Lov & Data

Juni 2026
Nr. 166 2/2026

Innhold















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

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

Pelham II-domen: Har EU-domstolen räddat internetkulturen?

En klassisk upphovsrättslig fråga är i vilken utsträckning delar av ett verk eller en annan skyddad prestation får bli föremål för kreativ återanvändning utan rättsinnehavarens tillstånd. I den digitala miljön är återanvändning av detta slag vanlig, exempelvis i form av samplingar, mashuper, memer och fanfiction. I samband med införandet av nya skyldigheter för vissa onlineplattformar (artikel 17 i DSM-direktivet) har risken för att sådana moderna nyskapelser felaktigt ska fastna i filter som syftar till att hindra upphovsrättsintrång varit föremål för intensiv diskussion.

Daniel Westman

Den konstnärliga friheten och yttrandefriheten talar för att element från befintliga verk i viss utsträckning ska kunna användas i nyskapande. Att förhålla sig till tidigare skapande är enmviktig del av de flesta skapandeprocesser. En oinskränkt frihet att använda sig av andras verk när något nytt skapas skulle emellertid göra den upphovsrättsliga ensamrätten innehållslös.

EU-domstolens nyligen avkunnade dom i mål C-590/23 (Pelham II) tydliggör – tillsammans med tidigare domar från domstolen – de unionsrättsliga ramarna för kreativ återanvändning av element från skyddade prestationer. Målet rörde tolkningen av artikel 5.3 k i det s.k. infosoc-direktivet (direktiv 2001/29/EG). Denna bestämmelse tillåter att medlemsstaterna inför inskränkningar i ensamrätten för «användning i karikatyr-, parodi- eller pastischsyfte». I det nationella målet var frågan om en kort sampling av en musikinspelning kunde anses ske i pastischsyfte.

Domstolen konstaterade att begreppet pastisch inte har någon entydig innebörd i det allmänna språkbruket. Med utgångspunkt i infosoc-direktivets systematik och ändamål slog domstolen fast att begreppet i detta sammanhang avser

«skapelser som erinrar om ett eller flera befintliga verk, samtidigt som de uppvisar märkbara skillnader i förhållande till dessa verk, i syfte att med dessa verk inleda en form av konstnärlig eller kreativ dialog som är igenkännbar som sådan».

Pastischundantaget innebär sålunda inte någon generell rätt att använda andras verk i det egna skapandet. Men domstolen tycks samtidigt ha givit begreppet pastisch en vid tolkning. Domstolen hänvisar till att den konstnärliga friheten, yttrandefriheten och allmänintresset kräver en sådan tolkning.

Det centrala kriteriet är att syftet med återanvändningen ska vara att inleda en form av konstnärlig eller kreativ dialog med det använda verket. Återanvändningen måste därmed ske öppet och ta sikte på det använda verkets karakteristiska drag. Som exempel på dialog nämner EU-domstolen öppen stilistisk imitation, hyllning eller humoristisk eller kritisk bearbetning. Men även andra former av dialog kan innebära att det rör sig om en pastisch. Utanför inskränkningens tillämpningsområde faller emellertid återanvändning som innebär en dold imitation eller ett förtäckt plagiat. Karaktären av pastisch ska vara igenkännbar för någon som är förtrogen med verket och som har den intellektuella förståelsen som krävs för att uppfatta pastischen.

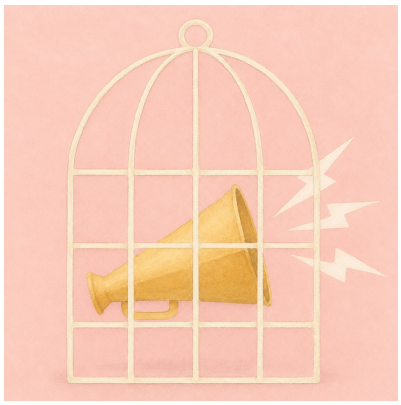
Hur kravet på dialog kommer att tolkas i nationell praxis återstår att se. Inget tyder dock på att kravet avser att begränsa tillämpningsområdet till etablerade kulturyttringar eller till diskussioner om viktiga samhällsfrågor. Även mer vardagliga uttrycksformer i internetkulturen, såsom memer och fanfiction, kan i många sammanhang omfattas av inskränkningen, men att så alltid är fallet går naturligtvis inte att säga.

Ett meme som saknar tillräcklig dialog med det befintliga verket kan i vissa fall istället vara tillåtet som en parodi. Av tidigare praxis från EU-domstolen (C-201/13, Deckmyn) framgår att det centrala kriteriet för en unionsrättsligt tillåten parodi är att det ska finnas ett humoristiskt eller förlöjligande syfte – som inte nödvändigtvis behöver rikta sig mot det använda verket eller dess upphovsman.

I Pelham II-målet var alltså den underliggande frågan om en sampling av en musikinspelning var tillåten. EU-domstolen konstaterar att sampling i princip omfattas av skyddet för den konstnärliga friheten och därför kan anses utgöra en pastisch om den sker i enlighet med de krav som diskuterats ovan, dvs. bland annat har till syfte att gå i en konstnärlig eller kreativ dialog med det befintliga verket (och inspelningen av detta). Domstolens ställningstagande kan på sikt påverka den marknad för licensiering av samplingar som finns i dag. Men eftersom bedömningen av vilka samplingar som faktiskt utgör pastischer ofta kan vara svår (jfr t.ex. användningen av en tvåsekunders trumsekvens i det nationella målet) och eftersom licensmarknaden är internationell och inte endast beroende av europeisk rätt, är det osäkert hur stor denna påverkan kommer att bli.

> I samband med det kommande genomförandet av förslaget från Utredningen om upphovsrättens inskränkningar förväntas dock även Sverige få ett pastischundantag, som får tolkas i linje med EU-domstolens dom i Pelham II.

Eftersom EU-domstolen i sin tidigare praxis har gett ensamrätten en vid tolkning och bl.a. slagit fast att även återanvändningen av mycket små – men ändå igenkännbara – delar av ett verk utgör en exemplarframställning, är den förhållandevis vida tolkningen av begreppet pastisch välkommen. Från rättighetshavarföreträdare har det dock uttryckts en oro för att domen skulle öppna för rent snyltningsbeteende i situationer där yttrandefriheten och den konstnärliga friheten inte gör sig gällande med någon större tyngd. Det kan ses som en viktig påminnelse om att balansen mellan skyddet för det som redan är skapat och skyddet för nyskapande hela tiden måste finjusteras utifrån omständigheterna i det enskilda fallet.



Colourbox / Chat GPT

I den svenska upphovsrättslagen finns det i dag inte något undantag för pastischer (annat än kopplat till rätten att ladda upp sådana i onlinetjänster för delning av innehåll som omfattas av artikel 17 i DSM-direktivet). Däremot anses det, i linje med de förarbetsuttalanden som gjordes i samband med upphovsrättslagens införande, finnas ett oskrivet undantag för travestier och parodier, genom att sådana skapelser anses vara självständiga verk med ett helt annat syfte. Detta trots att travestin och parodin kan innehålla synliga delar av befintliga verk. I samband med det kommande genomförandet av förslaget från Utredningen om upphovsrättens inskränkningar (SOU 2024:4) förväntas dock även Sverige få ett pastischundantag, som får tolkas i linje med EU-domstolens dom i Pelham II.

Daniel Westman. Oberoende rådgivare och forskare. Svensk redaktör för Lov & Data.

The CJEU's Russmedia Judgment: Joint Controllership and Platform Responsibility for User-Generated Content

By Päivi Korpisaari

The Grand Chamber of the Court of Justice of the European Union (CJEU) delivered a significant judgment on 2 December 2025 in *X v Russmedia Digital SRL and Inform Media Press SRL*, (C-492/23; ECLI (EU:C:2025:935), later Russmedia), clarifying the responsibilities of online platforms publishing user-generated content containing personal data. The Court held that the operator of an online marketplace may qualify as a joint controller together with the user posting unlawful content and that the liability exemptions of the eCommerce Directive (2000/31/EC) cannot limit obligations arising under the GDPR. The ruling is likely to have important implications for online marketplaces and other platforms relying on user-generated content.

Facts

Russmedia operated the Romanian website publi24.ro, an online marketplace where users could publish advertisements either free of charge or for a fee. An unidentified third party published a false advertisement presenting the applicant as offering sexual services. The advertisement included photographs of her and her telephone number, published without her consent.

Although Russmedia removed the advertisement within approximately one hour of being contacted by the applicant, the content had already spread to other websites reproducing the advertisement. The applicant subsequently brought proceedings against Russmedia, arguing that the publication infringed her right of personal portrayal, privacy, and reputation, and her data protection rights.

Russmedia argued that it merely acted as a hosting provider benefiting from the liability exemption under the eCommerce Directive. The Romanian appellate court accepted that argument. The applicant then appealed further, contending that the GDPR applied independently of the eCommerce Directive and that Russmedia had played an active role in managing and disseminating content published on its platform.

The referring Romanian court asked the CJEU to clarify the relationship between the GDPR and the eCommerce Directive, particularly in situations involving manifestly unlawful and harmful content containing personal data.

The CJEU Confirmed the GDPR Obligations for Online Marketplaces

The Court first noted that the advertisement contained personal data because it included information identifying the applicant, such as photographs of her and her telephone number. It further held that the data belonged to the special categories of personal data under Article 9 GDPR, since the advertisement concerned the applicant's alleged sex life. The Court emphasised that even false allegations relating to a person's sexual life remain sensitive personal data deserving enhanced protection.[1] The CJEU further clarified that uploading and publishing the adver-

Päivi Korpisaari

1 See Grand Chamber judgment *Commission v. Poland* (independence and private life of judges and publishing the data on the internet), C-204/21, ECLI: EU:C:2023:442 and *ZQ v. Medizinischer Dienst der Krankenversicherung Nordrhein, Körperschaft des öffentlichen Rechts* ('an employee's health data'), C667/21, EU:C:2023:1022.

tisement constituted processing of personal data under the GDPR.[2]

The Court then proposed a broad interpretation of the concepts of 'controller' and 'joint controllers', in line with its earlier case law.[3] Although the unlawful advertisement had been created by an anonymous user, Russmedia also qualified as a controller because it influenced the purposes and means of processing.[4] In particular, the platform published advertisements for its own commercial purposes, retained extensive rights over user content in its terms and conditions, and determined important aspects of dissemination, such as presentation, visibility, and distribution. Accordingly, the Court considered Russmedia and the anonymous advertiser to be joint controllers, even though Russmedia had neither created the harmful content nor shared the advertiser's unlawful intentions.

The judgment follows the Court's earlier case law, according to which each entity regarded as a joint controller must independently satisfy the requirements of controllership by significantly influencing the purposes and means of processing in pursuit of its own interests. At the same time, the Court has repeatedly emphasised that joint controllership does not require equal responsibility or participation in every stage of processing. Joint controllers need not exercise equal influence, participate in all stages of processing, or even have access to the personal data concerned. What is decisive is the actual influence exercised over the purposes and means of the processing of personal data. It may therefore be argued that the Court has interpreted the concept of joint controllership broadly and functionally.[5]

The Court further emphasised that, under Article 5 GDPR, personal data must be processed lawfully, fairly, transparently, accurately, and securely, and that controllers must take reasonable steps to rectify or erase inaccurate personal data without delay.

Online marketplace operators are therefore subject to the GDPR's accountability obligations if they are controllers of personal data. Therefore, they must implement appropriate technical and organisational measures before publishing advertisements containing personal data, particularly special categories of personal data under Article 9 of the GDPR. The Court's reasoning strongly reflects the logic of Articles 5(2), 24, 25, and 32 of the GDPR, effectively extending 'privacy by design' obligations to the architecture and operation of online platforms themselves.

The Court has already previously emphasised the particularly sensitive nature of special categories of personal data and the need for strict safeguards concerning their processing.[6] In this case, the Court stated that where advertisements may contain sensitive personal data, platforms must identify such advertisements in advance, verify the identity of the advertiser, and determine whether the advertiser is the data subject or has obtained the data subject's explicit consent. If identity verification is not possible, or if explicit consent cannot be demonstrated, the platform must refuse publication of the advertisement.

The Court also held that platforms must implement technical and organisational security measures to reduce the risk that sensitive personal data published online will be copied and unlawfully republished on other websites. The Court nevertheless clarified that platforms are not strictly liable for every subsequent unlawful dissemination of personal data online and must be allowed to demonstrate that their security measures were appropriate.

Furthermore, the Court observed that Article 26 of the GDPR requires joint controllers to define transparently their respective responsibilities under the Regulation.

Finally, the Court held that online marketplace operators cannot rely on the liability exemptions stated in Articles 12 to 15 of the eCommerce Directive in order to avoid responsibility for infringements of GDPR obligations. According to the Court, liability exemptions under the eCommerce

2 Regarding the concept of processing personal data, see, for example, Grand Chamber judgment *OT v. Vyriausioji tarnybinės etikos komisija* ('the operation of loading personal data on an internet page constitutes processing'), C184/20, EU:C:2022:601.

3 According to GDPR Article 4 subsection (7), "'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law" and according to the first sentence of GDPR Article 16(1) 'Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers'.

4 For example, in *Google Spain, S.L. y Google Inc. v. Agencia Española de Protección de Datos (AEPD) y Mario Costeja González* (C131/12), the CJEU interpreted Google as being a controller, even though a search engine such as Google does not control what is published on websites maintained by third parties.

5 See, for example, Grand Chamber judgmnet *Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos v. Valstybinė duomenų apsaugos inspekcija,* C683/21, EU:C:2023:949 and Fashion ID, C40/17, EU:C:2019:629 and *Wirtschaftsakademie Schleswig-Holstein GmbH v Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*, C-210/16, EU:C:2018:388.

6 For example, Grand Chamber judgment *OT v. Vyriausioji tarnybinės etikos komisija*, C184/20, EU:C:2022:601. See also note 1.

Directive cannot override or limit obligations arising under the GDPR. Even if a platform qualifies as an intermediary service provider, it must still comply with its own data protection obligations as a controller or joint controller.

The Court did not explicitly determine whether Russmedia qualified for the hosting liability exemption under the eCommerce Directive. Instead, it focused on the independent applicability of GDPR obligations, holding that intermediary liability exemptions cannot limit responsibilities arising under the GDPR.

Implications of the Judgment

Although the case formally concerned the eCommerce Directive, the reasoning is likely to have broader relevance under the Digital Services Act ('DSA'), which retained the core intermediary liability framework of the earlier directive. The judgment suggests that intermediary liability exemptions available to platform operators cannot limit obligations arising under the GDPR. Moreover, Article 2(4)(g) of the DSA expressly provides that the Regulation is without prejudice to Union law on the protection of personal data, in particular the GDPR and the ePrivacy Directive (Directive 2002/58/EC). This further supports the view that intermediary liability exemptions under the DSA cannot displace or limit obligations arising under EU data protection law.

More broadly, the judgment reflects an ongoing shift in EU digital law away from purely reactive notice-and-take-down systems, which are used, for example, to address copyright infringements, toward a more active model of platform responsibility. GDPR compliance obligations may already arise at the service-design stage, meaning that the architecture of digital platforms itself may be relevant when determining the legal status of the parties involved and the corresponding obligations under the GDPR.

The judgment therefore appears to move platform compliance from a primarily reactive model towards ex ante risk prevention and "preventive vigilance". Platforms enabling user-generated content may increasingly be expected to bear responsibility for the fundamental-rights risks inherent in the structure and functionalities of their services.

At the same time, the judgment should not be interpreted as establishing a general obligation to monitor all user-generated content. The decisive factors in the Court's reasoning were the presence of manifestly sensitive personal data under Article 9 of the GDPR, the obvious harmfulness of the content, the anonymous nature of the publication – which made it difficult, in practice, to hold the original author accountable – and the platform's structural role in enabling the dissemination and reuse of that content for its own commercial purposes.

Nevertheless, the obligations imposed by the Court create a certain tension with the prohibition on general monitoring obligations under EU intermediary law. In practice, ex ante identification of sensitive personal data may require automated screening systems or extensive moderation mechanisms capable of reviewing content before publication. At the same time, it would likely be impossible, in practice, to design an online platform or marketplace in a manner that entirely prevents the further dissemination or republication of content by third parties once published online, particularly given the ease with which digital content may be copied, captured, reproduced, and redistributed by users.

The case thus encourages platforms to adopt stricter identity verification systems and to limit anonymous publication. This creates a notable paradox: stronger protection of privacy and personal data may simultaneously incentivise platforms to collect more user identity data in order to reduce legal risk.

The judgment therefore raises important questions about the balance between freedom of expression, the right to private life, and the protection of personal data. This is particularly significant given that anonymous expression may itself constitute an important dimension of both freedom of expression and private life. Anonymity may enable individuals, for example, to seek peer support or information relating to illnesses, personal relationships, or sexual orientation without fear of stigma or exposure. More broadly, the ruling raises significant questions about the underlying logic and principles governing the regulation of digital platforms and online interaction in EU law.

The judgment may further contribute to a two-tier model of platform responsibility. Traditional notice-and-action procedures may remain sufficient for many forms of 'ordinary unlawful content', whereas content involving special categories of personal data may trigger significantly stricter ex ante obligations under the GDPR.

The significance of Russmedia's terms and conditions also remains noteworthy. The Court repeatedly referred to the platform's extensive contractual rights to use, distribute, reproduce, and commercially exploit user content. It therefore remains uncertain to what extent the finding of joint controllership depended on those particularly broad rights clauses. Platforms exercising more limited rights over user content might not necessarily qualify as joint controllers in the same way.

One notable aspect of the judgment is that the Court did not expressly rule on whether Russmedia fell within the scope of the hosting liability exemption under the eCommerce Directive. One particularly significant observation is that it may

reasonably be argued that the case did not concern a purely neutral hosting service. Russmedia did not merely passively store third-party content; rather, its core business activity consisted of publishing and disseminating third-party advertisements for commercial purposes. Moreover, the platform's terms and conditions appear to have granted Russmedia extensive powers over the publication, removal, distribution, and commercial exploitation of user-generated content, further distancing its role from that of a purely neutral intermediary.

It is also noteworthy that the GDPR's journalistic exemption under Article 85 does not appear to have been invoked in the proceedings. The implementation and scope of that exemption also vary considerably between Member States.[7] In any event, reliance on the journalistic exemption would have been fundamentally incompatible with Russmedia's own argumentation that it merely acted as a neutral hosting service provider within the meaning of the eCommerce Directive. Consequently, the judgment does not provide a comprehensive answer applicable to all forms of online publication, particularly journalistic and editorial contexts involving freedom of expression considerations.

In this respect, it is important to understand that digital platforms are often neither purely passive hosting services nor traditional publishers or editorial actors. Rather, they occupy an intermediate position and exercise significant structural power through, for example, algorithms, visibility management, moderation practices, and terms of service. From this perspective, platform responsibility may no longer be meaningfully assessed through a dichotomous model in which an actor is regarded either as a hosting provider benefitting from liability exemptions or as a publisher bearing full editorial responsibility for content.

Colourbox

The judgment additionally leaves several practical and doctrinal questions unresolved. The Court did not clarify the precise scope of liability for subsequent republication of unlawful content by third parties, nor did it explain when downstream dissemination may break the chain of causation for damages purposes. The Court nevertheless observed that the loss of control over personal data originated from the initial unlawful publication of the harmful advertisement in breach of the GDPR. The ruling therefore leaves substantial uncertainty regarding compensation claims under Article 82 GDPR in situations where information rapidly spreads across multiple online services.

Moreover, the Court imposed demanding compliance obligations without fully clarifying what level of identity verification, screening, or anti-copying measures should be regarded as sufficient or proportionate in practice. Considerable uncertainty therefore remains regarding how platforms can operationalise these obligations in technically and economically realistic ways. The broad and functional interpretation of joint controllership adopted by the CJEU may also create uncertainty concerning the allocation and limits of responsibility in complex digital platform environments involving multiple interconnected actors.[8]

The judgment may also incentivise platforms to remove or block

7 See Päivi Korpisaari, 'The journalistic exemption in personal data processing'in Taina Pihlajarinne & Anette Alén-Savikko (eds) *Artificial Intelligence and the Media: Reconsidering Rights and Responsibilities* (2022) 61–91.

8 Regarding the latter, see Benjamin Wong, 'Problems with controller-based responsibility in EU data protection law' (2021) *International Data Privacy Law, Volume 11, Issue 4,* 375–387.

lawful but potentially sensitive content more aggressively in order to minimise regulatory exposure. Consequently, the ruling may indirectly affect freedom of expression, anonymous speech, whistleblowing, and access to information online.

The judgment appears consistent with broader academic discussions according to which responsibility in platform environments increasingly stems from the functional role actors play in shaping dissemination, visibility, and interaction rather than merely from formally defined intermediary categories.[9]

Finally, Russmedia reinforces a broader trend in European law: responsibility increasingly follows platforms' actual influence over the conditions under which digital content is created, organised, moderated, and interacted with online, as well as over the dissemination architecture, visibility, and amplification of such content. In this respect, the judgment resembles the broader approach adopted by the European Court of Human Rights in the Grand Chamber judgments Delfi AS v. Estonia (Application no. 64569/09), concerning civil liability for unlawful user comments, and Sanchez v. France (Application no. 45581/15), concerning criminal liability relating to user-generated content.[10] Russmedia may therefore prove to be an important step in the development of EU digital law towards a model in which platforms that actively structure, disseminate, and commercially exploit user-generated content may bear increasing responsibility for the fundamental-rights risks connected to such activities. The judgment also reflects a broader understanding according to which digital infrastructures and technical architectures are not neutral, but actively shape the dissemination of information and the allocation of risks and responsibilities online.[11]

> Russmedia may therefore prove to be an important step in the development of EU digital law towards a model in which platforms that actively structure, disseminate, and commercially exploit user-generated content may bear increasing responsibility for the fundamental-rights risks connected to such activities.

Päivi Korpisaari is Professor of Communication Law at the University of Helsinki. Her research focuses on media and information law, data protection, constitutional and human rights law, tort law, and legal questions relating to new technologies and artificial intelligence. She has led several research projects and serves in multiple national and international expert positions, including the Council of Europe's Access Info Group.

9 See, for example, Natali Helberger, Jo Pierson & Thomas Poell, 'Governing online platforms: From contested to cooperative responsibility' (2017)*The Information Society*, 34, 91–14 and (very critical) Tobias Mast, 'Responsibility in the Platform Quadrangle: Balancing Rights between Content-Creating Users, Internet Service Providers, Affected Parties and Recipients; Also a Case Note on CJEU Russmedia, Case-492/23, [2025] ECLI:EU:C:2025:93' (2025) working paper, https://doi.org/10.21241/ssoar.108734

10 For further discussion, see Päivi Korpisaari 'From *Delfi to Sanchez* – when can an online communication platform be responsible for third-party comments? An analysis of the practice of the ECtHR and some reflections on the Digital Services Act' (2022) *Journal of Media Law, 14*(2), 352–377 and Päivi Korpisaari 'Sanchez v France: ECtHR judgment raises questions about a politician's liability to moderate his own Facebook "wall"' (2023) *Journal of Media Law,* 15(2), 140–151.

11 See Thomas Poell, David Nieborg, and José van Dijck,'Platformisation' (2019) *Internet Policy Review,* 8(4).

Skadeståndsansvaret enligt GDPR – en genomgång av EU-domstolens praxis

Av Fredrik Sandberg

Inledning

Det särskilda skadeståndsansvaret enligt artikel 82 i GDPR var länge mycket oklart och föremål för olika tolkningar. Genom en serie domar från EU-domstolen de senaste tre åren har rättsläget klarnat i flera väsentliga avseenden. Min avsikt är att i den här artikeln kort sammanfatta den praxisutveckling som skett och vad vi därigenom för närvarande vet om rättsläget, men även att peka på några viktiga punkter där det alltjämt finns behov av ytterligare klargöranden. En mer utförlig genomgång av praxis och analys av skadeståndsansvaret återfinns i min avhandling *Skadeståndsansvar vid personuppgiftsbehandling – En undersökning av skadeståndsansvaret enligt dataskyddsförordningen*.

Ansvaret

En fråga som det tidigare rådde delade meningar om gällde huruvida skadeståndsansvaret enligt GDPR är ett strikt ansvar eller ett oaktsamhetsansvar. Oenigheten gällde framför allt om redan en konstaterad överträdelse av förordningens regler är grund för ansvar, eller om det därutöver också krävs uppsåt eller oaktsamhet. Till stor del tycks de olika uppfattningarna ha grundat sig i olika tolkningar av vad regeln om att undgå ansvar i artikel 82.3 egentligen innebär.

Genom domarna i målen C-340/21 och C-667/21 har EU-domstolen numera fastställt att skadeståndsansvaret enligt artikel 82 inte är strikt, utan att det istället är ett slags presumerat ansvar för oaktsamhet. Enligt EU-domstolen behöver den registrerade visserligen endast visa att det förekommit en överträdelse av förordningens regler, men den personuppgiftsansvarige kan i sådana fall undgå skadeståndsansvar genom att visa att denne inte varit oaktsam. Om den registrerade visar att det har förekommit en regelöverträdelse presumeras således den personuppgiftsansvarige ha varit oaktsam, vilket det ankommer på den senare att motbevisa. Enligt EU-domstolen kan den personuppgiftsansvarige bryta presumtionen om oaktsamhet genom att visa att denne vidtagit lämpliga tekniska och organisatoriska åtgärder för att efterfölja förordningens regler (jfr artiklarna 24, 25 och 32), alternativt visa att bristen på sådana åtgärder saknade betydelse för skadans uppkomst (bristande orsakssamband). Framför allt domen i mål C-340/21 innehåller flera vägledande uttalanden om hur en nationell domstol ska bedöma huruvida den personuppgiftsansvariges åtgärder ska anses ha varit lämpliga.

Situationerna som EU-domstolen hade att bedöma i de ovan nämnda rättsfallen involverade endast en ensam personuppgiftsansvarig. Varken i de nämnda målen eller i senare domar har EU-domstolen tagit ställning till skadeståndsansvaret i en situation med flera gemensamt personuppgiftsansvariga. Visserligen kan man utgå ifrån att det presumtionsansvar domstolen har fastslagit gäller även för gemensamt personuppgiftsansvariga, men likväl kan en situation med gemensamt

Fredrik Sandberg

personuppgiftsansvar gestalta sig något annorlunda och tänkas ge upphov till särskilda frågor. Det kan till exempel nämnas att EU-domstolen i sin praxis beträffande gemensamt personuppgiftsansvariga har uttalat att ett sådant gemensamt ansvar inte nödvändigtvis innebär att de inblandade har samma ansvar, utan att skyldigheterna kan fördela sig olika (C-40/17). Det återstår emellertid för EU-domstolen att förtydliga vilken betydelse det nyssnämnda har inom ramen för det presumtionsansvar domstolen har etablerat enligt artikel 82.

EU-domstolen har hittills inte heller berört frågan om skadeståndsansvar vid behandling där det förekommer personuppgiftsbiträden. Det finns visserligen argument för att även personuppgiftsbiträden – inom ramen för sina mer begränsade skyldigheter – är underkastade ett presumtionsansvar motsvarande eller liknande det för personuppgiftsansvariga, men rättsläget får trots allt betraktas som osäkert. Det

är inte heller alldeles klart hur den personuppgiftsansvarige mer exakt kan undgå det presumerade ansvaret när skadan har orsakats av behandling som utförts av personuppgiftsbiträdet; blir saken beroende av de implementerade åtgärdernas lämplighet helt oberoende av om ett personuppgiftsbiträde har anlitats eller ej, eller ska bedömningen ta sikte på om den personuppgiftsansvariges val, instruktioner och övervakning av personuppgiftsbiträdet varit lämpliga?

Vad gäller den personuppgiftsansvariges ansvar för sina anställda har EU-domstolen i mål C-741/21 uttalat att det inte är möjligt att undgå ansvar med hänvisning till att anställda har försummat att följa interna instruktioner. Det tycks i praktiken innebära att anställdas försumliga handlingar eller underlåtenheter tillskrivs den personuppgiftsansvarige, vilket i allt väsentligt då skulle motsvara regler om principalansvar eller identifikation i nordisk skadeståndsrätt. Dock har EU-domstolen ännu inte tagit ställning till hur skadeståndsansvaret enligt GDPR förhåller sig till situationer där anställda med uppsåt bryter mot den personuppgiftsansvariges instruktioner. EU-domstolens tidigare praxis beträffande uppkomsten och gränserna för personuppgiftsansvar kan dock vara till viss ledning i det avseendet.

Skada

Skadebegreppen i artikel 82 utgör autonoma unionsrättsliga begrepp som det ytterst ankommer på EU-domstolen att uttolka. Enligt EU-domstolen utgör kraven på överträdelse och skada kumulativa krav, det vill säga att skadan måste utgöra en konsekvens av överträdelsen som kan särskiljas från överträdelsen som sådan (C-300/21). En överträdelse av reglerna i GDPR innebär således inte i sig en skada och medför inte heller en presumtion för skada (C-200/23 och C-526/24).

En ideell skada behöver inte vara av viss allvarlighetsgrad eller omfattning för att vara ersättningsgill (C-300/21). Med and ord behöver en ideell skada inte nå upp till en viss miniminivå, utan även en ringa ideell skada ska ersättas.

> Det finns visserligen argument för att även personuppgiftsbiträden – inom ramen för sina mer begränsade skyldigheter – är underkastade ett presumtionsansvar motsvarande eller liknande det för personuppgiftsansvariga, men rättsläget får trots allt betraktas som osäkert.

Det följer dock av EU-domstolens praxis att den registrerade måste visa att det varit fråga om en ideell skada i GDPR:s mening (C-300/21, C-340/21 och C-456/22). I viss utsträckning har EU-domstolen klargjort vad som utgör en ideell skada i GDPR:s mening. Enligt EU-domstolen är det till exempel inte risken för ett framtida missbruk som utgör den ideella skadan, men däremot kan fruktan för sådant missbruk innebära en ideell skada (C-340/21). Det behöver således inte nödvändigtvis ännu ha förekommit något missbruk av personuppgifterna eller liknande konkreta negativa effekter för att en ideell skada ska uppkomma.

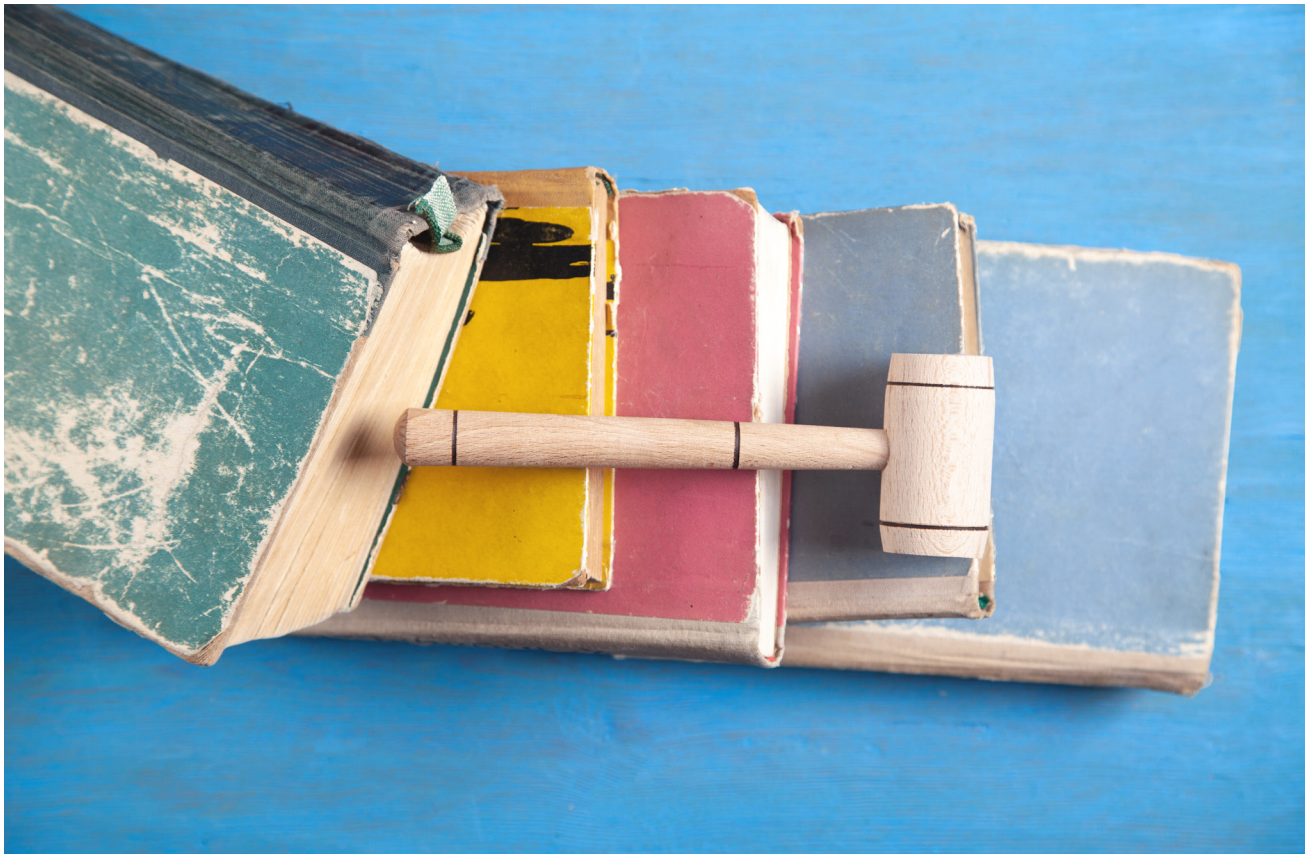
Med utgångspunkt i hittillsvarande praxis tycks med ideell skada framför allt avses olika typer av känslomässiga reaktioner (C-340/21, C-200/23, C-655/23 och C-526/24). Sådana känslomässiga reaktioner till följd av en förlorad kontroll eller ett spridande av personuppgifter efter dataintrång måste då framstå som välgrundade (C-340/21 och C-526/24). Det utesluter dock inte att även andra typer av faktiska konsekvenser för den registrerade utgör ideell skada i GDPR:s mening, vilket inte minst skäl 78 och 85 i GDPR antyder, men det återstår för EU-domstolen att utveckla sin praxis i det här avseendet.

Ersättning

Eftersom artikel 82 i GDPR saknar regler om ersättning, ska storleken på ersättningen fastställas enligt nationell rätt, med förbehåll för att principerna om likvärdighet och effektivitet då måste respekteras. Det innebär att ersättningsnivåerna blir en fråga för nationell rätt och de nationella domstolarna att fastställa. Några mer precisa uttalanden om ersättningsnivåer i beloppstermer kan därför inte förväntas från EU-domstolen. Dock har EU-domstolen i ett flertal domar gett vägledning om vilka krav effektivitetsprincipen innebär när nationell rätt ska tillämpas för att fastställa ersättningens storlek.

Av EU-domstolens praxis framgår att effektivitetsprincipen i det här sammanhanget framför allt innebär att ersättningen till den registrerade ska utgöra full *kompensation* för den faktiskt uppkomna skadan (C-300/21). I enlighet med det nyssnämnda har EU-domstolen betonat att ersättningen varken har en avskräckande eller bestraffande funktion (C-300/21 och C-667/21). Överträdelsens allvar eller graden av vållande saknar därför betydelse, liksom för övrigt de kriterier som tillämpas vid sanktionsavgifter enligt artikel 83 (C-667/21 och C-741/21). Av samma skäl är inte heller antalet överträdelser eller skadevållarens motiv relevant för ersättningens storlek (C-741/21 och C-507/23).

Eftersom även ringa skador ska ersättas finns det inte heller något som hindrar att ersättningen fastställs till ett ringa belopp, så länge ersättningen står i proportion till skadan och därför kan anses utgöra full kompensation (C-182/22 och



Colourbox

C-189/22). Vid bedömningen av om den registrerade är fullt kompenserad kan även beaktas att denne erhållit icke-ekonomisk kompensation, till exempel i form av er ursäkt, men däremot inte att den personuppgiftsansvarige blivit föremål för ett förbudsföreläggande (C-507/23 och C-655/23).

Avslutning

Genom de förhållandevis många avgöranden EU-domstolen meddelat de senast tre åren har skadeståndsansvaret enligt artikel 82 blivit klarlagt i flera viktiga avseenden. Som förhoppningsvis framgått av den här redogörelsen för praxis så finns det emellertid i vissa delar alltjämt ett behov av vägledning från EU-domstolen.

Fredrik Sandberg, jur.dr och disputerade 2025 på avhandlingen Skadeståndsansvar vid personuppgiftsbehandling – En undersökning av skadeståndsansvaret enligt dataskyddsförordningen. Han arbetar idag som dataskyddsombud på If Skadeförsäkring och är även knuten som fellow vid SCCL (Stockholm Centre for Commercial Law) och associate på IRI (Institutet för Rättsinformatik) vid Stockholms universitet.

Oppdaterte SSA-bestemmelser om data – hva er nytt?

Av Sara Lamøy Engberg, Lucia Maksim og Stian Sørensen Schilvold

Sara Lamøy Engberg

Lucia Maksim

Stian Sørensen Schilvold

1. Innledning

I mars 2026 oppdaterte Direktoratet for forvaltning og økonomistyring (DFØ) databestemmelsene i de fleste av statens standardavtaler (SSA).

Målet har blant annet vært å tydeliggjøre rettigheter til data, styrke kundens kontroll over egne data og presisere leverandørens bruksrett. Samtidig får leverandøren et klarere – men fortsatt begrenset – handlingsrom til å bruke enkelte datatyper til tjenesteforbedring. Oppdateringen har vært nødvendig, men den fritar ikke partene fra å måtte ta stilling til sentrale spørsmål om bruksrett, kostnader, formatkrav og exit i vedleggene til den enkelte avtale.

Som en del av arbeidet har DFØ også laget en *veileder* som forklarer hvordan DFØ mener at de oppdaterte bestemmelsene skal forstås.

I denne artikkelen går vi gjennom hovedtrekkene i de oppdaterte bestemmelsene. Vi ser ikke nærmere på endringene i SSA-F.

2. Et område i stadig utvikling

Reguleringen av rettigheter til data er i stadig utvikling, særlig i EU. Et gjennomgående trekk ved kommende lovgivning er økt kontroll over og bedre tilgang til egne data. To sentrale eksempler er Data Act (dataforordningen) og Data Governance Act (dataforvaltningsforordningen), som vil få betydning for regulering av data også i Norge. Begge forordningene er EØS-relevante, men foreløpig ikke gjennomført i norsk rett.

> Oppdateringen har vært nødvendig, men den fritar ikke partene fra å måtte ta stilling til sentrale spørsmål om bruksrett, kostnader, formatkrav og exit i vedleggene til den enkelte avtale.

Data Act regulerer blant annet rettigheter til og tilgang til data som skapes ved bruk av tilkoblede produkter og tjenester (Internet of Things), mens Data Governance Act blant har som mål å fremme bedre datahåndtering og –deling i EU.

I veilederen presiserer DFØ at de følger utviklingen tett, og vil vurdere behovet for nye revisjoner når nytt regelverk gjennomføres i norsk rett.

3. Hvordan bør leverandør og kunde håndtere de oppdaterte bestemmelsene?

Leverandører som er avhengige av datatilgang for å videreutvikle tjenestene sine, bør vurdere om de oppdaterte bestemmelsene gir tilstrekkelig bruksrett. Kunder som må sikre kritiske virksomhetsdata, bør på sin side vurdere om bestemmelsene gir tilstrekkelig kontroll og beskyttelse.

Leverandører og kunder med faste avvikskataloger, bør vurdere

om disse må oppdateres i lys av endringene. Begge parter bør dessuten avklare hvordan leverandørens utvidede forpliktelser i standardavtalene vil påvirke kostnadsbildet i prosjektet, og hvordan eventuelle økte kostnader skal håndteres. Ved å adressere dette på avtalestadiet får partene bedre forutberegnelighet, og kan redusere risikoen for senere konflikt.

Partene bør også merke seg at SSA-oppdateringene åpner for at «andre reguleringer kan angis av Kunden i Bilag 1», altså i kundens kravspesifikasjon. Vi mener denne formuleringen skaper en uklarhet. Isolert sett kan ordlyden tyde på at bare kunden kan endre standardteksten gjennom bilag 1, med den konsekvens at det er kunden alene som kan foreta slike endringer. Det ville i så fall vært et avvik fra den vanlige forrangstrukturen i SSA-avtalene, hvor leverandørens eksplisitte forbehold i bilag 2 går foran bilag 1. Etter vår vurdering er det likevel klart at dersom leverandør tar et eksplisitt forbehold i bilag 2, som kunden aksepterer, må slike forbehold gå foran i tilfelle motstrid, også når det gjelder datarettighetsbestemmelsene.

4. Hvilke avtaler er endret?

DFØ har oppdatert følgende avtaler:

- SSA-D (driftsavtalen)
- SSA-L (løpende tjenesteleveranse)
- SSA-store sky og SSA-lille sky
- SSA-V (vedlikeholdsavtalen)
- SSA-B og SSA-B enkel (bistandsavtalene)
- SSA-O (oppdragsavtalen)
- SSA-T (utviklings- og tilpasningsavtalen)
- SSA-S (smidigavtalen)
- SSA-F (forskningsavtalen)

SSA-R, som ikke ble endret i denne runden, brukes typisk sammen med en spesifikk leveranseavtale. Rettigheter til data vil da reguleres i det enkelte avrop, og løsningen kan variere med leveransen.

SSA-K er heller ikke endret. Den gjelder kjøp av standardkomponenter som utstyr, programvare og tilhørende komponenter.

DFØ har forsøkt å harmonisere endringene på tvers av avtalene. Samtidig påpeker DFØ i veilederen at de ulike avtalene gjelder svært forskjellige leveranser, og at reguleringen på enkelte punkter derfor er ulik.

5. Utgangspunktet: kunden beholder rettigheter til data leverandøren får tilgang til

De oppdaterte SSA-avtalene inneholder i hovedsak likelydende bestemmelser om at kunden «beholder rettigheter til data som tilgjengeliggjøres for Leverandøren». Kunden får også rettighetene til data som «samles inn, prosesseres, bearbeides, genereres, oppstår eller på annen måte behandles», samt resultatene av slik behandling. Varianter av bestemmelsen fantes også tidligere i de fleste SSA-avtalene. For SSA-B, SSA-B enkel, SSA-O og SSA-S er dette imidlertid nytt.

Formuleringen «beholder sine rettigheter» innebærer, naturlig nok, at avtalene ikke gir kunden videre rettigheter til data enn kunden allerede har. Data kan være underlagt begrensninger etter lov, avtale eller andre tredjepartsrettigheter. Det kan for eksempel følge av konkurranseregelene, av at dataene utgjør forretningshemmeligheter eller personopplysninger, eller av at de omfattes av sikkerhetsloven. Data kan også inngå i et åndsverk, eller være strukturert, samlet og bearbeidet på en måte som utløser databasevern. Hvis tredjepart har rettigheter til data leverandøren får tilgang til, endrer ikke SSA-reguleringen det underliggende rettighetsforholdet.

Det sentrale i SSA-sammenheng er likevel at kunden, i forholdet til leverandøren, beholder kontrollen over data som gjøres tilgjengelig for leverandøren. I praksis samsvarer dette med det mange profesjonelle aktører allerede legger til grunn: Data som gjøres tilgjengelig for leverandøren, kan ikke brukes fritt til andre formål enn dem avtalen åpner for. For leverandøren betyr det at nødvendige bruksrettigheter må forankres i avtale.

6. Leverandørens bruksrett

6.1 Leverandøren har begrenset bruksrett til kundens data

Hovedregelen i de oppdaterte avtalene er at leverandøren får den bruksrett som er nødvendig for å oppfylle avtalen.

Leverandøren vil ofte også ønske å bruke data til å videreutvikle egne produkter og tjenester. DFØ har delvis tatt høyde for dette ved i enkelte standardavtaler å regulere leverandørens rett til å bruke (i) anonymiserte bruksdata og (ii) etablerings- og prosjektdata.

Disse bruksrettene er ikke tatt inn i SSA-B, SSA-B enkel og SSA-O, som alle gjelder ulike former for konsulentbistand. I slike leveranser vil det ofte ikke oppstå data det er praktisk behov for å bruke videre, utover knowhow og lignende som leverandøren allerede kan utnytte etter gjeldende bestemmelser.

Hvis leverandøren ønsker en videre bruksrett, for eksempel til demonstrasjon eller markedsføring, må dette reguleres særskilt, enten i bilag 1 eller i egne avtaler om datatilgang. Kunden kan på sin side ønske å begrense bruksretten ytterligere, for eksempel hvis den kan gi leverandøren innsikt i konkurransesensitiv informasjon.

6.2 Leverandørens rett til å bruke anonymisert bruksdata til forbedring av egne tjenester

I standardavtalene for løpende tjenester får leverandøren rett til å bruke anonymiserte data om kundens bruk av tjenesten for å forbedre egne tjenester. Dette gjelder SSA-D, SSA-L, SSA-store sky og -lille sky og SSA-V.

En tilsvarende bestemmelse er ikke tatt inn i SSA-T eller SSA-S, fordi disse avtalene gjelder imple-

mentering av en løsning og ikke løpende tjenesteleveranse. Da vil det i utgangspunktet heller ikke oppstå denne typen bruksdata. Hvis behovet likevel oppstår i SSA-T eller SSA-S, må partene regulere dette i bilag 1.

Data om kundens bruk av tjenesten vil typisk kunne gi innsikt i kundens bruks- og handlingsmønstre. Det kan for eksempel være informasjon om volum (antall brukere), hyppighet (hvor ofte) og varighet (hvor lenge) av bruk, hvordan ulike funksjoner brukes, og logger knyttet til sikkerhet og etterlevelse. For leverandøren er slik informasjon ofte verdifull, og noe man ønsker tilgang til, fordi blant annet fordi den viser bruksmønstre, hvilke funksjoner som brukes mest, og hvilke brukertyper som logger seg inn oftest mv.

At bruksdataene bare kan brukes til å «forbedre egne tjenester», omfatter for eksempel formål som tjeneste- og produktforbedringer, videreutvikling av funksjoner, feilretting og annen optimalisering. Kommersielle formål som markedsføring, prisstrategi eller utvikling av tjenester utenfor avtalen faller antagelig utenfor.

Bestemmelsen er likevel vid. Bruksdata kan i noen tilfeller enten inneholde, eller gjøre det mulig å utlede, forretningssensitiv informasjon om kundens økonomi, ressursbruk eller strategiske prioriteringer. Kunden bør derfor vurdere om det er nødvendig å avgrense eller presisere rammene for leverandørens bruksrett i bilag 1.

For at leverandøren skal kunne bruke slik bruksdata, må de være anonymisert. DFØ viser her til anonymiseringsbegrepet i personvernforordningen. Det innebærer at fysiske personer ikke lenger er identifiserte eller identifiserbare, verken direkte eller indirekte, jf. artikkel 4 nr. 1 og fortalepunkt 26.

6.3 Etablerings- og prosjektdata

Alle de oppdaterte avtalene, unntatt SSA-B, SSA-B enkel og SSA-O, gir også leverandøren rett til å bruke «innsamlede eller genererte data knyttet til etablering for å forbedre sine tjenester». I SSA-T og SSA-S er «etablering» erstattet med «prosjektgjennomføring».

For avtalene som også gir bruksrett til anonymiserte bruksdata, presiserer bestemmelsene at de to bruksrettene gjelder side om side.

Ordlyden er ikke helt klar, men omfatter trolig data om testresultater, feillogger, estimeringsdata, utviklingsinnsikt og prosjektrapporter mv. Det forutsettes samtidig at disse dataene ikke inneholder kundens virksomhetsdata, sikkerhetsmessige forhold, taushetsbelagte opplysninger eller andre data underlagt lovbestemte begrensninger. Hvis dataen inneholder slik informasjon, kan leverandøren likevel ikke bruke dem til tjenesteforbedring.

7. Kundens kontroll over egne data

7.1 En kjent utfordring – kunden mister oversikt over egen data

I langvarige IT-leveranser er det en kjent utfordring at kunden gradvis mister oversikt og kontroll over egne data. Dette kan skape problemer underveis i avtaleforholdet, men blir ofte særlig tydelig i en exitsituasjon eller ved konflikt. Kunden forbereder et leverandørskifte, og innser at det er vanskelig å få oversikt over hva leverandøren faktisk gjør, og hvilke data leverandøren har tilgang til. Det kan igjen gjøre det vanskelig å koordinere overgangen til ny leverandør og å utforme en presis kravspesifikasjon.

Situasjonen kan også svekke kundens forhandlingsposisjon overfor leverandøren. Hvis avtalen i tillegg er uklar, blir det vanskeligere for kunden å stille tydelige og konkrete krav – både ved exit og ellers.

De oppdaterte SSA-avtalene skal motvirke denne typen situasjoner ved å gi kunden bedre kontroll over egne data. Det skjer blant annet ved at leverandøren ikke kan holde tilbake data, og ved at leverandøren får en løpende plikt til å gjøre data tilgjengelig. Reguleringen følger den generelle utviklingen mot sterkere kontroll over egne data, samtidig som den legger et betydelig ansvar på leverandøren.

7.2 Ingen tilbakeholdsrett, og løpende plikt til utlevering av data på forespørsel

I avsnittet om leverandørens bruksrett og tilgang til data heter det blant annet at «Kunden skal til enhver tid ha tilgang til data som Kunden har rettighetene til, og Leverandørens behandling av disse.».

Bestemmelsen sier imidlertid lite om hva denne tilgangsretten konkret innebærer. Hvis det er viktig for kunden å få data utlevert i bestemte formater, med bestemt hyppighet eller på andre nærmere vilkår, bør dette presiseres i bilag 1. Partene bør videre sikre at kostnader ved slik utlevering håndteres på en fornuftig måte. Desto mer spesifikke krav som stilles fra kunden, desto viktigere blir denne typen avklaringer for leverandør.

Videre slår avtalene fast at leverandøren under ingen omstendighet kan utøve tilbakeholdsrett i kundens data. Bestemmelsen styrker kundens vern ved konflikt eller uenighet om for eksempel endringsregimet, og hindrer at leverandøren bruker kundens data som pressmiddel.

For leverandøren betyr dette at databehandlingen bør innrettes slik at krav om tilgjengeliggjøring kan oppfylles uten unødige kostnader og forsinkelser. Gode forberedelser kan redusere både arbeidsomfanget og kostnadene ved formattilpasning og annen bearbeidelse før utlevering.

7.3 Leverandørens plikt til å tilgjengeliggjøre data ved avtalens opphør

Det er også innført en ny bestemmelse om tilgjengeliggjøring av data ved avtalens opphør.

Etter bestemmelsen skal leverandøren «ved avtalens opphør [skal] tilgjengeliggjøre data til Kunden el-

ler den Kunden utpeker på et allment tilgjengelig og maskinleselig format, med opprinnelige strukturer og metadata intakt.»

Tilpassede varianter av bestemmelsen er tatt inn i SSA-D, SSA-L, SSA-store sky, SSA-lille sky, SSA-V, SSA-B, SSA-B enkel og SSA-O. Bestemmelsen er derimot ikke tatt inn i SSA-T og SSA-S, fordi databehandlingen der normalt skjer i kundens egne miljøer. Leverandøren vil da som utgangspunkt ikke sitte med data som skal leveres tilbake. Hvis prosjekt- eller utviklingsmiljøer unntaksvis leveres gjennom leverandøren, bør partene ta høyde for dette i bilagene.

Bestemmelsen gir kunden en rett og leverandøren en plikt til å gjøre data tilgjengelige ved avtalens opphør. «Den kunden utpeker» kan for eksempel være en ny systemleverandør, integrator eller andre tredjeparter.

Bestemmelsen stiller også noen konkrete krav til format og datakvalitet.

For det første skal dataene gjøres tilgjengelige i et «allment tilgjengelig» format. DFØ presiserer at dette innebærer at formatet må være åpent. Formatet må være dokumentert, og dokumentasjonen må være fritt tilgjengelig.

For det andre må dataene gjøres tilgjengelige i et «maskinleselig format», altså i et format som annen programvare kan gjenkjenne og viderebehandle. Som DFØ påpeker, kan et maskinleselig format være både åpent og lukket. Det er derfor ikke automatisk overlapp mellom de to kravene, og de må leses i sammenheng.

For det tredje må dataene gjøres tilgjengelige «med opprinnelige strukturer og metadata intakt». Det betyr at struktur, sammenhenger og beskrivende informasjon ikke skal gå tapt. Leverandøren kan med andre ord ikke nøye seg med å levere rådata løsrevet fra sin sammenheng.

Disse kravene skal sikre at kunden faktisk får data som er brukbare

Colourbox / Chat GPT

ved videre bruk. Bestemmelsen er ment å motvirke leverandørinnlåsing, og styrke kundens digitale handlefrihet. Selv om bestemmelsen gir et betydelig minimumsvern, bør kunden vurdere om det er behov for mer detaljerte krav til format eller kvalitet i bilag 1.

Data skal gjøres tilgjengelige «ved avtalens opphør», men dette er neppe ment som en absolutt frist. DFØ skriver at hvor raskt data kan gjøres tilgjengelige, vil bero på blant annet datamengde, format og tekniske løsninger. For å unngå uklarhet anbefaler vi likevel at partene i bilag spesifiserer hva som ligger i «ved avtalens opphør», eller avtaler en konkret frist som hensyntar relevante forhold ved leveransen.

Det er bare SSA-D, SSA-store sky og SSA-T som uttrykkelig krever en avslutningsplan for bistand ved avtalens opphør. En tilsvarende ordning kan likevel være hensiktsmessig også i andre leveranser. En overordnet exit-plan, utarbeidet tidlig, kan gi begge parter bedre forutsigbarhet og struktur når leveransen går inn i avslutningsfasen.

Kravene til tilgjengeliggjøring av data vil antagelig medføre økte kostnader for leverandør. Et praktisk viktig spørsmål er hvem som skal dekke disse kostnadene. I SSA-D er det lagt opp til at bistand til dette skal skje på medgått tid. Alternativet er å prise dette som en del av produktet eller den løpende tjenesten.

7.4 Krav om sletting av data fra leverandørens systemer

Flere av avtalene pålegger leverandøren en automatisk plikt til å slette data ved avtalens opphør eller ved utløpet av garantiperioden.

DFØ legger til grunn at data først er slettet når de er fjernet fra leverandørens databaser og systemer på en måte som utelukker gjenoppretting. Plikten omfatter også sletting av kopier og at leverandørens tilgang til dataene opphører.

Bestemmelsen sier imidlertid ikke nærmere når slettingen skal skje. Kunden bør derfor presisere at sletting først skal skje etter at kunden har fått tilgang til de aktuelle dataene.

Selv om en slik sletteplikt ikke er uvanlig, kan fullstendig sletting av kundedata fra leverandørens systemer være både ressurs- og kostnadskrevende. Også på dette punkt bør derfor partene bli enig i hvordan kostnadene skal dekkes.

Det må dessuten tas høyde for at leverandøren i enkelte tilfeller kan ha lovpålagt plikt til å bevare visse kategorier av data, for eksempel etter bokføringsloven eller hvitvaskingsloven.

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

Lucia Maksim, advokatfullmektig i Advokatfirmaet Bulls avdeling for teknologi og immaterialrett.

Stian Sørensen Schilvold, partner i Advokatfirmaet Bull, jobber med teknologirett og transaksjoner.

Kan virksomheter si nei til GDPR-innsyn som følge av misbruk?

Av Håvard Sveier Ottemo og Line Helen Haukalid

Kan en virksomhet nekte innsyn etter GDPR dersom den mener at kravet er fremsatt som ledd i et misbruk? EU-domstolen har nå avklart at svaret i særlige tilfeller kan være ja, også der det gjelder det første innsynskravet fra den registrerte. Terskelen er likevel høy.

Håvard Sveier Ottemo

Line Helen Haukalid

Innsynsretten og unntaket for overdrevne krav

Retten til innsyn er blant de mest praktiske og mest brukte rettighetene etter GDPR. Den gir registrerte et konkret verktøy for å få oversikt over hvordan virksomheter behandler deres personopplysninger, og for å kontrollere om behandlingen er lovlig.

Hovedregelen følger av GDPR artikkel 15. Den registrerte har rett til innsyn i opplysningene om seg og nærmere informasjon om behandlingen. Etter artikkel 12 nr. 5 kan den behandlingsansvarlige likevel nekte å etterkomme et innsynskrav dersom det er åpenbart grunnløst eller overdrevent, særlig dersom det gjentas.

Den 19. mars 2026 avsa EU-domstolen en dom som gir nærmere veiledning om når et innsynskrav kan anses som overdrevent.[1]

Et sentralt poeng i dommen er at også en første anmodning kan omfattes av unntaket i artikkel 12 nr. 5. Samtidig understreker domstolen at dette er et snevert unntak som bare kan brukes under bestemte forutsetninger.

Saken for EU-domstolen

Saken gjaldt en tysk optiker som avslo en persons første krav om innsyn etter GDPR artikkel 15. Virksomheten mente at innsynskravet var overdrevent og derfor kunne avslås etter artikkel 12 nr. 5.

Som grunnlag for avslaget viste optikeren til ulike rapporter, bloggartikler og nyhetsbrev fra advokater. Etter virksomhetens syn viste dette at den registrerte systematisk og på en urimelig måte ba om innsyn, med sikte på å kreve erstatning for påståtte brudd på GDPR.

Ifølge virksomheten fulgte personen et fast mønster: Først tegnet han abonnement på et nyhetsbrev, deretter ba han om innsyn, og til slutt fremmet han erstatningskrav dersom kravet ikke ble oppfylt.

Et første innsynskrav kan være overdrevent

EU-domstolen godtok at også et første innsynskrav i prinsippet kan være overdrevent etter GDPR artikkel 12 nr. 5. Antallet tidligere krav er derfor ikke avgjørende i seg selv. Vurderingen må i stedet knyttes til om det foreligger misbruk av innsynsretten.

Det er ikke nok at virksomheten opplever kravet som belastende, strategisk eller som del av et mønster. Det avgjørende er om innsynsretten brukes på en måte som faller utenfor dens reelle formål.

To vilkår for å konstatere misbruk

EU-domstolen oppstilte to vilkår for å konstatere misbruk. For det første må det påvises at formålet med innsynsretten faktisk ikke oppnås, selv om de formelle vilkårene for å kreve innsyn er oppfylt. For det andre må det være grunnlag for å fastslå at den registrerte hadde til hensikt å oppnå en fordel ved kunstig å skape de omstendighetene som

1 Brillen Rottler GmbH & Co. KG v TC (C-526/24).

Colourbox / Chat GPT

gjorde at vilkårene for innsyn var oppfylt. Terskelen er høy, og bevisbyrden ligger hos den behandlingsansvarlige.

> Det er ikke nok at virksomheten opplever kravet som belastende, strategisk eller som del av et mønster. Det avgjørende er om innsynsretten brukes på en måte som faller utenfor dens reelle formål.

Offentlig tilgjengelig informasjon kan inngå i vurderingen

EU-domstolen åpnet samtidig for at offentlig tilgjengelig informasjon kan være relevant i denne vurderingen. Dersom slikt materiale tyder på at en person gjentatte ganger ber om innsyn og deretter fremmer erstatningskrav, kan dette inngå i bevisbildet. Slik informasjon vil likevel normalt ikke være tilstrekkelig alene, men bør støttes av annet relevant materiale som belyser den konkrete saken og den registrertes formål.

Urettmessig avslag kan gi grunnlag for erstatning

Dommen sier også noe om rekkevidden av erstatningsreglene etter GDPR. EU-domstolen slo fast at retten til erstatning ikke er begrenset til skade som springer direkte ut av selve behandlingen av personopplysninger i snever forstand. Erstatningsretten kan også omfatte skade som følger av et ulovlig avslag på innsyn.

Praktisk betydning for virksomheter

Avgjørelsen klargjør at virksomheter har et visst, men snevert, handlingsrom for å avslå innsynskrav der det foreligger konkrete og dokumenterte holdepunkter for misbruk. Dette kan også gjelde når kravet er det første virksomheten mottar fra den registrerte.

Adgangen må likevel praktiseres med stor varsomhet. Innsyn i egne personopplysninger er en grunnleggende rettighet, og et avslag må bygge på en konkret og godt dokumentert vurdering. Virksomheten må kunne forklare hvorfor innsynsrettens formål ikke gjør seg gjeldende i den aktuelle saken, og hvilke forhold som tilsier misbruk. Generelle antakelser, mistanke eller opplevelsen av at kravet er belastende, er ikke tilstrekkelig.

Et uriktig avslag kan dessuten i seg selv gi grunnlag for erstatningsansvar etter GDPR. Selv om innsynsretten ikke er absolutt, er adgangen til å nekte innsyn derfor forbeholdt klare og godt dokumenterte tilfeller av misbruk.

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

Line Helen Haukalid, Managing Associate, Advokatfirmaet Wiersholm.

Ny vägledning från IMY om riktad politisk onlinereklam

Av Alexander Persson, David Milger och Linn Karlsson

Alexander Persson

David Milger

Linn Karlsson

Med det svenska riksdagsvalet i september 2026 runt hörnet ökar intresset för att nå väljare genom digital annonsering. Samtidigt har frågan om vad som är tillåtet blivit mer komplex sedan EU:s förordning om politisk reklam trädde i kraft. I mars 2026 publicerade Integritetsskyddsmyndigheten (”IMY”) en vägledning som klargör hur reglerna om riktad politisk onlinereklam ska tillämpas i praktiken.

Bakgrund

Sedan den 10 oktober 2025 tillämpas EU:s förordning om transparens och inriktning när det gäller politisk reklam, ofta kallad TTPA (Transparency and Targeting of Political Advertising) (”TTPA”). Förordningen ställer bland annat krav på märkning av politiska reklambudskap och på att viss information ska lämnas genom så kallade transparensmeddelanden. Tillsynsansvaret är uppdelat och IMY ansvarar för artikel 18 och 19 i TTPA, som särskilt rör riktad politisk onlinereklam, medan Mediemyndigheten har det övergripande tillsynsansvaret för TTPA:s övriga delar. Dataskyddsförordningen (”GDPR”) gäller fortsatt parallellt och TTPA är tänkt att komplettera det befintliga dataskyddsregelverket.

Grundtanken bakom TTPA är att väljare ska kunna identifiera politisk reklam och förstå vem som står bakom budskapet. Samtidigt ska enskildas rätt till skydd för sina personuppgifter värnas. TTPA tar särskilt sikte på riskerna med avancerad inriktningsteknik, såsom microtargeting[1], som kan användas för att skräddarsy politiska budskap till individer eller grupper utan att mottagarna är medvetna om det.

> Transparency and Targeting of Political Advertising tar särskilt sikte på riskerna med avancerad inriktningsteknik, såsom microtargeting, som kan användas för att skräddarsy politiska budskap till individer eller grupper utan att mottagarna är medvetna om det.

Regler och förbud enligt artikel 18 och artikel 19 TTPA

I artikel 18 fastställs de centrala villkoren för när riktad politisk onlinereklam överhuvudtaget får användas. För det första krävs att den enskilde har lämnat ett uttryckligt och separat samtycke till att personuppgifterna används i politiskt reklamsyfte. Samtycket måste uppfylla GDPR:s krav, och det ska vara lika

1 Microtargeting är en form av riktad onlinereklam som bygger på analys av personuppgifter i syfte att identifiera en viss målgrupps eller individs intressen och därigenom påverka deras handlande. Tekniken kan användas för att leverera skräddarsydda budskap till enskilda eller grupper via onlinetjänster såsom sociala medier.

Colourbox / Chat GPT

lätt att avböja eller återkalla sitt samtycke som att lämna det. För det andra får den personuppgiftsansvarige inte använda personuppgifter som härrör från tredje part – uppgifterna måste ha samlats in direkt från den berörda personen. För det tredje råder förbud mot att använda inriktnings- eller annonsleveransteknik som bygger på profilering med hjälp av känsliga uppgifter, till exempel uppgifter om politisk övertygelse, hälsotillstånd eller etnisk bakgrund. Slutligen är det inte tillåtet att medvetet rikta sådan reklam mot personer under 17 år.

Det finns dock undantag. Reglerna i artikel 18 behöver inte tillämpas när ett parti eller en politisk organisation kommunicerar med sina egna medlemmar, tidigare medlemmar eller prenumeranter, eller när kommunikationen sker i form av ett nyhetsbrev med koppling till den politiska verksamheten. En förutsättning är att urvalet av mottagare enbart grundas på abonnemangsuppgifter och att ingen ytterligare personuppgiftsbehandling sker för att välja ut vilka som ska nås av budskapet.

Utöver kraven i artikel 18 innehåller artikel 19 särskilda transparensregler för den som använder inriktnings- eller annonsleveransteknik vid politisk onlinereklam. Med inriktningsteknik avses i korthet behandling av personuppgifter för att välja ut eller utesluta vissa mottagare. Annonsleveransteknik avser automatiserad optimering av hur, när och för vem ett politiskt budskap visas. Den personuppgiftsansvarige måste enligt artikel 19 bland annat ta fram en intern policy för den riktade reklamen, dokumentera vilka mekanismer och parametrar som används, ge mottagarna tydlig information om varför just de har nåtts av meddelandet samt årligen genomföra och offentliggöra en riskbedömning av teknikens inverkan på grundläggande rättigheter.

Tillsyn och sanktioner

Vid överträdelser av artiklarna 18 och 19 har IMY tillgång till samma verktyg som vid tillsyn enligt GDPR. Det innebär att myndigheten kan granska verksamheter, utfärda föreläggganden och besluta om sanktionsavgifter. Den registrerade kan också vända sig direkt till IMY med ett klagomål.

Vad innebär det i praktiken?

För aktörer som medverkar vid politisk onlinereklam innebär vägledningen att det inte längre räcker att enbart förlita sig på generella dataskyddsrutiner. Aktörer som erbjuder målgruppsstyrning, segmentering eller optimering av politiska budskap behöver säkerställa att den personuppgiftsbehandling som sker vilar på ett giltigt, uttryckligt och separat samtycke, att uppgifterna har samlats in direkt från den registrerade och att förbjudna parametrar eller känsliga uppgifter inte används i profileringen. Det kan också finnas skäl att se över ansvarsfördelningen mellan annonsör, plattform och eventuella underleverantörer, särskilt när flera aktörer tillsammans påverkar hur reklamen riktas och levereras.

IMY:s vägledning finns i sin helhet *här*.

Alexander Persson, Associate i Compliance & Regulatory-gruppen på RosholmDell Advokatbyrå.

David Milger, Associate och verksamhetsgruppchef i Compliance & Regulatory-gruppen på RosholmDell Advokatbyrå.

Linn Karlsson, Associate i Compliance & Regulatory-gruppen på RosholmDell Advokatbyrå.

Plikten i AI Act til å merke kunstig generert innhold

Av Ove A. Vanebo og Linn Cathrine Jøsendal

1. Innledning

Systemer basert på kunstig intelligens er blitt stadig bedre til å generere innhold som er vanskelig å skille fra «ekte vare». I det praktiske liv er det nyttig å kunne kjapt lage tekst og bilder som vi for få år siden hadde brukt timer og dager på å utforme. Samtidig gjør teknologien det mulig å utnytte og manipulere mennesker på en enklere måte enn før. EUs forordning for kunstig intelligens («AI Act») påpeker derfor at:[1]

> *«Den brede tilgjengeligheten og de økende kapabilitetene til disse systemene har en betydelig innvirkning på integriteten og tilliten til informasjonsøkosystemet, noe som skaper ny risiko for feilinformasjon og manipulering i stor skala, bedrageri, identitetstyveri og villeding av forbrukerne.»*

Som følge av denne situasjonen, har AI Act fastslått en merkeplikt i artikkel 50(2):

> *«Leverandører av KI-systemer, herunder KI-systemer for allmenne formål, som genererer syntetisk lyd-, bilde-, video- eller tekstinnhold, skal sikre at utdataene fra KI-systemet er merket i et maskinlesbart format og identifiserbare som kunstig generert eller manipulert.»*

2. Retningslinjer og regler for praksis: gjennomføring av åpenhetsforpliktelsene i AI act art. 50

EU-kommisjonen publiserte i mai 2026 et utkast til retningslinjer for gjennomføring av åpenhetsforpliktelsene for visse KI-systemer etter artikkel 50 i AI Act («Retningslinjene»).[2] Retningslinjene er utarbeidet av Kommisjonen (AI Office) med hjemmel i art. 96(1)(d) i AI Act, og har som formål å gi praktisk veiledning til kompetente myndigheter, leverandører og idriftsettere for å sikre en ensartet, effektiv og konsekvent etterlevelse av åpenhetsforpliktelsene. Retningslinjene er videre utformet på bakgrunn av innspill fra en bred interessenthøring og bidrag fra medlemsstatene i AI Board, og det er viktig å merke seg at det foreløpig er snakk om et utkast – dette kan altså endre seg. De er ikke rettslig bindende, og endelig tolkning av AI Act tilligger uansett EU-domstolen.

Retningslinjene dekker samtlige fire åpenhetsforpliktelser i art. 50:

i. informasjonsplikt ved interaktive KI-systemer som samhandler direkte med fysiske personer (art. 50(1)),
ii. merking og deteksjon av KI-generert eller manipulert syntetisk innhold (art. 50(2)),
iii. informasjon ved bruk av emosjonssystemer og biometrisk kategorisering (art. 50(3)), og
iv. merking av deep fakes og visse AI-genererte tekstpublikasjoner (art. 50(4)).

I tillegg behandles horisontale krav til hvordan informasjon gis etter art. 50(5) og håndheving. Selv om dette notatet primært fokuserer på merkeplikten i art. 50(2), er retningslinjene relevante for den samlede forståelsen av åpenhetsregimet i AI Act, og det vil derfor bli henvist til disse retningslinjene flere steder i det følgende.

Samtidig har to arbeidsgruppene fremlagt det andre utkastet til *Codes of Practice* (som er oversatt til «regler for god praksis» på norsk, som vi benytter under) vedrørende åpenhet

Ove A. Vanebo

Linn Cathrine Jøsendal

1 Fortalepunkt 133.

2 EU-kommisjonen, *Guidelines on the implementation of the transparency obligations for certain AI systems under Article 50 of the AI Act, 2026.*

om AI-generert innhold, i samsvar med AI Act.[3] Foreløpig er også disse reglene på utkaststadiet, men vi vil vise til dem for å belyse hva som er den mest sannsynlig korrekte forståelsen av regelverket.

3. Hvem er underlagt plikten til å merke innhold?

Forpliktelsene gjelder kun for «leverandører», som kan være både en fysisk eller juridisk person, en offentlig myndighet, et byrå eller ethvert annet organ, jf. definisjonen i art. 3(3). Disse faller inn i to hovedkategorier:

- Den «som utvikler et KI-system … eller som får utviklet et KI-system … og bringer det … i omsetning». eller
- Den som «tar KI-systemet i bruk under eget navn eller varemerke»

4. Hva slags teknologi er regulert?

4.1 Generelt

Plikten omfatter «KI-systemer, herunder KI-systemer for allmenne formål, som genererer syntetisk lyd-, bilde-, video- eller tekstinnhold». Med andre ord ser det ut til at denne bestemmelsen fokuserer på det som også ofte kalles «generativ AI».[4]

«KI-systemer» er definert i AI Act artikkel 3, som omfatter

> *«… et maskinbasert system som er konstruert for å operere med varierende grad av autonomi, som kan vise tilpasningsdyktighet etter idriftsetting, og som, for eksplisitte eller implisitte mål, ut fra inndataene det mottar, utleder hvordan man genererer utdata som prediksjoner, innhold og anbefalinger, eller beslutninger som kan påvirke fysiske eller virtuelle miljøer»*

Forordningen presiserer at også KI-systemer for «allmenne formål» er omfattet. Dette er «et KI-system som er basert på en KI-modell for allmenne formål, og som kan tjene en rekke ulike formål, både ved direkte bruk og ved integrering i andre KI-systemer».[5] Henvisningen til «KI-systemer for allmenne formål» skyldes antagelig at det var mye fokus på generelle språksystemer som ChatGPT da AI Act ble utformet.[6]

AI Act skiller mellom KI-systemer og KI-modeller. *Systemer* er innretninger som kan anvendes av en person direkte, bl.a. ved hjelp av et brukergrensesnitt. KI-modeller er ikke regulert av art. 50(2), slik at den rene algoritmen som utgjør modeller ikke underlegges merkeplikt.

4.2 Hva er «syntetisk innhold»?

«Syntetisk innhold» er ikke legaldefinert i AI Act. Trolig sikter det til at innholdet er kunstig laget eller er kunstig endret.[7]

Retningslinjene presiserer at «syntetisk innhold» skal forstås i tråd med praktisk og teknologisk utvikling. Tekst sikter til symbolsk innhold bestående av tegn eller tall som kan leses og tolkes semantisk av mennesker. Bilder sikter til statiske visuelle representasjoner. Lyd dekker tidsvarierte signaler som kan oppfattes gjennom hørsel, herunder tale, musikk og andre lydsignaler. Video sikter til tidsbaserte sekvenser av bilder, eventuelt synkronisert med lyd. Retningslinjene presiserer også at syntetisk multimodalt innhold, 3D-innhold, virtuell virkelighet (VR), utvidet virkelighet (AR) og blandet virkelighet faller innenfor virkeområdet til art. 50(2).

Noe av formålet med transparenskravene er å redusere nye risikoer for feilinformasjon og manipulasjon i stor skala, svindel, etterligning og forbrukerbedrag.[8] Det kan derfor argumenteres for at det må være en viss terskel før innhold anses som «syntetisk». Hvis en bakgrunn i et bilde er helt endret, vil det trolig være syntetisk. Men hvis KI-systemet bare har gjort farger i et bilde sterkere eller gjort bildet skarpere, kan det argumenteres for at det ikke er tale om «syntetisk innhold».[9] På samme måte bør tekst anses for å være syntetisk hvis den er generert på bakgrunn av et spesifikt spørsmål eller prompt, men ikke hvis det kun er tale om beskjedne endringer ved hjelp av kunstig intelligens, som eksempelvis kontroll av grammatikk.[10] Vår forståelse av Retningslinjene er at man oppfyller kravene til syntetisk innhold dersom innholdet enten fullt ut er AI-generert eller manipulert av AI utover standard redigering. Altså kan syntetisk innhold omfatte innhold som er en kombinasjon av menneskeskapt og AI-generert innhold.

> Vår forståelse av Retningslinjene er at man oppfyller kravene til syntetisk innhold dersom innholdet enten fullt ut er AI-generert eller manipulert av AI utover standard redigering.

Retningslinjene presiserer videre at visse typer output faller helt utenfor virkeområdet til art. 50(2), herunder korte sekvenser av tall, symboler eller bokstaver, kildekode, output som utelukkende er ment

3 Second Draft Code of Practice on Transparency of AI-Generated Content, 2026.

4 Thomas Gils, *«Article Commentary on Article 50 AI Act - Transparency Obligations for Providers and Deployers of Certain AI Systems»*. I: Ceyhun, Forgó og Valcke, The EU Artificial Intelligence (AI) Act: A Commentary, 2024 (s. 827-877), s. 791.

5 AI Act artikkel 3(66).

6 Gils (2024) s. 792.

7 Paul Voigt og Nils Hullen, *The EU AI Act: Answers to Frequently Asked Questions*, 2024.

8 Fortalepunkt 133.

9 Voigt og Hullen (2024) s. 123-124.

10 Voigt og Hullen (2024) s. 123-124.

for maskin-til-maskin-kommunikasjon uten eksponering for mennesker, samt output som kun brukes i lukkede industrielle miljøer.

Hva gjelder de ulike konkrete innholdstypene, kan ElevenLabs og Amazon Polly være systemer som genererer lydinnhold. DALL-E 3 og Midjourney er typisk systemer som generere syntetiske bilder. Sora og Kling AI er eksempler på systemer som kan fremstille videoinnhold. Tekstinnhold genereres ofte ved hjelp av CoPilot eller ChatGPT.

4.3 Omfattes også systemer som manipulerer innhold?

Ordlyden er noe uklar, siden plikten omfatter KI-systemer som «genererer» syntetisk innhold. Merkeplikten innebærer likevel å markere utdata *«som kunstig generert eller manipulert»*, som tilsynelatende setter opp et skille mellom å generere og manipulere. Vil «generering» være begrenset til situasjoner der KI -systemet lager nytt innhold, eller inkluderer begrepet også situasjoner der KI-systemer endrer («manipulerer») eksisterende innhold? Selv om ordlyden skiller mellom å generere og manipulere, var det lovgivers ønske å fange opp begge aktiviteter.[11] Vi antar derfor at både mer snever generering og manipulering omfattes av verbet «generere», slik at leverandører ikke fritas for merkeplikten under dekke av kun å drive med «manipulering».[12]

5. Hva innebærer merkeplikten?

5.1 Innledning

Leverandører av generative KI-systemer *«skal sikre at utdataene fra KI-systemet er merket i et maskinlesbart format og identifiserbare som kunstig generert eller manipulert»*. Forpliktelsen begrunnes i at det blir stadig vanskeligere for mennesker å skille syntetisk innhold fra mer «autentisk» og mer tradisjonelt menneskeskapt materiale.[13] Som nevnt er det også viktig å bevare informasjonens troverdighet og begrense negative konsekvenser av kunstig intelligens.

I den sammenhengen identifiserer betraktningen også et behov for nye metoder og teknikker for å spore informasjonens opprinnelse. Samlet sett sier betraktningen deretter at:

det er passende å kreve at leverandører av disse systemene bygger inn tekniske løsninger som muliggjør merking i et maskinlesbart format og deteksjon av at output er generert eller manipulert av et AI-system og ikke et menneske.

Dette siste utdraget fra betraktning 133 bringer oss til det første viktige spørsmålet angående merkingsplikten. Ved første øyekast kan art. 50(2) i AI Act tolkes som om den krever at leverandører av syntetisk innholdsgenererende KI-systemer sørger for at output fra deres AI-systemer er merket i et maskinlesbart format med det formål å legge til rette for deteksjon av innholdet som kunstig generert eller manipulert. Med andre ord, art. 50(2) pålegger en merkingsplikt som forfølger målet om å muliggjøre skillet mellom menneskeskapt og AI-generert innhold.

5.2 Er det også en plikt til å utforme løsninger for deteksjon av syntetisk innhold?

Merkeplikten er beskrevet i fortalepunkt 133 til AI Act, og påpeker at leverandørene av relevante systemer bør «bygge inn tekniske løsninger som gjør det mulig å merke utdataene i et maskinlesbart format med at de er generert eller manipulert av et KI-system og ikke et menneske, og å påvise at de er det.» (vår uthevning). Dette kommer tydeligere frem i den engelske språkdrakten, som nevner at *«it is appropriate to require providers of those systems to embed technical solutions that enable marking in a machine readable format and detection that the output has been generated or manipulated by an AI system and not a human.»*

Retningslinjene for AI Act går langt i å tilby en løsning for dette spørsmålet. Retningslinjene fastslår at art. 50(2) oppstiller to separate, men iboende sammenkoblede forpliktelser: For det første skal leverandøren sikre at utdataene er merket i maskinlesbart format. For det andre skal leverandøren sikre at utdataene er detekterbare som kunstig generert eller manipulert. Begge elementene må oppfylles for å oppnå formålet med åpenhetsforpliktelsene – det er ikke tilstrekkelig å kun oppfylle det ene elementet (f.eks. maskinlesbar merking uten å sikre detekterbarhet). Leverandøren er dermed forpliktet til å gjøre deteksjonsverktøy tilgjengelig for personer som eksponeres for innholdet, og deteksjonsverktøyet må kunne gi menneskelesbare resultater om hvorvidt innholdet er KI-generert eller manipulert, jf. art. 50(5).

Også utkastene til reglene for god praksis går imidlertid langt i å uttrykke at leverandørene bør sørge for at det finnes et offentlig tilgjengelig deteksjonsverktøy for innholdet som genereres eller manipuleres av deres KI-systemer.[14]

Etter vårt skjønn er det noe mer uklart hvorvidt det foreligger en plikt til å tilby deteksjonsverktøy – og i så fall hvor langt den går.

6. Hva innebærer «merking» av utdata?

6.1 Generelt om plikten

Det fremkommer ikke av artikkel 50(2) hvordan merkeplikten skal operasjonaliseres i praksis. Fortalepunkt 133 påpeker at: *«Slike teknikker og metoder bør være så pålitelige, samvirkende, effektive og robuste som teknisk mulig, tatt i betraktning de tilgjengelige*

11 Gils (2024) s. 792.

12 Se også støtte for en slik konklusjon i Nicolaj Feltes, *«Article 50 AI Act: Do the Transparency Provisions Improve Upon the Commission's Draft?»*, 16 (2025) JIPITEC, s. 222-237, på side 227.

13 Fortalepunkt 133.

14 Reglene for god praksis (2026) s. 14.

teknikkene eller en kombinasjon av slike teknikker».

Retningslinjene presiserer at den tekniske løsningen må oppfylle fire kvalitetskrav;

i. *effektivitet*, som innebærer at den tekniske løsningen må kunne detektere merkingen og gjøre det mulig å skille KI-generert innhold fra annet innhold,
ii. *pålitelighet*, som sikter til den tekniske løsningens evne til å nøyaktig identifisere KI-generert innhold under normale forhold,
iii. *robusthet*, som innebærer at den tekniske løsningen må opprettholde ytelsen under varierende forhold, inkludert vanlige endringer og forsøk på omgåelse, og
iv. *interoperabilitet*, som krever at ulike tekniske løsninger kan fungere smidig på tvers av systemer, aktører og tekniske implementeringer.

En rekke ulike teknikker eller metoder som kan brukes er nevnt, bl.a. *«vannmerker, identifikasjon av metadata, kryptografiske metoder for å bevise innholdets opprinnelse og ekthet, loggingsmetoder, fingeravtrykk eller andre teknikker».*[15] Kvalitetskravene er utdypet i utkastene til regler for god praksis.[16]

Det er uklart hvorfor akkurat de bestemte teknikkene er nevnt, siden det er diskutabelt om teknikkene som er nevnt er egnet til å oppnå bestemmelsens formålet. Slike teknikker brukes vanligvis i mindre grad for å tydeliggjøre skillet mellom kunstig og menneskelig innhold. Normalt brukes de heller for innholdsautentisering eller markere opprinnelse, forebygging av spredning av feilinformasjon, eller for å uttrykke forfatterskap og opphavsrettsbeskyttelse.[17]

Trolig bør leverandøren ta hensyn til at fortalepunkt 133 åpner for forskjellige teknikker, *«alt etter hva som er hensiktsmessig»,* noe som kan indikere at man bør se hva som kan oppnå formålet med merkingen. Dynamikken tydeliggjøres også ved at det er nevnt at:[18]

> *«Ved gjennomføringen av denne forpliktelsen bør leverandørene også ta hensyn til særtrekkene og begrensningene ved de ulike innholdstypene og den relevante teknologiske utviklingen og markedsutviklingen på området, slik som dette gjenspeiles i det allment anerkjente aktuelle tekniske utviklingstrinnet. Slike teknikker og metoder kan innføres på KI-systemnivå eller KI-modellnivå, herunder i KI-modeller for allmenne formål som genererer innhold, for på den måten å gjøre det lettere for nedstrømsleverandøren av KI-systemet å oppfylle denne forpliktelsen.»*

Utkast til reglene for god praksis går for øvrig langt i å uttrykke at ulike aktører må beholde og avstå fra å endre eller fjerne eksisterende metadata for å merke KI-innhold. Leverandørene skal inkludere et forbud i sine vilkår mot forsettlig fjerning av eller manipulering av merkene – med mindre fjerningen utføres for å teste sikkerheten til en merkeløsning.[19]

Det er trolig et betydelig handlingsrom, og valget vil nok mer unntaksvis bli overprøvd av tilsynsmyndighetene. Retningslinjene presiserer imidlertid at det etter gjeldende state-of-the-art ikke finnes én enkelt teknikk for merking og deteksjon som oppfyller alle fire kvalitetskravene samtidig. Det kreves derfor normalt en kombinasjon av ulike merkingsteknikker for å oppfylle forpliktelsen. Også utkast til reglene for god praksis påpeker at det bør benyttes en «flerlags merkemetode» for å sikre at innhold fra deres generative KI-systemer er merket med minst to lag med maskinlesbar aktiv merking.[20] Leverandører kan i fremtiden eventuelt demonstrere etterlevelse gjennom én enkelt teknikk dersom de kan påvise at den oppfyller alle fire kvalitetskravene, men dette vil kreve videre teknologisk utvikling.

6.2 Må merkingen kunne oppdages/sees av mennesker?

Utdata skal være *«merket i et maskinlesbart format og identifiserbare som kunstig generert eller manipulert».* Ettersom enkelte av teknikkene som er oppført i fortalepunkt 133 bare er mulig å avlese/observere gjennom maskinlesing, kan dette oppfattes som at det ikke er et krav at mennesker skal kunne oppdage merkingen gjennom bruk av egne sanser og uten tekniske hjelpemidler. Plikten vil uansett ikke utelukke at det brukes synlige, «menneskerettede» merketiltak som også kan være maskinlesbare.[21] Retningslinjene underbygger at merkeplikten i art. 50(2) er begrenset til maskinlesbar merking. Menneskelesbar informasjon oppnås derimot via deteksjonsverktøyet: Art. 50(5) krever at informasjonen meddeles berørte fysiske personer «på en klar og tydelig måte», og det er resultatet fra deteksjonsverktøyet som gir denne informasjonen til brukerne.

Det må imidlertid tas i betraktning at arty. 50(5) bestemmer at informasjonen nevnt i art. 50(2) «skal meddeles de berørte fysiske personene på en klar og tydelig måte senest på tidspunktet for den første samhandlingen eller eksponeringen.» Informasjonen må dessuten «være i samsvar med de gjeldende tilgjengelighetskravene».

7. Unntak fra merkeplikten

7.1 Innledning

Det følger av art. 50(2) i.f. at plikten til merking *«skal ikke gjelde i den grad KI-systemene utfører en hjelpefunksjon for standardredigering eller ikke i vesentlig*

15 Fortalepunkt 133.
16 Regler for god praksis (2026) s. 16-20.
17 Gils (2024) s. 793.
18 Fortalepunkt 133.
19 Reglene for god praksis (2026) s. 12.
20 Reglene for god praksis (2026) s. 10.
21 Gils (2024) s. 794.

grad endrer inndataene fra idriftsetteren eller semantikken i disse, eller dersom de er godkjent ved lov til å brukes for å avsløre, forebygge, etterforske eller straffeforfølge straffbare forhold.»

Begrunnelsen for unntakene, er plikten «skal være forholdsmessig», jf. fortalepunkt 133. Vi oppfatter at dette samsvarer med den risikobaserte tilnærmingen i AI Act, som skal håndtere de mest skadelige systemene.

7.2 Unntak for hjelpefunksjoner

Merkeplikten gjelder ikke KI-systemer som *«utfører en hjelpefunksjon for standardredigering eller ikke i vesentlig grad endrer inndataene fra idriftsetteren eller semantikken i disse».* Det kan synes som om dette er to unntak, men det er vanlig å oppfatte det som ett felles «hjelpefunksjonsunntak».

Det er ikke spesifisert hvilken type eksisterende AI-verktøy som faller inn under dette unntaket. Trolig bør det forstås i forlengelsen av at pliktens formål om å hindre forveksling av innhold og ivareta informasjonens troverdighet.

Umiddelbart vil man se for seg at det er stave- og grammatikkverktøy som omfattes. Ordlyden åpner imidlertid for at det også vil omfatte «standardredigering» av andre typer innhold, f.eks. bilde eller video.[22]

Retningslinjene gir nå konkrete eksempler på hva som anses som standardredigering og dermed er unntatt fra merkeplikten. Dette omfatter blant annet grammatikk- og stavekontroll, formatkonverteringer, teknisk komprimering, støyreduksjon, mindre beskjæring, mindre farge- og lysjusteringer, fjerning av støvflekker fra linse, fjerning av røde øyne fra blitz, rotering av bilder, videoskalering, begrenset videostabilisering og mindre justeringer av avspillingshastighet. Også KI-generert innhold som kun transformerer autentisk menneskelig input gjennom hjelpemiddelteknologi for personer med nedsatt funksjonsevne (f.eks. AAC eller tilpassede nevrale stemmer) faller inn under unntaket.

På den annen side gir retningslinjene også eksempler på semantiske endringer som krever merking. Dette omfatter blant annet KI-genererte oversettelser og sammendrag av tekst, tilføying av objekter eller informasjon som ikke var til stede i originalbildet eller -videoen, sletting eller tilsløring av bakgrunner eller objekter, pikselering eller uskarphet av ansikter, endring av en persons kroppsfasong eller hudfarge, ekstreme lys-, farge- og kontrastjusteringer (f.eks. å gjøre en grå himmel blå), konvertering fra svart-hvitt til fargebilde, samt opprettelse av sammensatte bilder eller videoklipp.

7.2 Unntak for rettshåndhevelsesformål

Også KI-systemer som *«er godkjent ved lov til å brukes for å avsløre, forebygge, etterforske eller straffeforfølge straffbare forhold»,* er unntatt fra merkeplikten.

Det kreves ikke at et KI-system som *brukes* for rettshåndhevelsesformål er beregnet eller utformet eksklusivt for slike formål, og det er tilstrekkelig at det er godkjent ved lov for å kunne brukes for slike formål.[23]

8. Idriftsetteres åpenhetsforpliktelser etter art. 50(4)

I tillegg til merkeplikten for leverandører etter art. 50(2), pålegger AI Act også idriftsettere («deployers») egne åpenhetsforpliktelser etter art. 50(4). Idriftsettere som bruker KI-systemer til å generere eller manipulere bilde-, lyd- eller videoinnhold som utgør en «deep fake» – definert som innhold som ligner eksisterende personer, objekter, steder eller hendelser og som feilaktig vil fremstå som autentisk for en person – må opplyse om at innholdet er kunstig generert eller manipulert. Denne opplysningsplikten gjelder i tillegg til og uavhengig av leverandørens merkeplikt.

For KI-generert eller manipulert tekst som publiseres med formål om å informere offentligheten om spørsmål av allmenn interesse, gjelder en tilsvarende opplysningsplikt for idriftsetteren. Det gjøres imidlertid unntak der teksten har gjennomgått menneskelig redaksjonell kontroll og en fysisk eller juridisk person har redaksjonelt ansvar for publiseringen. Retningslinjene presiserer at «publisert tekst» innebærer at teksten skal være tilgjengelig for et ubestemt, relativt stort antall ikke-relaterte, potensielle lesere. «Redaksjonelt ansvar» skal tolkes i samsvar med det eksisterende EU-medierammeverket.

9. Håndheving, sanksjoner og Code of Practice

Leverandører og idriftsettere som ikke overholder åpenhetsforpliktelsene i art. 50 kan bøtelegges med inntil EUR 15 000 000 eller, dersom overtrederen er et foretak, inntil 3 % av den totale globale årlige omsetningen for det foregående regnskapsåret, avhengig av hva som er høyest. EU-institusjoner, -organer og -byråer som overtrår forpliktelsene kan ilegges administrative bøter på inntil EUR 750 000.

I henhold til art. 113 skulle art. 50 få anvendelse i EU fra 2. august 2026. Alle KI-systemer som bringes i omsetning eller tas i bruk i EU må være i samsvar med kravene, uavhengig av når de ble satt i drift. Retningslinjene bemerker imidlertid at AI Omnibus-forslaget, som for tiden behandles av EU, tar sikte på en overgangsregel for merkings- og deteksjonspliktene i art. 50(2) for generative KI-systemer som er satt i drift før 2. august 2026. KI-generert eller manipulert output som er produsert og gjort tilgjengelig før 2.

22 Se også støtte for en slik konklusjon i Nicolaj Feltes, *«Article 50 AI Act: Do the Transparency Provisions Improve Upon the Commission's Draft?»,* 16 (2025) JIPITEC, s. 222-237, på side 228-229.

23 Gils (2024) s. 790.

Colourbox / Chat GPT

august 2026 trenger ikke å merkes eller opplyses om retroaktivt, men aktører som besitter eller distribuerer slikt innhold oppfordres til å gjøre dette. Det ser også ut til at plikten for merking først kommer til anvendelse 2. desember 2026, i samsvar med Omnibus-reformens foskyvning av frister.

Leverandører og idriftsettere kan demonstrere etterlevelse med åpenhetsforpliktelsene i art. 50(2) og (4) ved å slutte seg til reglene for god praksis (se punkt 2 over), som trolig vil bli vurdert som adekvat av AI Office, jf. art. 50(7). Tilslutning til reglene for god praksis er en enkel måte å demonstrere etterlevelse på, og innebærer at tilsynsmyndighetenes kontroll i første rekke vil fokusere på om undertegnerne har overholdt praksiskodeksen. Leverandører og idriftsettere som ikke har sluttet seg til adekvat regler for god praksis, må demonstrere etterlevelse gjennom andre egnede midler, og kan forvente mer detaljerte informasjonskrav fra tilsynsmyndighetene.

10. Avsluttende merknader

Merkeplikten i artikkel 50(2) er en interessant nyvinning som reiser mange nye og uavklarte spørsmål. Praksis og autoritative avgjørelser vil tydeliggjøre begrensninger og innhold i kravene. Vi oppfatter nok imidlertid at foreslåtte retningslinjer og regler for god praksis går langt i å oppstille strenge krav, og mener det kan være hensiktsmessig – iallfall i starten – å ha en mer moderat tilnærming til hva som er nødvendig for å oppfylle merkekravene.

Ove A. Vanebo, assosiert partner og advokat i CMS Kluge og er spesialist på personvern og cybersikkerhet.

Linn Cathrine Jøsendal, partner og advokat i CMS Kluge, spesialisert innen immaterialrett med over 15 års erfaring, og arbeider med blant annet varemerkerett, opphavsrett og markedsføringsrett. Hun har bred erfaring med transaksjoner, særlig innen teknologi og IP, samt kontraktsrett og forhandlinger.

Kampen mot datakriminalitet og cyberkriminalitet i 50 år – en innledning

Av Stein Schjølberg

1. Bakgrunnen

Jeg var ansatt som politiembetsmann ved Oslo Politikammer fra 1968–1984.

Plutselig en dag i 1975 fikk jeg saken som skulle få betydning for resten av mitt liv, og medføre 50 års virke som forsker og utreder både nasjonalt og internasjonalt. Forskningsvirksomheten kom i tillegg til stillingene som politiembetsmann og senere dommer, sorenskriver og pensjonist.

Som politifullmektig ved Kriminalavdelingen i Oslo Politikammer hadde jeg i 1975 økonomisk kriminalitet som spesialområde. En dag ble jeg innkalt til Kriminalsjefen og vist to identiske ihendehaverobligasjoner i Shell, som var oversendt fra Den norske Creditbank. Jeg ble gitt i oppdrag å lede etterforskingen av den såkalte *Obligasjonssaken,* som omhandlet ca. 3000 kopier av ihendehaverobligasjoner til en verdi av 3 millioner kroner, som var foretatt på fargekopieringsmaskiner. Etter omfattende spaning ble det kl. 06.00 en morgen gjennomført samtidig pågripelse av 6 gjerningsmenn, med bistand av en styrke på ca. 50 polititjenestemenn. En av de største økonomiske straffesaker i Norge på den tid ble etterforsket og pådømt.

Etterforskingen ble gjennomført i et utmerket samarbeid med to dyktige etterforskere, politiførstebetjentene Kaare Kongsfjeld og Leif Takle. Dette var økonomisk kriminalitet med bruk av ny teknologi som den moderne tekniske utvikling i 1970-årene hadde åpnet muligheter for, med nye utfordringer for etterforsking og påtale av straffbare handlinger.

Studietur til USA i 1976

Den 2. april 1976 møtte jeg FBI Agent Dennis R. Dickson, som da var Assistant Legal Attache ved USAs ambassade i London. Han var på besøk i Oslo, og under møtet nevnte jeg min interesse med et besøk i USA for å bli orientert om den erfaring amerikanerne hadde med moderne teknologi og betydningen for økonomisk kriminalitet. Han tilbød seg å bistå med forslag til reiseprogram, og møtet med han fikk en avgjørende betydning for mine senere studieturer til USA, og den helt fantastiske bistanden fra FBI.

Jeg søkte Justisdepartementet om et reisestipend i 1976 for et kort studieopphold i USA i ca. 3 uker i august 1976, med særlig formål å studere nye former for økonomisk kriminalitet som den moderne tekniske utvikling hadde åpnet muligheter for. Søknaden ble innvilget.

Som følge av bistanden fra Dennis R. Dickson, omfattet studieturen besøk i J. Edgar Hoover FBI Building som er hovedkvarteret til FBI, en dag på FBI Academy i Quantico, Virginia, og et besøk i Justisdepartementet i Washington D.C. Det ble Deputy Assistant Attorney General Nathaniel E. Kossack i Justisdepartementet, som gjorde meg oppmerksom på noe han kalte *computer crime*. Han var en meget sentral person i USA i arbeidet med slik kriminalitet. Han inviterte meg på et

Stein Schjølberg

møte og redegjorde for sitt syn på denne form for kriminalitet, og på den oppbygning av kunnskap som måtte finne sted i politiet.

Betegnelsen datakriminalitet ble skapt

Da jeg kom tilbake til Norge medførte min interesse for datamaskiner at jeg søkte om deltagelse på et grunnkurs for statsansatte: *Informasjon om EDB for saksbehandlere om datamaskiners oppbygning og virkemåte,* på Bergland Gjestgiveri, Sokna, 8–12. november 1976. Databehandlingen i datamaskinene ble den gang gjennomført med hullkort. Det ble opplyst at kursets formål var:

Hensikten med kurset er å orientere saksbehandlere om de oppgaver og problemer brukerne ville stå overfor ved innføring av EDB i en institusjon. Hovedvekten legges på hva brukerne kan gjøre for å løse disse oppgavene tilfredsstillende.

Det var 25 deltagere på konferansen, og Jon Bing, Avdeling for EDB-spørsmål, Institutt for privatrett, Universitetet i Oslo, holdt foredrag om integritetsproblem og personlighetsvern. En annen foredragsholder var Arve Føyen, som den gang var konsulent i Rasjonaliserings-direktoratet, og holdt foredrag blant annet om Kontroll og sikkerhet i EDB-systemer.

Jon Bing og jeg satte oss ned og snakket sammen etter hans foredrag:

– Hei, jeg heter Stein og er politifullmektig ved Kriminalavdelingen i Oslo. Det var et meget interessant foredrag du gav oss om integritetsproblem og personlighetsvern.

– Hva gjør en politifullmektig på et kurs som dette?

– Som politifullmektig har jeg økonomisk kriminalitet som spesialområde, og ledet etterforskningen i den såkalte Obligasjonssaken, kopiering av obligasjoner som var foretatt på fargekopieringsmaskiner. En av de største økonomiske straffesaker i Norge er blitt etterforsket og pådømt. Men det førte til at jeg ble interessert i muligheter for misbruk av moderne teknologi som hjelpemidler i kriminalitet.

– Det høres jo spennende ut. Da burde du også bli interessert i noe som amerikanere kaller computer crime.

– Nettopp, jeg har nylig vært på studietur til USA og jeg hadde lunsj med en ansatt i Department of Justice i Washington D.C. Han fortalte om noe han kalte computer crime som hadde skapt et stort problem for de amerikanske justismyndigheter, som også FBI fortalte meg.

– Dette blir også et problem for oss, og da blir det viktig hva vi skulle kalle fenomenet på norsk. Det er misbruk av datamaskiner.

– Og det er kriminalitet.

– Det blir jo data og kriminalitet. Skal vi kalle det datakriminalitet?

– Enig. Betegnelsen bør kunne kalles datakriminalitet. Jeg sender en innberetning til Justisdepartementet i slutten av denne måned, og da bruker jeg betegnelsen.

– Bra. Kan du sende en kopi til meg. Vi på Avdeling for EDB spørsmål er veldig interessert i å forske litt på dette.

Institutt for privatrett ved Det juridiske fakultet, Universitetet i Oslo, tok 16. mars 1970 initiativ til å organisere forskning innenfor området jus og EDB. Fra 1971 var arbeidet organisert som en egen Avdeling for EDB spørsmål, og bestyrer av Avdelingen var professor Knut S. Selmer. Avdelingen var også utgiver av Skriftserien Jus og EDB, som utkom første gang i 1971. Jon Bing skrev allerede i 1971 sin første artikkel om *JURIS – JURidisk InformasjonsSystem,* og sammen med Trygve Harvold artikkelen *Rettskildebruk og informasjonssystemer* i 1973.

I *Innberetning til Justis- og politidepartementet* av 30. november 1976 redegjorde jeg for gjennomføringen og utbyttet av studieturen til USA i august 1976. Det var særlig om at datamaskiner kunne misbrukes til straffbare handlinger, og betegnet for første gang handlingene som datakriminalitet. Denne nye form for kriminalitet åpnet også for en helt ny kategori av lovbrytere, hvor den enkelte hadde en vesentlig bedre sosial bakgrunn og høyere utdannelse enn det som var vanlig ved mer tradisjonell kriminalitet. Jeg foreslo at det måtte foretas en innføring og opplæring av personell innen politietaten som kunne foreta etterforsking av slike lovbrudd.

Samarbeidet med professor Jon Bing ved Universitetet i Oslo begynte i 1976, og førte til forskningsprosjektet *Datamaskinassistert kriminalitet.* Jeg ble prosjektleder, men hadde fortsatt full stilling på Kriminalavdelingen. Vi samarbeidet om forskningsprosjekter og utredningsprosjekter om datakriminalitet, og senere cyberkriminalitet. Målsettingen var å foreta en innsamling, bearbeiding og analyse av et størst mulig materiale særlig med henblikk på de strafferettslige og straffeprosessuelle virkninger. Virksomheten ble organisert innen rammen av Avdelingens forskningsprogram i EDB-rett som prosjektet TERESA (15).

I løpet av tidsrommet 1978-1980 skulle det gjennomføres en studie av kjente tilfeller av datakriminalitet, og hvilke virkninger dette ville få for strafferettsystemet i Norge. Prosjektet kunne føre til forslag om endringer i straffe- og straffeprosesslovgivningen, samt tiltak av annen art til forebygging av datakriminalitet. Justisdepartementet innvilget forskningsmidler til prosjektet.

Jeg hadde gleden av å kjenne Jon Bing fra 1976 og ble hans «disippel», forsker og utreder i grenseflaten mot etterforskning og påtale i straffesaker, og i strafferettens område av rettsinformatikken.

Jon Bing og jeg ble således grunnleggere av den nasjonale kunnskap om datakriminalitet, og den senere cyberkriminalitet.

Seminarer om datakriminalitet i Stockholm, København og Oslo i 1977

Samarbeidet med Avdeling for EDB spørsmål medførte også til seminarvirksomhet i september 1977 i de skandinaviske hovedsteder sammen med politi- og universitetsmyndigheter i Stockholm, København og Oslo. Justisdepartementet bevilget midler. I København var det politiinspektør H. O. Jørgensen, og i Stockholm byråsjef Hans Wranghult ved Rikspolisstyrelsen som bisto i arbeidet. Fra universitet i Stockholm bisto professor Peter Seipel. Vi holdt foredrag til representanter for skandinaviske forvaltningsmyndigheter, banker, kredittinstitusjoner m.v. om EDB og kriminalitet i alle hovedsteder og redegjorde for våre erfaringer og problemstillinger. I København deltok også 13 deltakere fra den danske politi- og påtalemyndighet med politidirektør Eefsen i spissen.

Hovedinformasjonen fikk seminardeltagerne fra den amerikanske forsker Donn B. Parker, SRI International (Stanford Research Institute) i California, som var invitert til å holde foredrag i alle de tre hovedsteder. Jeg holdt foredrag i en fullsatt sal i Ingeniørenes Hus i Oslo, og det var litt spesielt med professor Johs. Andenæs sittende i første rad.

Vi tre representanter for politiet i de skandinaviske hovedsteder, ble enige om å informere hverandre om utviklingen i hvert enkelt land.

Studietur til USA i 1978

Det var i 1978 behov for å innhente ytterligere informasjon om datakriminalitet. FBI bisto på nytt til organiseringen av min nye studietur til USA som skulle vare i 8 uker fra 29. mai–13. juli 1978, med informasjon og opplæring på FBI kontorer over hele USA, samt besøk i Senatet. Utenriksdepartementet informerte den norske ambassaden i Washington D.C. og generalkonsulatene i San Francisco, Los Angeles og New York om den forestående studieturen og anmodet om eventuell bistand. Besøkene og samtalene i Senatet var meget nyttige og viktige, fordi et spesielt lovforslag:*«Federal Computer Systems Protection Act of 1977», den såkalte Ribicoff Bill.* Dette var det første lovforslag i verden som var spesielt rettet mot computer crime. Lovforslaget ble ikke vedtatt i Senatet før i 1980-årene, men det skapte en internasjonal oppmerksomhet som ført til utredninger og lovforslag mot datakriminalitet i mange land.

Jeg orienterte i brev av 22. august 1978 både byråsjef Hans Wranghult i Stockhom, og politiinspektør H.O. Jørgensen i København, om resultatet av studieturen.

Etter avsluttet studietur i USA fikk jeg et hyggelig brev av 18. september 1978 fra den nye sjefen for FBI, William Webster. Han skrev blant annet:

I was certainly pleased to learn from your recent letter that you enjoyed your visit to the United States and that we were able to be of help to you in conducting your research project on computer-related crime.

We are looking forward to receiving the results of your study.

De foreløpige konklusjonene i forskningsprosjektet om datamaskinassistert kriminalitet i samarbeidet med Avdeling for EDB-spørsmål ble fremlagt i mitt foredrag om *Datamaskinassistert kriminalitet* på Nordisk Politisjefkonferanse i Oslo 13. juni 1979.

Visestatsadvokat B. Holm Frandsen, Statsadvokaten for særlig økonomisk kriminalitet i København, var også foredragsholder om samme tema.

Justisdepartementet bevilget midler til ytterligere en studietur i prosjektet, denne gang til England, Frankrike og Danmark i tiden 21. september–5. oktober 1979.

Besøket i London var meget nyttig med flere møter, blant annet besøkte jeg Company Fraud Department i New Scotland Yard. Deretter gikk turen den 28. september 1979 til Oxford University og Magdalen College, og ble mottatt til lunsj av professor Colin Tapper. Jeg besøkte Interpols hovedkvarter i Paris, 1.–3. oktober 1979.

Med fortsatt støtte fra Justisdepartementet deltok jeg den 30. januar-1. februar 1980 på en konferanse om datakriminalitet i Bundeskriminalamt, Wiesbaden, Vest-Tyskland. Et tilsvarende forskningsprosjekt hadde også vært gjennomført av Bundeskriminalamt, og prosjektet hadde ført til forslag om nye straffebestemmelser i Vest-Tyskland.

Samarbeidet med INTERPOL

Mitt samarbeid med Interpol startet i 1979 da jeg ble invitert som foredragsholder på *3rd INTERPOL Symposium on International Fraud* den 11.–13. desember 1979 i Paris, og ble en av dem som introduserte Interpol til computer crime. Interpols generalsekretariat hadde den

1. oktober 1979 sent følgende anmodning til Kripos (oversatt til norsk):

Viser til vårt brev av 10.8.79 angående Interpol symposium om internasjonale bedragerier 11-13. desember 1979. Bedragerier ved hjelp av EDB er et punkt på dagsorden, og vi har hørt at herr Stein Schjølberg har skaffet seg betydelig erfaring på dette felt. Hvis herr Schjølberg blir utpekt som norsk representant til dette symposiet, ville vi sette stor pris på om han kunne gi en kort – 20 til 30 minutters utredning for å åpne diskusjonen angående bedragerier ved hjelp av EDB. Takk for samarbeidet.

Justisdepartementet besluttet at jeg skulle være en norsk representant på symposiet. Jeg holdt derfor foredrag på *symposiet*. Mitt foredrag hadde som tittel: *Computer Fraud and Abuse.*

Jeg utarbeidet et spørsmålsskrift til alle medlemsland i INTERPOL om strafferettslige spørsmål, med henblikk på en mulig harmonisering av internasjonal straffelovgivning. Det var en anmodning om svar innen 1. september 1981.

Jeg ble således en av grunnleggerne for utviklingen av politiets etterforskingsmetoder i saker om computer crime, og den internasjonale harmoniseringen av straffelovgivningen om computer crime.

Etter anmodning og anbefaling til Justisdepartementet fra INTERPOL, deltok jeg på en konferanse om EDB og kriminalitet i Washington DC, 20.–22. oktober 1980. Konferansen ble betegnet *«National Conference on Computer Related Crime».* Anmodningen fra INTERPOL hadde blant annet følgende innhold:

We would therefore kindly ask you to consider the possibility of sending Mr. Schjolberg to the conference in Washington thus enabling both the Norwegian police and the General Secretariat to profit

from his increased knowledge in this type of crime.

Konferansen var den første av denne type i USA, og det deltok ca. 400 personer. Jeg besøkte også Senatet i USA og fikk en oppdatering av fremdriften av lovforslaget *The Ribicoff Bill.*

Forskningsopphold i USA 1981-1982

Den 27. februar 1981 ble jeg invitert til et års forskningsopphold på Stanford Research Institute (SRI International) i California. Jeg skulle delta i et forskningsprogram som het Computer Security Program i et år fra august 1981, som en International Research Fellow. Det var et samarbeid med Donn B. Parker i forskning på EDB og kriminalitet. Forskningen ble gjennomført som en Visiting Senior Fulbright-Hays Scholar, etter et vedtak i International Communication Agency and Board of Foreign Scholarships i Washington DC, USA, som også betalte reiseutgifter tur-retur til Stanford Research Institute. Returreisen tilbake til Norge ble satt til 1. juli 1982.

Forskningsoppholdet ble gjennomført i et samarbeid med Avdeling for EDB spørsmål ved Universitetet i Oslo[1] som en del av forskningsprosjektet Teresa (15). Det var også et samarbeid med Interpol i Paris. Justisdepartementet meddelte meg permisjon med lønn fra 1. august 1981 til 1. juli 1982. Etter søknader ble jeg også innvilget støtte fra flere private institusjoner.

Forskningsoppholdet på Stanford Research Institute (SRI International) i California, ble grunnlaget for en bok i 1983: *Computers and Penal Legislation – A study of the legal politics of a new technology.*[2]

Det var også grunnlaget for gjensidig informasjon om utviklingen av datakriminalitet med Juhani Saari, Sparebanksinspektionen i Finland.

Samarbeidet med Professor Jon Bing fortsatte, og den 24. januar 1983 ble det arrangert et seminar om EDB og kriminalitet på Hotel Scandinavia i Oslo sammen med Norsk forening for Jus og EDB og Det kriminalitetsforebyggende råd.[3] Jeg holdt tre foredrag på seminaret:[4]

- EDB og kriminalitet – oversikt og kategorier;
- Internasjonale erfaringer i forbindelse med EDB og kriminalitet;
- Er det behov for en ny lovgivning om EDB og kriminalitet?

Definisjonen av datakriminalitet ble i foredragene angitt til å omfatte *enhver ulovlig handling hvor kjennskap til datateknologi er nødvendig i utøvelsen av gjerningen.* Fra Stockholm deltok kriminalsjef Hans Wranghult, og han holdt også et foredrag.

2. Den nasjonale utvikling

Den første nasjonale milepælen om datakriminalitet i Norge ble rapporten fra forskningsprosjektet *Datamaskinassistert kriminalitet* som ble publisert av Avdeling for EDB spørsmål, Institutt for privatrett, Universitetet i Oslo.[5] To avsluttende delrapporter, samt sammendragsrapport, ble den 28. mars 1980 oversendt til Justisdepartementet.

Et annet hovedresultat var behovet for å gi politi- og påtalemyndighet opplæring av den alminnelig kunnskap om datamaskinens oppbygning og virkemåte, og spesialutdanning i etterforsking av datakriminalitet, samt oppnevnelse av eksterne sakkyndige. Det ble gjennomført en innsamling og analyse av vel 600 tilfeller av datakriminalitet fra flere land, og det ble foreslått inntatt en ny straffebestemmelse i straffeloven. Rapporten inneholdt derfor et forslag om en ny § 261 i straffeloven.

Avdeling for EDB spørsmål hadde et 10 års jubileum i 1980, og jubileums publikasjonen *A Decade of Computers and Law* inneholdt også en artikkel av meg med tittel: *Computer Crime in Norway.*

> Definisjonen av datakriminalitet ble i foredragene angitt til å omfatte *enhver ulovlig handling hvor kjennskap til datateknologi er nødvendig i utøvelsen av gjerningen*.

Den andre nasjonale milepælen var at saken ble tatt opp i Stortinget av stortingsrepresentant Morten Steenstrup. I et grunngitt spørsmål den 10. november 1982 spurte han om regjeringen ville foreta en nærmere kartlegging av forskjellige former for datakriminalitet i straffeloven. Statsråd Mona Røkke opplyste i Stortinget at Justisdepartementet nå hadde funnet det riktig å be

1 Støtteerklæring fra professor Knut S. Selmer og Jon Bing av 13. mars 1981.

2 Stein Schjølberg, «Computer and Penal Legislation», *CompLex* (Universitetsforlaget 1983), se *https://www.amazon.com/Computers-Penal-Legislation-Politics-Technology/dp/8200065707/ref=sr_1_5?dchild=1&keywords=Stein+Schjolberg&qid=1600700910&sr=8-5.*

3 Seminaret ble ledet av Professor Anders Bratholm. Det var foredrag av stortingsrepresentant Anne Lise Bakken, direktør Harald Omdahl i Bankforeningen, direktør Hans B. Thomsen, Eksportrådet, og kriminalsjef Hans Wranghult, Stockholms politi.

4 Foredragene ble publisert i Lov og Rett, se *Stein Schjølberg,* EDB og kriminalitet – oversikt og kategorier og Er det behov for en ny lovgivning om EDB og kriminalitet? Se Lov og Rett 1983 side 467–488.

5 Se Stein Schjølberg: Datamaskinassistert kriminalitet, Skriftserien for Jus og EDB nr. 42, Institutt for Privatrett, Avdeling for EDB-spørsmål, Universitetet i Oslo, 1980.

Straffelovrådet om en utredning av datakriminalitet og mulige lovgivningstiltak.[6]

Statsråd Mona Røkke uttalte videre:

Det er videre grunn til å tro at det man kaller datakriminalitet, vil øke i omfang og kompleksitet i årene som kommer. La meg også vise til at politiinspektør Stein Schjølberg ved Oslo politikammer har foretatt en undersøkelse på dette feltet, der det er gjort et visst kartleggingsarbeid når det gjelder datakriminalitet. Jeg kan her nevne at Justisdepartementet bidro til finansieringen av denne undersøkelsen og kartleggingsarbeidet.

Departementet har på bakgrunn av dette og etter å ha vurdert de forhold som representanten Steenstrup tar opp i sitt spørsmål, funnet det riktig å be Straffelovrådet om en utredning når det gjelder datakriminalitet og mulige lovgivningstiltak. Jeg vil understreke betydningen av at vi ligger i forkant med reaksjonsmidler når det gjelder den utvikling av datakriminalitet som det er holdepunkter for å tro kan komme i årene fremover.

Den tredje nasjonale milepælen ble utredningen fra Straffelovrådet under ledelse av professor Johs. Andenæs. Det ble oppnevnt særskilt sakkyndige medlemmer til å delta i Straffelovrådets arbeid med oppdraget om datakriminalitet.[7] Straffelovrådet avgav sin innstilling i NOU 1985: 31 og foretok en gjennomgang av bestemmelsene i straffeloven. Etter Straffelovrådets oppfatning kunne datakriminalitet hensiktsmessig defineres som kriminalitet hvor utnyttelse av data-teknologi har vært vesentlig for overtredelsen. Rådet fastslo som sin generelle konklusjon at de fleste former for straffverdige handlinger rettet mot data rammes av de eksisterende straffebestemmelsene, men at ikke alle former for datakriminalitet var tilfredsstillende dekket. Justisdepartementet sendte forslagene om endringer i straffeloven til Stortinget, som vedtok lovforslagene fra Straffelovrådet i lov av 12. juni 1987 nr. 54.

3. Den internasjonale utvikling

Den første internasjonale milepælen om datakriminalitet ble etablert av Interpol i 1981.

INTERPOL organiserte det første internasjonale seminar om etterforsking av computer crime i St. Cloud ved Paris den 7.–11. desember 1981. Seminaret ble betegnet som *The First Interpol Training Seminar for Investigators of Computer Crime.* Seminaret hadde 66 deltagere fra 26 medlemsland, og ble gjennomført i samarbeid med meg. Som en leder av seminaret holdt jeg tre foredrag. Hovedforedragsholder var Donn B. Parker, SRI International. Da jeg åpnet seminaret sa jeg at computer crime ville komme til å bli 1980-årenes kriminalitetsform. Etter en vurdering av opplysningene fra medlemslandene om straffelovgivningen tilfredsstillende omfattet denne nye kriminalitetsform, anbefalte jeg at internasjonale organisasjoner drøftet mulighetene for harmonisering eller anbefalinger om straffelovgivningen i de enkelte land slik at de omfattet alle former for computer crime.

Den andre internasjonale milepælen om datakriminalitet ble et initiativ fra *The Organization for Economic Cooperation and Development (OECD).* OECD fikk 27. januar 1982 et brev fra meg mens jeg hadde forskningsoppholdet på SRI i California, med følgende anbefaling:[8]

«I strongly advice that recommendations should be initiated to directly protect personal and other data from criminal activities. The extent of this subject will also include the national vulnerability on individual countries.»

OECD inviterte meg deretter til Paris i september 1982 for å drøfte forslaget mitt. På møtet i OECD ble det besluttet å invitere en gruppe av eksperter til OECD i Paris for å diskutere computer crime. Ekspertgruppen[9] møtte i OECD 30. mai 1983. Ekspertgruppen foreslo at OECD skulle utarbeide retningslinjer for harmonisering av straffebestemmelser om computer crime. Gruppen ble dermed grunnleggere av internasjonale tiltak for harmonisering av medlemslandenes straffebestemmelser om computer crime. OECD ble derfor den første internasjonale organisasjonen som tok initiativ til å utarbeide retningslinjer for harmonisering av straffebestemmelser om computer crime.

OECD utarbeidet en *Analytical Summary of Responses to the Questionnaire* som ble sendt medlemslandene 8. september 1983. Det ble blant annet henvist til min definisjon av computer crime som var: *any illegal act for which knowledge of computer technology is essential for its perpetration, investigation or prosecution.* I tillegg også henvist til min bok *Computer and Penal Legislation, Complex 2/83 (Universitetsforlaget).*

OECD vedtok i 1986 *Recommendations on Computer-Related Criminality: Analysis of Legal Politics in the OECD*

6 NOU 1985: 31 s. 5.

7 Straffelovrådets faste medlemmer var: Johs. Andenæs, Else Bugge Fougner, Lasse Qvigstad og Thor Oug. Særskilt oppnevnte sakkyndige medlemmer var: Ruth Drolsum, Knut S. Selmer og Stein Schjølberg. Straffelovrådets sekretær var Hans Petter Jahre.

8 Stein Schjølberg, brev av 27. januar 1982 ble sendt til Science and Technology Division, OECD, Paris.

9 Medlemmer av ekspertgruppen var: Mme C.M. Pitrat, Frankrike, Mr. M. Masse, Frankrike, Mr. A. Norman, Storbrittania, Mr. S. Schjolberg, Norge, Mr. B. de Schutter, Belgia, og Mr. U. Sieber, Tyskland.

Colourbox / Chat GPT

Area.[10] OECD anbefalte at medlemslandene kunne vurdere behovet for straffebestemmelser etter en liste av handlinger som ble publisert.

4. Internett

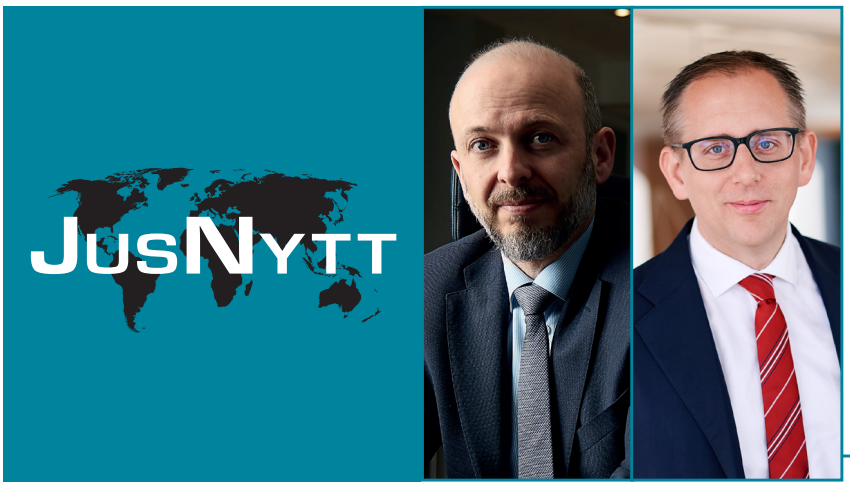
Internett slik som vi kjenner det i dag, har sin bakgrunn i et amerikansk nettverk som ble kalt ARPANET (Advanced Research Projects Agency Network). Det første eksperimentelle nettverket ble utviklet i 1968 av en forskningsgruppe ved Network Information Center (NIC) i et samarbeid med University of California (UCLA) i Los Angeles. Den 29. oktober 1969 ble den første meldingen mellom to forskjellige forskningsinstitusjoner i California sendt fra UCLA til Stanford Research Institute (SRI) i Palo Alto, og disse ble de to første funksjonelle nodene i ARPANET.

Den første internasjonale Internett milepælen og den første funksjonelle internasjonale noden i ARPANET ble sendt til Norge. Det var NORSAR (Norwegian Seismic Array) på Kjeller ved Lillestrøm, som mottok den første meldingen fra California. Meldingen ble deretter videresendt til University College i London i England, som ble den neste internasjonale noden.

Vi trodde at arbeidet med lovtiltak mot datakriminalitet stort sett var avsluttet rundt 1990, men lite visste vi at noe som ble kalt «Internett» skulle dukke opp til alminnelig benyttelse fra midten av 1990-årene. Da Mosaic og senere Netscape Navigator ble allment tilgjengelig forsto vi at vi måtte begynne helt på nytt igjen.

Stein Schjølberg, pensjonert sorenskriver.

10 Se side 19-21 i *https://www.oecd.org/content/dam/oecd/en/publications/reports/1986/09/oecd-observer-volume-1986-issue-5_g1g341c5/observer-v1986-5-en.pdf*



Schjødt

Halvor Manshaus

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

Thomas Hagen

Thomas Hagen er partner og advokat i Advokatfirmaet Schjødt og spesialisert innen immaterialrett (patent-, varemerke-, design- og opphavsrett), forretningshemmeligheter og markedsføringsrett. Han bistår særlig inn mot skjæringspunktet mellom teknologi og jus.

Immaterielle rettigheter og ny teknologi: strategisk juridisk rådgivning i offentlig forsvarssektor

Innledning

Forsvarssektoren i Norge og resten av Europa gjennomgår en periode med betydelige investeringer og endringer i leveransekjeden. Med raskt voksende anskaffelsesbudsjetter og nye internasjonale samarbeidsavtaler under utforming, har spørsmål knyttet til immaterielle verdier («**IP**») beveget seg fra periferien til selve sentrum av forsvarsavtalene. Norges oppdaterte retningslinjer for anskaffelser innen forsvarssektoren, som trer i kraft 1. januar 2026, sammen med tilhørende forskrifter om industrielt samarbeid, skaper et rikt og komplekst IP-landskap. Slike endringer over kort tid innebærer et behov for juridisk planlegging, tilrettelegging og rådgivning. I dette nye landskapet er det viktig å koble på erfarne juridiske rådgivere tidlig i prosessen.

Denne artikkelen gir en oversikt over de viktigste IP-bestemmelsene som gjelder for forsvarsanskaffelser i Norge, og belyser de praktiske områdene der vi mener spesialisert juridisk rådgivning gir størst merverdi.

Reguleringsrammen: IP og royalty i offentlige forsvarsanskaffelser

Kjerneprinsipp: Ikke-eksklusiv lisensiering som utgangspunkt

Retningslinjene for offentlige forsvarsanskaffelser krever at anskaffelsesmyndighetene fastsetter bestemmelser om IP og royalty i kontrakter, og at eierskap til IP og eventuell royalty for bruksrettigheter skal fremgå tydelig i forespørsel/konkurransegrunnlag og i selve kontrakten.

IP er i retningslinjene definert bredt som et samlebegrep som blant annet omfatter oppfinnelser, tekniske løsninger, opphavsrettsbeskyttede verk (inkludert programvare, kildekode og algoritmer), design, forretningshemmeligheter og know-how. Immaterielle rettigheter («**IPR**») som omfattes av retningslinjene, inkluderer patenter etter den norske patentloven, varemerker etter den norske varemerkeloven, designrettigheter etter den norske designloven, opphavsrett etter den norske opphavsrettsloven, forretningshemmeligheter etter den norske loven om forretningshemmeligheter og kontraktsfestede rettigheter til immaterielle rettigheter.

Som hovedregel skal forsvarssektoren inngå avtaler som gir bruksrettigheter som tilfredsstiller de faktiske behov i forbindelse med en anskaffelse og påfølgende drift, vedlikehold og videreutvikling. Avtalene skal altså ikke uten videre innebære overtakelse av eiendomsretten til den underliggende teknologien og kompetansen som ligger til grunn for anskaffelsen. Denne generelle preferansen for ikke-eksklusive lisenser fremfor direkte eiendomsoverdragelser innebærer at det konkrete omfanget, varigheten og begrensningene av bruksrettighetene må utformes og tilpasses

konkret til hver enkelt avtale. Et unntak fra dette utgangspunktet gjelder der det foreligger tungtveiende grunner til å erverve eierskap, eller til å kreve eksklusive bruksrettigheter, som omtalt nedenfor.

Når overføring av eierskap eller eksklusive lisenser kan være aktuelt

Unntaksvis kan forsvarssektoren ha behov for en overføring av eiendomsrett til immaterielle rettigheter fra leverandøren, eller en eksklusiv lisens, der dette klart er strengt nødvendig og det foreligger særlig tungtveiende sikkerhetshensyn. Dette gjelder spesielt der slik streng nødvendighet kan påvises, herunder situasjoner som faller inn under lov av 26. juni 1953 nr. 8 om oppfinnelser av betydning for riket med tilhørende forskrifter. Det samme vil gjelde dersom en slik overføring eller eksklusiv lisens utgjør det mest økonomisk fordelaktige alternativet (som utdypet i Forsvarsdepartementets retningslinjer for anskaffelsesprosedyrer innen forsvarssektoren). Slike ordninger kan være begrenset i tid og omfang til utvalgte elementer av teknologi eller kunnskap.

Rådgivning om når disse strenge terskelverdiene er oppfylt og hvordan man balanserer en regulering som tilfredsstiller de regulatoriske kravene opp mot leverandørens kommersielle og langsiktige interesser på en fornuftig måte, er et kjerneområde for spesialiserte juridiske rådgivere. En viktig del av dette arbeidet vil være ikke bare struktur og mekanismer for overgang eller eksklusivitet, men gode og gjennomtenkte definisjoner av know-how og teknologi som berøres. I en slik prosess vil det ofte være nødvendig å legge opp til et samarbeide mellom juridiske rådgivere og øvrige ressurser med spesialisert teknisk kompetanse.

Viktige forpliktelser knyttet til immaterielle rettigheter og teknologi ved utarbeidelse av kontrakter

Grensesnittdokumentasjon og brukerrettigheter

Forsvarssektoren har rett til, uten kostnad, å benytte teknisk dokumentasjon som er levert i henhold til en kontrakt, og som det er nødvendig å inkludere i anbudsdokumenter eller på annen måte gjøre offentlig tilgjengelig for å beskrive grensesnitt og funksjonalitet i forbindelse med anskaffelse av tilstøtende systemer eller materiell – såkalt «*Grensesnittdokumentasjon*».

Grensesnittdokumentasjon kan omfatte overordnede beskrivelser av form, tilpasning og funksjon; informasjon som er nødvendig for generell installasjon, drift, vedlikehold og opplæring; rettelser og endringer i teknisk dokumentasjon; offentlig tilgjengelig informasjon; og annen teknisk informasjon som forsvarssektoren har levert til leverandøren.

Forsvarssektoren må også sikre at den, uten kostnad og for eget internt bruk, kan reprodusere og distribuere teknisk dokumentasjon levert av leverandøren.

Å definere de nøyaktige grensene for grensesnittdokumentasjon i kontrakter – og sikre at leverandørens kommersielt sensitive dokumentasjon opprettholder passende konfidensialitetsbeskyttelse – er et område der nøye juridisk utforming er avgjørende.

Omfattende kontraktsmessig vurdering av immaterielle rettigheter

Ved hver kontraktsinngåelse må anskaffelsesmyndigheten blant annet vurdere at de avtalte immaterielle rettighetene dekker både nåværende og fremtidige behov og formål innen forsvarssektoren.

Kontrakter må også omhandle retten til å dele IP innenfor den bredere offentlige forsvarssektoren der det er nødvendig, inkludert deling innenfor det totale forsvarsrammeverket (for eksempel brukerhåndbøker), deling med andre aktører i bransjen (for eksempel grensesnittdokumentasjon) og deling med andre lands væpnede styrker (for eksempel tekniske håndbøker).

Kontrakter må omhandle spørsmål om ansvar og erstatning i tilfelle brudd på tredjeparts rettigheter, for å beskytte forsvarssektoren og sikre alternative løsninger dersom et brudd på tredjeparts rettigheter ikke kan løses.

Kontrakter må også omhandle juridiske scenarier der utviklingen som skal gjennomføres av en eller annen grunn ikke fullføres, eller der leverandøren senere blir insolvent, avslutter driften eller oppgir sitt fokus på den aktuelle teknologien, slik at forsvarssektoren i slike tilfeller kan sikre seg alle nødvendige rettigheter for å beskytte sine interesser.

Konkret må kontrakter sikre overholdelse av loven om ansattes oppfinnelser, loven om forretningshemmeligheter, loven om oppfinnelser av betydning for rikets forsvar og opphavsrettsloven – både for å sikre de rettighetene forsvarssektoren har krav på og for å sikre overholdelse av konfidensialitetskrav. Dette gjelder i like stor grad for forsvarssektorens egne ansatte som deltar i FoU-prosjekter med en leverandør.

Omfanget av denne lovpålagte sjekklisten – som spenner fra patentlovgivning til opphavsrett, forretningshemmeligheter og spesifikk lovgivning for forsvarssektoren – understreker hvorfor IP-ekspertise i denne sektoren ikke bare er nyttig, men nødvendig for å unngå problemer på et senere punkt i tidslinjen.

Royalties: Et særlig komplekst område

Forpliktelsen til å avtale royalty

Der forsvarssektoren helt eller delvis har finansiert forskning og utvikling av et produkt, må det inngås en avtale om royalty.

Royaltysatsen skal tilpasses det enkelte tilfellet. Som hovedregel

skal royalty ikke overstige 5 % av salgsprisen for et produkt/en tjeneste, eller delkomponenter i et system, der forsvarssektoren har finansiert en utvikling eller anskaffelse (investeringsanskaffelse). Dette taket på 5 % gjelder både som et maksimumsbeløp per kontrakt og, som omtalt nedenfor, som et samlet tak for alle etater innen forsvarssektoren for det samme produktet. Royaltysatsen skal vurderes ut fra markedspotensial, utviklingskostnader i forhold til produksjonskostnader og eventuelle avgifter per enhet. Det er viktig å merke seg at royalty normalt ikke skal kreves i FoU-kontrakter der forsvarssektorens bidrag til utviklingen ikke overstiger 5 millioner kroner (ekskl. mva.), uavhengig av hvilken budsjettpost finansieringen hentes fra. I tillegg kan fritak for royalty vurderes for små og mellomstore bedrifter i tidlige faser av en utviklingssyklus der forsvarssektoren bidrar med finansiering i et produkts oppstartsfase; et slikt fritak må godkjennes av Forsvarsdepartementet.

Royalty skal betales fra første salg. Som hovedregel skal royalty frafalles så snart det offentlige forsvarssektorens bidrag eller investering er tilbakebetalt, og det kan vurderes å fastsette en sluttdato for royaltybetalinger basert på en vurdering av teknologiens levetid. Denne regelen om fritak ved tilbakebetaling og tidsbegrensning skal imidlertid ikke gjelde for immaterielle rettigheter som forsvarssektoren selv har utviklet; i slike tilfeller skal lisensavtaler og royaltykrav overfor industrien i stedet baseres på kravene som gjelder for forsvarssektorens virksomhet som markedsaktør etter statsstøttereglene, hvor en veiledende royaltysats på 5 % anses som markedsstandard innenfor forsvarssegmentet.

Forsvarssektoren skal i prinsippet behandles som én aktør, noe som innebærer at det ikke skal kreves royalty for samme sak flere ganger av ulike etater. Følgelig skal den samlede royaltyen som skal betales til alle etater samlet sett ikke overstige det ovennevnte taket på 5 % for det samme produktet, uavhengig av antall separate avtaleforhold.

Royalty ved videreutvikling

Dersom en leverandør videreutvikler et produkt, eller bruker deler av et utviklet produkt som del av et annet system, skal det også betales royalty. Ved videreutvikling beregnes royaltyen som: Forsvarssektorens royalty = X × (A / (A + B)), der X er den opprinnelig beregnede royaltyen, A er forsvarssektorens utviklingskostnader (inkludert eget bidrag), og B er leverandørens videreutviklingskostnader.

Leverandøren må fremlegge dokumentasjon for anskaffelsesmyndigheten som underbygger en redusert royalty-sats, og kan ikke rapportere royalty til en redusert sats før anskaffelsesmyndigheten har mottatt og godkjent grunnlaget for denne reduksjonen.

Rapporterings-, revisjons- og verifiseringsrettigheter

Anskaffelsesmyndigheten må pålegge leverandøren en registreringsplikt, herunder en plikt til å føre en spesifikk oversikt over det nøyaktige antallet solgte enheter og fakturaverdien. Leverandøren må rapportere om salg og innkrevde avgifter for hvert kalenderår, selv om det ikke har vært noe salg i perioden.

Forsvarssektoren har rett til innsyn hos leverandøren for å verifisere underliggende dokumentasjon, og rett til å innhente opplysninger gjennom relevante etater om eventuelle salg til utlandet.

Forsvarsmateriell («**FMA**») forvalter forsvarssektorens mulighet til å kreve royalty for utvikling finansiert ved investeringer sektoren gjør via sine investeringsanskaffelser, mens Forsvarets forskningsinstitutt («**FFI**») forvalter royalty ved lisensiering av forsvarssektorens egne immaterielle rettigheter til industrien.

Der både FFI og FMA kan kreve royalty for det samme produktet, har royaltybetaling til FFI forrang når royaltyen gjelder lisensiering av forsvarssektorens egne immaterielle rettigheter innenfor taket på 5 %.

For å illustrere dette kan det oppstå en royaltykonflikt der en leverandør videreutvikler et produkt finansiert av forsvarssektoren og krever en redusert royaltysats i henhold til formelen angitt ovenfor, men anskaffelsesmyndigheten er uenig i leverandørens beregning av egne videreutviklingskostnader (B). I et slikt scenario kan leverandøren ikke anvende den reduserte satsen før anskaffelsesmyndigheten har godkjent den underliggende dokumentasjonen – noe som skaper en potensiell kontantstrøm- og regnskapskonflikt som krever både teknisk og juridisk løsning. Tilsvarende kan det oppstå uenighet om hvorvidt det samlede taket på 5 % er nådd, og hvilken etats krav på royalty som har prioritet, når flere etater hver for seg har finansiert deler av det samme produktet.

Forgrunns- og bakgrunnsinformasjon i FoU- og utviklingsprosjekter

Forgrunnsinformasjon er informasjon som skapes eller utvikles i løpet av gjennomføringen av et samarbeids- eller utviklingsprosjekt – typisk i forbindelse med et spesifikt anskaffelsesprosjekt, eller i FoU-prosjekter som går forut for en anskaffelse.

Forgrunnsinformasjon som oppstår fra et anskaffelsesprosjekt, kan være relevant for senere oppgraderinger og vedlikehold, eller for muligheten til å foreta en ny anskaffelse dersom en leverandør blir insolvent eller avslutter driften. Av denne grunn må forsvarssektoren sikres retten til å bruke forgrunnsinformasjon fra et prosjekt til senere anskaffelser og potensielle oppfølgingskonkurranser, samtidig som forretningshemmeligheter og kom-

mersielt sensitiv informasjon beskyttes.

Avtalene må inneholde klare beskrivelser og må ikke gi forsvarssektoren rett til å dele rettigheter eller forgrunnsinformasjon med tredjeparter, med mindre dette er uttrykkelig avtalt. I påfølgende konkurranser bør forsvarssektoren som hovedregel benytte aggregerte, ikkesensitive resultater fra forgrunnsinformasjonen når den samarbeider med tredjeparter.

Eierskapet til et produkt som stammer fra forgrunnsinformasjon generert gjennom et FoU-prosjekt før en (potensiell) anskaffelse, forblir normalt hos leverandøren. Dette prinsippet har betydelig kommersiell betydning: det innebærer at en leverandør beholder muligheten til å utnytte produktet kommersielt, herunder gjennom eksportsalg til tredjeland, forutsatt at slikt salg ikke strider mot gjeldende eksportkontrollbestemmelser (som utgjør et strengt forbud snarere enn en ren formalitet for etterlevelse). Forsvarssektoren sikrer seg de brukerrettighetene den trenger. Den nøyaktige avgrensningen av hva som utgjør «produktet» i forhold til den underliggende forgrunnsinformasjonen – og i hvilken grad forsvarssektoren kan bruke denne informasjonen i påfølgende konkurranser – er imidlertid ofte et sentralt forhandlingspunkt som krever nøye utforming av kontrakten.

Industrisamarbeidsavtaler og overføring av immaterielle rettigheter

Et særskilt, men nært beslektet område omfatter IP-aspektene ved forpliktelser til industrisamarbeid som utløses av utenlandske forsvarsanskaffelser.

Godkjente kategorier av industrisamarbeidsprosjekter omfatter teknologisamarbeid (inkludert FoU-samarbeid) og teknologi- og kunnskapsoverføring til norske partnere.

Teknologisamarbeid defineres som prosjekter der norske og utenlandske partnere deltar på like fot og med en rimelig grad av like innsats, med sikte på å produsere et neste generasjons produkt, helst på systemnivå.

I sammenheng med teknologisamarbeid utgjør den norske partnerens rettigheter til teknologi og kunnskap et av elementene i verdivurderingen av prosjektet.

Tilsvarende er den norske partnerens rettigheter til teknologi og kunnskap et sentralt element i verdivurderingen ved teknologi- og kunnskapsoverføring.

Industrisamarbeidsprosjekter må ikke føre til eksport av norsk forsvarsmateriell, teknologi eller kompetanse i strid med gjeldende eksportkontrollbestemmelser.

Kryssfeltet mellom IP-eierskap, forpliktelser til teknologioverføring og overholdelse av eksportkontroll er et av de mest teknisk krevende områdene innenfor immaterielle rettigheter innen forsvarssektoren, og et område som regelmessig krever spesialisert juridisk strukturering.

Colourbox / Chat GPT

Praktiske områder der spesialistrådgivning tilfører verdi

Det regulatoriske rammeverket som er skissert ovenfor gir opphav til en rekke praktiske utfordringer der spesialisert juridisk rådgivning i skjæringspunktet mellom IP-rett og forsvarsanskaffelser er ønskelig:

1. **IP-revisjoner og kartlegging av rettigheter før kontraktsinngåelse**
   Kartlegging av en leverandørs eller anskaffelsesmyndighets eksisterende IP-portefølje – og identifisering av hvilke rettigheter som sannsynligvis vil bli berørt av en bestemt forsvarsavtale – er et avgjørende skritt før kontraktsinngåelse. Dette inkluderer bakgrunnsinformasjon, potensiell forgrunnsinformasjon og ansattes oppfinnelser.

2. **Utarbeidelse og forhandling av klausuler om immaterielle rettigheter og royalty**
   Retningslinjene stiller detaljerte krav til innholdet i IP-bestem-

melser, herunder brukerrettigheter, grensesnittdokumentasjon, tredjeparts erstatningsansvar, insolvensbeskyttelse og royaltyformler. Spesialiserte rådgivere bør bistå både leverandører og forsvarssektoren med å utarbeide balanserte, regelverksmessige og kommersielt beskyttende klausuler. Det bør videre bemerkes at reglene for gjennomføring av anskaffelsesprosedyrer innen forsvarssektoren («**RAF**») er en intern instruks som i seg selv ikke gir rettigheter eller forpliktelser til tredjeparter, inkludert leverandører; kravene i instruksen får imidlertid kontraktsmessig virkning gjennom anskaffelsesdokumentene og de resulterende kontraktene, noe som gjør kjennskap til RAF avgjørende for enhver part som forhandler om forsvarsavtaler.

3. **Strukturering av FoU-kontrakter og samarbeidsavtaler**
   For utviklingsprosjekter er en klar fordeling av rettigheter til forgrunnsinformasjon og bakgrunnsinformasjon – og å sikre at forsvarssektoren oppnår de spesifikke rettighetene den trenger uten unødvendig å frata leverandøren kommersiell verdi – en oppgave som krever dyktighet i utformingen.

4. **Rådgivning om royalty-tvister og verifisering**
   Gitt forsvarssektorens omfattende revisjons- og inspeksjonsrettigheter, samt kompleksiteten ved beregning av royalty på videreutvikling, er tvister om royaltyforpliktelser og rapporteringskrav et voksende område for rettstvister og tvisteløsning.

5. **Teknologioverføring i industrisamarbeidsavtaler**
   Spesialiserte rådgivere kan gi råd til utenlandske leverandører og norske industripartnere om de immaterialrettslige implikasjonene av teknologioverføringsprosjekter under industrisamarbeidsavtaler, herunder strukturering av immaterialrettighetseierskap, rettigheter til resultater og samspillet med eksportkontrollovgivningen.

6. **Håndtering av *forsvarsviktige oppfinnelser***
   Når en anskaffelse faller inn under loven om oppfinnelser av betydning for rikets forsvar, og sikkerhetshensyn kan gjøre det nødvendig med en overføring av eierskap eller en eksklusiv lisens, er det nødvendig med spesialistrådgivning for å vurdere den strenge nødvendighetsgrensen og for å strukturere ordningen på en hensiktsmessig måte.

7. **Overholdelse av avtalen etter kontraktsinngåelse og rapportering av royalty**
   Løpende støtte til leverandører som er underlagt årlige rapporteringsforpliktelser for royalty, revisjonsrisiko og verifiseringsprosesser er et område med vedvarende etterspørsel etter hvert som langsiktige forsvarsavtaler nærmer seg utløpet.

Konklusjon og fremtidsutsikter

IP innen forsvarssektoren er ikke lenger et sekundært anliggende i forsvarsanskaffelser. IP er i dag en sentral pilar i kontraktsforhandlinger og en kilde til betydelig kommersiell risiko og mulighet. Norges oppdaterte retningslinjer for forsvarsanskaffelser for 2026 har kodifisert et detaljert og krevende IP-rammeverk som gjelder for alle kontrakter i sektoren.

Fremover vil den økende rollen til kunstig intelligens, autonome systemer og multinasjonale samarbeidsprogrammer for utvikling ytterligere komplisere IP-landskapet – og reise nye spørsmål om eierskap til AI-genererte oppfinnelser, grenseoverskridende lisensiering av fellesutviklede teknologier og anvendelsen av eksisterende lovverk på nye kategorier av immaterielle eiendeler. For å navigere vellykket i dette rammeverket i endring – enten som leverandør, industripartner eller selve innkjøpsmyndigheten – kreves det spesialistkompetanse i skjæringspunktet mellom immaterialrett, lovgivning om forsvarsanskaffelser og kommersiell avtalerett. Dette er viktig for Forsvaret som mottaker av anskaffelser, leverandørenes fremtidige konkurransegrunnlag og for den videre utviklingen av norsk forsvarsindustri som leverandør til partnere og allierte utenfor Norge.

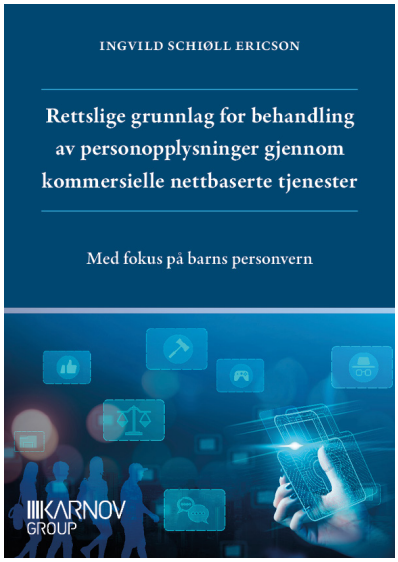
> For å navigere vellykket i dette rammeverket i endring – enten som leverandør, industripartner eller selve innkjøpsmyndigheten – kreves det spesialistkompetanse i skjæringspunktet mellom immaterialrett, lovgivning om forsvarsanskaffelser og kommersiell avtalerett.

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

Thomas Hagen er partner og advokat i Advokatfirmaet Schjødt og spesialisert innen immaterialrett (patent-, varemerke-, design- og opphavsrett), forretningshemmeligheter og markedsføringsrett. Han bistår særlig inn mot skjæringspunktet mellom teknologi og jus.

Rettslige grunnlag for behandling av personopplysninger gjennom kommersielle nettbaserte tjenester – Med fokus på barns personvern

Forfatter: Ericson, Ingvild Schiøll
Utgiver: Karnov Group Norway
Versjon: 1. utgave, 1. versjon
ISBN: 978-82-93816-95-9



En rekke nettbaserte tjenester finansieres ved at brukernes personopplysninger behandles i stor skala for selskapenes inntjening. Kommersielle tjenester som sosiale medier, videospill og strømming tilbys ofte gratis eller til lav pris, men henter store inntekter gjennom praksis som målrettet markedsføring, personlig tilpassede tjenester, og sporing på tvers av nettsider, apper og utstyr. All behandling av personopplysninger krever et rettslig grunnlag etter personvernforordningen art 6. Rettsgrunnlagene ivaretar ulike formål, oppstiller ulike vilkår, og gir registrerte ulike rettigheter.

Databehandling for kommersielle formål forankres ofte i en kombinasjon av samtykke, avtalerettslig nødvendighet og berettiget interesse. I antologien analyseres rettslige krav for bruk av de tre behandlingsgrunnlagene. Analysene av gjeldende rett er «aldersnøytrale», men vurderer også barns personvern særskilt. Til tross for stort fokus på barn og nettbruk, er det i liten grad foretatt juridiske vurderinger av de særlige spørsmål som reiser seg for kommersiell bruk av barns personopplysninger – dette til tross for åpenbare rettslige hindre etter gjeldende rett.

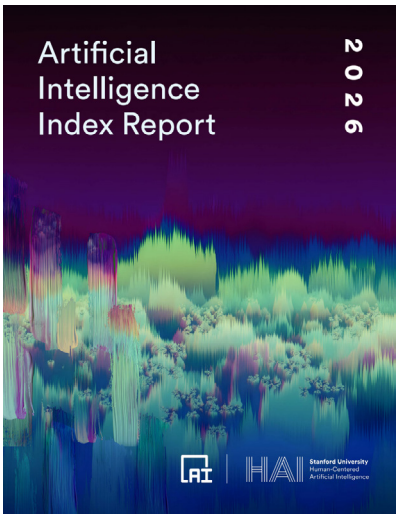
Krav til behandlingsgrunnlag etter personvernforordningen art. 6, vurderes her i lys av barns særskilte beskyttelse, knyttet til blant annet mekanismer for alderskontroll og nasjonale krav til rettslig handleevne. Samlet gir antologien en helhetlig analyse av de vanligste rettslige grunnlagene for å behandle personopplysninger for kommersielle formål gjennom nettbaserte tjenester, med særlig fokus på barns vern.

Omtalen er hentet fra Karnov Group Norway: https://www.karnovgroup.no/rettslig-grunnlag-for-behandling-av-personopplysninger-gjennom-kommersielle-nettbaserte-tjenester

Les boken i Lovdata Pro

AI Index Report 2026

Stanford University
The AI Index is an independent initiative at the *Stanford Institute for HumanCentered Artificial Intelligence (HAI).*



Introduction

Welcome to the ninth edition of the AI Index report. As AI continues to advance rapidly, the question becomes whether the systems built around it can keep up. Governance frameworks, evaluation methods, education systems, and the data infrastructure needed to track AI's impact are struggling to match the pace of the technology itself. That gap—between what AI can do and how prepared we are to manage it—runs through every chapter of this year's report. New in this edition, the report tracks how AI is being tested more ambitiously across reasoning, safety, and real-world task execution, and why those measurements are increasingly difficult to rely on. It also features new estimates of generative AI's economic value alongside emerging evidence of its labor market effects, an analytical framework on AI sovereignty, and a science chapter developed in collaboration with Schmidt Sciences. For the first time, the report features standalone chapters on AI in science and AI in medicine, reflecting AI's growing impact across these two domains.

For close to a decade, the AI Index has worked to bring reliable global data to a field that is evolving faster than most efforts to measure it. The report equips policymakers, researchers, executives, journalists, and the public with the necessary evidence to make informed decisions about AI. As the technology moves deeper into classrooms, clinics, and legislatures—and reshapes how people work, learn, and govern—the cost of incomplete data continues to rise.

In a field where much data is produced by organizations with a stake in the technology's success, the demand for neutral and rigorous measurement continues to grow. The AI Index remains independent and focused on revealing the long-term patterns underneath the headlines. The report is relied on by governments, research institutions, and companies around the world, and referenced by media outlets and in academic papers.

The pages that follow offer the most comprehensive, independently sourced picture of AI's trajectory that is available. They also make clear where that picture remains incomplete—because what we cannot yet measure matters just as much as what we can.

The full report can be found here: https://hai.stanford.edu/assets/files/ai_index_report_2026.pdf

Delphi

Sophie Wichmann

Nytt avgörande från Arbetsdomstolen: Arbetsgivares granskning av fysiskt belastningsregisterutdrag omfattas inte av GDPR

Arbetsdomstolen meddelade den 25 mars i år ett avgörande (AD 2026 nr 27) som behandlade frågan om huruvida en arbetsgivares åtgärd att ta del av en anställds utdrag ur belastningsregistret utgör sådan behandling av personuppgifter som omfattas av dataskyddsförordningen (GDPR).

I det aktuella fallet hade en arbetsgivare uppmanat en nyanställd att uppvisa ett utdrag ur belastningsregistret efter att anställningen hade påbörjats. Den anställde begärde själv ut handlingen från Polismyndigheten och överlämnade den i ett förseglat kuvert till sin närmaste chef, som öppnade kuvertet och tog del av innehållet. Av utdraget framgick att den anställde hade en tidigare brottmålsdom. Efter att arbetsgivaren hade läst innehållet förstördes registerutdraget i en dokumentförstörare.

Det fackförbund som företrädde den anställde menade att arbetsgivaren genom detta förfarande hade behandlat personuppgifter om lagöverträdelser i strid med GDPR och framställde ett skadeståndskrav om 60 000 kronor.

Som grund åberopade fackförbundet bland annat EU-domstolens avgörande C-740/22 (”Endemol Shine Finland Oy”), där domstolen slog fast att muntligt utlämnande av uppgifter om fällande domar utgör behandling av personuppgifter enligt artikel 4.2 i GDPR, och att sådan behandling omfattas av förordningens tillämpningsområde när uppgifterna ingår i ett register. Fackförbundet menade därför att bolaget, redan genom att ta emot och läsa igenom belastningsregisterutdraget, hade behandlat personuppgifter i strid med artikel 10 i GDPR. Avgörande var enligt fackförbundet att uppgifterna härstammade från ett register, och hur bolaget sedan hanterade utdraget efter mottagandet saknade betydelse för bedömningen.

Arbetsdomstolen landade i motsatt slutsats och slog fast att det var just bolagets egen hantering av registerutdraget som var avgörande. Enligt domstolen uppfyllde hanteringen visserligen definitionen av behandling av personuppgifter enligt artikel 4.2 i GDPR, men enligt artikel 2.1 i GDPR är förordningen tillämplig på manuell behandling av personuppgifter endast under förutsättning att uppgifterna ingår i, eller är avsedda att ingå i, ett register. Det avgörande var alltså inte varifrån uppgifterna härstammade, utan hur bolaget organiserade sin hantering av dem. Att uppgifterna härstammade från belastningsregistret, för vilket Polismyndigheten är personuppgiftsansvarig, saknade enligt domstolen betydelse för bedömningen.

> ”För en arbetsgivare innebär avgörandet att det inte utgör personuppgiftsbehandling i GDPR:s mening att ta emot, läsa och sedan förstöra ett fysiskt belastningsregisterutdrag, så länge uppgifterna inte sparas i något register.

Eftersom det inte ens gjorts gällande att bolaget avsett att låta uppgifterna ingå i något register, konstaterade domstolen att hanteringen

Colourbox / Chat GPT

inte var en sådan manuell behandling som avses i artikel 2.1 i GDPR. Till stöd för den bedömningen jämförde domstolen med EU-domstolens avgörande C-740/22, och noterade att det målet, till skillnad från det nu aktuella, avsåg en domstols muntliga utlämnande av uppgifter från domstolens *eget* personregister. Skadeståndskravet lämnades utan bifall.

Fackförbundet yrkade också att domstolen skulle inhämta förhandsavgörande från EU-domstolen avseende dels ersättningens storlek vid överträdelse av GDPR, dels huruvida arbetsgivarens granskning av ett fysiskt belastningsregisterutdrag utgör behandling av personuppgifter i förordningens mening. Arbetsdomstolen konstaterade att frågan om ersättningens storlek inte var aktuell med hänsyn till utgången i målet. Vad gällde den andra frågan bedömde domstolen att det inte förelåg någon EU-rättslig oklarhet som gjorde det nödvändigt att inhämta ett förhandsavgörande, eftersom svaret framgick av artikel 2.1 i GDPR.

En skiljaktig mening pekade emellertid på skäl till att inhämta ett förhandsavgörande. Ledamoten noterade att den svenska lagstiftaren visserligen uttalat sig om att motsvarande förfarande *inför* anställning sannolikt faller utanför förordningens tillämpningsområde, men att vägledning saknades för kontroller som genomförs *under* pågående anställning. Mot bakgrund av GDPR:s syfte, artikel 10 om uppgifter rörande fällande brottmålsdomar, samt att det i prop. 2025/26:174 (”Utökade registerkontroller i skolväsendet”) getts uttryck för att rättsläget kring registerkontroll under pågående anställning inte är klarlagt, ansåg den skiljaktiga ledamoten att det inte stod tillräckligt klart att förfarandet skulle falla utanför förordningens materiella tillämpningsområde.

För en arbetsgivare innebär avgörandet att det inte utgör personuppgiftsbehandling i GDPR:s mening att ta emot, läsa och sedan förstöra ett fysiskt belastningsregisterutdrag, så länge uppgifterna inte sparas i något register. Avgörandet är välkommet eftersom det har funnits en oklarhet i vilket utsträckning som arbetsgivare får hantera ett sådant registerutdrag inom ramen för en anställning utan att det blir fråga om behandling av personuppgifter.

Sophie Wichmann, Associate, Tech & IP, Advokatfirman Delphi, Stockholm.

Gorrissen Federspiel

Tue Goldschmieding

Nyt om persondataret i Danmark

Retten i Viborg tilkendte godtgørelse for uberettiget videregivelse af personoplysninger til skadevolder

Retten i Viborg afsagde den 12. januar 2026 dom i sag BS-53777/2023-VIB. Sagen angik, hvorvidt den danske Civilstyrelse (»Civilstyrelsen«) skulle betale godtgørelse til A og hendes mor, B, for uberettiget at have videregivet personoplysninger fra A's sag hos det danske Erstatningsnævn (»Erstatningsnævnet«) til skadevolderen C.

A blev som 13-årig udsat for seksuelle overgreb begået af C. Erstatningsnævnet tilkendte A godtgørelse for svie og smerte på 80.000 kr., hvilket beløb blev udbetalt af Civilstyrelsen. Da Civilstyrelsen efterfølgende rejste regreskrav mod C for det udbetalte beløb, udleverede Civilstyrelsen sagsakter til C's advokat. Det danske Datatilsyn (»Datatilsynet«) udtalte efterfølgende alvorlig kritik af videregivelsen, idet den skete i strid med Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 (»GDPR«). Civilstyrelsen anerkendte, at videregivelsen udgjorde en culpøs retsstridig handling, og at der var grundlag for godtgørelse for tort efter § 26, stk. 1 i lovbekendtgørelse nr. 1080 af 30. august 2025 om erstatningsansvar (»den danske lov om erstatningsansvar«), dog ikke overstigende 15.000 kr.

Retten bemærkede indledningsvist, at enhver videregivelse af oplysninger i sager om seksuelle overgreb kræver en særlig grundig gennemgang af nødvendigheden i videregivelsen af de enkelte oplysninger og en afvejning af behovet for videregivelse over for de berørtes ret til fortrolighed. Retten fandt, at navnlig de nærmere beskrivelser af A's psykiske forhold i de børnefaglige undersøgelser samt sundhedsoplysninger om hendes fysiske helbred var særdeles personfølsomme, og at videregivelsen udgjorde en krænkelse af A's ret til respekt for privatliv efter artikel 8 i Den Europæiske Menneskerettighedskonvention (»EMRK«), idet indgrebet hverken var proportionalt med det tilsigtede mål eller nødvendigt i et demokratisk samfund. Retten tillagde det betydning, at de videregivne oplysninger fra Civilstyrelsen oversteg, hvad der var nødvendigt for at løfte bevisbyrden med hensyn til regreskravet, idet fraværsrapporter og psykolognotater i tilstrækkelig grad ville have dokumenteret grundlaget for det rejste krav.

Retten fastsatte godtgørelsen til A til 112.500 kr. svarende til referencebeløbet efter Den Europæiske Menneskerettighedsdomstols praksis. For B fandt retten, at videregivelsen udgjorde en krænkelse af hendes ret til privatliv efter EMRK artikel 8, men at selve anerkendelsen heraf udgjorde en tilstrækkelig kompensation.

Læs Retten i Viborgs dom her: *https://domsdatabasen.dk/#/sag/10379/12211*

Læs Datatilsynets afgørelse her: *https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2026/mar/hvad-maa-partierne-bruge-om-dig-i-folketingsvalgkampen*

Datatilsynet eskalerer undersøgelse af Rejsekort-app til Det Europæiske Databeskyttelsesråd

Det danske Datatilsyn (»Datatilsynet«) offentliggjorde den 14. januar 2026, at tilsynet fortsat undersøger den nye Rejsekort-app, som Datatilsynet indledte en nærmere undersøgelse af i 2024. Datatilsynets initiale undersøgelse blev omtalt i *4. udgave af Lov og Data i 2024 (nr. 160)*. På baggrund af uklarheder i retstilstanden har Datatilsynet i den forbindelse planlagt, som godkendt af Datatilsynets øverste organ, det danske Dataråd (»Datarådet«), at anmode om en formel udtalelse fra Det Europæiske Databeskyttelsesråd (»EDPB«).

Datatilsynets undersøgelse fokuserer på, hvorvidt appens indsamling af personoplysninger lever op til GDPR artikel 5, stk. 1, litra c, om dataminimering, samt om appen er designet i overensstemmelse med GDPR artikel 25, stk. 1, om databeskyttelse gennem design. Den nye Rejsekort-app sporer brugernes fysiske placering under rejsen, bl.a.

for at beregne billetprisen. Kernen i undersøgelsen angår, hvor mange personoplysninger om brugerne er nødvendige for at levere en digital billetteringsløsning, herunder om det er nødvendigt at brugere fortsat kan spores, efter rejsen er afsluttet.

Anmodningen udspringer af, at det ikke har været muligt at udlede et entydigt billede af retstilstanden gennem Datatilsynets indhentning af uformelle udtalelser fra øvrige europæiske tilsynsmyndigheder om lignende billetløsninger baseret på lokationssporing. Datatilsynet har bedt Rejsekort & Rejseplan A/S om at besvare en række spørgsmål om appens funktionalitet og tekniske opbygning, og virksomheden har fremsendt flere redegørelser.

Datatilsynet forventer ikke at modtage svar fra EDPB før sommeren 2026, hvorefter Datarådet skal tage endelig stilling til sagen. Afhængigt af udfaldet kan sagen føre til kritik, påbud eller politianmeldelse af Rejsekort & Rejseplan A/S.

Læs Datatilsynets pressemeddelelse her: *https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2026/jan/datatilsynet-undersoeger-fortsat-den-nye-rejsekort-app*

Læs Datatilsynets pressemeddelelse fra 2024 her: *https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2026/mar/hvad-maa-partierne-bruge-om-dig-i-folketingsvalgkampen*

Datatilsynet udtaler alvorlig kritik af 51 kommuners brug af Google-produkter i folkeskolen

Det danske Datatilsyn (»Datatilsynet«) traf den 29. januar 2026 afgørelse i den såkaldte Chromebook-sag om 51 kommuners brug af Googles produkter til undervisning i folkeskolen. Sagen blev behandlet under journalnummer 2025-431-0053.

Sagen omhandler kommunernes brug af Google Workspace for Education og Google Chrome Education til undervisningsformål i de danske folkeskoler og er det sidste led i et større sagskompleks, som Datatilsynet har behandlet over flere år og som også har været behandlet i de tidligere udgivelser af Lov og Data. Afgørelsen er truffet som opfølgning på Udtalelse 22/2024 fra Det Europæiske Databeskyttelsesråd (»EDPB«) om den dataansvarliges forpligtelser ved brug af databehandlere. Datatilsynet havde i tilsynets tilbagevenden til sagskomplekset i nærværende sag et særligt fokus på kommunernes overvejelser og dokumentation for lovliggørelsen af den behandling af personoplysninger, der fandt sted hos Googles underdatabehandlere uden for EU.

Datatilsynet udtalte alvorlig kritik af kommunerne, eftersom tilsynet fandt, at kommunernes behandling af personoplysninger ikke var sket i overensstemmelse med GDPR, herunder GDPR's principper om lovlig og gennemsigtig behandling samt reglerne om den dataansvarliges ansvar og brug af (under-)databehandlere.

Datatilsynet advarede endvidere kommunerne om, at det sandsynligvis vil være i strid med GDPR artikel 6, stk. 1, jf. artikel 6, stk. 3, om behandlingens lovlighed, hvis kommunerne ikke har konfigureret deres opsætning af de pågældende programmer i overensstemmelse med de krav, Kommunernes Landsforening (»KL«) har specificeret, og hvilke indstillinger tjener til formål at afgrænse kommunernes brug af Googles services ud af de behandlinger, som der ikke er hjemmel til. Datatilsynet advarede tilsvarende om, at det sandsynligvis vil være i strid med GDPR artikel 28, stk. 1, at antage en databehandler, hvis der ikke kan sikres et beskyttelsesniveau svarende til EU/EØS, ved videre-behandling hos underdatabehandlere i tredjelande.

Datatilsynet bemærkede afslutningsvist, at hele forløbet kunne have været undgået ved, at de relevante databeskyttelsesretlige vurderinger var blevet foretaget, inden det konkrete produkt var blevet anskaffet, og at det ikke er muligt lovligt at købe og ibrugtage et produkt, der behandler personoplysninger, hvis den dataansvarlige ikke kan skabe klarhed over de behandlinger, der finder sted.

Læs Datatilsynets afgørelse her: *https://www.datatilsynet.dk/afgoerelser/afgoerelser/2026/jan/datatilsynet-giver-51-kommuner-alvorlig-kritik-i-chromebook-sag*

Datatilsynet afslutter tilsyn med skolefotoudbydere

Det danske Datatilsyn (»Datatilsynet«) offentliggjorde den 6. januar 2026 resultatet af sit tilsyn med skolefotoudbyderes behandling af personoplysninger. Sagen blev behandlet under journalnummer 2025-41-0140.

Tilsynene havde fokus på ansvars- og rollefordelingen mellem skolefotoudbyderen og skolerne, særligt i forhold til sikring af de registreredes rettigheder samt udbydernes opbevaring og sletning af oplysninger. Tilsynene er en del af Datatilsynets planlagte tilsynsaktiviteter og har omfattet fem skolefotoudbydere.

Datatilsynet bemærkede, at en skolefotoudbyder og en skole er selvstændige dataansvarlige for den behandling af personoplysninger, der finder sted som led i klasse- og portrætfotografi, idet parterne selvstændigt fastsætter formålet og midlerne for behandlingen. For skolefotoudbyderen er det særlig relevant at overveje, i hvilken udstrækning behandlingen kan ske med hjemmel i nødvendigheden af opfyldelse af de kontrakter, der indgås med de registrerede, jf. GDPR artikel 6, stk. 1, litra b.

Fire ud af fem skolefotoudbydere oplyste at have en opbevaringsperiode for fotos og dertilhørende identifikationsoplysninger på 1-3 år, mens en enkelt skolefotoudbyder

havde en opbevaringsperiode på 10 år; perioder der alle primært begrundes i muligheden for at genbestille skolefotos. Datatilsynet bemærkede, at formålet med opbevaringen i sig selv er sagligt, men at nødvendighedskravet forudsætter et dokumenteret forretningsmæssigt behov for genbestillinger, og at der for fotos ældre end 2-3 år ikke synes et egentligt forretningsmæssigt behov herfor. Datatilsynet fandt derfor anledning til at anmode én af skolefotoudbyderne om at tilpasse sin opbevaringsperiode, om end tilsynet samtidig bemærkede, at opbevaringsperioden på 2-3 år blot var et pejlemærke, der kunne modificeres af den enkelte ved tilstrækkelig dokumentation af et sagligt forretningsmæssigt behov.

Læs Datatilsynets afsluttende brev her: *https://www.datatilsynet.dk/afgoerelser/afgoerelser/2026/jan/datatilsynet-afslutter-tilsyn-med-skolefotoudbydere*

Datatilsynet offentliggør fokusområder for tilsyn i 2026

Det danske Datatilsyn (»Datatilsynet«) offentliggjorde den 7. januar 2026 sine fokusområder for det kommende tilsynsarbejde i 2026. Fokusområderne afspejler den teknologiske udvikling samt områder, hvor Datatilsynet vurderer, at der er særlige risici for borgernes rettigheder.

I 2026 vil Datatilsynet særligt rette opmærksomheden mod overvågning gennem nye teknologier, herunder brugen af kunstig intelligens til overvågning og kontrol af borgere i pleje, måle- og overvågningsenheder til patientbehandling i hjemmet, danske hjemmesiders sporing af borgere samt overvågning af ansatte.

Derudover vil Datatilsynet have fokus på persondatasikkerhed og de registreredes rettigheder, herunder sikker anvendelse af auto-complete, tilsyn med store databehandlere, registreredes ret til gennemsigtighed samt behandling af personoplysninger i fælleseuropæiske informationssystemer og tilsyn med behandling af PNR-oplysninger.

Læs Datatilsynets pressemeddelelse her: *https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2026/jan/datatilsynets-fokusomraader-for-tilsyn-i-2026*

Datatilsynet orienterer om databeskyttelsesregler for politiske partier og opdaterer vejledning om valgkampagner

Det danske Datatilsyn (»Datatilsynet«) offentliggjorde den 6. marts 2026 en pressemeddelelse om reglerne for politiske partiers behandling af personoplysninger i forbindelse med den igangværende folketingsvalgkamp. Pressemeddelelsen inddrog databeskyttelseskrav i medfør af GDPR samt Europa-Parlamentets og Rådets forordning (EU) 2024/900 af 13. marts 2024 om gennemsigtighed og målretning i forbindelse med politisk reklame (»forordningen om politisk reklame«), som trådte i kraft den 10. oktober 2025.

Datatilsynets pressemeddelelse præciserede, at partiernes behandling af personoplysninger som alder, bopæl, eller telefonnummer til målretning af budskaber skulle ske på et lovligt grundlag, og at partierne skulle informere klart om, hvilke oplysninger de behandlede, hvorfra oplysningerne stammede, samt behandlingens formål. Manglende overholdelse af informationspligterne kunne gøre udsendelsen af de politiske budskaber ulovlig.

Datatilsynet opdaterede den 17. marts 2026 endvidere vejledningen om databeskyttelsesreglerne i forbindelse med valgkampagner med henblik på at inkorporere de nye krav efter forordningen om politisk reklame.

Forordningen om politisk reklame har indført nye krav om samtykke fra den enkelte vælger forud for målretning af politisk onlinereklame, informationskrav over for vælgerne, samt dokumentations- og offentliggørelsesforpligtelser. Forordningen forbyder endvidere profilering på baggrund af særlige kategorier af personoplysninger, herunder oplysninger om politisk eller religiøs overbevisning, fagforeningsmæssigt tilhørsforhold samt helbredsoplysninger. Den nye forordning finder anvendelse sideløbende med GDPR.

Læs Datatilsynets pressemeddelelse her: *https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2026/mar/hvad-maa-partierne-bruge-om-dig-i-folketingsvalgkampen*

Datatilsynet præciserede retstilstanden for tredjelandsoverførsler i databehandleraftaler

Det danske Datatilsyn (»Datatilsynet«) offentliggjorde den 29. januar 2026 et svar på en konkret forespørgsel fra Det Fælleskommunale Databehandlersekretariat (»DBS«) om vilkår i databehandleraftaler, hvor databehandleren forbeholdt sig retten til at overføre personoplysninger til tredjelande i særlige tilfælde. Sagen blev offentliggjort under journalnummer 2025-211-3556.

Som led i sit tilsyn med databehandlere for kommunerne havde DBS en tilbagevendende problemstilling i, hvornår sådanne vilkår i databehandleraftaler skulle anses som instrukser i databeskyttelsesretlig forstand, og hvorvidt den dataansvarlige hertil skulle sikre et overførselsgrundlag efter GDPR, kapitel V, om overførsler af personoplysninger til tredjelande.

Datatilsynet havde tidligere forholdt sig til dele af problematikken i tilsynets udtalelse til KOMBIT om tilsigtede og utilsigtede overførsler til tredjelande, offentliggjort under journalnummer 2022-212-3529, men ifølge DBS bestod der stadig en vis usikkerhed om de vilkår, der fremgår af databehandleraftaler ved brug af cloudleverandører.

Datatilsynets besvarelse var med afsæt i Det Europæiske Databeskyt-

Colourbox / Chat GPT

telsesråds (»EDPB«) Udtalelse 22/2024 om brugen af databehandlere, der havde skabt et afgrænset område, som hverken udgjorde tilsigtede eller utilsigtede overførsler. Det ville ifølge Datatilsynet sige, at der i praksis ikke foreligger utilsigtede overførsler, og dermed overførsler uden for instruks, medmindre den dataansvarlige aktivt har instrueret databehandleren udtømmende i hvilke overførsler der er accepteret eller ved at instruere om ikke at overføre oplysninger på baggrund af en uafgrænset og/eller uspecifik formulering. Hvor der er en uklarhed i det aftalte, vil der ifølge Datatilsynet opstå en situation, hvor den dataansvarlige ud fra *dolus eventualis*-betragtninger potentielt kan ifalde et strafferetligt ansvar efter databeskyttelsesreglerne, ved at have forholdt sig accepterende til den mulige ulovlige følge af en eller flere uspecifikke formuleringer.

Datatilsynet understregede, at dette beror på ansvarlighedsprincippet, hvorefter den dataansvarlige til enhver tid har ansvaret for at overholde databeskyttelsesreglerne, herunder kravene i GDPR kapitel V. Det indbefatter også den dataansvarliges indirekte accept i form af at lade uklare formuleringer være indeholdt i databehandleraftalen, som kunne skabe fortolkningstvivl.

Datatilsynet opfordrede på den baggrund dataansvarlige til nøje at gennemgå databehandleraftaler for åbne formuleringer, gå i dialog med databehandleren om, hvorvidt de pågældende formuleringer skulle udgøre en instruks, og hvis ikke, aktivt instruere databehandleren i, at formuleringen ikke måtte føre til, at visse overførsler vil finde sted, eller alternativt sørge for, at en sådan formulering udgik af kontrakten.

Læs Datatilsynets pressemeddelelse her: *https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2026/jan/vilkaar-i-databehandleraftalen-om-overfoersler-af-personoplysninger-til-tredjelande*

Læs Datatilsynets besvarelse her: *https://www.datatilsynet.dk/afgoerelser/afgoerelser/2026/jan/vilkaar-i-databehandleraftalen-om-overfoersler-af-personoplysninger-til-tredjelande*

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

Gorrissen Federspiel

Tue Goldschmieding

Nyt om immaterielle rettigheder i Danmark

Norsk modebrand undgår forbud hos Sø- og Handelsretten

Sø- og Handelsretten afsagde den 17. marts 2026 kendelse i sagen BS-50361/2025-SHR mellem DK Company A/S (»DKC«) som sagsøger og Zuccarello AS som sagsøgte. Sagen drejede sig om, hvorvidt DKC opfyldte betingelserne for at nedlægge et midlertidigt forbud mod Zuccarello AS' brug af varemærket »Wardrobe Essentials«.

DKC er en dansk virksomhed, der designer, producerer, distribuerer og sælger beklædning i Danmark og internationalt, og som er indehaver af ordmærket »MY ESSENTIAL WARDROBE«. Zuccarello AS, en norsk virksomhed, var registreret indehaver af varemærket »Wardrobe Essentials«, indtil selskabet overdrog varemærket til den norske virksomhed Wardrobe Essentials AS.

Udstillerlisten for modemessen Mandatory CPH, der fandt sted i København den 5.-7. august 2025, viste, at brandet Wardrobe Essentials deltog. DKC indleverede den 14. oktober 2025 en forbuds- og påbudsbegæring til Sø- og Handelsretten. DKC anførte, at Zuccarello AS krænkede § 4 om indehaveren af varemærkets eneret i lovbekendtgørelse nr. 88 af 29. januar 2019 om varemærker (»den danske varemærkelov«) samt § 3, stk. 1 om god markedsføringsskik, og § 22 om forretningskendetegn i lovbekendtgørelse nr. 1420 af 2. december 2024 om markedsføring (»den danske markedsføringslov«) ved at markedsføre konkurrerende beklædningsgenstande under betegnelsen »WARDROBE ESSENTIALS« på messen.

Retten lagde til grund, at brandet Wardrobe Essentials optrådte på Mandatory CPH den 5.-7. august 2025, og vurderede, at brugen af varemærket udgjorde en varemærkekrænkelse. Da Zuccarello AS på dette tidspunkt var indehaver af den norske varemærkeregistrering, anså retten Zucarello AS for ansvarlig for brugen af varemærket på messen.

Retten afviste dog at meddele forbud og påbud over for Zucarello AS, eftersom der ikke kunne anses at foreligge forbudsretlig aktualitet ved DKC's påstand. Retten fandt, at Zuccarello AS til Wardrobe Essentials AS havde overdraget den norske varemærkeregistrering og efterfølgende overdraget EU-varemærkeregistreringen. Retten fandt det således ikke sandsynliggjort, at Zucarello AS, der fortrinsvist beskæftigede sig med investeringer i fast ejendom, aktuelt brugte eller planlagde at bruge varemærket. Det kunne ikke føre til et andet resultat, at ejeren af Zuccarello AS også besad kapitalandele i Wardrobe Essentials AS. DKC havde dermed heller ikke godtgjort betingelsen i § 413, nr. 2, lovbekendtgørelse nr. 1298 af 7. november 2025 (»den danske retsplejelov«), hvorefter modpartens adfærd skal nødvendiggøre en meddelelse af forbud eller påbud. Retten frifandt herefter Zuccarello AS.

Læs Sø- og Handelsrettens afgørelse her: *https://domstol.fe1.tangora.com/media/-300011/files/KENDELSE_anonymiseret_-_BS-50361-2025-SHR.pdf?rev1*

Sø- og Handelsretten giver delvist medhold i tvist om kursusrettigheder

Sø- og Handelsretten afsagde den 2. marts 2026 kendelse i sagen BS-39547/2025-SHR mellem »A« som sagsøger og »B« som sagsøgte. Sagen drejede sig navnlig om, hvorvidt B ved at udbyde en række kurser om konflikthåndtering via hjemmesiden 'KompetenceUniverset.dk' krænkede A's rettigheder efter bl.a. lovbekendtgørelse nr. 1093 af 20. august 2023 (»den danske ophavsretslov«), lovbekendtgørelse nr. 1420 af 2. december 2024 (»den danske markedsføringslov«), lov nr. 164 af 26. februar 2014 (»den danske internetdomænelov«) og almindelige immaterialretlige grundsætninger.

Parterne indledte i efteråret 2022 et samarbejde om afholdelse af kur-

ser om konflikthåndtering, målrettet bl.a. dagtilbud, og udarbejdede i den forbindelse kursusmateriale. Parterne afsluttede samarbejdet om KompetenceUniverset i foråret 2025 uden at have indgået aftaler om fordelingen af de immaterielle rettigheder knyttet til KompetenceUniverset, herunder rettigheder til navn, hjemmeside og kursusmateriale.

A anlagde herefter sag mod B, og nedlagde bl.a. påstande om forbud mod B's brug af forretningskendetegnet KompetenceUniverset, hjemmesiden og domænet samt mod brug af billeder, video, telefonnummer og LinkedIn-profil tilhørende A.

Retten fandt, at A ikke havde sandsynliggjort, at B's fortsatte brug af forretningskendetegnet KompetenceUniverset og det tilhørende domæne var i strid med markedsføringslovens § 3 om god markedsføringsskik, § 5 om vildledende handlinger og § 6 om vildledende udeladelser, den danske lov om internetdomæner eller almindelige retsgrundsætninger. Omvendt fandt Retten dog, at B's brug af billeder, video, telefonnummer og LinkedIn-profil tilhørende A var i strid med selvsamme bestemmelser i markedsføringsloven, samt grundsætninger om retten til eget billede og navn, og tog på den baggrund A's påstande til følge.

Læs Sø- og Handelsrettens afgørelse her: *https://domstol.fe1.tangora.com/media/-300011/files/Kendelse_BS-39547-2025-SHR.pdf*

Sø- og Handelsretten frifinder Ankenævnet i patentsag om stjernerenser

Sø- og Handelsretten afsagde den 14. januar 2026 dom i sagen BS-21902/2024-SHR mellem GST Denmark ApS (»GST«) som sagsøger og Ankenævnet for Patenter og Varemærker (»Ankenævnet«) som sagsøgte. Sagen angik prøvelse af Ankenævnets kendelse af 26. februar 2024, hvorved nævnet stadfæstede den danske Patent- og Varemærkestyrelses afgørelse om, at GST's patent på et stjernerensearrangement til lugning af marker var ugyldigt efter § 2 i lovbekendtgørelse nr. 93 af 29. januar 2019 (»den danske patentlov«) om nyhedskravet for patenterbare opfindelser.

GST fremsatte påstand om, at patentet opretholdes som gyldigt og bestred Ankenævnets kendelse i sin helhed. GST gjorde gældende, at Ankenævnet havde anvendt en ukorrekt bevisstandard ved bedømmelsen, og at fremlagte beviser ikke var tilstrækkelige til at fastslå, at nyhedskravet i den danske patentlov § 2, ikke var opfyldt.

Retten fandt, at hverken Ankenævnets kendelse eller øvrige omstændigheder gav grundlag for at fastslå, at nævnet havde anvendt en ukorrekt bevisstandard ved bedømmelsen af, om tegningernes indhold var gjort almindeligt tilgængeligt inden patentansøgningens indleveringsdag. Ankenævnets bevismæssige bedømmelse udgjorde en skønsmæssig vurdering, som krævede et sikkert grundlag at tilsidesætte, og det af GST anførte udgjorde ikke et sådant grundlag. Retten frifandt herefter Ankenævnet.

Dommen bekræftede, at domstolenes prøvelse af Ankenævnets skønsmæssige bevisbedømmelse i patentsager er begrænset, og at uklarheder om forudgående offentliggørelse af en opfindelse kan medføre ugyldighed af et meddelt patent.

Læs Sø- og Handelsrettens afgørelse her: *https://domstol.fe1.tangora.com/media/-300011/files/Dom_BS-2190-2024-SHR.pdf*

Patentet Apixaban fundet gyldigt

Sø- og Handelsretten afsagde den 17. februar 2026 dom i sag BS-22186/2022-SHR mellem Teva Denmark A/S og Teva GmbH (»Teva«) som sagsøgere, og Bristol-Myers Squibb Holdings Ireland Unlimited Company (»BMS Ireland«) som sagsøgte. Sagen drejede sig om stridspatentet apixabans gyldighed.

Teva påstod, at BMS Irelands patent på den kemiske forbindelse apixaban, der bl.a. benyttes i lægemidler til forebyggelse og behandling af blodpropper, var ugyldigt. BMS Ireland nedlagde tilsvarende, udover frifindelsespåstående, selvstændig påstand om at Teva skulle ophøre med at markedsføre lægemidler i Danmark, som indeholdt apixaban.

Teva argumenterede for, at patentet manglede opfindelseshøjde, subsidiært at beskrivelsen var utilstrækkelig, og endvidere at stridspatentets prioritetskrav var ugyldigt, da prioritetsretten ikke var gyldigt overdraget til ansøgeren forud for indleveringen af den internationale patentansøgning.

Rettens afsæt for vurderingen i sagen udgjordes af § 2, stk. 1, jf. stk. 2, om nyhed og opfindelseshøjde, og § 8, stk. 2, 3. pkt., om tilstrækkelig beskrivelse, i lovbekendtgørelse nr. 90 af 29. januar 2019 om patenter (»den danske patentlov«). Retten fandt, at Teva ikke havde godtgjort den manglede opfindelseshøjde, da apixaban ikke var nærliggende at udlede af den nærmeste kendte teknik. Selvom Den Europæiske Patentmyndighed (»EPO«) vurderede apixaban som en udvalgsopfindelse, lagde retten vægt på efterindleverede data i vurderingen og konkluderede på den baggrund af opfindelsen havde særlig teknisk effekt. Retten vurderede endvidere, at prioritetsretten var gyldigt overdraget efter EPO's praksis, da der internt i BMS-koncernen var aftalt en overdragelse af prioritetsretten inden indgivelsen af patentansøgningen.

Retten frifandt følgelig BMS Ireland for Tevas påstande, eftersom sagsøger ikke havde afkræftet formodningen for patentets gyldighed. I samme ombæring tog retten BMS Irelands selvstændige forbudspåstand mod Tevas markedsføring af lægemidler i Danmark, som indeholdt apixaban, til følge.

Læs Sø- og Handelsrettens dom her: *https://domstol.fe1.tangora.com/media/-300011/files/Dom_-_BS-22186-2022-SHR.pdf*

Ompakning af parallelimporterede lægemidler var ikke objektivt nødvendigt

Sø- og Handelseretten afsagde den 6. februar 2026 dom i en sambehandling af ti sager mellem varemærkeindehaverne Merck Sharp & Dohme Corp., Novartis AG, H Lundbeck A/S, Ferring Lægemidler A/S som sagsøgere, og parallelimportørerne Abacus Medicine A/S, Paranova Danmark A/S, og 2care4 ApS som sagsøgte. Det centrale spørgsmål i sagerne var, om det var objektivt nødvendigt for parallelimportørerne at ompakke lægemidlerne, fremfor blot at omettikere de eksisterende pakninger.

Sagsøgerne påstod, at parallelimportørerne havde krænket deres varemærkeret i ompakningen af de originalproducerede lægemidler, uden at det var objektivt nødvendigt, og at efterfølgende markedsføring var i strid med § 4 og § 10 a, stk. 2, i lovbekendtgørelse af 29. januar 2019 nr. 88 om varemærker (»den danske lov om varemærker«).

Som led i sambehandlingskomplekset forelagde Sø- og Handelsretten ved fælleskendelse af 3. april 2020 en række præjudicielle spørgsmål for EU-Domstolen i sag C-224/20. Det centrale spørgsmål var, om indførelsen af FMD-reglernes krav om sikkerhedselementer på lægemidlers emballage, jf. artikel 47a i Direktiv 2001/83/EF, ændrede den varemærkeretlige vurdering af, hvornår parallelimportørers ompakning til nye ydre pakninger kunne anses for objektivt nødvendig. Baggrunden var bl.a., at den danske Lægemiddelstyrelses praksis og forståelse vedrørende artikel 47a pegede på ompakning som altovervejende hovedregel, mens EU-retten åbnede mulighed for, at originalpakningen kunne genanvendes, hvis sikkerhedselementerne kan udskiftes korrekt.

EU-Domstolen fastslog i dom af 17. november 2022, at direktivets regler om sikkerhedselementer på lægemiddelpakninger ikke i sig selv medfører, at ompakning er objektivt nødvendig; originalpakningen kan som udgangspunkt genanvendes, hvis sikkerhedselementerne udskiftes med tilsvarende effektive elementer. Domstolen præciserede i denne retning, at synlige eller følbare spor efter åbning af originalpakningen ikke i sig selv udelukker, at genforsegling kan ske i overensstemmelse med artikel 47a. Domstolen afviste, at en medlemsstat kan operere med en hovedregel om, at parallelimportører principielt skal ompakke til nye pakninger, og at ommærkning alene kan ske undtagelsesvist.

Retten fandt, med udgangspunkt i de retlige rammer fastlagt i C-224/20, at sagsøgte ikke havde godtgjort, at det var objektivt nødvendigt at ompakke lægemidlerne og gav derfor de sagsøgende parter medhold i de behandlede sager. Retten lagde bl.a. vægt på, at EU-reglerne om sikkerhedselementer ikke nødvendiggør ompakning, idet parallelimportøren lovligt kan åbne og genforsegle en originalpakning med nye sikkerhedselementer, at de sagsøgte parter ikke havde bevist modstand hos forbrugere eller apotekere mod omettikering, og at der ikke var bevist hindringer for, at de originale pakningsstørrelser kunne markedsføres effektivt på importmarkederne grundet ordinationspraksis og sygeforsikringsregler. Desuden understregede retten at nødvendighed ikke kan begrundes med parallelimportørens kommercielle fordel.

Læs Sø- og Handelsrettens dom her: *https://domstol.fe1.tangora.com/media/-300011/files/Deldom_af_6._februar_2026.pdf*

Prodamp idømt bøde for ulovlig reklame for elektroniske cigaretter og nikotinposer

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) offentliggjorde den 3. februar 2026, at Retten i Hjørring havde idømt virksomheden Prodamp en bøde på 400.000 danske kroner for at overtræde tobaksreklameforbuddet i § 3 i lovbekendtgørelse af 26. marts 2021 nr. 586 om forbud mod tobaksreklame m.v. (»den danske lov om tobaksreklame«) og reklameforbuddet mod elektroniske cigaretter i § 16 i lovbekendtgørelse af 4. april 2024 nr. 1166 om elektroniske cigaretter (»den danske lov om elektroniske cigaretter«).

Retten i Hjørring fandt at Prodamp havde overtrådt reklameforbuddene i den danske lov om tobaksreklame og den danske lov om elektroniske cigaretter, ved at benytte sig af metoden 'linkbuilding', for at søgemaskiner rangerede hjemmesiden højere i søgeresultaterne. Det indebar at betale andre hjemmesider for at udgive artikler med hyperlinks til Prodamps egen hjemmeside. Strategien bygger på, at disse bagvedliggende hyperlinks opfattes af søgemaskiner som et udtryk for, at den pågældende hjemmeside er relevant og værd at besøge, hvorved søgemaskinen vil prioritere visningen af denne hjemmeside i dets søgeresultater. Retten fandt desuden, at Prodamp havde overtrådt reklameforbuddene ved at reklamere for gratis fragt på ordrer over et minimumsbeløb, fordi tilbuddet virkede som et incitament til at købe yderligere tobaksprodukter, og dermed havde til formål at fremme salget på hjemmesiden.

Læs forbrugerombudsmandens pressemeddelelse her: *https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2026/20260203-prodamp-idoemt-boede-paa-400000-kroner-for-ulovlig-reklame-for-elektroniske-cigaretter-og-nikotinposer*

Salling Group A/S idømt bøde for vildledende markedsføring efter ny bødemodel

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) offentliggjorde den 12. marts 2026, at Salling Group A/S (»Salling«) havde accepteret at betale en bøde på 10 millioner danske kroner for vildledende markedsføring af Nettos ØGO-mærke.

Denne markedsføring var baseret på en spørgeundersøgelse blandt danske forbrugere om opfattelsen af visse udvalgte mærkers bæredygtighed, hvorfor Forbrugerombudsmanden vurderede, at resultatet af spørgeundersøgelsen udelukkende var udtryk for subjektive opfattelser af ØGO-mærket. Da bæredygtighedsudsagnet imidlertid blev klassificeret som et udsagn om faktiske forhold, der i medfør af § 13 i lovbekendtgørelse af 2. februar 2024 nr. 1420 (»den danske lov om markedsføring«) skal kunne dokumenteres, var markedsføringen egnet til at give forbrugerne et fejlagtigt indtryk af produkternes reelle klima- og miljøbelastning. Det forhold, at ØGO-produkterne var økologiske, kunne ikke begrunde, at produktserien blev markedsført som bæredygtigt.

Bøden blev udmålt efter den nye bødemodel, der fremgår af § 37, stk. 6, i den danske markedsføringslov. Bødemodellen er kategoriseret efter omsætning, hvorefter der tildeles bøder efter et nedsat, normalt eller forhøjet bødeniveau, afhængig af overtrædelsens grovhed og varighed. Ordningen tilsigter at skærpe bødeniveauet for overtrædelser af den danske lov om markedsføring.

Læs forbrugerombudsmandens pressemeddelelse her: *https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2026/20260312-salling-group-betaler-10-millioner-kroner-i-boede-for-vildledende-markedsfoering-af-nettos-oego-maerke*

Inkassofirma opkrævede ulovlige gebyrer for knap en halv million kroner

Den danske Forbrugerombudsmand (»Forbrugerombudsmanden«) har den 7. januar 2026 fundet, at inkassofirmaet Intrum A/S (»Intrum«) uretmæssigt havde opkrævet gebyrer fra forbrugere for tilbageførsel af fejlbetalinger. Forbrugerombudsmanden fastslog, at opkrævningerne stred mod god inkassoskik i § 9 om forbud mod metoder, der udsætter skyldnere for urimeligt pres eller ulempe, jf. lovbekendtgørelse nr. 1018 af 19/09/2014 (»den danske inkassolov«), samt god markedsføringsskik i § 3, stk. 1, jf. lovbekendtgørelse nr. 1420 af 02/12/2024 (»den danske markedsføringslov«).

Forbrugerombudsmanden fastslog, at erhvervsdrivende kun kan opkræve gebyrer fra forbrugere, hvis gebyret er direkte og udtrykkeligt lovhjemlet, eller hvis parterne har aftalt det og aftalen ikke strider mod loven. Forbrugerombudsmanden fastslog endvidere, at forbrugere har krav på fuld tilbagebetaling af fejlbetalinger, når betalingen er sket i forbindelse med et inkassofirmas inddrivelse af gæld, uanset om fejlen kan tilregnes forbrugeren.

Intrum oplyste, at virksomheden havde ophørt med den ulovlige praksis, der i den undersøgte periode havde udmøntet sig til i alt 494.620 danske kroner, og at de ulovligt opkrævede gebyrer ville blive tilbagebetalt inden udgangen af 2026.

Læs Forbrugerombudsmandens pressemeddelelse her: *https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2026/20250107-inkassofirma-opkraevede-ulovlige-gebyrer-fra-forbrugere-for-knap-en-halv-million-kroner*

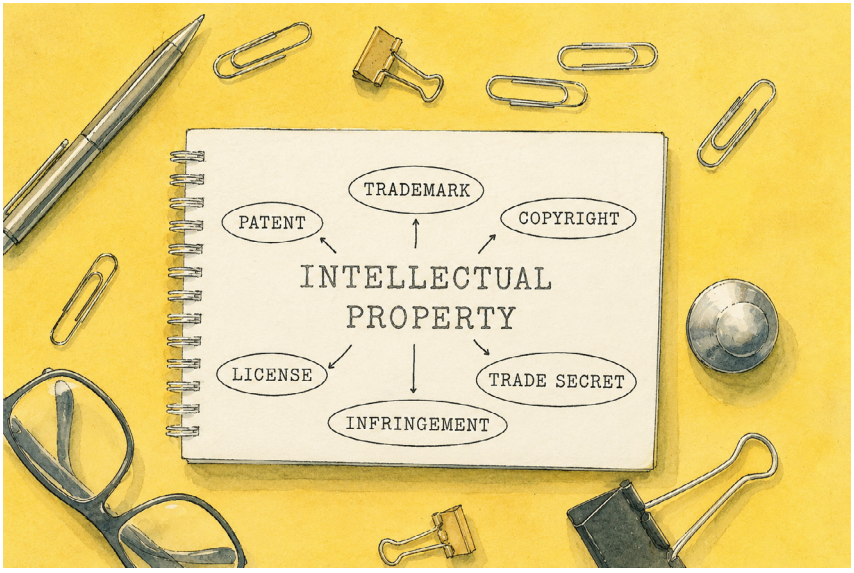
Modstrøm vedtager bøde på 400.000 kr. for ulovligt telefonsalg og vildledende markedsføring

Den danske forbrugerombudsmand (»Forbrugerombudsmanden«) offentliggjorde den 8. januar 2026 at Elselskabet Modstrøm Danmark A/S (»Modstrøm«) havde overtrådt forbuddet mod uanmodet telefonsalg i § 4, stk. 1, i lovbekendtgørelse nr. 1184 af 28. september 2025 (»Den danske forbrugeraftalelov«) og forbuddet mod vildledende markedsføring i § 5, stk. 1, og § 6, stk. 1, i lovbekendtgørelse nr. 1420 af 2. december 2024 (»den danske lov om markedsføring«).

I perioden fra 4. december 2020 til 2. august 2021 samt fra 24. maj 2023 til 8. november 2024, modtog 27 forbrugere uanmodede telefoniske henvendelser fra Modstrøm uden at have givet gyldigt samtykke hertil. Derudover blev otte forbrugere vildledt af selskabets sælgere under telefonsamtalerne, idet sælgerne gav et indtryk af, at de ringede fra forbrugerens nuværende elselskab eller undlod at oplyse forbrugerne om væsentlige priselementer. Modstrøm havde allerede tidligere i 2021 vedtaget en bøde for tilsvarende overtrædelser.

Forbrugerombudsmanden udtalte, at det ikke var lovligt for elselskaber at kontakte forbrugere telefonisk uden udtrykkeligt samtykke, og at der henset til selskabets tidligere overtrædelse af samme forbud, blev set meget alvorligt på sagen. Forbrugerombudsmanden indskærpede på den baggrund reglerne over for Modstrøm, som vedtog en bøde på 400.000 kr.

Læs Forbrugerombudsmandens pressemeddelelse her: *https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2026/20260108-modstroem-betaler-400000-kroner-i-boede-for-ulovligt-telefonsalg-og-vildledning*



Colourbox / Chat GPT

Energi+ politianmeldt for opkrævning af skjult månedligt gebyr

Den danske forbrugerombudsmand (»Forbrugerombudsmanden«) offentliggjorde den 18. februar 2026 at have politianmeldt Energi+ A/S (»Energi+«) for at vildlede forbrugere ved ikke klart og tydeligt at oplyse om et månedligt gebyr på selskabets hjemmeside. Dette fandt Forbrugerombudsmanden i strid med vildledningsforbuddet i lovbekendtgørelse nr. 1420 af 2. december 2024 (»den danske lov om markedsføring«).

Sagen vedrørte markedsføring af tre elprodukter, »Strøm+«, »Strøm+39« og »Strøm+ Fastpris«, samt oplysningen om et månedligt »certificerings- og servicebidrag« på 33,34 kr. Oplysningen om det månedlige gebyr fremgik ikke på selskabets forside eller kampagneside, hvor de øvrige prisoplysninger var angivet. Oplysningen fremgik alene af selskabets leveringsbetingelser og en gebyroversigt, som blev sendt til kunder via e-mail.

Forbrugerombudsmanden vurderede, at den måde, hvorpå Energi+ oplyste om sine priser på hjemmesiden, var egnet til at give forbrugerne indtryk af, at der ikke ville være andre tillæg end dem, som var fremhævet på hjemmesiden.

Forbrugerombudsmanden sendte et høringsbrev om sagen til Energi+ den 21. maj 2025. Først herefter tilføjede selskabet oplysningen om det månedlige gebyr på deres hjemmeside. Denne tilføjelse ændrede dog ikke Forbrugerombudsmandens vurdering af, at der var sket vildledende markedsføring, eftersom oplysningen stadig ikke fremgik i umiddelbar tilknytning til de øvrige prisoplysninger. Overtrædelse af forbuddet mod vildledende markedsføring straffes med bøde i medfør af den danske lov om markedsføring § 37, stk. 3.

Læs Forbrugerombudsmandens pressemeddelelse her: *https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2026/20260218-forbrugerombudsmanden-politianmelder-energiplus-for-skjult-gebyr*

Wolt politianmeldt for vildledende rabatmarkedsføring

Den danske forbrugerombudsmand (»Forbrugerombudsmanden«) offentliggjorde den 18. marts 2026, at madleveringsplatformen Wolt Danmark ApS (»Wolt«) var blevet politianmeldt for vildledende markedsføring ved at markedsføre en rabat, som forbrugerne umuligt kunne opnå.

I perioden den 20. august 2025 til den 24. oktober 2025 sendte Wolt push-notifikationer til omkring 45.000 forbrugere om, at de kunne opnå 25 procent rabat på deres næste køb ved bestilling for mindst 189 kr. Rabatten var dog begrænset til 30 kr., hvilket betød, at forbrugerne i realiteten maksimalt ville kunne opnå knap 16 procent i rabat.

Forbrugerombudsmanden vurderede, at markedsføringen af den uopnåelige rabat var vildledende, og var egnet til at påvirke forbrugernes købsbeslutning i strid med § 5, stk. 1 og § 6, stk. 1 i lovbekendtgørelse nr. 1420 af 2. december 2024 (»den danske lov om markedsføring«).

Læs Forbrugerombudsmandens pressemeddelelse her: *https://forbrugerombudsmanden.dk/nyheder/forbrugerombudsmanden/pressemeddelelser/2026/20260318-forbrugerombudsmanden-politianmelder-wolt-danmark-aps-for-vildledende-markedsfoering-om-rabat*

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


Selmer

Av Amanda Johnson med bistand fra Kine Emilie Helgeneseth

Mindreårige på sosiale medier: aldersgrense og skjerpede krav til alderskontroll

Innledning

29. april 2026 kunngjorde EU-kommisjonen at den foreløpig har funnet Meta i brudd med EUs Digital Services Act («DSA»), fordi selskapet gjør for lite for å hindre at barn under 13 år får tilgang til Facebook og Instagram.[1] Samme uke kunngjorde den norske regjeringen at den vil legge frem et lovforslag om absolutt aldersgrense for sosiale medier innen utgangen av 2026.[2] Utviklingen er en del av en bredere internasjonal trend. Myndighetene stiller stadig strengere krav til alderskontroll og verifikasjon på sosiale medier, og Australia har allerede innført en lovfestet aldersgrense på 16 år. Samtidig reiser skjerpede krav til aldersverifikasjon grunnleggende spørsmål om teknologisk gjennomførbarhet, personvern, ytringsfrihet og digital inkludering.

Artikkelen gjennomgår det rettslige og praktiske landskapet for alderskontroll på sosiale medier, fra EU-regulering og nasjonale lovforslag til teknologiske løsninger, og drøfter hvilke implikasjoner den skjerpede reguleringen har for plattformer og rådgivere.

DSA og retningslinjer for alderskontroll

DSA artikkel 28 omhandler beskyttelse av mindreårige på nett og 1. ledd pålegger tilbydere av internettplattformer å iverksette «appropriate and proportionate measures» for å sikre en høy grad av personvern, trygghet og sikkerhet for mindreårige på tjenesten. Artikkel 28 nr. 2 forbyr annonser basert på profilering når plattformen «with reasonable certainty» vet at mottakeren er mindreårig.

For tilbydere av «Very Large Online Platforms» («VLOP-er») oppstiller DSA utvidede plikter. Artikkel 34 nr. 1 pålegger VLOP-er å identifisere, analysere og vurdere systematiske risikoer, herunder negative effekter på grunnleggende rettigheter, inkludert barns rettigheter, og på mindreåriges fysiske og psykiske helse.[3] Artikkel 35 nr. 1 pålegger videre VLOP-ene å innføre rimelige, forholdsmessige og effektive risikoreduserende tiltak for å beskytte barns rettigheter, herunder aldersverifikasjon.[4]

For å konkretisere hva som kreves for å oppfylle pliktene etter DSA artikkel 28 nr. 1, publiserte kommisjonen 14. juli 2025 egne retningslinjer for bestemmelsen.[5] Retningslinjene gjelder for alle tilbydere av internettplattformer som er tilgjengelige for mindreårige, med unntak av mikro- og småselskaper. Kommisjonen har presisert at en plattform anses som «tilgjengelig for mindreårige» selv om den har vilkår som forbyr mindreåriges bruk, så lenge plattformen ikke har iverksatt tilstrekkelig effektive tiltak som hindrer tilgang for denne gruppen.[6]

Retningslinjene fremhever særlig effektiv alderskontroll som et sentralt tiltak under artikkel 28.[7] Kommisjonen skiller mellom tre metoder for alderskontroll: selvdeklarasjon, aldersestimering og aldersverifikasjon. Selvdeklarasjon, dvs. at brukeren selv oppgir fødselsdato eller bekrefter å være over en viss alder, anses som hovedregel ikke som til-

1 *https://ec.europa.eu/commission/presscorner/detail/en/ip_26_920*
2 *https://www.regjeringen.no/no/aktuelt/loven-kommer-etter-planen-i-ar-slik-blir-aldersgrensen-for-sosiale-medier/id3157276/*
3 DSA artikkel 34 nr. 1, bokstav b og d.
4 DSA artikkel 35 nr. 1, bokstav j.
5 EU (C/2025/5519).
6 Retningslinjene, underpunktene 5 til 8.
7 Retningslinjene, punkt 6.1 («Age assurance»)

strekkelig fordi metoden verken er nøyaktig eller robust.[8] Aldersverifikasjon gjennom offisiell ID eller digital lommebok anses som den mest pålitelige metoden, og Kommisjonen anser det som et egnet og forholdsmessig tiltak særlig der tjenesten innebærer høy risiko for mindreårige.[9] Uansett metode stiller retningslinjene krav om at teknologien skal være nøyaktig, pålitelig, robust mot omgåelse, ikke-inngripende og ikke-diskriminerende.[10]

Kommisjonen legger opp til at alderskontrollen kan utføres gjennom tredjepart, men at dette må opplyses på en tilstrekkelig klar, og barnevennlig måte. Ansvaret for sikkerheten av metodene som utføres av tredjepart ligger hos plattformene.[11]

Meta-saken

EU-kommisjonen har, med retningslinjene som målestokk, vurdert Metas overholdelse av DSA på plattformene Facebook og Instagram og funnet brudd på tre hovedgrunnlag:[12]

Brudd på artikkel 28: Til tross for at Meta selv opererer med 13 års aldersgrense på begge plattformer, fant Kommisjonen at tiltakene for å håndheve aldersgrensen ikke er tilstrekkelig effektive. Slik plattformene fungerer i dag, kan mindreårige brukere enkelt opprette konto ved å oppgi falsk fødselsdato - uten at Meta fører noen ytterligere kontroll. Videre fant Kommisjonen at Metas rapporteringsverktøy for å melde inn brukere under 13 år er vanskelig å bruke og lite effektivt. Rapportering krever flere steg før brukeren kommer seg frem til rapporteringsskjemaet, og det er ingen garanti for at rapporterte kontoer faktisk blir stengt.

Brudd på artikkel 34: Både Facebook og Instagram kan betegnes som såkalte Very Large Online Platforms og er derfor underlagt kravet om risikovurdering etter DSA artikkel 34. Kommisjonen omtaler Metas risikovurdering som «incomplete and arbitrary». Vurderingene tar i for liten grad hensyn til dokumentert bruk av plattformene blant barn under 13 år. Kommisjonen viste blant annet til lett tilgjengelig statistikk som indikerer at om lag 10–12 % av barn under 13 år bruker Instagram og/eller Facebook, samt forskning som viser at yngre barn er særlig sårbare for potensielle skader fra sosiale medier.

Brudd på artikkel 35: Kommisjonen fant at de risikoreduserende tiltakene Meta har iverksatt ikke er effektive nok til å forhindre, avdekke og fjerne brukere under 13, eller til å motvirke og redusere risiko for at mindreårige utsettes for skade på plattformene.

Kommisjonen angir at Meta må endre risikovurderingsmetodikken og styrke tiltakene, og samtidig sikre et høyt nivå av personvern, sikkerhet og trygghet for mindreårige.

Meta har nå muligheten til å gjennomgå Kommisjonens dokumenter, komme med et skriftlig svar og iverksette tiltak for å utbedre de påståtte bruddene i henhold til retningslinjene. Samtidig vil European Board of Digital Services bli konsultert. De foreløpige funnene prejudiserer ikke endelig utfall, men dersom Kommisjonens funn bekreftes, kan den treffe en non-compliance-beslutning og dermed utløse bøter på inntil 6% av Metas globale årlige omsetning samt tvangsmulkt.

Kommisjonen har også varslet at etterforskingen mot Meta fortsetter. Det skal blant annet vurderes om plattformens grensesnittdesign utnytter mindreåriges sårbarhet og bidrar til avhengighetsskapende bruk eller kaninhull-effekter.

Det norske lovforslaget

Regjeringens første utkast til lov om aldersgrense i sosiale medier kan leses i høringsnotatet fra juli 2025.[13] Opprinnelig ble det foreslått en aldersgrense på 15 år, men etter tilbakemeldinger fra høringsrunden skal aldersgrensen gjelde til 1. januar det året brukeren fyller 16 år, slik at hele skolekull får tilgang samtidig.[14] Loven skal ifølge notatet, pålegge tilbydere av sosiale medier å iverksette «nødvendige tiltak» for å sikre at de ikke tilbyr tjenestene til brukere de «med rimelig sikkerhet» er klar over at er under aldersgrensen. Tiltakene skal utformes slik at de ikke hindrer tilgang for personer over aldersgrensen og tilbyderne skal ikke innhente flere personopplysninger enn nødvendig for å verifisere alder.[15]

Forslaget legger samtidig opp til at departementet skal kunne fastsette nærmere krav til metode for aldersverifisering i forskrift. Ansvaret for overholdelse legges på tilbyderne, som kan ilegges tvangsmulkt og overtredelsesgebyr.[16]

En lov om felles absolutt aldersgrense markerer et viktig skille med DSA, som bygger på en risikobasert tilnærming der tiltakene skal tilpasses tjenestenes risiko og utforming. DSA er totalharmoniserende innenfor sitt område og inneholder ingen regler om absolutte aldersgrenser. Departementet har selv pekt på at nasjonale krav om aldersgrense og verifikasjon kan være i strid med DSA. Departementet erkjenner at forholdet til DSA og EØS-retten ikke er endelig avklart, men argu-

8 Retningslinjene, underpunkt 52.
9 Retningslinjene, underpunkt 37.
10 Retningslinjene, underpunkt 49-50.
11 Retningslinjene, underpunkt 53.
12 *https://ec.europa.eu/commission/presscorner/detail/en/ip_26_920*

13 Høringsnotat om forslag til lov om aldersgrenser for bruk av sosiale medier (sosiale medierloven), hentet her: *https://www.regjeringen.no/contentassets/da5340ace79941afad938ab18985e042/horingsnotat-lov-om-aldersgrense-for-bruk-av-sosiale-medier.pdf*
14 *https://www.regjeringen.no/no/aktuelt/loven-kommer-etter-planen-i-ar-slik-blir-aldersgrensen-for-sosiale-medier/id3157276/*
15 Høringsnotatet, forslag til § 5.
16 Ibid.

menterer for at DSA ikke uttrykkelig forbyr nasjonale aldersgrenser og at nasjonal lovgiving med andre formål enn DSA kan stå seg. Handlingsrommet skal avklares gjennom EØS-høring før lovforslaget fremmes.[17]

I tillegg kan en generell norsk aldersgrense utfordre etableringsprinsippet i e-handelsdirektivet. Norge kan som hovedregel ikke pålegge plattformer etablert i andre EØS-stater generelle krav gjennom nasjonal lovgivning. En norsk lov om aldersgrense vil derfor måtte spesifisere hvilke bestemte tjenesteplattformer som omfattes av aldersgrensen. Denne begrensningen kan skape risiko for omgåelse ved hurtig opprettelse av nye plattformer utenfor lovens lister.[18]

Loven kan også komme i konflikt med grunnleggende rettigheter som retten til ytrings- og informasjonsfrihet, retten til ikke-diskriminering, retten til privatliv og forsamlingsfriheten.[19]

Parallelt med dette lovarbeidet har Regjeringen også sendt på høring et forslag om heving av aldersgrensen i personopplysningsloven § 5 fra 13 til 15 år.[20] Bestemmelsen regulerer fra hvilken alder barn selv kan gi samtykke til behandling av personopplysninger i forbindelse med bruk av informasjonssamfunnstjenester, herunder sosiale medier. Bestemmelsen fastsetter ikke en aldersgrense for bruk av slike tjenester som sådan, men avgjør når barnet selv, uten foreldres samtykke eller godkjenning, kan samtykke til at tilbyderen behandler barnets personopplysninger. Hevingen vil dermed innebære at det kreves foreldresamtykke for behandling av personopplysninger som skjer på grunnlag av samtykke også for barn i aldersgruppen 13 til 15 år. Hevingen er ment å skape sammenheng med det foreslåtte alderskravet i sosiale medierloven, slik at aldersgrensen for bruk og samtykke til behandling av personopplysninger følger hverandre.

Erfaringer fra Australia

Australia er foreløpig det eneste landet i verden med effektiv lovfestet aldersgrense for sosiale medier. Aldersgrensen ble innført gjennom «Online Safety Amendment (Social Media Minimum Age) Act 2024» («SMMA») og trådte i kraft i desember 2025. Den australske loven fastsetter 16 års aldersgrense for bestemte «age-restricted social media platforms» og den siste tiden har de første rapportene om lovens effekt rullet inn. Blant annet publiserte eSafety Commissioner - organet med hovedansvar for å følge opp og overvåke etterlevelsen av den australske loven - sin første «compliance update» på SMMA i mars 2026.[21]

Rapporten viser at om lag 5 millioner kontoer har blitt sperret, deaktivert eller begrenset, likevel oppga rundt 7 av 10 foreldre at barna fremdeles hadde konto på Facebook, Instagram, Snapchat og TikTok og omtrent 50% rapporterte at barna fremdeles hadde YouTube-konto.[22]

Rapporten viser også at enkelte plattformer lot brukere forsøke aldersverifikasjon flere ganger helt til systemet ga et «16+»- resultat. eSafety undersøkte samtidig om mindreårige migrerer til andre plattformer som faller utenfor lovens virkeområde. Rapporten viser at det per nå ikke skjer i større skala.[23]

Tekniske utfordringer ved aldersverifikasjon

En sentral utfordring ved håndheving av aldersgrensen er at det foreløpig ikke finnes noen sikker metode for aldersverifisering som samtidig er tilstrekkelig treffsikker, personvernvennlig og inkluderende.

Selvdeklarasjon er lett å omgå, mens biometriske løsninger og atferdsanalyse kan være både unøyaktige og gjøre inngrep i personvern. eID-løsninger som BankID er treffsikre og troverdige, men innebærer behandling av flere personopplysninger enn det som er nødvendig for å fastslå alder. Slike løsninger kan også virke ekskluderende for brukergrupper uten tilgang til nasjonal eID.

> I praksis vil gjennomslaget for enhver regulering derfor avhenge av om det etableres aldersverifikasjonsløsninger som er tilstrekkelig robuste, men samtidig ivaretar dataminimering, personvern og digital inkludering.

Som et svar på disse utfordringene har EU-kommisjonen nå lansert en egen app for aldersverifikasjon.[24] Appen skal gjøre det mulig å bekrefte om en bruker er over en bestemt alder uten å dele flere opplysninger enn nødvendig. Appen kan brukes som en frittstående løsning eller som en del av EUs digitale identitetslommebok. Appen lanseres innledningsvis i syv land

17 Høringsnotatet, punkt 3.2.2.
18 Høringsnotatet, punkt 3.2.4.
19 Høringsnotatet, punkt 3.1.
20 *https://www.regjeringen.no/no/dokumenter/horing-endringer-i-personopplysningsloven-aldersgrense-for-barns-samtykke-ved-bruk-av-informasjonssamfunnstjenester-sosiale-medier-mv/id3114264/?expand=horingsnotater*
21 Social Media Minimum Age: Compliance update, hentet her: *https://www.esafety.gov.au/sites/default/files/2026-03/SocialMediaMinimumAge-ComplianceUpdateMarch2026.pdf?v=1774905032806*
22 Rapporten, s. 13.
23 Rapporten, s. 29.
24 *https://commission.europa.eu/news-and-media/news/european-age-verification-app-keep-children-safe-online-2026-04-15_en*

som skal gå foran og teste, men kildekoden er åpen slik at ethvert privat selskap står fritt til å bruke den til å videreutvikle egne innovative løsninger.[25]

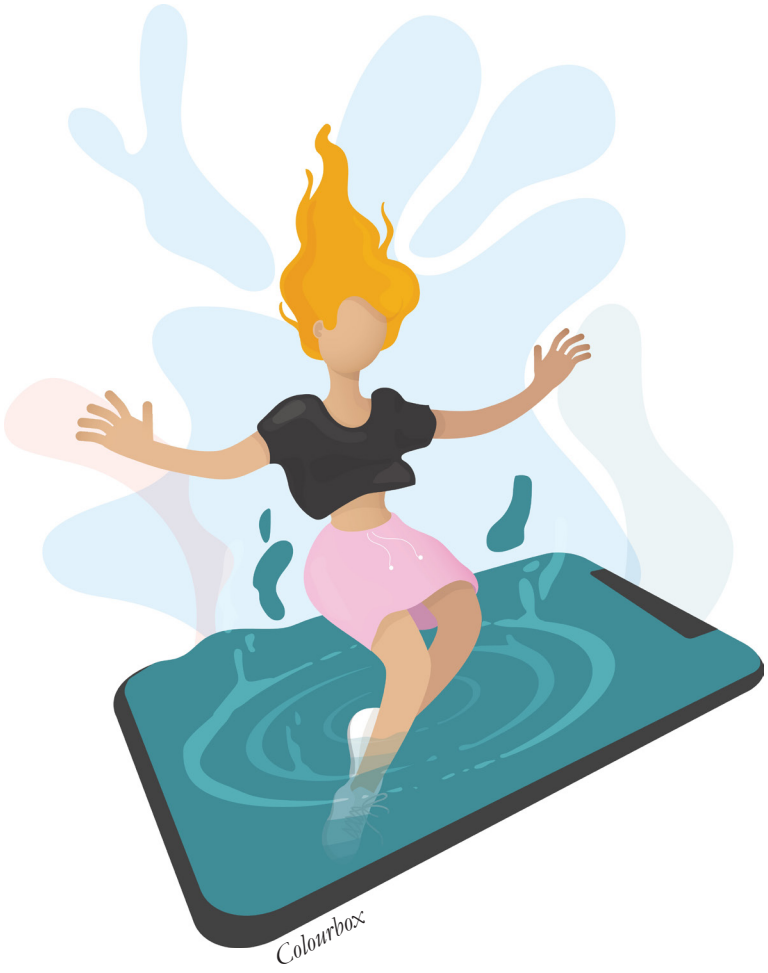
Kort tid etter at EU annonserte at appen var «klar til bruk», ble det imidlertid hevdet at hackere kunne knekke den på to minutter.[26] Foreløpig virker det dermed klart at appen krever ytterligere sikring før den kan anbefales som verifikasjonsløsning i stor skala.

Veien videre

Gjennomgangen har vist at kravene til alderskontroll på sosiale medier skjerpes gjennom DSAs risikobaserte tilnærming og nasjonale lovforslag om absolutte aldersgrenser. Spørsmålet fremover er ikke «om» plattformene må verifisere alder, men «hvordan» og med hvilke konsekvenser for personvern, ytringsfrihet og tilgang.

Dagens velbrukte løsning med selvdeklarasjon er klart på vei ut. For plattformer med aldersgrense innebærer utviklingen at effektiv alderskontroll må iverksettes og forankres i dokumenterte risikovurderinger og egnede tekniske løsninger. Erfaringene fra Australia viser at det ikke er noen automatikk i at en aldersgrense alene holder mindreårige ute fra sosiale medier. Effektiviteten avhenger av de tekniske løsningene som velges, og av plattformenes vilje til å tilpasse seg strenge krav til kontroll. I praksis vil gjennomslaget for enhver regulering derfor avhenge av om det etableres aldersverifikasjonsløsninger som er tilstrekkelig robuste, men samtidig ivaretar dataminimering, personvern og digital inkludering. Den europeiske digitale identitetslommeboken kan på sikt gi et mer standardisert rammeverk, men ligger fremdeles frem i tid.

Det norske forslaget er ambisiøst og rettslig uavklart på noen områder. For aktører som utvikler, tilbyr eller rådgir om digitale tjenester rettet mot norske brukere, bør utviklingen gi grunn til å gjennomgå krav til alderskontroll, personvern, ansvarsfordeling og etterlevelsesdokumentasjon allerede nå.


Colourbox

Amanda Johnson, advokatfullmektig i Advokatfirmaet Selmer, Oslo.

Kine Emilie Helgeneseth, fast advokat i avdelingen HITEK i Advokatfirmaet Selmer, Oslo.

25 *https://ec.europa.eu/commission/presscorner/detail/en/statement_26_820*

26 *https://www.tek.no/nyheter/nyhet/i/M75oxM/eu-lanserte-aldersjekk-app-hackere-knakk-den-paa-to-minutter?srsltid=AfmBOooLogvewe4Qd4hFJ2j17nOb6iVMAf4fWi2WNFXRHah44_AmaiX-*


kahn pedersen

Hanna Bogsjö Österberg og Fredrik Sandström

MCF:s nya förslag till föreskrifter om säkerhetsåtgärder och utbildning enligt cybersäkerhetslagen

Myndigheten för civilt försvar (MCF) har publicerat *en reviderad remissversion* av föreskrifter om säkerhetsåtgärder och utbildning enligt den kommande cybersäkerhetslagen (CSL). Föreskrifterna är ett centralt led i genomförandet av NIS2-direktivet i svensk rätt och syftar till att konkretisera dels de olika typer av säkerhetsåtgärder en verksamhetsutövare är skyldig att vidta för att uppfylla 2 kap. 3 § CSL, dels vilken utbildning som ledningen ska genomgå enligt 2 kap. 4 § CSL.

Det nya förslaget togs fram efter omfattande synpunkter på det första utkastet som skickades ut på extern remiss hösten 2025. Kritiken rörde då bland annat bristande tydlighet, särskilt kring vägledning hur proportionalitetsprincipen och riskbaserade avvägningar skulle tillämpas i praktiken, samt svårigheterna i att förena kraven med olika sektorers behov. Ändringarna i det reviderade förslaget tar i huvudsak sikte på att gå från detaljerade, tvingande regler till mer övergripande funktionskrav, där detaljerna istället hanteras i form av rekommendationer i allmänna råd.

I korthet innebär det reviderade förslaget bland annat:

- Ett tydligt skifte av fokus mot att etablera processer och ett fungerande styrsystem istället för att i detalj ange vilka åtgärder som ska vidtas.
- Mer utförliga krav på ansvarsfördelning, roller och ledningens involvering samt krav på uppföljning och rapportering till ledningen.
- Att arbetet med cybersäkerhet ska integreras i den ordinarie verksamhetsstyrningen, vilket markerar en förskjutning från en isolerad IT-fråga till en central del av verksamhetsledningen.
- Nya och mer utvecklade krav på teknisk samverkan, omvärldsbevakning och kriskommunikation, inklusive användning av nationella stödfunktioner för hantering av sårbarheter, cyberhot och kriskommunikation.
- Att kraven på säkerhet i leveranskedjan i huvudsak har gått från tvingande regler för avtalsinnehåll med underleverantörer till allmänna råd, samtidigt som behovet av att se över och komplettera befintliga avtal med krav på cybersäkerhet tydliggörs.
- Att utbildningskraven har konkretiserats, särskilt när det gäller ledningens kompetens, vilket också har lyfts upp till ett eget kapitel.
- Att begrepp och struktur har förtydligats, vilket gör regleringen mer konsekvent och lättare att tillämpa.

Sammanfattningsvis ger det nya förslaget verksamhetsutövare större flexibilitet att anpassa sitt cybersäkerhetsarbete utifrån sin egen specifika kontext och riskprofil. Samtidigt får ledningen ett tydligare ansvar, inklusive kraven på tillräcklig kompetens och utbildning. Ändringarna medför således att NIS2-direktivets fokus på ledningsansvar speglas i större utsträckning och att cybersäkerhet i högre grad lyfts till en strategisk nivå.

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.

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.

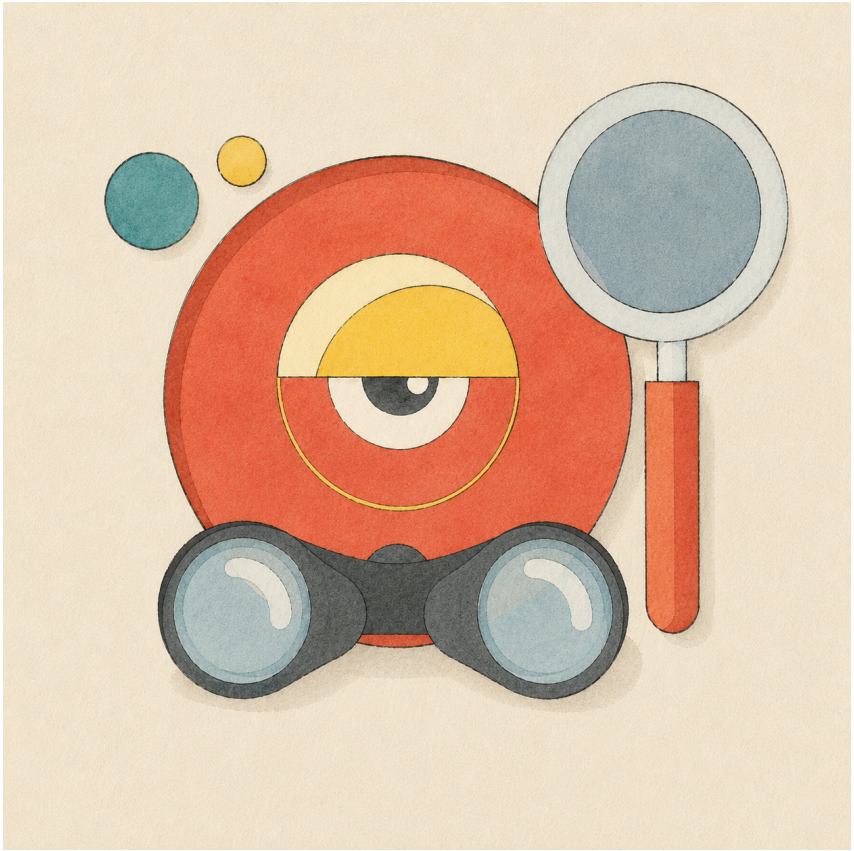
Gorrissen Federspiel

Tue Goldschmieding

SAMSIK varsler styrket tilsyn i 2026

Styrelsen for Samfundssikkerhed (»SAMSIK«) offentliggjorde den 25. februar 2026, at tilsynsindsatsen i telesektoren vil blive styrket i 2026 som følge af et skærpet trusselsbillede samt den nye lov nr. 435 af 6. maj 2025 om sikkerhed og beredskab i telesektoren. Loven er en særskilt implementering i dansk ret på teleområdet af Europa-Parlamentet og Rådets direktiv (EU) 2022/2555 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen (NIS 2-direktivet). Loven trådte i kraft den 1. juli 2025 og gav SAMSIK udvidede tilsyns- og håndhævelsesbeføjelser.

SAMSIK vil i 2026 føre tilsyn med overholdelsen af den nye registreringspligt for teleudbydere samt med de udbydere, der som såkaldte væsentlige teleudbydere er underlagt skærpede sikkerheds- og beredskabskrav. Dette tilsyn vil have fokus på informationssikkerhedsledelse, risikostyring og underretningspligter. På baggrund af en konkret risikovurdering vil SAMSIK endvidere gennemføre målrettede tilsyn hos udvalgte teleudbydere vedrørende fysisk sikkerhed med fokus på sabotagetruslen, redundans i relation til søkabler, cybersikkerhed, beredskab og krisestyringsplaner samt drift af mobilnet fra udenlandske driftscentre. Reaktive tilsyn ville endvidere kunne iværksættes på baggrund af rapporterede hændelser eller andre forhold.



Colourbox / Chat GPT

> SAMSIK vil i 2026 føre tilsyn med overholdelsen af den nye registreringspligt for teleudbydere samt med de udbydere, der som såkaldte væsentlige teleudbydere er underlagt skærpede sikkerheds- og beredskabskrav.

Læs Styrelsen for Samfundssikkerheds pressemeddelelse her: *https://samsik.dk/artikler/2026/02/styrket-tilsyn-i-telesektoren/*

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

LOVDATA