

Innsynsrettens rekkevidde – logginnsyn og identitetsinformasjon

Av Hanne P. Gulbrandsen

1. Innledning

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

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

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

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

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

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

2. De rettslige rammene

2.1. Krav til logger som sikkerhetstiltak

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

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



Hanne P. Gulbrandsen

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

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

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

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

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

2.2 Retten til innsyn

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

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

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

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

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

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

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

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

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

2.4. EU-domstolens praksis

2.4.1. Innledning

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.5. Norsk rettspraksis og et knippe eksempler fra særlovgivningen

2.5.1. Innledning

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

2.5.2. Stortingets prinsipputtalelse om logginnsyn

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

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

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

2.5.3. Særregulering av innsynsretten

2.5.3.1. Helsesektoren

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

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

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

2.5.3.2. Politiet

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

2.5.4. Norsk rettspraksis

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

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

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

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

3. Identitetsopplysninger skal ikke utleveres automatisk ved logginnsyn

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

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

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

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

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

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

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

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

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

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

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

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

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

Hanne Pernille Gulbrandsen partner og advokat i Deloitte Advokatfirma AS.

¹⁰ Dette oppleves også i helsesektoren.