Den digitale omnibus-pakken: forenkling eller regulatorisk kursendring?

Av Lars Arnesen, Sebastian Schwemer og Emily Mary Weitzenboeck

Lars Arnesen

Sebastien Schwemer

Emily Mary Weitzenboeck

1. Bakgrunn

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

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

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

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

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

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

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

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

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

1.1. Et markant kursskifte i EU-lovgivningen

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ekstraordinære i en EU-rettslig kontekst.[19]

1.2. Den politiske dimensjonen

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

1.3. Veien videre

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

2. De sentrale byggeplassene i korte trekk

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

2.1. Data acquis: En samlet data regulering

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

2.2. KI-forordningen

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

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

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

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

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

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

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

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

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

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

3. Noen sentrale endringsforslag i personvernregelverket

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

36 Ibid. 47-48.

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

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

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

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

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

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

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

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

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

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

39 Artikkel 29-gruppen (n 36).

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

41 ***EDPS mot SRB*** (n 33).

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

43 Forordning 2018/1725 artikkel 3(1).

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

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

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

47 Ibid. avsnitt 68.

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

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

50 EDPS og EDPB (n 18).

51 Ibid. 9-11.

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

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

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

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

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

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

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

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

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

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

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

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

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

57 Wirtschaftsakademie (n 44), avsnitt 43.

tensiv diskusjon i lovgivningsprosessen og til å bli modifisert.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

63 Digital Omnibus, Fortalepunkt 30.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

69 Se foreslått artikkel 4a, Omnibuspakken om KI.

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

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

3.4. Den registrertes rett til innsyn: for vid innskrenkning

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

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

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

3.5. Ny cookie-bestemmelse: Forenkling for hvem?

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

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

72 Ibid.

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

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

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

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

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

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

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

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

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

75 Ibid. 6.

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

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

78 Ibid.

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

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

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

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

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

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

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

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

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

4. Avsluttende bemerkninger

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

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

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

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

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

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

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

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

86 Se Begrunnelse til Digital Omnibus, side 7.