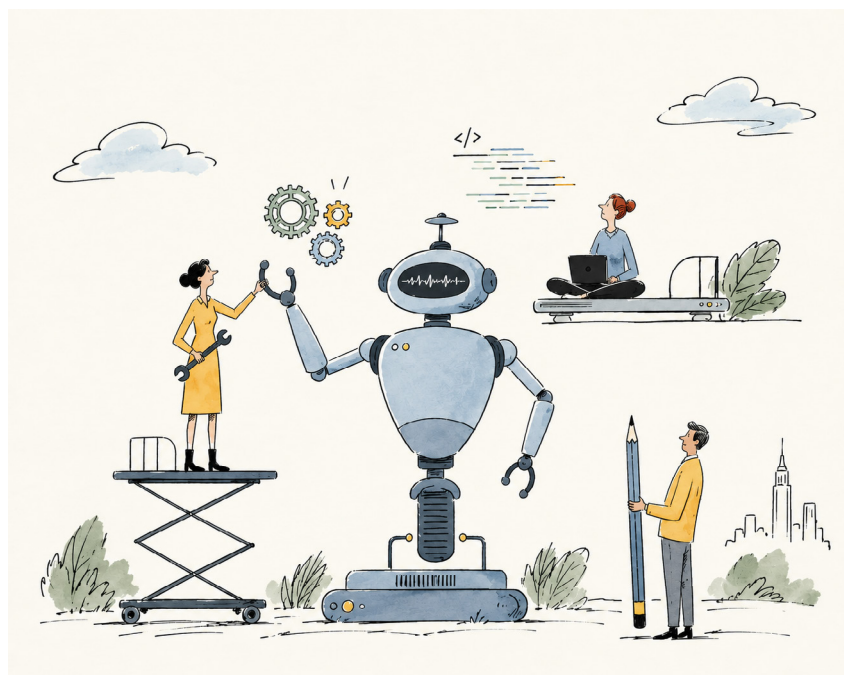
Domen visar tydligt att den som vill hävda upphovsrätt till en modern mjukvaruprodukt har en omfattande bevis- och förklaringsbörda. Domstolen understryker att den (eller någon annan som inte är sakkunnig på området) inte kan bedöma hur alstrets olika delar (källkodsfiler) förhåller sig till varandra. Det urval som Phenixid gjort från den totala mängden källkod som ligger till grund för företagets produkter har inte heller hjälpt domstolens bedömning då Phenixid inte förklarat vilka delar som getts in, vad som har utelämnats och varför. Inte heller de sakkunnigutlåtanden som getts in av Phenixid har lett till att domstolen kunnat göra någon bedömning av vad verket egentligen kan sägas bestå av.

Som följd därav är en ytterligare reflektion är att skyddet för före-

tagshemligheter får allt större praktisk betydelse för skyddet av mjukvara. Målet är ett tydligt exempel på att det på samma processmaterial många gånger kan vara lättare att vinna framgång i ett påstående om angrepp på företagshemligheter än upphovsrättsintrång. Och ett vitesförbud behöver, till skillnad från vad som gäller på immaterialrättsens område, inte utformas så att det ansluter till det angrepp som angriparen faktiskt har utfört.⁴

Därtill kommer att det sedan den 1 januari 2026 är straffbart att uppsåtligt och olovligen utnyttja eller röja en teknisk företagshemlighet som man har fått del av till följd av sin anställning eller en affärsförbindelse.⁵ Samma handlingsmönster i dag hade alltså också kunnat prövas straffrättsligt mot de tidigare anställda personligen.⁶

Fokusförflyttningen från upphovsrätt mot företagshemligheter förstärks ytterligare av att modern mjukvaruutveckling i allt större grad sker med hjälp av AI-verktyg. Upphovsrätten skyddar endast det som utgör upphovsmannens egen intellektuella skapelse. Ju större andel av en kodbas som genereras av AI-verktyg, desto svårare blir det att visa att den är upphovsrättsligt skyddad och i vilka delar. Lagen om företagshemligheter ställer däremot ingen fråga om vem eller vad som har skapat informationen, utan bara



Illustrasjon: Coulorbox/ChatGPT

om den varit hemlig, om rimliga åtgärder vidtagits för att hemlighålla den och om ett röjande varit ägnat att medföra skada i konkurrenshänseende.⁷

Baksidan är att användningen av AI-verktyg också riskerar att underminera skyddet. AI-verktyg för kodning levereras ofta som en tjänst,⁸ vars användande förutsätter att hela eller delar av kodbasen avslöjas för – eller uppstår hos – en extern leverantör. Och ett sådant röjande kan påverka bedömningen av om rimliga hemlighållandeåtgärder har vidtagits. Villkoren för AI-verktygen, dvs. var koden får behandlas, av vem och med vilka förbehåll om lagring och träning, blir därför en central fråga.

Båda parter har överklagat domen till Högsta domstolen. I skrivande stund har frågan om prövningstillstånd inte avgjorts.

Frågorna som aktualiseras är ytterst unionsrättsliga,⁹ och ett avgörande kan därmed få betydelse för rättstillämpningen i hela Norden.

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

Hanna Bogsjö Österberg, 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.

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

4 12 § lagen om företagshemligheter och prop. 2017/18:200 s. 162.

5 26 a § lagen om företagshemligheter. Källkod och datorprogram anges uttryckligen som exempel på tekniska företagshemligheter i förarbetena (prop. 2024/25:208 s. 54).

6 26 a § tredje stycket lagen om företagshemligheter samt prop. 2024/25:208 s. 51 och 58. Att gärningen begås efter att anställningen upphört innebär dock att den normalt ska bedömas som ringa och därmed vara straffri om inte agerandet framstår som särskilt illojalt, till exempel genom att överföringen av information till konkurrenten förbets redan under anställningen.

7 2 § första stycket lagen om företagshemligheter. I kravet på skada i konkurrenshänseende ligger att informationen ska ha kommersiellt värde på grund av att den är hemlig (prop. 2017/18:200 s. 139).

8 Exempelvis Github Copilot, Claude Code eller OpenAI Codex.

9 Den nya svenska straffbestämmelsen är däremot ett nationellt tillägg.



Viveca Still

Ny lagstiftning främjar digital förvaltning i Finland

Under denna regeringsperiod (2023-2027) är ett av regeringens fokusområden att främja den digitala förvaltningen i Finland. Reformarbetet bygger inte på stora ekonomiska satsningar. Utgångspunkten är i stället att digitaliseringen ska effektivisera den offentliga förvaltningen och bidra till besparingar som stärker de offentliga finanserna.

1. Regeringens initiativ för prioritering av elektronisk delgivning i myndighetsverksamhet

Ny lagstiftning om prioritering av elektronisk delgivning i myndighetsverksamhet har godtagits av riksdagen. Reformen har genomförts i två faser. Den första propositionen *RP 124/2025* lämnades in till riksdagen redan i september 2025 och avsikten var ursprungligen att lagstiftningen skulle ha trätt i kraft i januari 2026. Behandlingen i riksdagen drog ut på tiden, bland annat på grund av oro för hur reformen skulle påverka personer med begränsad digital kompetens. Lagförslagen kunde dock slutligen antas i mars 2026. Lagpaketet trädde slutligen i kraft den 14.4.2026. Lagstiftningen innebär att myndigheternas delgivningar i första hand ska sändas elektroniskt till de förvaltningskunder som har möjlighet att ta emot elektronisk delgivning. Reformen

men berör handlingar som avses i 54 § i förvaltningslagen, såsom myndighetsbeslut, som därmed ska sändas till Suomi.fi-meddelanden för kännedom. Det kan vara fråga om antingen vanlig elektronisk delgivning eller bevislig elektronisk delgivning som ska kvitteras som mottagen innan meddelandet öppnas. En myndighet kan dessutom skicka även andra meddelanden till Suomi.fi-meddelandena, såsom påminnelser eller tidsbokningsuppgifter. Genom reformen utvidgades tillämpningsområdet för elektronisk delgivning till att också omfatta polisundersökning och förundersökning samt bötesförfarande.

Tidigare levererades delgivningarna per post om kunden inte separat gett samtycke till elektronisk delgivning (*opt in*). Trots att användningen av elektronisk delgivning på frivillig väg stadigt ökat var användningen inte tillräckligt utbredd för att leda till betydliga inbesparingar för myndigheterna. Den nya lagstiftningen innebär att ett konto i Suomi.fi-meddelanden öppnas automatiskt när en förvaltningskund identifierar sig med Suomi.fi-identifikation. Användaren kan ändå välja att avstå från tjänsten (*opt out*) genom att ändra användarkontots inställningar eller genom att kontakta kundtjänsten i Myndigheten för digitalisering och befolkningsdata. I enlighet med riksdagens beslut, som

baserar sig på grundlagsutskottets utlåtande, ska *opt out*-meddelandet vara i kraft i 365 dagar, varefter delgivning via Suomi.fi-meddelanden igen kan aktiveras ifall man identifierar sig i Suomi.fi-identifikation.

Avsikten med reformen är att medborgarna ska kunna uträtta ärenden smidigare och oberoende av plats och dessutom att myndighetsförfarandena ska bli effektivare och billigare. Den förväntade inbesparingen i form av minskade postningskostnader är tiotals miljoner euro årligen för den offentliga förvaltningen.

Den andra fasen i reformen innebär att man kan välja att motta myndighetsmeddelanden via kommersiella digitala posttjänster, såsom Kivra och OmaPosti. *RP 58/2026* avgavs till riksdagen den 16.4.2026, dvs. bara några dagar efter att den första fasen i reformen trätt i kraft. Reformens andra fas trädde i kraft den 1.9.2026. Därefter måste ännu avtal ingås mellan intresserade kommersiella digitala posttjänster och myndigheten för digitalisering och befolkningsdata innan dessa tjänster i praktiken kan lanseras.

Reformen gör det möjligt att läsa myndigheters delgivningar och andra myndighetsmeddelanden via kommersiella digitala posttjänster som anslutit sig till Suomi.fi-meddelanden. Användare av Suomi.fi-meddelanden kan alltså i fortsätt-

ningen själva välja om de vill läsa myndighetens delgivningar i Suomi.fi-meddelanden eller via kommersiella digitala posttjänster som anslutit sig till Suomi.fi. Användaren kan utnyttja en eller flera tjänster. Myndigheters delgivningar kan dock alltid läsas också i tjänsten Suomi.fi-meddelanden. Användningen av kommersiella digitala posttjänster baserar sig alltid på frivillighet.

Tanken är att reformen till denna del ska bidra till att medborgarna får en högklassig användarupplevelse och möjlighet att välja vilken tjänst de använder för mottagande av delgivningar samtidigt som det skapar förutsättningar för nya digitala affärsmodeller, en starkare digital tillväxtmiljö och innovationer. Ett annat mål är att elektronisk post från såväl myndigheter som privata avsändare i regel kan tas emot i en enda tjänst.

Det återstår att se om reformens andra fas ger användarna ett mer värde som motsvarar kostnaderna. Ur den offentliga förvaltningens perspektiv finns en risk att reformen främst leder till ökade kostnader utan att ge motsvarande nytta. Finland har ju redan sedan tidigare en offentlig tjänst för delgivning av myndighetsmeddelanden, och denna infrastruktur behöver även framöver upprätthållas. Projektet för att möjliggöra privata digitala posttjänster medför ca 8,5 miljoner euro i merkostnader plus kostnader för att fortlöpande upprätthålla dem. I värsta fall kan satsningarna på privata elektroniska posttjänster leda till att infrastrukturen för Suomi.fi-meddelandetjänsten eftersätts.

Det är möjligt att utvecklandet av elektronisk delgivning fortgår under nästa regeringsperiod med fokus på tjänster för företag och organisationer.

2. Utvecklandet av lagstiftning för användning av AI inom förvaltningen

Användning av AI för rådgivning och beslutsfattande inom förvalt-



Illustrasjon: Coulorbox/ChatGPT

ningen har varit ett viktigt tema i statminister Orpos regeringsprogram. Utveckling av artificiell intelligens går snabbt framåt, och myndigheterna ser allt större möjligheter att ta det i bruk. Under denna regering har man inlämnat en proposition till riksdagen för att möjliggöra användning av AI inom rådgivning och dessutom utreder man behovet av ändringar för att möjliggöra användning av AI inom beslutsfattande.

Myndigheter har redan i flera år använt tjänster som interagerar med förvaltningskunder (särskilt s.k. chattbottar). Innan 6 a § i lagen om tillhandahållande av digitala tjänster trädde i kraft i maj 2023 fanns det dock inte nationell allmän lagstiftning om myndigheternas automatiserade rådgivning. Bestämmelsen fogades till lagen om digitala tjänster i samband med regeringens proposition RP 145/2022 rd om automatiserat beslutsfattande. Vid den tidpunkten ansågs bestämmelsen

vara nödvändig för att tydliggöra gränsen mellan automatiserad rådgivning och automatiserat beslutsfattande. Bestämmelsen var avsedd att genomföra principen om god förvaltning och tjänsteansvar vid automatiserad rådgivning. Lagstiftaren ville uttryckligen utesluta användning av generativ AI i myndigheternas rådgivande verksamhet och invänta resultatet av förhandlingarna gällande EU:s AI-förordning innan man gick vidare.

Regeringen lämnade den 4 juni 2026 proposition 106/2026 till riksdagen med förslag till ändringar i lagen om tillhandahållande av digitala tjänster. I propositionen föreslås det att 6 a § i lagen om digitala tjänster ändras och att en ny 6 b § fogas till lagen.

I lagens 6 a § föreskrivs de allmänna förutsättningarna för användningen av automatiserad rådgivning. Enligt förslaget ska myndigheten säkerställa att kunderna alltid är informerade om att de

inte utväxlar meddelanden med en människa utan med en automatiserad rådgivningstjänst, och att kunderna kan spara utväxlingen av meddelanden. Myndigheten ska också alltid erbjuda sina kunder en möjlighet att kontakta en människa för att få rådgivning. I syfte att myndigheterna ska kunna fullfölja serviceprincipen effektivare och på fler sätt föreslås 6 a § bli ändrad så att myndigheterna förutom rådgivning också får ge anvisningar och handledning automatiserat.

I den föreslagna 6 b § finns det bestämmelser om skyldigheterna i anslutning till ibruktagandet och användningen av automatiserad rådgivning. Myndigheten ska före ibruktagandet säkerställa att den automatiserade rådgivningen uppfyller de krav som ställs på den. Myndigheten ska också övervaka den automatiserade rådgivningens lagenlighet under den tid den är i bruk. Myndigheten ska fästa särskild uppmärksamhet vid sina kunders rättsskydd och förbudet mot diskriminering.

Den föreslagna regleringen innebär i praktiken en riskbaserad modell för användning av AI inom myndigheternas digitala rådgivning. Myndigheterna kommer att måste etablera rutiner för att notera och avvärja risker för felaktiga svar som

” Syftet med utredningen är att bedöma under vilka rättsliga förutsättningar artificiell intelligens kan utnyttjas i olika skeden av myndighetens förvaltningsförfarande och vilka eventuella författningsändringar eller ny reglering som krävs för att AI-system ska kunna utnyttjas i olika skeden av förvaltningsförfarandet

genereras av den automatiserade rådgivningen. Det är också värt att notera att den föreslagna lagstiftningen inte möjliggör användning av AI i telefonrådgivning, utan enbart i digitala tjänster. Däremot utesluts det inte att ljudbaserad rådgivning ges i digitala tjänster. Att möjliggöra användning av AI i telefonrådgivning skulle ha krävt att ändringarna görs i förvaltningslagen som hör till justitieministeriets ansvarsområde. Lagen om tillhandahållande av digitala tjänster hör till finansministeriets ansvarsområde.

Under den här regeringsperioden har behovet av ändringar i lagstiftningen för att möjliggöra användning av AI vid beredning av beslut inom förvaltningen analyserats inom ramen för *projektet för undanröjande av hinder för digitalisering och informationens rörlighet*. Under projektets första fas var det ännu svårt att hitta exempel på situationer där myndigheterna hade planer på att använda AI inom beslutsfattning. Under den andra fasen tillsatte justitieministeriet en *utredning gällande användning av AI i förvaltningsförfaranden*. Som en del av denna utredning har man samlat in ny information om möjliga användningsexempel. Syftet med utredningen är att bedöma under vilka rättsliga förutsättningar artificiell intelligens kan utnyttjas i olika skeden av myndighetens förvaltningsförfarande och vilka eventuella författningsändringar eller ny reglering som krävs för att AI-system ska kunna utnyttjas i olika skeden av förvaltningsförfarandet. Utredningen utmynnar i en förstudie som ska vara klar innan den 31.12.2027. Beredningen av eventuella lagändringar kan påbörjas därefter.

Viveca Still, juris doktor, lagstiftningsråd. Finske redaktör.



Gorrissen Federspiel

Tue Goldschmieding

Forbud mod Huawei-udstyr var lovligt, men udgjorde ekspropriation

Østre Landsret afsagde den 24. juni 2026 dom i sag BS-61725/2023-OLR mellem TDC NET A/S og Forsvarets Efterretningstjeneste v/ Center for Cybersikkerhed (»CFCS«). Sagen angik, hvorvidt CFCS' forbud mod TDC NET A/S' brug af Huawei-udstyr i den danske telekommunikationsinfrastruktur var lovligt og, i givet fald, om forbuddet forpligtede staten til at betale erstatning.

TDC NET A/S havde siden 2011 anvendt udstyr fra Huawei i selskabets datatransmissionsnetværk. I 2023 nedlagde CFCS i medfør af § 3, stk. 1 og 2, i lov nr. 1156 af 8. juni 2026 om leverandørsikkerhed i den kritiske teleinfrastruktur (»den danske telesikkerhedslov«) forbud mod, at TDC NET A/S opretholdt og anvendte Huawei-udstyr. Forbuddet var begrundet i sik-



Illustrasjon: Coulorbox/ChatGPT

kerhedsmæssige betænkeligheder ved Huaweis udstyr, herunder manglende testning og adgang til fuld kildekode.

Da det ikke var teknisk muligt blot at udskifte dele af netværket, var TDC NET A/S nødsaget til at udskifte hele infrastrukturen. TDC NET A/S påstod, at forbuddet var uhjemlet og erstatningspådragende.

Landsretten fandt, at CFCS' afgørelse havde den fornødne hjemmel i den danske telesikkerhedslov.

Landsretten fandt imidlertid, at de vidtgående økonomiske konsekvenser for TDC NET A/S udgjorde ekspropriation, og tilpligtede CFCS at betale 80 millioner kr. i ekspropriationserstatning.

Læs afgørelsen her: <https://domstoldk.euwest01.umbraco.io/media/wgelogp5/bs-61725-23.pdf>

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

” Forbuddet var begrundet i sikkerhedsmæssige betænkeligheder ved Huaweis udstyr, herunder manglende testning og adgang til fuld kildekode.

