Datatilsynet

JUSTIS- OG BEREDSKAPSDEPARTEMENTET
Postboks 8005 Dep.
0030 OSLO

Deres referanse	Vår referanse	Dato
24/4162	24/03021-2	05.11.2024

Innspill fra Datatilsynet - Etterkontroll av personopplysningsloven

Vi viser til Justis- og beredskapsdepartementets invitasjon til å sende innspill til etterkontrollen med personopplysningsloven. Vi stiller oss til disposisjon for å utdype innspillene ved ønske.

1. Overgangsregler om behandling av personopplysninger

Datatilsynet mener at alle konsesjonsordninger bør avvikles. Se innspill til de enkelte ordningene under.

1.1. Overgangsreglene § 1

Datatilsynet har ved mange anledninger påpekt ulempene ved overgangsreglene for disse områdene. Prinsipielt er det uheldig at materielle regler ligger i overgangslovgivning, som i sin natur er midlertidig. Vi har også påpekt at det ikke er hensiktsmessig med den formen for regulering som nå ligger i overgangsreglene (konsesjon). Vi er kjent med at det pågår et eget lovarbeid for enkelte av områdene nedenfor (behandling av personopplysninger ved straffegjennomføring, varetekt og ved strafferettslige reaksjoner i konfliktrådene, og Datatilsynet er involvert her), og at det har vært spilt inn behov for endring fra flere hold over år, for eksempel finansnæringen. Datatilsynet har i stor grad støttet disse innspillene.

Overgangsreglene var ment til å være midlertidig inntil nye lover er på plass. Det ikke en ønskelig situasjon at Datatilsynet fortsatt skal gi tillatelser for behandling av personopplysninger for enkelte formål over seks år etter at personvernforordningen trådte i kraft. Det er også potensielle utfordringer med eksisterende tillatelser. Flere av de øvrige formålene det per i dag er gitt eller kan gis tillatelser for i medhold av overgangsreglene, har i dag pågående lovarbeid for en permanent ordning gjennom en demokratisk prosess.

1.2. Overgangsreglene § 6 første ledd bokstav a – dopingkontroll

Konsesjonsordningen bør oppheves. Datatilsynet mener at ordningen ikke bør erstattes med ny lovgivning som tillater dopingkontroll på treningssentre i den nåværende formen.

Våre synspunkter går frem av vårt høringssvar til ny lov om antidoping, som omhandlet antidopingarbeid i både konkurranseidretten, breddeidretten og på treningssentre[1].

1.3. Overgangsreglene § 6 første ledd bokstav b – Integrity Due Diligence

Konsesjonsordningen bør oppheves. Adgangen til å behandle artikkel 9 og 10-opplysninger ved gjennomføring av IDD-undersøkelser bør reguleres i egen lov eller forskrift.

Vi sendte i 2022 et brev til Justisdepartementet hvor vi redegjorde for generelle juridiske utfordringer med overgangsbestemmelsen om IDD. I brevet la vi frem hvilke særlige problemstillinger vi har sett i praksis, og vi pekte på hvilke praktiske utfordringer bestemmelsen medfører for de registrerte, de behandlingsansvarlige virksomhetene og for Datatilsynet.

1.4. Overgangsreglene § 6 første ledd bokstav c – elektronisk publisering av rettsavgjørelser

Hjemmelen bør oppheves og erstattes med regulering i lov.

Det bør også igangsettes for lovgivningsarbeid for tillatelser elektronisk publisering av rettsavgjørelser, hvor lovgiver samtidig har mulighet til å se på blant annet viderebruk av rettsavgjørelser dersom det er ønskelig at slike data skal kunne brukes for innovasjon og utvikling av tjenester innen legal tech.

I eventuelle nasjonale regler om tilgjengeliggjøring og bruk av rettsavgjørelser må personvernkonsekvensene vurderes, og det må sikres egnede og særlige tiltak for å verne den registrertes grunnleggende rettigheter. Datatilsynet vurderer at en effektiv avidentifisering av rettsavgjørelser utført av eller på vegne av det offentlige, vil være helt nødvendig for bredere tilgjengeliggjøring av rettsavgjørelser. Datatilsynet uttrykte allerede i 2005 i brev til domstolsadministrasjonen at avidentifisering av dommer bør skje så nærme kilden som mulig.

Direkte identifiserende opplysninger, og andre opplysninger som gjør risikoen for identifisering stor, har sjeldent betydning for rettskildeverdien til avgjørelsene. Vi vurderer at dette også i stor grad gjelder for deres anvendelighet for innovasjon og utvikling av løsninger[2].

---

[1] Høringssvar i lov om antidoping | Datatilsynet

[2] De databasene som per i dag eksisterer over avidentifiserte rettsavgjørelser er i det vesentlige vernet av åndsverkloven (Lovdata og Rettsdata), og ofte bak betalingsmur. Det er for øvrig kun Høyesterett av domstolene som publiserer sine avgjørelser elektronisk i avidentifisert form.
I arbeidsgruppen som ble satt ned av domstolsadministrasjonen i 2020 for Allmenn offentliggjøring av rettsavgjørelser, ble det anbefalt å etablere en plattform for domstolsdata. Det ble da anbefalt at slik tilgjengeliggjøring måtte ha grunnlag i lov, og at avidentifisering måtte være et krav. Slik tilgjengeliggjøring av rettsavgjørelser i avidentifisert form fra det offentlige skjer i dag i både Danmark og Sverige. Arbeidsgruppen uttalte også at når det gjelder rettsinformasjonssystemene og viderebruk av rettsavgjørelsene som ledd i «legal tech», er det behov for en særskilt regulering. Per nå er ikke gruppens anbefalinger fulgt opp med lovgivning.

2. Personopplysningsloven 2018

2.1. Rettspleielovunntaket § 2, andre ledd, bokstav b).

Ordlyden i bestemmelsen har medført at rettstilstanden uklar. Dette kan ha medført rettighetstap for enkeltpersoner ved at rekkevidden av unntakene har blitt tolket for vidt. Datatilsynet anbefaler at departementet klargjør følgende:

- Hvorvidt personopplysningsloven går lengre i å gjøre unntak fra virkeområdet til personvernforordningen enn det som er forutsatt
    - For eksempel gir artikkel 9 nr. 2 bokstav f et unntak fra forbudet mot behandling av særlige kategorier av opplysninger dersom den *«…er nødvendig for å fastsette, gjøre gjeldende eller forsvare rettskrav eller når domstolene handler innenfor rammen av sin domsmyndighet»*
    - Fortalepunkt 20 presiserer at forordningen gjelder, men at tilsynsmyndigheten har begrenset kompetanse når det berører domstolenes uavhengighet når de utfører sine juridiske oppgaver, herunder når de treffer avgjørelse. Videre åpner fortalepunktet for at tilsynet med etterlevelse av forordningen kan overlates til særskilte organer innen rettssystemet.
- Hvorvidt unntaket gjelder bestemmelsene i personvernforordningen i sin helhet, eller om enkelte bestemmelser gjelder
    - For eksempel knyttet til personopplysningssikkerhet
- Hvordan den registrertes interesser er ivaretatt gjennom rettspleielovene når personvernforordningen ikke gjelder
- Rekkevidden av formuleringen «mv.» i § 2, andre ledd, bokstav b) i.f.
    - Det er uklart hvor langt dette begrepet strekker seg og hvilke behandlinger som er tenkt unntatt
- Rekkevidden av begrepet *«saker som behandles eller avgjøres»*
    - Spørsmålet er for eksempel aktuelt i saker som behandles parallelt som sivil sak etter tvisteloven
        - Det er uklart hvilke aktører unntaket gjelder for
        - Det er uklart hvilke behandlingsaktiviteter som omfattes, herunder:
            - Innhenting av personopplysninger som bevis
            - Utveksling av personopplysninger til vitne
        - Datatilsynet har i vår saksbehandling vurdert at disse tilfellene ikke var omfattet av rettspleieunntaket, ettersom de innklagde behandlingsaktivitetene ikke skjedde i prosesskriv eller på annen måte var direkte omfattet av tvisteloven.
        - Vi har også sett at domstolene selv vurderer lovligheten etter personvernregelverket i spørsmål om bevisavskjæring, og derfor lagt til grunn at regelverket gjelder

Datatilsynet mener det hadde vært hensiktsmessig om departementet utredet hvordan andre land har fortolket og implementert unntaksbestemmelsen.

2.2. Barns samtykke i forbindelse med informasjonssamfunnstjenester § 5

Personopplysningsloven § 5 angir en 13 års aldersgrense for barns samtykkekompetanse overfor informasjonssamfunnstjenester.

Datatilsynet er involvert i parallelle prosesser knyttet til denne tematikken, og vil gi innspill i disse prosessene.

2.3. Behandling av personopplysninger for arkivformål, statistikk og forskning §§ 9-11

Personopplysningsloven §§ 9-11 pålegger den behandlingsansvarlige å rådføre seg med personvernombudet etter personvernforordningen artikkel 37 eller en annen som oppfyller vilkårene i personvernforordningen artikkel 37 nr. 5 og 6 og artikkel 38 nr. 3 første og annet punktum. *Rådføringsplikten gjelder likevel ikke dersom det er utført en vurdering av personvernkonsekvenser etter* personvernforordningen artikkel 35.

Gjennom praksis har det vist seg å være uklart hvilken rolle de forskjellige aktørene har dersom en virksomhet som har personvernombud helt eller delvis benytter rådføringstjenester fra *andre som oppfyller vilkårene* i artikkel 37 og 38. Dette er særlig uklart i tilfellene hvor det er pålagt å gjennomføre en personvernkonsekvensvurdering, som personvernombudet skal kontrollere gjennomføring av slike vurderinger i tråd med forordningen artikkel 39 nr. 1 bokstav c.

Adgangen til å benytte «andre» for vurdering av behandlingsaktiviteter etter §§ 9-11 bør klargjøres, særlig sett opp mot hvilke lovpålagte oppgaver et personvernombud skal involveres i.

Datatilsynet har begrenset kjennskap til erfaringene forskjellige aktører har med anvendelsen av bestemmelsene. Formålet med reglene er å gi tilstrekkelig supplerende rettslig grunnlag for de angitte behandlingsaktivitetene dersom det ikke finnes annet grunnlag, gjennom for eksempel dispensasjoner fra taushetsplikt. Datatilsynet er usikker på om bestemmelsene fungerer som forutsatt og håper Justisdepartementet finner å kunne evaluere dette også.

2.4. Bruk av fødselsnummer og andre entydige indentifikasjonsmidler § 12

Datatilsynet erfarer at det er usikkerhet knyttet til om § 12 i praksis innebærer et forbud mot å bruke biometriske data til å trene KI-modeller. Dette er knyttet til forutsetningen i § 12 som angir at slike kjennetegn kun kan benyttes når det er saklig behov for sikker identifisering og metoden er nødvendig for å oppnå slik identifisering.

Det kan argumenteres for at bruk av biometriske opplysninger til trening av KI-modeller som benyttes i forbindelse med sikker identifisering omfattes av ordlyden i § 12. Samtidig er det naturlig å anse trening av KI-modeller som et særskilt formål som skiller seg fra behovet for identifisering.

Datatilsynet mener i lys av dette at det er behov for klargjøring av rammene for § 12.

2.5. Unntak fra den registrertes rettigheter – personopplysningsloven § 16

Unntakene i § 16 fremstår i stor grad som absolutte. I Pankki-dommen C-579/21 trekker EU-domstolen inn fortalepunkt 63, og legger i vurderingen vekt på om unntak fra

personvernrettighetene får negativ innvirkning på andres rettigheter og friheter. I forordningsteksten er dette vurderingstemaet kun omtalt i artikkel 15 nr. 4, men EU-dommen slår fast at det også skal vurderes opp mot andre rettighetsbestemmelser.

Datatilsynet mener det er behov for å vurdere om dagens regulering i § 16 fanger opp rettsutviklingen i tilstrekkelig grad.

2.6. Taushetsplikt § 24

Datatilsynet ser behov for at taushetspliktsbestemmelsen i personopplysningsloven § 24 klargjøres. Dette er viktig siden brudd på taushetsplikten er straffbart, jf. strl. § 209.

- Varslingsbegrepet:

Både arbeidsmiljøloven § 2 A-7 og taushetsplikten etter § 24 bruker begrepet "varsling", men disse har ikke noe direkte med hverandre å gjøre. Taushetsplikten i § 24 bygger på forordningens artikkel 54 nr. 2, som i den engelske versjonen er "*reporting* by natural persons of infringements of this Regulation". "Reporting" er et vidt begrep. Når vi snakker om *varsling* i norsk forstand, og i AML sin forstand, er det nok kanskje ofte snakk om det engelske begrepet "*whistleblowing*", slik som i direktiv 2019/1937.

Vi anbefaler at man vurderer om «varsling» er riktig oversettelse, og man bør i alle tilfeller klargjøre rekkevidden av som menes med "enkeltpersoners varsling om overtredelser av loven her" i § 24. I dette ligger også en anbefaling om å klargjøre hvilke deler av «varslingen» som er unntatt, det vil si hvorvidt det er saksdokumenter i sin helhet eller opplysninger som er underlagt taushetsplikt.

Vi har spurt andre land i IMI hvordan de tolker artikkel 54, og de fleste tolker det slik at "reporting by natural persons of infringements of this Regulation" omfatter alle former for henvendelser til DPA om brudd på forordningen, herunder klager etter artikkel 77, tips osv. Dette er også slik vi praktiserer den i dag.

Vi viser også til at begrepet "reporting by natural persons" også brukes i artikkel 70(1)(m). EDPB skal gi ut veiledning om felles prosedyrer for slik rapportering.

- Opplysninger om sikkerhetstiltak etter personvernforordningen artikkel 32:

Datatilsynet mener at rekkevidden av taushetsplikten knyttet til sikkerhetstiltak i artikkel bør 32 klargjøres. Artikkel 32 pålegger den behandlingsansvarlige å etablere tekniske og organisatoriske tiltak, og alle disse omfattes av taushetsplikten. Organisatoriske tiltak kan være av forskjellig art, og behovet for taushetsplikt vil variere. En mulig presisering kan være å avgrense taushetsplikten til tiltak som er av betydning for personopplysningssikkerheten.

På tilsvarende måte som for varslingsbegrepet over, mener vi at det bør klargjøres om det er dokumenter med informasjon om sikkerhetstiltak eller kun beskrivelser av selve tiltakene som er underlagt taushetsplikt.

Datatilsynet anser det for begge temaene mest hensiktsmessig å underlegge *dokumenter* taushetsplikt. Det er krevende å skille ut enkeltstående opplysninger som er av relevans i en henvendelse, og tilsvarende med informasjon som kan regnes som sikkerhetstiltak.

Vi presiserer at prinsippet om meroffentlighet i offentlighetsloven § 11 vil medføre at tilsynsmyndigheten ved krav om innsyn må vurdere konkret om taushetsbelagt informasjon likevel kan offentliggjøres.

2.7. Gebyr til offentlige myndigheter og organer § 26

Personopplysningsloven § 26 gir Datatilsynet kompetanse til å ilegge overtredelsesgebyr til offentlige myndigheter og organer i tråd med vilkårene i personvernforordningen artikkel 83, herunder utmålingsreglene i GDPR. Følgelig gis ingen øvre grense eller retning for overtredelsesgebyr til offentlige myndigheter i Norge.

I Sverige er det innført en beløpsmessig grense på SEK 10 000 000 for overtredelsesgebyr til offentlige myndigheter, se *kapittel 6 § 2 i Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning*. Andre EU-land skiller tilsvarende eller på lignende måter mellom gebyrer til offentlige og ikke-offentlige aktører.

Datatilsynet har ilagt gebyr til offentlige myndigheter og organer i flere saker etter 2018. Vår erfaring tilsier at det er hensiktsmessig å vurdere endringer i personopplysningsloven knyttet til utmåling av overtredelsesgebyr.

Rammene for utmåling av overtredelsesgebyr som følger av personvernforordningen er kompliserte å benytte overfor offentlige aktører. Vi ser også at formålene med å ilegge overtredelsesgebyr trolig fullt ut oppnås gjennom andre og mer begrensede rammer for gebyrets størrelse.

Vi mener derfor at man i etterkontrollarbeidet bør innføre særskilte nasjonale rammer for utmåling av overtredelsesgebyr til offentlige myndigheter og organer. I den forbindelse peker vi på forslag til forskrift til digitalsikkerhetsloven § 23, som angir følgende utmålingsregler:

> *Ved forsettlig eller uaktsom overtredelse av digitalsikkerhetsloven § 14 eller bestemmelser i eller i medhold av digitalsikkerhetsloven §§ 7, 8, 10 eller 11, kan tilsynsmyndigheten ilegge overtredelsesgebyr på opptil 25 ganger grunnbeløpet eller, dersom det dreier seg om et foretak, på opptil 4 prosent av den samlede årsomsetningen i det forutgående regnskapsår, der det høyeste beløpet anvendes.*

Datatilsynets vurdering er at tilsvarende rammer bør innføres for overtredelser etter personvernregelverket for offentlige myndigheter og organer.

2.8. Datatilsynets adgang til å ilegge tvangsmulkt i grensekryssende saker § 29

Etter § 29 kan Datatilsynet fastsette tvangsmulkt. Personvernnemnda har i vedtak PVN-2023-31 og PVN-2024-04 lagt til grunn at adgangen til å ilegge tvangsmulkt bare gjelder for å sikre etterlevelsen av pålegg i ikke-grenseoverskridende saker.

I grenseoverskridende saker står vi etter dette i dag uten tvangsmidler til å sikre etterlevelse. Erfaring tilsier at vi trenger slike midler. Videre innebærer Personvernnemndas avgjørelser en forskjellsbehandling av norske og internasjonale virksomheter som opererer i Norge eller mot norske brukere. Datatilsynet har i dag bedre muligheter til å sikre etterlevelse hos aktører som kun har virksomhet i Norge enn vi har når det gjelder norske og utenlandske aktører med virksomhet i flere land. Dette er prinsipielt problematisk og har flere uønskede effekter, som også kan treffes av andre regler som for eksempel konkurranseretten.

Overtredelsesgebyr etter GDPR artikkel 58 kan ikke kompensere for manglende kompetanse til å ilegge tvangsmulkt. Tvangsmulkt gir den ansvarlige økonomisk motivasjon for å etterleve et eller flere krav som er fastsatt. Overtredelsesgebyr er ikke tilsvarende egnet til å sikre etterlevelse, og Datatilsynet mener derfor at loven bør endres til å presisere at vi har tilgang til å ilegge tvangsmulkt i alle typer saker, også saker etter personvernforordningen artikkel 56 og kapittel VII dette må endres i pol.

Datatilsynet mener at det i den sammenhengen bør lovfestes at Personvernnemnda ikke kan behandle klager på vedtak om tvangsmulkt i saker etter personvernforordningen artikkel 56 og kapittel VII, herunder hastesaker etter artikkel 66. En forutsetning for å kunne fatte et vedtak om tvangsmulkt er at pålegget i det underliggende vedtaket ikke er oppfylt. Et vedtak om tvangsmulkt kan derfor ikke fattes på selvstendig grunnlag. I vedtak PVN-2023-31 og PVN-2024-04 kom Personvernnemda frem til at den kan overprøve alle sider av saken når tvangsmulkt er ilagt, også de materielle vurderingene i det underliggende vedtaket som tvangsmulkten skal sikre etterlevelse av.

Dersom loven endres slik at Datatilsynet kan ilegge tvangsmulkt i saker etter personvernforordningen artikkel 56 og kapittel VII, vil Personvernnemda sin konklusjon innebære at nemda vil kunne overprøve de materielle vurderingene i saker etter samarbeids- og konsistensmekanismen som nemnda i dag ikke har kompetanse/myndighet til, og at personopplysningsloven § 22 annet ledd dermed i praksis vil settes til side. Dette vil innebære et ulovlig inngrep i samarbeids- og konsistensmekanismen, hvor det er lagt opp til at alle berørte datatilsynsmyndigheter i EØS fatter avgjørelser sammen. Det bør derfor vurderes å innføre eksplisitt unntak fra forvaltningsloven §§ 28 og 51 siste ledd for disse sakene.

I tillegg foreslår Datatilsynet at det gjøres en vurdering av om ordlyden i personopplysningsloven § 22 andre ledd er dekkende når den sier at nemnda er avskåret fra å overprøve «vedtak etter personvernforordningen artikkel 56 og kapittel VII». I saker som behandles etter personvernforordningen artikkel 56 og kapittel VII, fatter Datatilsynet også vedtak som ikke er hjemlet i artikkel 56 eller kapittel VII, men som likevel utgjør en integrert del av behandlingen etter samarbeids- og konsistensmekanismen. Et eksempel på dette er hvilke spørsmål man pålegger virksomheten å besvare eller omfanget av undersøkelsene, noe de berørte tilsynsmyndigheter av erfaring kan ha innspill om og diskutere. Klager på denne typen vedtak vil imidlertid i dag gå til Personvernnemnda uavhengig av samarbeids- eller konsistensmekanismen. Det bør vurderes om en mer hensiktsmessig avgrensing hadde vært «vedtak i saker som behandles etter personvernforordningen artikkel 56 og kapittel VII» eller liknende.

Videre forstår Datatilsynet at avgjørelser om hvorvidt en sak er grenseoverskridende er en prosessledende avgjørelse. Der Datatilsynet mener at en sak er grenseoverskridende, vil den i praksis behandles i tråd med artikkel 56 og kapittel VII. Det er imidlertid uklart om Personvernnemnda har

eller skal ha kompetanse til å overprøve Datatilsynets vurderinger av at en sak er grenseoverskridende. Hvis slik overprøvingsmulighet foreligger, betyr det at Personvernnemnda i praksis vil kunne behandle klager på vedtak som er fattet i samarbeid med datatilsynsmyndighetene i andre EØS-land og eventuelt etter behandling i EDPB, noe § 22 eksplisitt skal motvirke. Datatilsynet ønsker derfor en klargjøring av spørsmålet om hvorvidt en sak er grenseoverskridende er en prosessledende avgjørelse. Dette bør lovfestes, eventuelt bør det lovfestes at i denne typen saker må spørsmålet fremlegges for domstolene.

2.9. Oppreisning for overtredelse av personopplysningsloven § 30 (jf. GDPR art 82)

Datatilsynet mener det må foretas en utredning av om personopplysningsloven § 30 samsvarer med GDPR artikkel 82, herunder om § 30 eventuelt kan oppheves dersom artikkel 82 kan anvendes direkte.

Uttalelser i forarbeidene[3] til personopplysningsloven kan tyde på at det var tiltenkt at personopplysningsloven § 30 skal gå lengre enn artikkel 82:

> *Departementet mener det er grunn til å innta en bestemmelse om erstatning for ikke-økonomisk skade (oppreisning) da det ikke er klart om forordningen artikkel 82 nr. 1 alene gir et tilstrekkelig grunnlag for å ilegge erstatningsansvar for dette. Etter artikkel 82 nr. 1 har den som har lidd «materiell eller ikke-materiell skade» som følge av en overtredelse av forordningen, rett til erstatning for skaden, men det kan stilles spørsmål ved om ansvaret etter artikkel 82 nr. 1 også omfatter tap av ikke-økonomisk karakter. Etter departementets vurdering er det adgang til å gi en slik nasjonal bestemmelse om erstatning for ikke-økonomisk tap (oppreisning) i nasjonal rett, jf. forordningen artikkel 84. Tilsvarende er lagt til grunn i betenkningen Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, Betænkning nr. 1565 på side 914, utgitt av det danske justisdepartementet.*

I dag er det usikkert om personopplysningsloven § 30 gir dårligere vern enn artikkel 82, noe som potensielt kan innebære utilsiktet motstrid med våre EØS-rettslige forpliktelser. Datatilsynet anbefaler at bestemmelsen strykes dersom praksis fra EU-domstolen innebærer at man nå praktiserer erstatningsordningen artikkel 82 i tråd med den rekkevidden personopplysningsloven § 30 var tiltenkt. I motsatt fall bør ordlyden i § 30 revideres for å sikre det tiltenkte vernet.

3. Særreguleringer

3.1. Forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale

Forskriften er gitt med hjemmel i personvernforordningen artikkel 88, og inneholder bestemmelser med vilkår for når arbeidsgiveren har lov til å gjøre enkeltstående innsyn, et forbud mot overvåking, prosedyrekrav, bestemmelser om sletting m.m.

[3] Prop. 56 LS (2017–2018) kapittel 22

I Lehrerin-dommen C-34/21 (Hessen) presiseres kravene i art. 88 nr. 2. Domstolen understreker at de nasjonale reglene må være spesifikke, og ikke bare gjenta innholdet i forordningen (særlig avsnitt 71).

Primært mener Datatilsynet at forskriften bør oppheves.

Hvis forskriften skal bestå, mener Datatilsynet overordnet at det bør tas inn en generell henvising til personvernforordningen. Dette kan gjøres på samme måte som i § 2 i forskrift om kameraovervåking i virksomhet. Dette er viktig for å klargjøre at personvernforordningens regler virker parallelt med forskriften. I tillegg mener vi at hele forskriften bør gjennomgås og oppdateres.

Vi her vil knytte noen kommentarer til de delene av forskriften vi mener er uklare.

- **§ 1 – virkeområdet**

Vi erfarer at det er uklarhet knyttet til i § 1 bokstav b.

Det bør for det første klargjøres hva som menes med «virksomhetens datanettverk» og hva som skiller dette fra «annet elektronisk utstyr».

Det er uklart om ordlyden «annet elektronisk utstyr» skal leses i sammenheng med «personlige områder» eller om «personlige områder» kun skal leses i sammenheng med «områder i virksomhetens datanettverk». Med andre ord, er det uklart om kravet til «personlige område» gjelder ved innsyn i «annet elektronisk utstyr».

Videre vil vi påpeke at vilkåret «elektronisk utstyr» var tenkt å være teknologinøytralt, men vi oppfatter at det er uklart hvilket utstyr som omfattes av vilkåret. Digitale arbeidsverktøy og teknologiske løsninger som benyttes i ulike virksomheter utfordrer forståelsen av «elektronisk utstyr». Videre er skillet mellom arbeidsliv og fritid utvisket og det er ikke lenger slik at man enkelt kan snakke om virksomhetens elektroniske utstyr og arbeidstakers private utstyr i samme grad.

Vi har for eksempel fått spørsmål om skannere som brukes av lagerarbeidere kan omfattes. Slike skannerne kan etter det vi har forstått, ligne på datamaskiner, hvor ansatte logger seg på et eget brukerområde og skanner varer som plukkes og kjøres, og det registreres lokasjon og antall plukk per time. Etter vår oppfatning er det ikke naturlig at slikt utstyr omfattes av en forskrift om «arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale».

- **§ 2 - vilkår for innsyn**

Første ledd:
Vilkårene i § 2 første ledd bokstav a fremstår i stor grad som en gjentakelse av det som allerede følger av personvernforordningen artikkel 6 nr. 1 bokstav f.

I lys av Lehrerin-dommen C-34/21 (Hessen) og at personvernforordningen ikke bare skal gjentas i særregulering i medhold av personvernforordningen artikkel 88, mener vi bokstav a kan strykes. Det er tilstrekkelig med en henvisning til vilkårene i personvernforordningen artikkel 6 nr. 1 bokstav f.

Dersom vilkårene for å gjøre innsyn skal spesialreguleres i forskriften bør interesseavveiningen komme tydelig frem. Verken bokstav a eller bokstav b får klart frem interesseavveiningen som man skal gjøre etter artikkel 6 nr. 1 bokstav f.

I § 2 første ledd bokstav b mangler også et krav om at innsyn må være nødvendig for formålet.

Andre ledd:
Hvis det har vært lovgivers intensjon å oppstille et overvåkningsforbud i arbeidslivet, bør dette klargjøres. Forbudet mot overvåking i § 2 andre ledd bør i så fall synliggjøres bedre. Dette fremkommer i dag noe bortgjemt i bestemmelsen annet ledd. Bestemmelsen har overskriften "Vilkår for innsyn", og dette gjenspeiler ikke at bestemmelsen også kan tolkes som å inneholde et forbud mot overvåking mer generelt.

Utrykket «overvåke» bør defineres i forskriften. Det er i dag usikkerhet knyttet til når et tiltak er å anse som overvåking. Uklarhetene kan blant annet skape risiko for at virksomhetene ikke tar i bruk ny teknologi (for eksempel KI-systemer), i frykt for å bryte forskriften. Datatilsynet har forsøkt å klargjøre hva som menes med «overvåking» gjennom en nylig publisert veileder om temaet, men dette bør også komme tydeligere frem i bestemmelsens ordlyd.

Datatilsynet har registrert at noen har tatt til orde for at bestemmelsen bør fjernes i sin helhet, fordi den med dagens ordlyd er for uklar, samtidig som man mener dette ville vært tilstrekkelig regulert i de generelle bestemmelsene i personvernregelverket. Datatilsynet forstår dette synspunktet, og mener at det må utredes om det er mest hensiktsmessig å fjerne bestemmelsen eller om det er bedre å gjennomføre en revidering og klargjøring av bestemmelsens virkeområde.

Noen har også tatt til orde for at bestemmelsen ikke inneholder et generelt overvåkingsforbud, men at bestemmelsen bare presiserer prinsippet om formålsbegrensning.

Videre er det uklarheter om hvilke regler som gjelder hvis arbeidsgiver vil gjøre *innsyn* i et overvåkingstiltak som er etablert i tråd med andre ledd, eksempelvis innsyn i logg. Vi har fått spørsmål om man da må vurdere innsynet etter første ledd, eller om det er et spørsmål om innsynet er i tråd med administrasjons- eller sikkerhetsformålet i andre ledd. Vi har også fått spørsmål om arbeidsgiver i slike tilfeller må følge prosedyrereglene i § 3.

- **§ 3 - prosedyrer ved innsyn**

Det følger av § 3 andre ledd at arbeidstaker har innsigelsesrett etter personvernforordningen artikkel 21.

Etter artikkel 21 kan behandlingen av personopplysninger bare fortsette hvis arbeidsgiver kan påvise at det foreligger «tvingende berettigede grunner» som går foran den registrertes interesser, rettigheter og friheter, eller «for å fastsette, gjøre gjeldende eller forsvare rettskrav».

Konsekvensene og rettighetene som utløses av arbeidstakers protest bør beskrives i § 3. Vi har i flere saker sett at arbeidsgiver ved protest opprettholder vurderingene om at det er grunnlag for innsyn, uten å nevne eller vurdere vilkårene i artikkel 21.

- **§ 4 - sletting av opplysninger ved opphør av arbeidsforholdet**

Bestemmelsen har overskriften «Sletting», men regulerer både det at opplysninger skal «slettes» og det at arbeidstakers e-postkonto skal «avsluttes».

Første ledd sier at «Arbeidstakers e-postkasse skal avsluttes ved arbeidsforholdets opphør, med mindre det foreligger særskilt behov for å holde e-postkontoen åpen i en kort periode etter opphøret».

Vi anbefaler at det benyttes ett felles begrep i første ledd, i motsetning til dagens ordlyd som bruker både begrepet «e-postkasse» og «e-postkonto».
Med kravet om at arbeidstakers e-postkonto skal «avsluttes», forstår vi at kontoen skal deaktiveres, slik at det ikke lenger er mulig å sende e-poster dit. Avsenderen vil i så fall få en feilmelding til svar.

Dette bør tydeliggjøres ved å skille ut første ledd om avslutning av e-postkonto i en egen bestemmelse.

3.2. Hjemmel for overtredelsesgebyr for personvernsaker etter arbeidsmiljøloven

Datatilsynet har tidligere foreslått å innføre en gebyrhjemmel i arbeidsmiljøloven, blant annet i vårt høringssvar av 19.12.2023 som gjaldt rammene for overtredelsesgebyr for Arbeidstilsynet[4]. Fra sammendraget i vårt høringsinnspill:

> *I tillegg føreslår Datatilsynet ei føresegn i arbeidsmiljølova om at Datatilsynet kan ileggje lovbrotsgebyr for brot på forskriftene til arbeidsmiljølova, som Datatilsynet fører tilsyn med, e-postforskrifta og kameraforskrifta.*
>
> *Dersom Datatilsynet vil gje lovbrotsgebyr til verksemder som bryt forskriftene til arbeidsmiljølova, må vi i dag vurdere om verksemdene samtidig bryt dei generelle personvernreglane i personvernforordninga.*
>
> *Å gje gebyr berre på grunnlag av personvernforordninga har følgjande uheldige konsekvensar:*
>
> - *Spesialreglar i forskriftene til arbeidsmiljølova, som ikkje står i personvernforordninga, blir ikkje handheva med gebyr. Dette gjeld for eksempel prosedyrereglar for innsyn i e-post, sjå e-postforskrifta § 3.*
> - *Å gje gebyr etter personvernforordninga inneber ei unødvendig dobbeltbehandling,som stel ressursar frå eit tilsyn, som har store restansar.*
> - *For arbeidsgjevarar med tilknyting til andre land, kan tilsynsstyresmakter i utlandet få ansvaret for å undersøkje og sanksjonere innsyn i e-post og kameraovervaking overfor norske arbeidstakarar. Dette kan gje norske arbeidstakarar dårlegare vern og vere meir tungvint for arbeidstakarane*

[4] Vårt saksnummer 23/03995

3.3. Forskrift om kontrolltiltak overfor arbeidstakere som er omfattet av lov om stillingsvern mv. for arbeidstakere på skip

Datatilsynet er tilsyn for forskrift om kontrolltiltak overfor arbeidstakere som er omfattet av lov om stillingsvern mv. for arbeidstakere på skip, tilsvarende epostforskriften og kameraforskriften for arbeidere på skip.

Etter forskriftens § 6 skal opptak slettes etter én uke, men Datatilsynet kan gjøre unntak dersom det foreligger "særlig behov". Når skip som seiler under norsk flagg ligger til kai i andre stater oppstår det spørsmål om forholdet mellom flaggstatens og kyststatens jurisdiksjon.

Vi har mottatt søknader om unntak basert på at kyststaten har krav om lengre lagringstid enn det som gjelder etter norsk lov. I disse sakene er det vanskelig for Datatilsynet å ta stilling til komplekse havrettsproblemstillinger og jurisdiksjonsspørsmål.

Vi anbefaler en vurdering av om Datatilsynet er rett tilsynsorgan for denne forskriften. Alternativt ser vi behov for klarere føringer på hvilke tilfeller vi har kompetanse, forskriftens geografiske virkeområde og hva som skjer i tilfeller med motstridende regler om f.eks. lagringstid.

4. Andre tema

4.1. Søksmålsadgang for Datatilsynet om vedtak fra Personvernnemnda

Datatilsynet anser det hensiktsmessig å ha søksmålsadgang for avgjørelser fattet av Personvernnemnda. Vi håper Justisdepartementet utreder denne muligheten, herunder om personvernforordningen artikkel 58 nr. 5 forutsetter slik søksmålsadgang for Datatilsynet.

Til sammenligning har staten ved Konkurransetilsynet adgang til å saksøke Konkurranseklagenemnda, en adgang som ble innført i 2023 (Konkurranseloven § 39, Prop 63 L (2022-2023). Datatilsynet mener at mange av de samme hensynene som lå bak denne endringen også gjør seg gjeldene for tilsynet.

4.2. Personvernnemnda

Personvernnemnda er en særnorsk klageordning som er regulert i personopplysningsloven § 22, og av forarbeidene går følgende frem:

> *«Alternativet til å kunne klage til Personvernnemnda vil være at den enkelte borger eller bedrift vil måtte ta tilsynsmyndighetens vedtak inn for domstolene ved uenighet, noe som kan representere en stor byrde for den enkelte»*

Datatilsynet mener det kan være naturlig i forbindelse med etterkontrollarbeidet å vurdere om Personvernnemnda fungerer etter sin hensikt. Under følger spørsmål vi mener bør utredes:

- Personvernnemndas sammensetning, ressurssituasjon og kapasitet til å behandle et økende antall klagesaker, herunder når saker behandles av domstolene og en betydelig mer kompleks sakstype.

- Datatilsynets søksmålskompetanse, se over.
- Personvernnemndas rolle ved søksmål mot staten ved Personvernnemnda, jf. personopplysningsloven § 25, andre ledd. Dette innebærer at det er Personvernnemnda som opptrer som part og tar prosessbeslutningene. Datatilsynet har ingen formell rolle i slike søksmål. I konkurranseloven § 39 er motsatt løsning valgt, og søksmål om Konkurranseklagenemndas vedtak skal rettes mot staten ved Konkurransetilsynet. Det vil si at det er Konkurransetilsynet som opptrer som part i søksmål mot Konkurranseklagenemndas vedtak, og deres organisasjon er satt opp for å håndtere dette. Hensiktsmessigheten av hvem som opptrer som part kan variere ut fra om Personvernnemnda har stadfestet Datatilsynets vedtak eller om de har kommet til en annen beslutning i sin klagebehandling.
- Hvorvidt klageadgangen til Personvernnemnda skal gjelde alle aktører og sakstyper, eller om det er hensiktsmessig å avgrense muligheten til forvaltningsklager.

4.3. Alternativer til klagebehandling

Datatilsynet vil gi innspill til alternativer til dagens regulerte plikt til å behandle klagesaker i et eget dokument/spor, etter avtale med Justisdepartementet.

4.4. Akkreditering av sertifiseringsorganer

Datatilsynet anbefaler lov- eller forskriftsregulering av akkreditering av sertifiseringsorganer. I praksis vil Norsk akkreditering akkreditere sertifiseringsorganer i Norge.

Forordningen artikkel 43 nr. 1 sier at "Medlemsstatene skal sikre at nevnte sertifiseringsorganer akkrediteres av en eller begge av følgende". Guidelines 4/2018 fra EDPB sier i avsnitt 31:

> *«It is for the individual member state to decide whether the national accreditation body or supervisory authority or both together will carry out these accreditation activities but in any case it should ensure that adequate resources are provided (see Article 4(9) of Regulation (EC) 765/2008)»*

Datatilsynet kan være behjelpelig med å illustrere hvordan dette er gjort i øvrige europeiske land dersom det er ønskelig.

4.5. Inkorporasjon i personopplysningsloven av ny EU-forordning om grensekryssende saker

En ny forordning om saksbehandlingsregler ved grensekryssende saker er under utarbeidelse i EU. Datatilsynet mener den bør innlemmes i EØS-avtalen og gjennomføres i personopplysningsloven slik at den kan starte å gjelde samtidig i Norge som i EU.

4.6. Oversettelser

4.6.1. Virksomhet

Datatilsynet anbefaler at "virksomhet" erstattes med "etablering". Til sammenligning bruker den danske versjonen av GDPR ordet "etablering" (entall), mens den svenske versjonen bruker ordet

"verksamhetsställe" - artikkel 4 nr. 24 bokstav b). Den danske versjonen av GDPR bruker imidlertid ordet "virksomheder" (flertall) for "establishments" i artikkel 4 nr. 24 bokstav a.

4.6.2. Ideelt organ eller en ideell organisasjon eller sammenslutning – artikkel 80

I artikkel 80 som gjelder representasjon av registrerte, fremgår det det må være et "*ideelt organ eller en ideell organisasjon eller sammenslutning*" for å kunne representere registrerte.
Personvernnemnda kom i PVN-2022-22 til at:

> *Forbrukerrådet er ikke en ideell organisasjon, men et forvaltningsorgan som ifølge egen nettside skal «veilede forbrukere og påvirke samfunnet i en forbrukervennlig retning». Forbrukerrådet faller derfor ikke inn under den typen organisasjoner som etter nemndas vurdering kan gis representasjonsrett etter artikkel 80.*

I den engelske versjonen brukes "not-for-profit" der den norske versjonen bruker "ideelt". Den danske versjonen bruker "ikke arbejder med gevinst for øje". Den engelske og danske ordlyden kan synes å være noe videre enn den norske, siden det er lettere å få et offentlig organ som f.eks. Forbrukerrådet til å passe inn ordlyden i "ikke-kommersielt" organ e.l. sammenlignet med "ideelt" organ.

Det fremstår som uhensiktsmessig at ikke Forbrukerrådet skal kunne representere klagere, og dette vil i betydelig grad vanskeliggjøre slike organers oppgaver. Datatilsynet mener derfor at oversettelsen bør endres, eventuelt at forståelsen av bestemmelsen presiseres.

4.7. Organiseringen av tilsynsmyndigheten

Personvernforordningen kapittel VI regulerer medlemsstatenes etablering og organisering av tilsynsmyndigheter som har ansvar for å føre tilsyn med personvernforordningen.

Schengenevaluering av Norge ble sist gjennomført i 2022, og der ble det gitt merknader, med etterfølgende tiltak, knyttet til organiseringen av Datatilsynet.

Det kan være hensiktsmessig at departementet som ledd i etterkontrollarbeidet vurderer om Norge oppfyller de forutsetningene som kapittel VI angir for etablering og organisering av tilsynsmyndigheter etter personvernforordningen.

Med vennlig hilsen

Line Coll
direktør

Camilla Nervik
fung. juridisk direktør

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer

Kopi til: DIGITALISERINGS- OG FORVALTNINGSDEPARTEMENTET (DFD)

Vedlegg: Innspill fra Datatilsynet - Etterkontroll av personopplysningsloven