

JUSTIS- OG BEREDSKAPSDEPARTEMENTET
Postboks 8005 Dep.
0030 OSLO

Deres referanse Vår referanse
17/4200 ES ØMO/bj- 17/01179-3/SBL

Dato
16.10.2017

Høringsuttalelse fra Datatilsynet - utkast til ny personopplysningslov - gjennomføring av personvernforordningen i norsk rett

Vi viser til høringsbrev datert 6. juni 2017 – utkast til ny personopplysningslov – gjennomføring av personvernforordningen i norsk rett.

1. Innledning og generelle merknader

Innføringen i norsk rett av Europaparlamentets og Rådets forordning (EU) 2016/679 av 27. april 2016¹ («forordningen») er det viktigste som har skjedd på personvernområdet på lang tid. Selv om forordningen viderefører mange rettigheter og plikter fra dagens regelverk, er det også mye som er nytt. Konsekvensene av endringene vil langt på vei måtte avklares i praksis i tiden som kommer.

Samtidig er gjennomføring i nasjonal rett, herunder avklaring av nasjonalt handlingsrom og valg av nasjonale reguleringer, svært viktig for å sikre god etterlevelse av forordningen. Vårt høringsinnspill er derfor omfattende, og vi omtaler de fleste problemstillinger som tas opp i høringen.

Vi er i hovedsak enige i departementets beskrivelse av nasjonalt handlingsrom, og i departementets valg av områder som er gjenstand for nasjonale tilpasninger. På de fleste punkter er vi også enige i departementets beskrivelse av gjeldende rett, og av hvilke krav som følger av forordningen. Samtidig mener vi at det er forholdsvis mange problemstillinger departementet med fordel kunne ha gått nærmere inn i.

Vi har forståelse for at det ikke er rom for å utrede alle problemstillinger fullt ut. Samtidig er det uheldig at enkelte spørsmål er så lite utredet at det trolig vil være vanskelig for høringsinstansene å gi presise innspill. Dette gjelder for eksempel spørsmålene om behovet

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

for straffebestemmelse, overgangsregler for bruk av konsesjoner, og foreldelse av adgangen til å gi overtredelsesgebyr.

Forordningsteksten er svært omfattende og vanskelig tilgjengelig.² Det foreligger naturlig nok ingen rettspraksis etter forordningen ennå, og det finnes begrenset med rettskilder for øvrig, som direkte belyser hvorledes reglene i forordningene er å forstå. Den kommende lovproposisjonen om ny personopplysningslov blir derfor en viktig rettskilde. Særlig vil den kunne bidra til å klargjøre hva som kreves for at nasjonal særlovgivning skal være i tråd med forordningen – dette er et viktig poeng, mener vi.

Vi hadde gjerne sett at høringsnotatet beskrev kravene som forordningen stiller til nasjonal lovgivning mer inngående. Dette ville ha gjort det enklere å ta stilling til om det nye regelverket medfører behov for endringer eller ikke, sammenlignet med de reglene som gjelder i dag.

Vi mener at departementet kunne ha kommentert prinsippene i forordningens artikkel 5 mer inngående, ettersom disse prinsippene langt på vei er en videreføring av eksisterende prinsipper, som dessuten er belyst gjennom en rekke avgjørelser i EU-domstolen.

Vi håper at departementet i lovproposisjonen i større grad enn i høringsnotatet viser til de grunnleggende prinsippene i personvernretten, og at det samtidig gir mer veiledning i hvordan lov som behandlingsgrunnlag skal utformes. Vår erfaring er at lovforslag som er på høring ofte er mangelfullt utredet når det gjelder personvernkonsekvensene. Nettopp av denne grunnen mener vi at departementet bør benytte muligheten til å understreke viktigheten av dette i proposisjonen.

Vi har i kapittel 2 i vårt høringssvar gitt en oversikt over våre viktigste merknader. Videre følger våre nærmere merknader sortert etter de samme temaer som i høringsnotatet. I kapittel 3 har vi redegjort grundig for hvordan vi forstår de grunnleggende personvernprinsippene. Dette har vi gjort fordi vi oppfatter at prinsippene har nær sammenheng med de øvrige merknadene våre.

² Vi viser til at departementet bemerker i høringsnotatets kapittel 3 at «forordningens struktur, språk og regeloppbygning på en rekke punkter avviker fra det man vil betegne som alminnelig norsk lovgivningsteknikk», og videre at «de pedagogiske utfordringene forsterkes ved at personopplysningslovens regler dels vil følge av den inkorporerte forordningen og dels av de utfyllende nasjonale bestemmelsene».

Innhold

1. Innledning og generelle merknader	1
2. Oversikt over høringsuttalelsens viktigste merknader	4
3. De grunnleggende prinsippene for behandling av personopplysninger	8
4. Behandlingsgrunnlag.....	15
5. Behandling av sensitive personopplysninger	24
6. Behandling av sensitive personopplysninger for arkiv, forskning og statistiske formål .	33
7. Samtykke	39
8. De registrertes rettigheter	39
9. Tilpasninger i særlover som følge av forordningen	46
10. Lovens saklige virkeområde.....	48
11. Behandling av personopplysninger om straffedommer og lovovertridelser	54
12. Vurdering av personvernkonsekvenser	56
13. Personvernråd giver.....	58
14. Melde- og konsesjonsplikt	63
15. Overføring av personopplysninger til tredjestater.....	67
16. Tilsynsmyndighetenes organisering.....	67
17. Domstolsprøving	68
18. Datatilsynets og Personvernemndas taushetsplikt og tilgang til opplysninger	69
19. Klage over Datatilsynets vedtak.....	70
20. Overtrjedelsesgebyr.....	73
21. Administrativ inndragning	74
22. Straffebestemmelser	75
23. Tvangsmulkt.....	76
24. Behandling i journalistisk, akademisk, kunstnerisk og litterær virksomhet	76
25. Offentlighet og innsyn.....	80
26. Fødselsnummer og andre entydige identifikasjonsmidler.....	84
27. Unntak fra den registrertes rettigheter ved behandling for arkivformål i allmenhetens interesse, vitenskapelig eller historisk forskning eller for statistiske formål	87
28. Behandling av barns opplysninger	88
29. Kameraovervåking	89
30. Arbeidsgiveres innsyn i e-postkasse mv.	96
31. Økonomiske og administrative konsekvenser	99

2. Oversikt over høringsuttalelsens viktigste merknader

De grunnleggende personvernprinsippene for behandling av personopplysninger

- Departementet omtaler prinsippene på en overordnet og kortfattet måte i høringsnotatet. Det er uheldig at departementet ikke har gått dypere inn dette, særlig fordi prinsippene legger klare rammer og begrensninger for handlingsrommet norske myndigheter har til å utforme nasjonale regler
- Høringsnotatet omtaler i liten grad prinsippenes betydning, samt tilhørende rettspraksis fra EU-domstolen og EMD
- Det er særlig uheldig at det ikke er redegjort for lovlighetsprinsippet. Etter Datatilsynets mening legger departementet til grunn et lavere krav til klarhet enn det som følger av våre forpliktelser etter forordningen

Lovforslag om unntak fra formålsbegrensningen ved lovpålagte tilsynsoppgaver (§ 12)

- Datatilsynet mener at lovforslaget om unntak fra formålsbegrensningen ved lovpålagte tilsynsoppgaver er problematisk av flere grunner
- Blant annet er det problematisk at forslaget ikke er nærmere begrunnet, og fordi departementet trekker frem ett område i den generelle personopplysningsloven hvor det foregår samarbeid, uten å ha sett på andre områder

Behandlingsgrunnlag

- Datatilsynet mener at departementets beskrivelse av kravene til behandlingsgrunnlag i høringsnotatet er ufullstendig, og på enkelte punkter er vi uenige med departementet
- Slik vi ser det burde departementet i større grad ha trukket inn sentrale rettskilder i sin gjennomgang av forordningens artikkel 6 om behandlingsgrunnlag
- Departementet har ikke fått tilstrekkelig frem de kravene til nasjonal lovgivning som følger av forordningen, herunder kravet om klarhet, nødvendighet, proporsjonalitet og formålsbegrensning

Behandling av sensitive personopplysninger

- Departementet redegjør i liten grad for kravene til nasjonale regler for behandling av sensitive personopplysninger
- Høringsnotatets korte omtale av disse kravene gjør at vi mener det kan stilles spørsmål ved om høringsinstansene har fått et godt nok utgangspunkt for å gi innspill om de mener dagens sektorlovgivning er i samsvar med kravene som forordningen stiller, slik departementet ber om
- Det er også en vesentlig svakhet ved høringsnotatet at departementet ikke har gått nærmere inn i kravet til nødvendige garantier i nasjonal lovgivning
- Vi har merknader til alle de konkrete behandlingsformålene som departementet tar opp

Særlig om behandling av sensitive personopplysninger for arkiv, forskning og statistiske formål

- Datatilsynet mener at den foreslåtte bestemmelsen i § 6 er for vidt formulert, og at det er grunn til å tro at den ikke oppfyller kravene til klarhet i hjemmelsgrunnlaget som følger av lovlighetsprinsippet og forordningen, samt forordningens krav til garantier

- Særlig er forslaget om at det skal være et vilkår om at «den behandlingsansvarlige har utpekt personvernrådgiver og personvernrådgiveren har tilrådd behandlingen» i lovforslagets § 6 først ledd bokstav d problematisk
- Det er behov for lovregulering av behandling av data til forskningsformål

De registrertes rettigheter

- Det er problematisk at departementet foreslår å videreføre gjeldende rett om unntak fra de registrertes rettigheter, så langt forordningen åpner for det, uten å vurdere om den gjeldende bestemmelsen er i tråd med forordningen
- For å kunne videreføre disse reglene må det foretas en konkret vurdering av om de foreslåtte unntakene er tydelige, presise og forutsigbare nok til at de kan anses i tråd med forordningen. Vi kan ikke se at det er gjort i høringsnotatet
- Det er behov for å foreta en kartlegging av om det må foretas endringer av rettighetsbestemmelser i sektorlovgivningen. Notatet sier ingenting om dette
- Flere av de de alternative unntaksgrunnlagene i lovforslagets § 13 er problematiske, særlig bokstav e om åpenbare og grunnleggende private og offentlige interesser. Vi mener denne bestemmelsen er i strid med forordningen

Lovens saklige virkeområde

- Det bør spilles inn overfor Stortinget at riksrevisjonsloven § 17 bør revideres, siden det er Stortinget selv som er ansvarlig for denne loven
- Departementet foreslår å videreføre gjeldende regel om begrensning i Datatilsynets myndighet til å kreve informasjon og gjøre andre undersøkelser der man står overfor behandling av personopplysninger som er nødvendig av hensyn til rikets sikkerhet mv. Datatilsynet mener at dette er uheldig av flere grunner, blant annet fordi gjeldende bestemmelse har skapt store uklarheter
- Departementet foreslår å videreføre bestemmelsen om at personopplysningsloven ikke gjelder for saker som behandles eller avgjøres i medhold av rettspleielovene. Dette har i praksis medført uklarhet, fordi det i tilknytning til saker som behandles etter rettspleielovene vil være mange forskjellige aktører involvert
- Departementet legger til grunn at «behandling av saker i medhold av rettspleielovene ligger utenfor EØS-avtalens saklige virkeområde og at Norge ikke er bundet av forordningen på dette punkt». Vi mener det er tvilsomt at dette er riktig, og ber om at departementet vurderer dette spørsmålet grundigere i proposisjonen enn det som er gjort i høringsnotatet

Personvernrådgiver

- Vi er kritiske til at begrepet «personvernombud» er erstattet med «personvernrådgiver» av flere grunner. Blant annet fordi «personvernombud» er et godt innarbeidet begrep både i Norge og Sverige, og en endring av rollens betegnelse vil signalisere en svekkelse av rollens uavhengighet, selvstendighet og autoritet
- Det er behov for en avklaring av hvor langt plikten til å ha personvernrådgiver i det offentlige strekker seg

- Vi stiller spørsmål ved om det er adgang til å utvide plikten til å ha personvernrådgiver til å omfatte alle forskningsinstitusjoner (jf. lovforslaget § 6 første ledd bokstav d)

Melde- og konsesjonsplikt

- Datatilsynet støtter departementets forslag om å ikke videreføre konsesjonsplikt som hovedregel ved behandling av sensitive personopplysninger
- Når det gjelder lovforslagets § 7, konsesjon til behandling som er nødvendig av hensyn til viktige samfunnsinteresser, er vi usikre på om det er adgang til å ha en slik hjemmel i nasjonal lovgivning. Dersom departementet kommer til at det er adgang til slik regulering, bør denne adgangen gjøres svært snever
- Det bør gis overgangsregler for gjeldende konsesjoner. Datatilsynet foreslår at det settes en absolutt grense for gjeldende konsesjonenes gyldighet på to år, men med en mulighet for Datatilsynet til å oppheve slike tillatelser tidligere, etter en konkret vurdering

Barns behandling av personopplysninger

- Når det gjelder barns samtykke ved informasjonstjenester foreslår departementet en bestemmelse i ny personopplysningslov som setter en aldersgrense på 13 år. Dette er i tråd med Datatilsynets praksis og vi støtter departementets forslag

Kameraovervåking

- Datatilsynet støtter forslaget om særregulering om bruk av kameraovervåking på arbeidsplassen, men mener det er nødvendig med en rekke presiseringer av forslaget
- Blant annet bør det inntas en egen bestemmelse som henviser til forordningens øvrige bestemmelser. Det bør gis en mer utfyllende bestemmelse om informasjonsplikt
- Bestemmelsen om sletting er for vidt formulert, og det må inntas presiseringer
- Videre mangler det hjemmel for politiets bruk av kameraovervåking i forebyggingsøyemed
- Det må også presiseres når kameraovervåking innebærer en behandling av sensitive personopplysninger

Klage over Datatilsynets vedtak og domstolsprøving

- Datatilsynet er enig i at det bør være en administrativ klageordning
- Vi stiller imidlertid spørsmål ved om klageordningens innretning. Klageordningen bør innrettes mer mot Personvernemnda som et domstolliknende organ, med større innslag av partprosess
- Vi ber om avklaringer med hensyn til hvilke vedtak som kan påklages til nemnda
- Det er nødvendig å gi regler knyttet til Datatilsynets posisjon i rettslig prosess der vi er involvert. Vi foreslår at Datatilsynet gis selvstendig partsevne

Datatilsynets og Personvernemndas taushetsplikt og tilgang til opplysninger

- Vi støtter forslaget om å videreføre en bestemmelse om dette, men vi mener at taushetsplikten må forsterkes

- Det bør inntas en bestemmelse om at taushetsplikten også skal gjelde overfor sakens parter og deres representanter

Overtredelsesgebyr

- Datatilsynet mener det bør innføres en foreldelsesfrist for adgangen til å ilegge overtredelsesgebyr, og anbefaler at dette utredes nærmere, ettersom spørsmålet reiser en rekke prinsipielle, komplekse og praktiske spørsmål
- I europeisk sammenheng har det vært sett hen til konkurranseregelverket ved utforming av regler om dette

Straffebestemmelse

- Departementet har bedt høringsinstansene om innspill på om brudd på personopplysningsloven bør være straffbart, men har ikke selv utredet dette
- Datatilsynet mener at det bør vurderes å gi en slik straffebestemmelse og at dette bør utredes
- Vi mener at det kan ligge en avskrekkende virkning i at man kan risikere politietterforskning, tatt i betraktning at Datatilsynet er et relativt lite organ

Behandling i journalistisk, akademisk, kunstnerisk og litterær virksomhet

- Datatilsynet støtter forslaget om å regulere dette særskilt, men har noen merknader basert på de utfordringer vi ser ved praktisering av gjeldende bestemmelse
- Vi ber departementet vurdere å innta noe om nødvendighetsvurderinger i lovforslaget

Offentlighet og innsyn

- Vi er enig i at en bestemmelse tilsvarende personopplysningsloven § 6 første ledd, om forholdet til offentleglova, ikke er nødvendig
- Fremstillingen som departementet gir av forordningens artikkel 86 om offentlighet og betydingen av nasjonale regler fremstår imidlertid som misvisende

Fødselsnummer og biometri

- Vi støtter forslaget om å videreføre dagens bestemmelse, men har enkelte merknader
- Det bør nedlegges et eksplisitt forbud mot at fødselsnummer og andre nasjonale identifikasjonsnumre blir brukt til autentisering
- Det bør vurderes en separat bestemmelse om biometri

Innsyn i e-post

- Vi støtter forslaget om å videreføre reglene om innsyn i e-post, disse skaper god forutberegnelighet og klarhet på et område vi får mange henvendelser om
- Vi foreslår imidlertid at reglene bør avgrenses til ikke å gjelde aktivitetslogger
- Videre bør arbeidstager gis innsigelsesrett, ikke bare ha rett til å uttale seg

3. De grunnleggende prinsippene for behandling av personopplysninger

I høringsnotatets kapittel 6 omtales personvernprinsippene og forordningens artikkel 5 på en overordnet og kortfattet måte.

Det hadde vært en fordel med en grundigere gjennomgang av prinsippene i artikkelen, særlig fordi prinsippene legger klare rammer og begrensninger for handlingsrommet norske myndigheter har til å utforme nasjonale regler etter blant annet artikkel 6 og artikkel 9. Vi kommer nærmere tilbake til det nedenfor.

3.1. Prinsippenes betydning

Artikkel 5, som angir prinsippene for behandling av personopplysninger, er etter vår vurdering den mest sentrale artikkelen i hele personvernforordningen. Ikke bare har prinsippene betydning for hvorledes de øvrige bestemmelsene i forordningen skal forstås, artikkel 5 har også normativ kraft i seg selv; Datatilsynet skal for eksempel kunne ilegge overtredelsesgebyr for brudd på prinsippene i artikkel 5 alene, jf. forordningens artikkel 83 nr. 1 og nr. 5 a.

Innholdet i prinsippene er konkretisert nærmere i forordningens øvrige bestemmelser. Ordlyden i disse bestemmelsene er imidlertid ikke alltid like klar, og prinsippene vil dermed bli en sentral tolkningsfaktor.

Prinsippene i artikkel 5 er langt på vei en videreføring av prinsippene i personverndirektivet artikkel 6.³ Prinsippene fra direktivet bygger igjen i stor grad på Europarådets konvensjon 29 Januar 1981 nr. 108 om personvern i forbindelse med elektronisk databehandling av personopplysninger § 5. Prinsippene har blitt belyst og presisert i en rekke avgjørelser fra EU-domstolen, og i uttalelser fra Artikkel 29-gruppen (EU-kommisjonens ekspertorgan på personvern). Selv om Artikkel 29 gruppens uttalelser er av veiledende karakter tillegges de stor vekt i praksis – også av EU-domstolen.

På bakgrunn av dette, mener vi at det hadde vært en fordel om det i proposisjonen blir gjort nærmere rede for prinsippene, og hvilken betydning de har for norsk lovgivning om behandling av personopplysninger, og dessuten for forståelsen og etterlevelsen av forordningen for øvrig.

Høringsnotatet omtaler i liten grad rettspraksis fra EU og EMD. Dette er uheldig fordi EMD og EU-domstolen har tolket og presisert de grunnleggende prinsippene for behandling av personopplysninger. EU-domstolen har tolket direktivet i lys av EMK, og etter 2010 i henhold

³ To viktige forskjeller sammenlignet med personverndirektivet er at gjennomsiktighetsprinsippet og prinsippet om integritet og fortrolighet har kommet inn i lovbestemmelsen om prinsipper. Prinsippene representerer imidlertid ingen nyhet som sådan. Europarådskonvensjonen artikkel 7 om sikring av opplysninger er tatt inn i kapittelet om hovedprinsipper. Nevnte prinsipper er også lagt til grunn i flere uttalelser fra artikkel 29 gruppen. Se for eksempel uttalelsen 8/2001 om gjennomsiktighetsprinsippet. De er også lagt til grunn i praksis til Datatilsynet.

til EUs pakt om grunnleggende rettigheter. Selv om pakten ikke gjelder direkte for Norge, mener vi at EU-domstolens tolkning likevel er relevant for Norge. Vi viser til at rettighetene i pakten tilsvarer bestemmelsene i EMK, som Norge er bundet av, og at EU-domstolens tolkning i stor grad bygger på EMDs rettspraksis.

I det følgende går vi gjennom noen av de meste sentrale prinsippene i forordningen. Vi har valgt å gå forholdsvis grundig til verks, fordi vi mener det nærmere innholdet i prinsippene har stor betydning for våre øvrige merknader til departementets lovforslag.

Særlig er lovlighetsprinsippet sentralt for vurderingen av kravene til nasjonale regler etter artikkel 6 og 9, men også for kravet til lovgivning som unntar fra prinsipper og rettigheter etter artikkel 23 nr. 2. Vi vil også komme inn på rettferdighetsprinsippet, formålsbegrensningsprinsippet og prinsippet om dataminimering og proporsjonalitet.

3.2. Lovlighetsprinsippet

Gjeldende nasjonal rett

I Norge er lovlighetsprinsippet gjennomført i personopplysningsloven § 11 bokstav a. Etter denne bestemmelsen kan personopplysninger bare behandles når dette er tillatt etter §§ 8 og 9.

Det er uklart hvorfor lovlighetsprinsippet ikke er synliggjort som et eget prinsipp i personopplysningsloven. I forarbeidene uttales det at: «Departementet finner det selvsagt at formålet med behandlingen må være lovlig, og har ikke funnet grunn til å presisere dette nærmere i lovteksten.»⁴

At prinsippet er utelatt fra § 11 kan være en av grunnene til at prinsippet, etter vårt syn, i liten grad har vært vurdert som en rettslig ramme for lovgiver for nasjonal lovgivning som regulerer behandling av personopplysninger.

Høringsnotatet redegjør ikke for lovlighetsprinsippet

Høringsnotatet redegjør ikke for lovlighetsprinsippet.⁵ Dette er beklagelig, fordi vi ikke tror det lar seg gjøre å gi en fullstendig beskrivelse av forordningens krav til nasjonale regler uten å ha vurdert lovlighetsprinsippet først.

Etter Datatilsynets mening legger departementet til grunn et lavere krav til klarhet enn det som følger av våre forpliktelser etter forordningen. Dette gjelder spesielt de krav til nasjonale regler som følger av artikkel 6 og 9, men også regler som unntar fra prinsipper og rettigheter etter artikkel 23 nr. 2. Se kapittel 4, 5 og 8 om dette. I gjennomgangen av disse bestemmelsene nedenfor, kommer vi nærmere inn på prinsippet om lovlig behandling.

Lovlighetsprinsippet bør etter vårt syn gjøres til gjenstand for en grundig utredning i proposisjonen. Dersom departementet mener at lovlighetsprinsippet har et annet innhold i norsk rett enn i EU-retten, anbefaler vi i så fall at dette kommenteres og utdypes.

⁴ Se Ot.prp.nr 92 (1998-199) side 114

⁵ Så vidt vi kan se er prinsippet kun omtalt i en setning på side 21.

Vår vurdering av lovlighetsprinsippet

Lovlighetsprinsippet er fastsatt i forordningens artikkel 5 nr. 1 bokstav a er en videreføring fra direktivet artikkel 6 nr. 1 bokstav a. Prinsippet innebærer at det kreves at behandling av personopplysninger må ha et rettslig grunnlag for at behandlingen skal være lovlig. Med det menes at behandlingen må være hjemlet i et av de alternative rettslige grunnlagene som er listet opp artikkel 6 nr. 1.⁶ En slik tolkning tilsvarer det Artikkel 29-gruppen har lag til grunn for direktivet.⁷

Et viktig side ved dette prinsippet er at det oppstiller visse krav til nasjonal lovgivning, herunder et krav til klarhet, nødvendighet og forholdsmessighet der det aktuelle rettslige grunnlaget for en behandling er hjemmel i lov.

Lovlighetsprinsippet omtales i fortalens punkt 40 og 41. Punkt 41 forklarer nærmere kravene til klarhet i nasjonal lovgivning og henviser til relevante rettskilder.

«Når det i denne forordning vises til et rettslig grunnlag eller et lovgivningsmessig tiltak, krever dette ikke nødvendigvis en regelverksakt vedtatt av et parlament, med forbehold for kravene fastsatt i henhold til forfatningsordningen i den berørte medlemsstat. Nevnte rettslige grunnlag eller lovgivningsmessige tiltak bør imidlertid være tydelig og presist, og anvendelsen av det bør være forutsigbar for personer som omfattes av det, i samsvar med rettspraksisen til Den europeiske unions domstol («Domstolen») og Den europeiske menneskerettighetsdomstol.»

Prinsippet om lovlig behandling er også presisert i Den europeiske menneskerettskonvensjonen (EMK) artikkel 8 nr. 2 og EUs pakt om grunnleggende rettigheter artikkel 8.⁸ Paktens artikkel 8 nr. 1 beskriver beskyttelse av personopplysninger som en grunnleggende rettighet, og bestemmelsens nr. 2 fastsetter at personopplysninger skal behandles på grunnlag av de berørte personers samtykke eller «på et andet berettiget ved lov fastsatt grundlag».

Lovlighetsprinsippet har blitt tolket av både EMD og EU-domstolen. I avgjørelsen i de forente sakene mot *Österreichischer Rundfunk*⁹ av 20. mai 2003 vurderte EU-domstolen lovlighetsprinsippet og kravene til nasjonal lovgivning etter direktivet, tolket i lys av EMK artikkel 8. Dommen klargjør sentrale krav som følger av lovlighetsprinsippet.

Det følger av dommens premiss 72 at:

⁶ Se også bestemmelser i forordningens kapittel IX, for eksempel artikkel 88. Se også fortalens punkt 40.

⁷ Artikkel 29-gruppen uttaler i 08/2001 på side 3 seg om prinsippet «legitimacy». Der går det frem at artikkel 7 lister opp kriteriene for at en behandling oppfyller dette kravet. Det følger også av Artikkel 29-gruppens uttalelse 01/2006 side 7 at behandling er lovlig når det oppfyller et av grunnlagene i artikkel 7 i direktivet.

⁸ Forordnings fortale punkt 1 henviser til artikkel 8 nr. 1 i Den europeiske unions pakt om grunnleggende rettigheter.

⁹ Forente saker C-465/00, C-138/01 and C-139/01.

«Det er derfor af hensyn til anvendelsen af direktiv 95/46 og navnlig direktivets artikel 6, stk. 1, litra c), artikel 7, litra c) og e), og artikel 13 nødvendigt at undersøge for det første, hvorvidt en lovgivning, som den i hovedsagerne omhandlede, indebærer et indgreb i privatlivets fred og i så fald, om dette indgreb er berettiget i henhold til EMK's artikel 8.»»

Deretter vurderte EU-domstolen om det forelå et inngrep i retten til privatliv i premiss 73 til 75. Den påpeker blant annet i premiss 73 at «udtrykket «privatlivet» ikke skal fortolkes indskrænkende».

I premiss 77 uttalte domstolen at det var «ubestrideligt» at det aktuelle inngrepet var fastsatt i lov, men at spørsmålet var om denne bestemmelsen var «affattet tilstrækkelig præcist til, at lovens adressater kan tilpasse deres adfærd, og dermed opfylder kravet om forudsigelighed, som er fastslået i Menneskerettighedsdomstolens praksis (jf. bl.a. Menneskerettighedsdomstolens dom af 20.5.1999, Rekvényi mod Ungarn)»

I premiss 91 uttales det:

«Hvis de forelæggende retter fastslår, at de omtvistede nationale bestemmelser er uforenelige med EMK's artikel 8, kan bestemmelserne heller ikke oppfylle det proporsjonalitetskrav, der er fastsat i artikel 6, stk. 1, litra c), og artikel 7, litra c) og e) i direktiv 95/46.»

I premiss 92 presiserer domstolen at selv om lovgivningen er vurdert som nødvendig, og at den «står i et rimeligt forhold til det formål af almen interesse, som varetages», så må man i tillegg vurdere om den nasjonale lovgivningen oppfyller kravet om forutsigbarhet.

I «*Håndbog om europæisk databeskyttelseslovgivning*» oppsummerer EUs agentur for grunnleggende rettigheter (FRA), Europarådet og EMDs justiskontor rettspraksis om lovlighetsprinsippet fra EU-domstolen og EMD. I punkt 3.1 fremgår det at prinsippet om lovlig behandling tar utgangspunkt i «betingelserne for lovlige begrænsninger af retten til databeskyttelse i lyset av charterets artikkel 52, stk 1, og kravene til begrundede indgreb i artikel 8, stk 2, i den europæiske menneskerettighedskonvention.» .

Håndboken oppsummerer hovedpunktene slik: Behandling av personopplysninger er kun lovlig hvis den (1) er i overensstemmelse med loven, (2) forfølger et legitimt formål, og (3) er nødvendig i et demokratisk samfunn for å oppfylle det legitime formålet. I håndbokens punkt 3.1.1 gis det blant annet en nærmere beskrivelse av hva EMD mener med kravet om at en behandling skal være i overensstemmelse med loven:

«I henhold til Menneskerettighedsdomstolens retspraksis er indgreb i overensstemmelse med loven, hvis de er baseret på en bestemmelse i en national retsforskrift, som oppfylder bestemte kriterier. Retsforskriften skal være tilgjengelig, og virkningene af den skal være forudsigelige. En regel betragtes som forudsigelig, hvis den er formulert tilstrækkelig præcist til, at enhver person – om nødvendigt med passende

rådgivning – kan regulere sin adfærd. Kravene til retsgrundlagets klarhed afhænger i denne forbindelse af den konkrete sag».

I punkt 3.1.2 redegjøres det for lovlige begrensninger i henhold til EU-pakten. Det uttales blant annet at EU-pakten artikkel 52 nr. 3 siste punktum åpner for at

«...betingelserne for begrundede ingrep i medfør af artikel 8, stk. 2, i EMK er minimumskrav, for så vidt angår lovlige begrensninger af retten til databeskyttelse i henhold til charteret. Som følge deraf kræver lovlige behandling af personoplysninger i henhold til EU-retten at betingelserne i artikel 8, stk 2, i EMK som minimum er opfylt.»

Paktens artikkel 8 tilsvarer en rettighet som har blitt tolket inn under EMK artikkel 8. Dette gir klare føringer for hvordan lovlighetsprinsippet i forordningen skal tolkes, og hvilke krav som stilles til nasjonal lovgivning. EU-pakten er som kjent ikke en del av norsk rett, men artikkel 8 og 52 nr. 1 tilsvarer EMK artikkel 8,¹⁰ som er tatt inn i norsk rett i menneskerettsloven,¹¹ og det er dermed grunn til å anta at de omtalte rettsavgjørelsene vil ha betydning for forståelsen av lovlighetsprinsippet også i norsk intern rett.

3.3. Rettferdighetsprinsippet

Rettferdighetsprinsippet følger av forordningens artikkel 5 bokstav a. Prinsippet er et av de mest sentrale i direktivet, og videreføres i forordningen. Artikkel 29-gruppen har i en rekke uttalelser trukket frem dette prinsippet.¹²

Prinsippet er ikke gjennomført i personopplysningsloven § 11. Begrunnelsen for dette er ikke omtalt i lovforarbeidene.¹³ Vi mener derfor at det er hensiktsmessig å omtale prinsippet, og dets betydning, nokså utførlig i lovproposisjonen.

3.4. Formålsbegrensningsprinsippet

Formålsbegrensningsprinsippet i forordningens artikkel 5 nr.1 bokstav b fremstår som en videreføring fra direktivet artikkel 6 nr. 1 bokstav b. Dette gjelder både kravet til formålsspesifikasjon og kravet til ikke uforenlig gjenbruk. Det samme gjelder regelen om viderebehandling av opplysninger for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål. Dette prinsippet er tatt inn i personopplysningsloven § 11 første ledd bokstav c.

¹⁰ EU Domstolen, forente saker C-92/09 og C-93/09, Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen, 9. november 2010, paras. 51 og 52.

¹¹

Lov 1999-05-21-30 om styrking av menneskerettighetenes stilling i norsk rett.

¹² Se også «Håndbok om den europeiske databeskyttelseslovgivningen» punkt 3.4.

¹³ Se Ot.prp.nr92 (1998-199).

Prinsippet må gjelde for enhver behandling av personopplysninger, også der det rettslige grunnlaget er lovhjemmel. Eventuell uforenlig gjenbruk må hjemles i unntaket i direktivets artikkel 13.¹⁴ Dette følger av ordlyden i direktivet artikkel 5 og 6, og av praksis i EU-domstolen.¹⁵ Prinsippet om uforenlig gjenbruk har imidlertid sjelden blitt vurdert som en selvstendig begrensning på hva lovgiver kan vedta.¹⁶

Vi viser blant annet til forarbeidene til personopplysningsloven (Ot.prp. nr. 92 (1998-1999), side 112 i, der det uttales at «Når den senere bruken av opplysninger er bestemt i egen lov, vil denne bruken ikke være uforenelig med innsamlingsformålet». I rapport 2006 om utredning av behov for endringer i personopplysningsloven uttales det på side 178 at «[b]estemmelsen kan selvsagt ikke forstås slik at den legger begrensninger på hva lovgiver kan vedta.» I Stortingsmeldingen «Personvern og utfordringer» (Meld. St. 11 (2012-2013)) punkt 5, uttales det at «dersom det er gitt lovregler om at personopplysninger kan benyttes til et annet formål enn det opprinnelige, betegnes ikke slik behandling som gjenbruk.»

I Norge har altså formålsbegrensningsprinsippet ikke vært sett på som en skranke for lovgiver, bare for den behandlingsansvarlige. En slik forståelse later ikke til å være i samsvar med fortolkningen i EU-retten, som nevnt over.

Det er viktig at det fremgår klart av proposisjonen at dette prinsippet gjelder som en rettslig skranke ved utarbeidelse av lovhjemmel som behandlingsgrunnlag, og i sektorlovgivningen.¹⁷ Vi minner om at prinsippet i utgangspunktet gjelder for all behandling av personopplysninger for alle forvaltningsorganer.¹⁸ Det er derfor viktig at departementet gir veiledning om hvordan prinsippet skal praktiseres, for eksempel for den behandling som skjer etter forvaltningsloven og offentleglova. Det er også viktig å utforme noen formelle garantier som sikrer ivaretagelse av dette prinsippet.

For ordens skyld, vi er enig i at både gjeldende direktiv og forordningen åpner opp for å tillate uforenlig gjenbruk i nasjonal lovgivning, men dette må vurderes konkret og innenfor rammene til unntaksbestemmelse.

Lovforslag om unntak fra formålsbegrensningen ved lovpålagte tilsynsoppgaver

I høringsnotatets punkt 6.4.3 peker departementet på at det i dag er «en rekke lovregler i spesiallovgivningen» som åpner for viderebruk av personopplysninger til formål som ikke er forenelige med innsamlingsformålet, herunder regler om deling av informasjon mellom forvaltningsorganer til kontrollformål. Det pekes videre på at forordningens artikkel 6 nr. 4

¹⁴ Se nærmere i kapittel 9 om direktivet som et fullharmoniseringsdirektiv

¹⁵ Se for eksempel sak C-342/12 avsnitt 31 til 34. Der gikk domstolen inn på spørsmålet om noen bestemmelser i direktivet har til hinder for nasjonal lovgivning som pålegger en arbeidsgiver å stille sitt arbeidsregister til rådighet på en slik måte som muliggjør umiddelbar avlesning. Til dette spørsmålet uttalte domstolen blant annet at enhver behandling av personopplysninger skal foregå i overensstemmelse med artikkel 6 og artikkel 7, med enkelte unntak i artikkel 13. Se også dokumentet «Analysis and impact study on the implementation of Directive EC 95/46 in Member States» side 8 til 9 om ulik gjennomføringen av prinsippet i flere medlemsland.

¹⁶ Med mindre det kan gjøres unntak i direktivets artikkel 13.

¹⁷ Med mindre det kan gjøres unntak etter artikkel 23.

¹⁸ Se imidlertid begrensningen i artikkel 2 om saklig virkeområde.

åpner for å opprettholde slike regler. Det bes om høringsinstansenes syn på om det er behov for en bestemmelse som understrenger at formålsbegrensningen ikke er til hinder for at offentlige myndigheter som har til oppgave å håndheve lovgivningen om arbeidsmiljø, trygd, skatter og avgifter og utveksler informasjon så langt det er nødvendig for å utføre en tilsynsoppgavene, som foreslått i lovforslaget § 12.

Som nevnt over mener vi det er problematisk at lovgiver ofte ikke foretar en reell vurdering av hvorvidt den nye bruken er uforenelig med det opprinnelige formålet og det ikke gjøres noen vurdering av om en eventuell uforenelig gjenbruk kan hjemles i unntaket i direktivets artikkel 13. Vi mener departementet i høringsnotat bidrar til dette ved å ikke få tydelig frem at unntak fra prinsippet om uforenelig gjenbruk må hjemles i forordningens artikkel 23 nr. 1 og nr. 2.

Lovforslagets § 12 er problematisk. Det må først foretas konkrete vurderinger av om den aktuelle spesiallovgivningen (om arbeidsmiljø, trygd, skatt og avgifter) faktisk er i strid med forbudet om ikke uforenelig gjenbruk. Hvis dette er tilfellet må det vurderes om det kan gjøres spesifikke unntak fra prinsippet etter kravene i artikkel 23 nr.1 og nr. 2. Slike vurderinger bør trolig foretas av de ulike departementer innenfor sin sektorlovgivning. Det fremgår ikke av høringsbrevet hvilke vurderinger som konkret er gjort, herunder av artikkel 23 nr. 1. og nr. 2

Som departementet skriver foregår det utveksling av informasjon mellom offentlige etater på en rekke områder. Vi tror det vil kunne bli mer forvirrende enn oppklarende fordi departementet trekker frem ett område i den generelle personopplysningsloven hvor det foregår samarbeid, uten å ha sett på andre områder. Vi får ofte spørsmål om adgang til utveksling av informasjon innen justissektoren, for eksempel på utlendingsfeltet, de ulike tjenestene som kommunene tilbyr, for eksempel barnevern, helsetjeneste og skole, og mellom ulike aktører innen samferdselssektoren.

Vårt generelle inntrykk er at de aktuelle instansene ofte er mest opptatt å om de har tilstrekkelige unntak fra taushetspliktreglene, og i for liten grad vurderer de krav som følger av personvernreglene. En slik generell bestemmelse i personopplysningsloven vil ikke bidra til at bedre oppmerksomhet omkring kravene som følger av personvernreglene, heller tvert imot.

3.5.Dataminimering og proporsjonalitet

Dataminimerings- og proporsjonalitetsprinsippet i forordningens artikkel 5 nr. 1 bokstav c er etter vårt syn i stor grad er en videreføring fra direktivet artikkel 6 nr. 1. bokstav c.¹⁹ Dette prinsippet er omtalt kort på side 21 i høringsnotatet. Vi mener prinsippet bør omtales bredere i proposisjonen. Dette for å sikre at dagens sektorlovgivning og nye lover er i samsvar med kravene i forordningen.

¹⁹ Det er enkelte språklige nyanser og forskjeller mellom ordlyden i den danske direktiv- og forordningsbestemmelsen om dette prinsippet. Det samme gjelder for de tilsvarende engelske bestemmelsene.

Tolkningen av prinsippet etter personopplysningsloven synes å avvike noe fra direktivet, og vi mener at dette burde ha vært belyst i høringsnotatet. Personopplysningsloven § 11 bokstav d sier at personopplysningene skal være tilstrekkelige og relevante for formålet med behandlingen. Den norske bestemmelsen skiller seg fra den engelske som bruker formuleringen «adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed».

I norsk rett er oppfatningen at «tilstrekkelig» innebærer et krav om at opplysningsgrunnlaget må være så *fullstendig* som behandlingsformålet krever.²⁰ Problemet med en slik tolkning er at vilkåret kan trekke i retning av krav om flere opplysninger, og ikke minimalitet. At den behandlingsansvarlige skal sikre at opplysningsgrunnlaget skal være så fullstendig som mulig, gir etter vår vurdering et større rom for behandling av personopplysninger enn krav om at behandlingen blant annet skal være «adequate» og «not excessive».²¹

Samlet sett betegnes reglene i direktivets artikkel 6 nr. 1 bokstav c som proporsjonalitetsprinsippet. Kravene som artikkelen oppstiller er strenge. Dette forholdet har imidlertid ikke alltid kommet tilstrekkelig frem i norsk praksis eller juridisk teori. I *Österreichischer Rundfunk* premiss 91, ble forholdet til det tilsvarende prinsippet i EMK artikkel 8 vurdert. Det fremgår av denne avgjørelsen at direktivets bestemmelse om proporsjonalitet oppstiller et like strengt krav som EMK artikkel 8. Vi legger til grunn at det samme må gjelde også etter forordningen.

Prinsippet er i norsk rett relevant både for vurderingen av forordningens artikkel 5 nr. 1 bokstav c og for vurderingen av nasjonale regler som bygger på artikkel 6 nr. 1 bokstav c og e. Et praktisk eksempel i dag er vurderingen av prinsippet ved etablering av sentrale helseregistre, hvor det egentlig ikke er noen grenser for hvilke opplysninger som kan være ønskelige å registrere for ubestridt gode formål.²² En klargjøring av innholdet i dette grunnleggende prinsippet ville etter vårt syn tvunget frem utredninger av personvernkonsekvenser som i dag ikke gjøres tilstrekkelig ved opprettelse av de fleste helseregistre.

4. Behandlingsgrunnlag

4.1. Innledning

Forordningens artikkel 6 nr. 1 bokstav a til f oppstiller seks alternative behandlingsgrunnlag for lovlig behandling av personopplysninger. Minst ett av grunnlagene må være oppfylt for at en behandling av personopplysninger skal være lovlig. Grunnlagene i bokstav c (rettslig

²⁰ Se Ot.prp.nr.92 (1998-1999) side 114 hvor det går det frem at i kravet til at personopplysningene «må være tilstrekkelige, ligger at opplysningsgrunnlaget må være så fullstendig som behandlingsformålet krever.» Peter Blume tolker det danske begrepet «tilstrækkelige» dit hen at «der ikke må indsamles flere oplysninger, end det er påkrævet for at kunne opfylde formålet.» Se Peter Blume «Den nye persondataret» side 73.

²¹ Det vises også fortalen i forordningen punkt 39 om at «Personopplysninger bør kun behandles, hvis formålet med behandlingen ikke med rimelighed kan opfyldes på anden måde.»

²² Se også Innst.O.nr.62 (2000-2001) punkt 2.1

forpliktelse) og bokstav e (oppgave i offentlighets interesse mv.) krever et supplerende rettslig grunnlag i nasjonal rett, jf. den samme artikkelens nr. 3.

Behandlingsgrunnlagene i artikkel 6 er i stor grad en videreføring av behandlingsgrunnlagene personverndirektivet artikkel 7.²³ Dette er også lagt til grunn i flere utredninger om personvernforordningen, se for eksempel den danske og den svenske utredningen.²⁴

Datatilsynet mener at høringsnotatets beskrivelse av kravene til behandlingsgrunnlag er ufullstendig, og på enkelte punkter er vi dessuten uenige med departementet. Slik vi ser det, mangler høringsnotatet omtale av sentrale rettskilder som belyser disse kravene. Vi mener derfor at departementet på flere punkter legger til grunn mindre strenge krav til nasjonale regler enn det som følger av forordningen.

4.2. Om behandlingsgrunnlaget «fastsatt i lov» og norsk praksis

Departementet skriver i punkt 7.1.2 i høringsnotatet at grunnlaget «fastsatt i lov» i personopplysningsloven § 8 ikke har noen parallell i forordningen. Videre står det at «[d]ette antas imidlertid ikke å medføre noen realitetsendring». Departementet viser til at det ikke er kjent med lovbestemmelser som gir adgang til behandling av personopplysninger uten at behandlingen har «tilknytning» til utførelsen av en oppgave i allmennhetens interesse, utøvelse av offentlig myndighet eller oppfyllelse av en rettslig forpliktelse, jf. forordningens artikkel 6 nr. 1 bokstav e og c.

Vi mener at det er uriktig at dette ikke er en realitetsendring. Grunnlaget «fastsatt i lov» i § 8 har vært forstått og praktisert som et *alternativ* til de andre grunnlagene opplistet i personopplysningsloven § 8 og direktivets artikkel 7. I direktivets artikkel 7, på samme måte som i forordningen, er ikke lovhjemmel et selvstendig alternativ. Måten man har valgt å implementere direktivet på i norsk rett, har ført til at dette ved overgang til forordningen faktisk vil bli en reell endring. I tillegg oppstiller direktivet og forordningen andre krav til nasjonale regler enn det som har vært praktisert i Norge. Vi kommer tilbake til Artikkel 29-gruppens tolkning av artikkel 7 bokstav c og e i punktene 4.3 nedenfor.

I høringsnotatets punkt 7.1.3 går departementet gjennom kravene til supplerende rettsgrunnlag etter forordningen artikkel 6 nr. 1 bokstav c og e, og nummer 2 og 3. De viser her til at forordningen skiller seg fra personopplysningsloven ved at lovens § 8 bokstav b, d og e *ikke* stiller krav om supplerende rettslig grunnlag.

Vi er enige med departementet i at § 8 bokstav d og e ikke krever et supplerende rettslig grunnlag.

²³ Sml. Artikkel 29-gruppens uttalelse 6/2014 på side 9.

²⁴ Se Databeskyttelsesforordningen – og de rettslige rammer for dansk lovgivning Del I – bind 1 punkt 3.3 og SOU 2017: 39 punkt 8.2.

Departementet ber om høringsinstansenes tilbakemelding på om det finnes tilfeller der disse alternativene til grunnlag brukes i dag og det ikke i dag foreligger supplerende rettsgrunnlag som fyller vilkårene som følger av forordningen artikkel 6 nr. 1 bokstav c og e.

For å kunne komme med innspill her, ville det ha vært nødvendig med en svært grundig analyse av eksisterende sektorlovgivning. Noen slik analyse har vi ikke hatt anledning til å gjennomføre i denne omgang. På noen områder vet vi at det behandles personopplysninger basert på personopplysningsloven § 8 bokstav d og e, og som ikke har hjemmel i lov. Lovens § 8 bokstav d brukes for eksempel mye i forskning.²⁵ Bestemmelsen i § 8 bokstav e er også et praktisk grunnlag for behandling som er nødvendig for offentlig myndighetsutøvelse, men som ikke har et supplerende rettslig grunnlag.²⁶ Vi kommer tilbake med våre innspill om sektorlovgivning om forskning nedenfor i kapittel 6.

4.3. Nærmere om krav til supplerende rettslig grunnlag

Departementets vurdering av krav til supplerende rettslig grunnlag

Departementet går i punkt 7.1.3 gjennom de nærmere kravene som stilles til supplerende rettslig grunnlag etter forordningens artikkel 6 nr.1 bokstav c og e, jf. nummer 2 og 3.

Departementet sier at ordlyden i artikkel 6 nr. 3 er uklar, men at den gir grunnlag for to slutninger om hva det rettslige grunnlaget *må* inneholde, og hva det rettslige grunnlaget *kan* (men ikke *må*) inneholde.

Departementet forstår forordningen artikkel 6 nr. 1 bokstav c og e, sammenholdt med nr. 3, slik at forordningen ikke oppstiller formelle krav til innholdet av det rettslige grunnlaget bortsett fra at det for behandlingen som bygger på bokstav c med rimelig grad av klarhet må kunne utledes et eller flere formål fra rettsgrunnlaget.

Etter departementets syn vil en lov eller forskrift som gir et rettssubjekt rett eller plikt til å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet, og der utføringen av disse oppgavene direkte eller indirekte forutsetter behandling av personopplysninger, tilfredsstille kravet til rettslig grunnlag. Det stilles ikke krav om at det supplerende rettslige grunnlaget eksplisitt regulerer behandling av personopplysninger.

Departementet påpeker imidlertid at det ved utformingen av nasjonale lov- eller forskriftsbestemmelser ikke bør være et mål i seg selv å kun oppfylle de minimumskrav

²⁵ Se for eksempel PVN-2002-6, PVN-2004-04. Et mer korrekt behandlingsgrunnlag ville trolig vært § 8 bokstav f.

²⁶ Se for eksempel Schartum og Bygrave «Personvern i informasjonssamfunnet» 2010 side 165. Der uttales følgende om bokstav e: «Bestemmelsen innebærer at et forvaltningsorgan kan behandle alle personopplysninger som er nødvendige for å treffe enkeltvedtak eller treffe andre avgjørelser mv. Innhentning av samtykke eller identifisering av klar lovhjemmel er således ikke nødvendig. Dersom myndigheten som ledd i saksbehandlingen også ønsker å samle inn opplysninger som ikke er nødvendige for å utøve offentlig myndighet (for eksempel ved gjennomføre brukerundersøkelse) er det ikke omfattet fordi det ikke er «nødvendig».

forordningen oppstiller til rettslig grunnlag etter artikkel 6 nr. 1 bokstav c og e. Departementet peker videre på at mer spesifikke bestemmelser enn det forordningen krever ofte vil være «ønskelig av personvern- og rettsikkerhetsgrunner.»

Vår vurdering – generelle krav til nasjonal lovgivning etter fellesskapsretten

Vi mener at de generelle betingelse for lovlig behandling i artikkel 5 oppstiller sentrale og konkrete krav til lovgiver. For det første oppstiller artikkel 5 nr. 1 bokstav a krav til innholdet i det supplerende rettslige grunnlaget etter forordningens artikkel 6 nr.1 bokstav c og e. Vi viser her til gjennomgangen av prinsippet om lovlig behandling ovenfor i. Österreichischer Rundfunk-dommen er relevant for vurderingen av kravene til klarhet, nødvendighet og proporsjonalitet i artikkel 5 og 6. En lovbestemmelse som ikke oppfyller kravene til klarhet, nødvendighet eller forholdsmessighet i EMK artikkel 8 nr. 2, vil heller ikke oppfylle de tilsvarende kravene i forordningen.

Formålsbegrensningsprinsippet i artikkel 5 nr. 1 bokstav b er også relevant i denne sammenheng. Bestemmelsen oppstiller krav om formålsspesifikasjon og forbud mot gjenbruk av personopplysninger til nye og uforenlige formål. Krav til formålsspesifikasjon innebærer at enhver behandling av personopplysninger skal innsamles til spesifikke, uttrykkelig angitte og berettigede formål. Lovgiver må dermed forholde seg til spesifikasjonskravet ved utarbeidelse av supplerende rettslig grunnlag etter artikkel 6 nr.1 bokstav c og e.²⁷

Lagringsbegrensningsprinsippet i artikkel 5 nr. 1 bokstav e kan også nevnes som en relevant rettslig ramme for nasjonal lovgivning. Vi viser i den forbindelse til dom av 7. mai 2009 fra EU-domstolen om det tilsvarende prinsippet i direktivet.²⁸

«Ifølge stk. 1, litra e), skal medlemsstatene fastsette bestemmelser til sikring af, at personopplysninger ikke opbevares i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil de indsamles, eller med henblik på hvilke de behandles på et senere tidspunkt. Oplysningerne skal altså slettes, når disse formål er opfyldt.»

I «*Håndbok om europæisk databeskyttelseslovgivning*» punkt 3.3.3 gis det også en beskrivelse av prinsippet i direktivet og Europarådskonvensjonen, og hvordan lagringsbegrensningsprinsippet har blitt trukket frem i praksis fra EMD.

Det stilles også andre krav til rettslige grunnlag som bygger på artikkel 6 nr. 1 bokstav c og e. Kravene til nasjonal lovgivning har blitt tolket av EU-domstolen og Artikkel 29-gruppen. Det er viktig å merke seg at EU-domstolen har fastslått at begrepet «nødvendig» er et selvstendig fellesskapsrettslig begrep.²⁹ Også begrepet «oppgave i allmennhetens interesse» etter artikkel

²⁷ Se også C-342/12. Se også Artikkel 29-gruppens uttalelse 03/2013, se også eksempel 13 og 14 på side 54 som belyser forholdet mellom spesifikasjonskravet og nasjonal lovgivning.

²⁸ Se EF-domstolens dom i prejudisiell sak av 7. mai 2009, C-553/07, punkt 33.

²⁹ Se sak C-524/06 punkt 52: «I betragtning af hensynet til at sikre et ensartet beskyttelsesniveau i alle medlemsstater må nødvendighedsbegrebet i artikel 7, litra e), i direktiv 95/46, som netop har til formål at afgrænse et af de tilfælde, hvor behandling af personopplysninger er lovlig, følgelig ikke tillægges forskelligt indhold i medlemsstaterne. Dermed er det et selvstændigt fællesskabsretligt begreb, som skal fortolkes i fuld

6 nr. 1 bokstav e er et fellesskapsrettslig begrep.³⁰ Medlemslandene står altså ikke fritt til selv å definere hvilke behandlinger av personopplysninger som omfattes av de nevnte begrepene.

Artikkel 29-gruppens tolkning

Artikkel 29-gruppen har gjort en tolkning av de tilsvarende grunnlagene i direktivets artikkel 7 bokstav c og e i uttalelse 6/2014.

Om direktivets artikkel 7 bokstav c, om rettslige forpliktelser, uttales det at nasjonal lovgivning må oppfylle alle relevante betingelser for at forpliktelsen skal være gyldig og bindende. Deretter peker gruppen på at den også skal være i overensstemmelse med:

«databeskyttelseslovgivningen, herunder kravet om nødvendighet, proportionalitet og formålsbegrænsning.»

Når det gjelder det supplerende rettslige grunnlaget gis det føringer på krav til klarhet og formålsangivelse:

«Den retlige forpliktelse skal være tilstrækkelig klar med hensyn til den behandling af personoplysninger, den kræver. Artikel 7, litra c), gælder således på grundlag af retlige bestemmelser, der udtrykkeligt henviser til karakteren af og genstanden for databehandlingen. Den registeransvarlige må ikke have unødige skønsbeføjelser med hensyn til, hvordan den retlige forpliktelse skal overholdes.

I nogle tilfælde fastlægger lovgivningen kun et generelt formål, mens mere specifikke forpliktelser pålægges på et andet niveau, f.eks. i sekundær lovgivning eller ved bindende afgørelse truffet af en offentlig myndighed i en konkret sag. Dette kan også føre til retlige forpliktelser efter artikel 7, litra c), hvis databehandlingens art og genstand er veldefineret, og den sker på et hensigtsmæssigt retligt grundlag.»

Når det gjelder direktivets artikkel 7 bokstav e, gis det blant annet veiledning om kravet til supplerende rettslig grunnlag når behandlingen innebærer en krenkelse av privatlivets fred, og om kravet til identifisering av den samfunnsmessige interessen:

«Hvis databehandlingen medfører en krænkelse af privatlivets fred, eller hvis dette på anden måde er påkrævet i henhold til national lovgivning af hensyn til beskyttelsen af de berørte personer, skal det retlige grundlag tilstrækkeligt specifikt og præcist angive den type behandling af personoplysninger, der tillades.»

overensstemmelse med direktivets formål, som det er formulert i dets artikkel 1, stk. 1.» (Vår utheving) Se også Artikkel- 29s uttalelse 06/2014 punkt II.3.

³⁰ Se SOU 2017: 39 side 122-123. Artikkel 29-gruppen har nedsatt en arbeidsgruppe som skal gi veiledning til sentrale bestemmelser og begrep i forordningen, se Artikkel 29-gruppen Work programme 2016-2018, dok. 417/16/EN. Forhåpentligvis kommer begrepet "oppgave i allmennhetens interesse" å belyses nærmere i dette arbeidet.

Det uttales også at artikkel 7 bokstav e potensielt har et meget bredt anvendelsesområde, og at «det fordrer en streng fortolkning og klar identifikasjon af den berørte samfundsmæssige interesse og den offentlige myndighedsudøvelse, der berettiger databehandlingen.»

EDPS' veileder om nødvendighetskravet

EDPS³¹ har utarbeidet en veileder «Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit»,³² til lovgivere i EU om hvordan spesielt kravet til nødvendighet skal vurderes i lovgivningsarbeid. Det gis også en vurdering av forholdet mellom krav til proporsjonalitet og nødvendighet, samt forholdet mellom pakten og EMK. Veiledning til proporsjonalitetskravet er opplyst å komme i et eget dokument.³³

Beskrivelsen av retten til personopplysningsvern og forholdet til retten til privatliv

EPDS trekker i punkt 5 frem hvordan nødvendighetstesten skal vurderes opp mot den grunnleggende retten til personopplysningsvern.

Retten til personopplysningsvern og retten til privatliv etter EMK artikkel 8 er to forskjellige størrelser. Terskelen for når en behandling anses for inngrep i retten til personopplysningsvern er i EU-retten satt lavt. EPDS er pekt på at EU-domstolen har kommet til at:³⁴

«an act constitutes an interference with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter because it provides for the processing of personal data. In principle, therefore, any data processing operation (such as collection, storage, use, disclosure of data) laid down by legislation is a limitation on the right to the protection of personal data, regardless of whether that limitation may be justified.»

EPDS peker videre på andre forhold som er relevant for vurderingen av når nasjonal lovgivning griper inn i retten til personopplysningsvern:

«Furthermore, the CJEU has held in the vast majority of the cases dealing with legislative acts that a processing operation limited both the right to the protection of personal data and the right for respect of private life. The Court has held also that for the establishment of a limitation “*it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way*”».

Sjekklisten

EDPS har utarbeidet en nyttig sjekkliste for «new legislative measures», som også er relevant for lovgivning etter forordningen. I veilederens side 9 til 24 er det utarbeidet en sjekkliste. Vi kan i denne sammenheng vise til hovedpunktene i sjekklisten på side 9:

³¹ European Data Protection Supervisor, som er EUs datatilsynsombudsmann.

³² https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf

³³ Se side 4.

³⁴ Se veilederens fotnote 32. Der er det vist til en rekke avgjørelser fra EU-domstolen om underbygger standpunktet.

«The Checklist for assessing necessity consists of four consecutive steps. Each step corresponds to a set of questions which will facilitate the assessment of necessity.

Step 1 is preliminary; it requires a detailed factual description of the measure proposed and its purpose, prior to any assessment.

Step 2 will help identify whether the proposed measure represents a limitation on the rights to the protection of personal data or respect for private life (also called right to privacy), and possibly also with other rights.

Step 3 considers the objective of the measure against which the necessity of a measure should be assessed;

Step 4 provides guidance on the specific aspects to address when performing the necessity test, in particular that the measure should be effective and the least intrusive.

If the assessment of any of the elements detailed in Steps #2 to #4 leads to the conclusion that a measure might not comply with the requirement of necessity, then the measure should either not be proposed, or should be reconsidered in line with the results of the analysis.»

Veilederen er relevant for lovgiver i Norge

Vi mener veilederen også er relevant for lovgiver i Norge. Den kan utgjøre et viktig utgangspunkt for utarbeidelse av en utredningsinstruks som oppstiller formelle garantier på ivaretagelse av de krav som følger av forordningen.

Datatilsynets vurdering av departementets redegjørelse for krav til nasjonale regler

Departementet har utelatt å omtale fortalens punkt 41 om krav til tydelige, presise og forutsigbare regler. I dette punktet fremgår det at det stilles krav til nasjonal lovgivning, jf. også forordningens artikkel 5 nr. 1 bokstav a, som det nevnte punktet i fortalen er egnet til å belyse.

Vi er ikke enige med departementet i at krav til nasjonalt rettsgrunnlag utelukkende skal baseres på slutninger av ordlyden i artikkel 6 nr. 3 om hva det rettslige grunnlaget *må* inneholde og hva det *kan* (men ikke *må*) inneholde.

Siden artikkel 6 nr. 3 favner om svært vidt bred spekter av behandlinger av personopplysninger, ville det ikke vært mulig å i forordningen foreskrive en liste av elementer som det supplerende rettsgrunnlaget *skal* inneholde. Det følger også av artikkel 6 nr. 3 og fortalens punkt 45 at medlemsstatene har et nasjonalt handlingsrom til å presisere forordningens generelle betingelser for disse rettslige grunnlagene.

Vi er videre uenig i departementets tolkning av at artikkel 6 nr. 3 ikke oppstiller noe krav om at formålet med behandlinger som er hjemlet i bokstav c må fremgå eksplisitt av en egen

lov/forskriftsbestemmelse, men at det er tilstrekkelig at det fremgår mer indirekte gjennom det rettslige grunnlaget, for eksempel i lovforarbeidene.

Slik vi forstår høringsnotatet mener departementet at det etter forordningen *alltid* er tilstrekkelig at formålet fremgår mer *indirekte* gjennom det rettslige grunnlaget, for eksempel i lovforarbeider. Dette mener vi vanskelig lar seg forene med ordlyden «[f]ormålet skal være fastlagt i dette rettsgrunnlag». Vi kan heller ikke se at departementets oppfatning er i overensstemmelse med kravene til klarhet og formålsspesifikasjon som følger av artikkel 5 nr. 1 bokstav a og b, og fortalens punkt 41. Det er også vanskelig å finne støtte for en slik tolkning i den ovenfor nevnte uttalelsen fra Artikkel 29-gruppen om det tilsvarende grunnlaget i direktivets artikkel 7 bokstav c.

Vi er også uenige i departementets vurdering av krav til rettslig grunnlag som bygger på bokstav e. Departementet peker på at det etter forordningens ordlyd kun kreves at formålet med behandlingen skal være nødvendig for å utøve en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt. Det stilles ikke krav om at det supplerende grunnlaget eksplisitt regulerer behandling av personopplysninger. Vi har også her problemer med å se at departementets forståelse er forenlig med de krav til klarhet og formålsspesifikasjon som følger av artikkel 5 nr.1 bokstav a og b.

Forordningen oppstiller særlige strenge krav til nødvendighetsvurderingen for dette rettslige grunnlaget fordi det potensielt har et meget bredt anvendelsesområde. Det innebærer en klar identifikasjon av den berørte samfunnsmessige interessen og den offentlige myndighetsutøvelsen som berettiger behandlingen av opplysninger, se uttalelsen fra Artikkel 29-gruppen. Vi kan ikke se at dette forholdet kommer klart frem i høringsnotatet.

Et annet poeng er at lover som bygger på dette rettslige grunnlaget i mange tilfeller innebære behandlinger som griper inn i privatlivets fred. Ut fra Artikkel 29-gruppens uttalelse skal det rettslige grunnlaget i slike tilfeller «tilstrækkeligt specifikt og præcist» angi den type behandling av personopplysninger som tillates. Vi mener derfor at det er flere momenter i artikkel 6 nr. 3 som er relevante å spesifisere i nasjonal lov/forskrift i et tilfelle hvor behandlingen griper inn i retten til privatlivets fred.

Vi minner også om at det er lovgiver og norske myndigheter som må kunne sannsynliggjøre at en lovbestemmelse oppfyller det grunnleggende krav til proporsjonalitet når det gjelder avveiningen mellom personopplysningsvern og samfunnsinteresser.³⁵ Vi bemerker i den forbindelse at EU-domstolen i flere saker har vurdert lovgivning i EU-medlemsland opp mot proporsjonalitetsprinsippet.³⁶

Departementet skriver også i høringsnotatet at det prinsipielt må skilles mellom kravene til supplerende rettsgrunnlag i forordningen og hjemmelskravet som oppstilles etter legalitetsprinsippet og Grunnlovens § 102.

³⁵ Proporsjonalitetskravet følger av både artikkel 5 nr. 1 bokstav c og artikkel 6 nr. 1 bokstav c og e.

³⁶ Se C-92/09 og C-93/09.

Slik vi forstår dette mener departementet at lovhjemler, som strengt tatt ikke er presise nok til for å oppfylle kravene etter Grunnloven og legalitetsprinsippet, likevel kan være i tråd med forordningen. Vi mener at det har liten hensikt å trekke å slikt prinsipielt skille, og stiller også spørsmål ved om det er en riktig slutning. Departementet nevner riktignok ikke EMK, men bare legalitetsprinsippet og Grunnloven. Slik vi forstår det vil en lovbestemmelse i strid med Grunnloven, jf. Grunnloven § 92, også være i strid med EMK – og dermed også forordningen.

For å oppsummere: Vi mener at den ovenfor nevnte gjennomgangen viser at forordningen artikkel 5 og artikkel 6 nr. 1 bokstav c og e, jf. nummer 3 oppstiller strengere krav til nasjonalt rettsgrunnlag enn det departementet tilsynelatende legger til grunn. Vi viser særlig til at lovgiver må forholde seg til kravene til klarhet, nødvendighet, proporsjonalitet og formålsbegrensning.³⁷ Andre prinsipper som gjennomsiktighet, rettferdighet og lagringsbegrensning kan også oppstille krav til nasjonal lovgivning.

Hvis det i tillegg skal behandles sensitive personopplysninger må rettsgrunnlaget også oppfylle de ytterligere betingelser som følger av artikkel 9, herunder krav til nødvendige garantier. Se mer om slike i gjennomgangen av artikkel 9 i kapittel 5 og 6. Vi mener forordningen samlet sett oppstiller nokså strenge krav til det supplerende rettslige grunnlaget.

Datatilsynet mener at kravene til nasjonale regler etter artikkel 5 og artikkel 6 nr. 1 bokstav c og e, jf. nummer 3, vil avhenge av en *konkret vurdering i hvert enkelt tilfelle* hvor det blant annet må tas stilling til i hvilken grad behandlingen griper inn i retten til personopplysningsvern etter forordningen, og eventuelt retten til privatliv etter EMK artikkel 8, samt hvilke garantier som eventuelt kan avhjelpe ulempene for de aktuelle registrerte. Terskelen for når nasjonale regler anses for å utgjøre et inngrep i retten til personopplysningsvern er lav i EU-retten.³⁸ Dette bør lovgiver i Norge være oppmerksom på.

Departementets beskrivelse av kravene etter artikkel 6 nr. 3 i proposisjonen kan få stor betydning for hvilke krav som stilles til sektorlovgivningen, både ved innføringen av forordningen, men også fremover. Vi ser fra tid til annet eksempler på lovgivning som ikke er tilstrekkelig klar. Ett eksempel er kommuneloven § 77 nr. 7 og hvorvidt den er tilstrekkelig klar og gir nødvendig garantier for at et kontrollutvalg i en kommune kan gjennomføre innsyn i ansattes e-post. Et annet eksempel er om personopplysningsloven § 8 bokstav f og § 9 bokstav e kan utgjøre et tilstrekkelig rettslig grunnlag for behandling av personopplysninger ved skjult overvåking av forsikringskunder, eller om slik behandling krever et supplerende rettslig grunnlag.³⁹ Både underrettspraksis og de norske datatilsynsmyndighetene sitt syn på det siste spørsmålet spriker.⁴⁰

³⁷ I Österreichischer Rundfunk dommen punkt 91 trekkes proporsjonalitetskravet også frem i direktivets artikkel 7 bokstav c og e.

³⁸ Jf. EDPS' veileder «Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit»

³⁹ Et supplerende rettslig grunnlag kunne for eksempel vært vurdert etter direktivets artikkel 7 bokstav e og artikkel 8 nr. 4.

⁴⁰ Det vises spesielt til LB-2014-48321, LB-2014-35455 og PVN-2013-20. Se også vår sak 16/00657-5 om lovligheten av skjult overvåking.

Dersom det i proposisjonen legges stor vekt på hva lovgiver *kan* og *skal* regulere, er vi redd for det kan få en uheldig signaleffekt. Vi er opptatt av at det i fremtidig arbeid med særlovgivningen blir lagt vekt på hva som gir forutsigbarhet og på best mulig måte ivaretar personvern hensyn. Det er derfor uheldig hvis listen for hva som *må* gjøres legges for lavt.

5. Behandling av sensitive personopplysninger

Datatilsynet er enig i det departementets skriver innledningsvis i høringsnotatets punkt 8.2, om at artikkel 6 og 9 skal anvendes kumulativt når det behandles sensitive personopplysninger. I forordningen er dette muligens enda tydeligere enn i direktivet når artikkel 6 nå er formulert som en bestemmelse om lovlig behandling, noe som gjør koblingen til lovlighetsprinsippet klarere. Det er neppe tilfeldig at artikkel 6 er formulert slik, mens artikkel 9 er formulert som et forbud med visse unntak. Det er naturlig å forstå dette som at krav til rettslig grunnlag først og fremst må utledes av artikkel 6, mens artikkel 9 setter ytterligere betingelser.⁴¹

Flere av unntakene i artikkel 9 nr. 2 i forordningen er i stor grad en videreføring av direktivets artikkel 8. Det er også noen klare forskjeller, bokstav i og j bygger ikke direkte på noen unntaksbestemmelser i direktivet, men direktivets generelle unntak i artikkel 8 nr. 4 kan antageligvis sies å gi rom for slike unntak etter dagens regelverk også.

En sentral uttalelse fra Artikkel 29-gruppen på dette området er WP 131. Uttalelsen gjelder behandling av helseopplysninger i elektroniske pasientjournaler. I uttalelsen foretas en gjennomgang av flere av unntakene i direktivets artikkel 8, som i stor grad videreføres i forordningens artikkel 9. Et viktig poeng er at Artikkel 29-gruppen peker på at unntakene i artikkel 8 er «begrænsede, udtømmende og skal tolkes snævert.»⁴² Dette innebærer at all gjeldende sektorlovgivning må være innenfor de unntakene som følger av direktivet artikkel 8. Vi kan her nevne at vi i praksis har sett at Personvernemnda har åpnet opp for et nytt ulovfestet grunnlag (etter en interesseavveining) for behandling av personopplysninger etter personopplysningsloven § 9.⁴³ Vi vurderer det som tvilsomt at dette er i tråd med de forpliktelser som følger av direktivets artikkel 8.⁴⁴

⁴¹ Artikkel 29-gruppen uttalelse 06/2014 side 15 og fotnote 30 foretatt en tolkning av forholdet mellom direktivets artikkel 7 og 8. Bestemmelsene er like med forordningen i form av at artikkel 7 gir et rettslig grunnlag, mens artikkel 9 er utformet som en forbudsbestemmelse. I fotnoten uttales det at «Da artikkel 8 er formulert som et *forbud med undtagelser*, kan disse undtagelser fortolkes som krav, der kun begrænser omfanget af forbuddet, men tilvejebringer ikke i sig selv et tiltrækkelig retsgrundlag for behandlingen.» (Vår utheving)

⁴² Se side 8.

⁴³ I PVN-2016-10 har Personvernemnda lagt til grunn at personopplysningsloven § 9 gir rom for at også sensitive personopplysninger kan behandles etter en interesseavveining hvor de hensyn som tilsier behandling (retten til å fremsette ytringer og allmennhetens tilgang på informasjon) holdes opp imot de hensyn som trekker i motsatt retning (vernet av omdømmet og privatlivets fred).

⁴⁴ I Artikkel 29-gruppens uttalelse WP 55 side 17 slås det også fast at direktivets artikkel 8 ikke åpner for muligheten til avveining av interesser slik direktivets artikkel 7 bokstav f gjør.

For vi går inn på de konkrete behandlingsformålene som departementet tar opp i notatet vil vi si noe generelt om hvordan vi forstår på kravene til nasjonale regler for behandling av sensitive personopplysninger, herunder krav til nødvendige garantier mv. i nasjonale regler. Våre merknader til lovforslagets § 6 om arkiv, statistikk og forskningsformål følger av kapittel 6.

5.1. Om krav til nasjonale regler som gjelder behandling av sensitive opplysninger

Departementet drøfter i liten grad kravene til nasjonale regler for behandling av sensitive personopplysninger. Vurderingen er basert på ordlyden i artikkel 9 om krav til «grunnlag» og at behandlingen må være «tillatt», og de skriver at formålet med artikkel 9 kan tilsi at det «kan gjelde et noe strengere krav til lovgrunnlaget enn det som kreves i artikkel 6 nr. 3.» Når det offentlige behandler personopplysninger pekes det også på at legalitetsprinsippet stiller krav til lovhjemmelens klarhet, jf. Grunnlovens § 102.

Vi mener departementets burde gått nærmere inn de krav som kan utledes av forordningen på dette området, herunder prinsippet om lovlig behandling etter artikkel 5 nr.1 bokstav a og de krav til nasjonale regler som følger spesifikt av artikkel 6. Vi savner at departementet peker på hvilke rettslig grunnlag i artikkel 6 som er aktuelle i vurderingen av unntakene i artikkel 9 nr. 2, og hvilken betydning bestemmelsene samlet sett har når det gjelder krav til nasjonale regler. Vi viser til det vi har sagt tidligere om forholdet til legalitetsprinsippet og Grunnloven i kapittel 4.2

For eksempel kunne det vært vist til, innledningsvis og i gjennomgangen av de enkelte grunnlagene i artikkel 9, de punktene i fortalen som gir veiledning til hvordan de ytterligere kravene til nasjonale regler i artikkel 9 nr. 2 skal forstås. Fortalen gir også veiledning til hvordan formålsangivelse i artikkel 9 nr. 2 skal fortolkes.

Det at departementet har bare omtalt disse kravene helt kort gjør at vi stiller oss tvilende til om høringsinstansens har fått et godt nok utgangspunkt for å gi innspill på om de mener dagens sektorlovgivning er i samsvar med de krav som forordningen stiller, slik departementet ber om.

5.2. Om kravene til nødvendige garantier mv. i nasjonale regler

Departementet peker i høringsnotatets punkt 8.3.1 på at tre av bestemmelsene i artikkel 9 nr. 2 stiller krav om «egnede og særlige tiltak for å verne den registrertes rettigheter og friheter», samt at en bestemmelse krever at det gis «nødvendige garantier». Departementet skriver at forordningen ikke klargjør nærmere hva som ligger i disse kravene, og hvordan slike krav og garantier skal forholde seg til forordningens alminnelige regler. Videre pekes det på at kravene heller ikke er utdypet i fortalen.

Det er en vesentlig svakhet ved høringsnotatet at departementet ikke har gått nærmere inn i dette. Det er heller ikke riktig å si at forordningen ikke utdyper hva som ligger i slike tilleggskrav til det nasjonale rettsgrunnlaget. Vi viser blant annet til artikkel 89 nr. 1, som

stiller krav om at nødvendige garantier kan gis gjennom tekniske og organisatoriske tiltak især for å sikre dataminimering. Mer konkret er det pekt på at slike tiltak kan være pseudonymisering og anonymisering. Disse kravene representerer heller ingen nyhet, og er velkjente ut fra tilsvarende krav om nødvendige garantier etter direktivet.⁴⁵

Garanti om anonymisering og pseudonymisering følger også av prinsippet om dataminimering, jf. artikkel 5 nr.1 bokstav c. Ved hjelp av særskilte teknologier for beskyttelse av personopplysninger og privatlivet kan bruk av personopplysninger i noen tilfeller helt unngås. Eventuelt kan det anvendes pseudonymiserte opplysninger som sikrer en løsning som bedre ivaretar hensynet til privatlivets fred.⁴⁶ Det vises også til artikkel 6 nr. 4 bokstav e om begrepet nødvendige garantier.

Videre kan momentene i artikkel 23 nr. 2. gir et tolkningsbidrag til garantier/tiltak som det også kan være aktuelle å vurdere etter unntakene i artikkel 9 nr. 2. Det vises særlig til at artikkel 23 nr. 2 bokstav d, garantier for å unngå misbruk eller ulovlig adgang eller overføring.⁴⁷ Vi viser også til artikkel 25 om innebygget personvern. Dette er forpliktelser som påligger behandlingsansvarlig og databehandler, men den er også relevant for lovgiver.

Krav om beskyttelse av enkeltindivider er også tolket av sentrale instanser i EU. For eksempel i Artikkel 29-gruppens uttalelse WP 131, 03/2013 og 6/2014, samt i «Håndbok om den europæiske databeskyttelseslovgivningen». Der fremheves det at bruk av pseudonymisering som «et af de vigtigste hjælpemidler til at opnå databeskyttelse» på et området hvor bruk av personopplysninger ikke kan unngås fullstendig.⁴⁸

Mange av de situasjoner som følger av artikkel 9 nr. 2 vil være gjenbruk og videre oppbevaring av personopplysninger hvor både formåls- og lagringsbegrensingsprinsippet gjør seg gjeldende, jf. artikkel 5 nr.1 bokstav b og e. Slik vi ser det oppstiller disse prinsippene klare rammer for lovgiver.

Vi viser også til de særskilte garantier som er trukket frem i fortalepunkt 29 i direktivet, der det gis en beskrivelsen av formålsbegrensingsprinsippet og gjenbruk til historiske, statistiske og vitenskapelige formål. Det uttales i den forbindelse til at slike garantier «skal især udelukke at opplysningene bliver anvendt til at underbygge foranstaltninger eller afgørelser, der træffes overfor en bestemt person». For øvrig inneholder sektorlovgivningen allerede i dag mange eksempler på særskilte garantier på dette området. Se for eksempel Forskrift om innsamling og behandling av helseopplysninger i Reseptbasert legemiddelregister. Her er det straffesanksjonert å bruke opplysningene til andre formål enn de som er opplistet i forskriftens § 1-3.⁴⁹

⁴⁵ Se for eksempel direktivets artikkel 6 (1) bokstav b og c, samt artikkel 8 (4).

⁴⁶ Se for eksempel «Håndbok om europæisk databeskyttelseslovgivning» punkt 3.3.1.

⁴⁷ Se også direktivets fortale punkt 29 om garantier etter artikkel 6 (1) bokstav b. Der går det frem at garantier skal især udelukke, at opplysningene bliver anvendt til at underbygge foranstaltninger eller afgørelser, der træffes over for en bestemt person;

⁴⁸ Se punkt 2.1.3 om anonyme og pseudonyme opplysninger.

⁴⁹ Se forskriftens § 6-2 jf § 13 jf 1-4.

I Artikkel 29-gruppens uttalelse 03/2013 på side 28 til 31 gis det en nærmere redegjørelse av hva som ligger i kravet nødvendige garantier når det kommer til formålsbegrensningsprinsippet etter direktivet. Det pekes på at det er opp til hver enkelt medlemsstat «... to specify what safeguards may be considered as appropriate.» Artikkel 29-gruppen peker deretter på at ulike typer av formål krever ulike typer av garantier.

Når det gjelder *historiske formål* vises det for eksempel til denne uttalelsen på side 29:

«Processing for ‘historical’ purposes can also have specific characteristics and this may require a different set of safeguards. Member States often have specific laws governing access to national archives, archives on recent history of particular interest (such as archives evidencing oppressive regimes), and court files kept by the judiciary. These laws often call for safeguards beyond anonymisation or pseudo-anonymisation, including appropriate security measures and restrictions on access. ... Although historians are often more interested in facts than in the precise identity of the individuals concerned (and for these cases anonymised or pseudonymised data may often be appropriate), in some cases, the research may focus on specific individuals, such as historical figures or family history. It may also be that researchers wish to use historical data that pose little or no risk to persons concerned, due to the lapse of time since the data were collected.

Vi viser også til følgende uttalelse om *vitenskapelige formål* på side 29:

«As regards ‘scientific’ purposes, there may also be a need to access different kinds of data. Some research may require raw microdata, which are only partially anonymised or pseudonymised. In some cases, the research purposes involved can only be fulfilled if the pseudonymisation is reversible: for example, when research subjects need to be interviewed at a later stage in a longitudinal study. Other research, however, may require less detail, and therefore allow a higher level of aggregation and anonymisation. Further, publication of research results should, as a rule, be possible in such a way that only aggregated and/or otherwise fully anonymised data will be disclosed.»

Vi viser videre til følgende uttalelse til på side 29, om at det i vurdering av garantier også må skilles mellom situasjoner hvor behandlingen foretas av opprinnelige behandlingsansvarlig eller utleveres til andre tredjepersoner:

«Finally, as will be shown below, it will also be relevant to distinguish between situations where the further processing will be carried out by the initial data controller and those where personal data will be transferred to a third party. In this context, some research projects may require very precise protocols (rules and procedures) to ensure a strict functional separation between participants in the research and outside stakeholders. This may include technical and organisational measures, such as securely key-coding the personal data transferred and prohibiting outside stakeholders from re-identifying data subjects (as in the case of clinical trials and pharmaceutical research) and possible other measures. Considering the diversity of potential

situations, it is all the more important to once again follow the generally applicable multi-factor approach in order to identify the appropriate safeguards.

For øvrig mener vi at krav om garantier/tiltak for å beskytte den enkeltes personopplysningsvern må tolkes i tråd med praksis fra EMD.⁵⁰ Slik vi tolker EU-domstolens praksis er det vanskelig å se at behandling av personopplysninger kan være ulovlig etter EMK artikkel 8, uten at den samtidig bryter med forordningen.⁵¹ Departementet bør derfor foreta en vurdering av om lovforslag også står seg mot krav til garantier som følger av slik rettspraksis, se for eksempel §§ 6, 13 og 14.

Vi nevner i denne forbindelse to eksempler på saker hvor EMD har vurdert garantier ved behandling av personopplysninger. I saken *Leander mot Sverige* var de særlige garantier som var fastlagt i nasjonal rett for å beskytte den registrertes interesser avgjørende for at EMD konkluderte med at kravene i artikkel 8 nr. 2 var oppfylt.⁵²

Et annet tilfellet er sak 335/2016. Der kom EMD til at skjult overvåking av en person representerte et brudd på artikkel 8 om retten til privatliv. Saken gjaldt et sveitsisk forsikringsselskap som opptrådte som organ for den sveitsiske staten. Overvåkingen representerte et brudd på retten til privatliv etter EMK artikkel 8 nr. 1. Spørsmålet var om vilkårene for inngrep var oppfylt etter EMK artikkel 8 nr. 2. Domstolen vurderte om inngrepet var «in accordance with the law». Etter en vurdering av sveitsisk lovgivning kom domstolen til at lovskravet ikke var oppfylt. Sentralt i vurderingen var manglende klarhet i sveitsisk lovgivning og at det ikke forelå «sufficient safeguards against abuse».

5.3.Behandling som gjelder arbeidsrett, trygderett og sosialrett

Departementet viser til at behandling av sensitive personopplysninger på arbeidsrettens område følger av personopplysningsloven § 9 første ledd bokstav f, i den utstrekning det er «nødvendig for at den behandlingsansvarlige skal gjennomføre sine arbeidsrettslige plikter eller rettigheter». Departementet er i tvil om det bør videreføres et slikt unntak og om det bør plasseres i arbeidsmiljøloven eller den generelle personopplysningsloven.

Departementet presiserer ikke at behandlinger som skjer etter dette unntaket må ha et rettslig grunnlag i artikkel 6. Vi tror at de aktuelle grunnlagene først og fremst er bokstav c og e.

Av pedagogiske grunner kan det vurderes å utforme en bestemmelse i den generelle personopplysningsloven som klargjør når lov, forskrift eller tariffavtale kan utgjøre et rettslig grunnlag på dette området.

Slik vi ser det må behandling av sensitive personopplysninger på grunnlag av tariffavtale skje innenfor de rammer som følger av nasjonal lov med nødvendige garantier, jf. artikkel 9 nr. 2

⁵⁰ Se også i «Håndbok om den europæiske databeskyttelseslovgivningen» punkt 3.1.

⁵¹ Se for eksempel gjennomgangen av *Österreichischer Rundfunk*. 20. mai 2003 i kapittel 3.

⁵² Se mer om avgjørelsen i «Håndbok om den europæiske databeskyttelseslovgivningen» punkt 3.1.1.

bokstav b. Det mest praktiske er derfor trolig at arbeidsmiljøloven med forskrifter regulerer forholdet til behandling av sensitive personopplysninger på grunnlag av en tariffavtaler nærmere.

Det vil variere utfra tema hva som kan fremgå av tariffavtale og hva som må inn i lov. Det er en vesentlig forskjell mellom behandling av sensitive personopplysninger i forbindelse med en lønnsforhandling og i forbindelse med inngripende kontrolltiltak. For inngripende kontrolltiltak, som for eksempel hemmelig overvåking av elektronisk kommunikasjon på arbeidsplassen, mener vi det rettslige grunnlaget bør være nasjonale lovbestemmelser som også fastsetter nødvendige garantier.⁵³

Vi savner for øvrig at departementet sier noe om behovet for gjøre endringer i sektorlovgivningen, for eksempel om arbeidsmiljøloven, folketrygdloven og sosialtjenesteloven, anses å oppfylle de krav til nasjonale regler som følger av forordningens artikkel 5, 6 og 9.

5.4. Behandling som er nødvendig av hensyn til viktige samfunnsinteresser

Departementet skriver at forordningens artikkel nr. 2 viderefører personopplysningsloven § 9 første ledd bokstav b om behandlinger som er «fastsatt i lov».⁵⁴ I høringsnotatets punkt 8.3.3 uttaler departementet at unntaket er en «sekkebestemmelse som er aktuelle i de tilfeller der behandlingen av sensitive personopplysninger har grunnlag i lovgivning som ikke faller inn under en av de øvrige unntaksbestemmelsene». Deretter påpekes det at lovgivingen må skje innenfor de rammer som følger av lovteksten. Det bes til slutt om høringsinstansenes syn på om det i dag skjer behandling av sensitive personopplysninger som ikke kan sies å oppfylle de nevnte kravene.

Som nevnt over mener vi grunnlaget «fastsatt i lov» har vært praktiser som et *alternativt grunnlag* til den uttømmende opplistingen i direktivet artikkel 8. Det er derfor ikke riktig å si at forordningen viderefører praksis omkring grunnlaget «fastsatt i lov». Siden forordningens artikkel 9 nr. 2. bokstav g oppstiller strenge krav for at nasjonale regler skal kunne sies å være omfattet av dette unntaket, mener vi at det ikke er helt treffende å kalle dette en «sekkebestemmelse». Vi viser for øvrig til at slike behandlinger skal være nødvendig av hensyn til «viktige samfunnsinteresser», og at bestemmelsen har et snevert anvendelsesområde.⁵⁵

⁵³ Se tilsvarende vurdering i Artikkel 29-gruppen uttalelse WP 55 side 17. Vi har i denne omgang ikke hatt anledning til å gå nærmere inn på spørsmålet om arbeidsmiljøloven kapittel 9, herunder § 9-1 nr. 1, oppfylle forordningens krav til nasjonal lovgivning i møte med slike typer kontrolltiltak.

⁵⁴ Se høringsnotatet side 33.

⁵⁵ Direktivets fortale punkt 34, 35 og 36 gir viktig tolkningsbidrag til som ligger i begrepet «viktige samfunnsinteresser». Forordningens fortale punkt 53 til 56 gir også veiledning på hvilke behandlinger som har skjer ut fra allmennhetens interesser.

Artikkel 29-gruppen har tolket det tilsvarende grunnlaget i direktivets artikkel 8 nummer 4. Der er det blant annet pekt på at direktivets fortalespunkt 34 gir eksempler på hva som kan anses som «viktige samfunnsmessige interesser».

Videre oppstilles det i uttalelsen nokså strenge krav til identifikasjon av den viktige samfunnsmessige interessen og krav til nødvendighet og forholdsmessighet:

«Medlemsstaterne skal i hvert enkelt tilfælde kunne bevise, at der er tale om viktige samfunnsmessige interesser i forbindelse med hele behandlingen af følsomme personoplysninger, der falder ind under undtagelsen, og behandlingen skal være nødvendig i lyset af viktige samfunnsmessige interesser. Alle sådanne foranstaltninger skal være forholdsmæssige for så vidt angår formålet. Det indebærer, at hvis der findes foranstaltninger, der i mindre grad krænker den personlige integritet, skal de anvendes.»

Artikkel 29-gruppen peker også på forholdet til EMK artikkel 8:

«For så vidt angår indgreb i privat- og familielivets fred skal foranstaltningerne desuden være i overensstemmelse med menneskerettighedskonventionens artikel 8 og tolkes i lyset af Menneskerettighedsdomstolens retspraksis, nemlig at det skal ske "i overensstemmelse med loven" og være «nødvendigt i et demokratisk samfund» af hensyn til samfunnsmessige interesser. Menneskerettighedsdomstolen i Strasbourg har i sin retspraksis gentagne gange påpeget, at den lov, der fastsætter indgrebet, klart bør afgrænse omfanget af de skønsmessige foranstaltninger, der tildes de offentlige myndigheder, samt hvordan de skal udøves under hensyntagen til det legitime formål med den pågældende foranstaltning for at sikre passende personbeskyttelse mod arbitrære indgreb.»

Til slutt peker Artikkel 29-gruppen på at:

«[m]edlemsstatene har en plikt til at give spesifikke og passende garantier, således at den enkeltes grundlæggende rettigheder og privatliv beskyttes i den forbindelse.»

Vi kan ikke se at den tilsvarende bestemmelsen i forordningen oppstiller noe lempeligere krav enn direktivet. Det er derfor relevant å se hen på hvordan Artikkel 29-gruppen har tolket denne bestemmelsen.⁵⁶ Spørsmålet blir dermed etter vår vurdering dermed i hvilken grad sektorlovgivningen står seg mot de krav Artikkel 29-gruppen har oppstilt for dette unntaket. Siden departementet i høringsnotatet bare har gitt en helt overordnede gjennomgang av de krav som stilles til dette grunnlaget, er det grunn til å tro at denne høringsrunden ikke vil gi et godt nok grunnlag for å belyse det reelle behovet for gjennomgang og tilpasninger i sektorlovgivningen.

⁵⁶ Se WP 131 punkt 7.

En lov som i dag kan være relevant å vurdere etter dette grunnlaget er sosialtjenesteloven. I proposisjonen til denne loven er ikke kravene etter personverndirektivet engang omtalt.⁵⁷ En annen lov som er relevant etter dette unntaket er folketrygdloven. Også her kan det stilles spørsmål ved hvilke vurderinger som ble gjort opp mot de krav som følger av direktivet når det gjelder nasjonale regler om behandling av sensitive personopplysninger.⁵⁸ Disse to lovene bør trolig vurderes etter forordningens artikkel 9 nummer 2 bokstav b.

5.5.Behandling i forbindelse med helsetjenester mv.

Forordningen artikkel 9 nr.2 bokstav h angir at behandling av sensitive opplysninger er lov når:

«Behandlingen er nødvendig med henblikk på forebyggende medisin eller arbeidsmedisin, for å vurdere en arbeidstakers arbeidskapasitet, i forbindelse med medisinsk diagnostikk, yting av helse- eller sosialtjenester, behandling eller forvaltning av helse- eller sosialtjenester og -systemer på grunnlag av unionsretten eller medlemsstatenes lovgivning eller i henhold til en kontrakt med helsepersonell og med forbehold for vilkårene og garantiene nevnt i nr. 3.»

Bestemmelsen bygger på direktivets artikkel 8 nr. 3. Det følger av ordlyden i forordningsbestemmelsen at den gir større rom for unntak enn det som følger av direktivbestemmelsen. Direktivbestemmelsen var i stor grad innrettet mot pasientbehandling og forvaltning av slike tjenester. Artikkel 29-gruppen har tolket rekkevidden av direktivets bestemmelsen i en uttalelse.⁵⁹ Uttalelsen er relevant for vurdering av hvorvidt dagens helselovgivning oppfyller de forpliktelser som følger av forordningen artikkel 9 første ledd bokstav h.

Departementet peker på at ytelse og forvaltning av helse- og sosialtjenester er underlagt en omfattende lov- og forskriftsregulering, herunder om behandling av opplysninger og om taushetsplikt. Departementet legger derfor til grunn at det neppe er nødvendig med en generell lovbestemmelse som åpner opp for behandling på disse områdene. Departementet foreslår derfor ingen generell lovbestemmelse slik det finnes i dag i personopplysningsloven § 9 bokstav g. Det bes imidlertid om høringsinstansenes syn på om det fremkommer at sensitive personopplysninger i dag behandles utelukkende på grunnlag av personopplysningsloven § 9 første ledd bokstav g.

En lov som ligger i kjerneområdet av direktivbestemmelsen er pasientjournalloven. Vi kan ikke se at det i lovens forarbeider er foretatt en nærmere vurdering av hvorvidt loven er innenfor de rammer som følger av direktivets artikkel 7 og 8. Det er for eksempel ikke angitt hvilke grunnlag i artikkel 7 og 8 loven bygger på. Vi antar at loven bygger på direktivets

⁵⁷ Ot.prp.nr. 103 (2008-2009)

⁵⁸ Grunnlaget for denne loven ble lagt allerede i Ot.prp.nr 29 (1995-1996). Personopplysningsloven trådte imidlertid ikke i kraft før 1. januar 2001. I Prop.7 L 8 (2012-2013) er ikke direktivet omtalt, selv om det foretas en omfattende vurderinger av personvernet.

⁵⁹ Se WP 131punkt 6.

artikkel 7 bokstav e og artikkel 8 nummer 3. Det kan likevel stilles spørsmål ved om det er andre alternativ i artikkel 8 som er aktuelle.⁶⁰

Det er også eksempler på sektorlovgivning som blander sammen flere formål, for eksempel helsehjelpsformål, kvalitetssikringsformål, styringsformål og forskningsformål. Se for eksempel SYSVAK-registerforskriften § 1-3 og forskrift om Kommunalt pasient- og brukerregister § 1-1.

Vi presiserer at nevnte lover er ikke nødvendigvis i strid med de krav som følger av direktivet, men det er imidlertid vanskelig å etterprøve dette når slike vurderinger mangler i forarbeidene.

5.6. Behandling som er nødvendig av allmenne folkehelsehensyn

Forordningens artikkel 9 nr. 2 er omtalt i et avsnitt i høringsnotatet punkt 8.3.5 Vi anbefaler at departementet i proposisjonen gjøre oppmerksom på at begrepet «allmenne folkehelsehensyn» er definert i fortalens punkt 54. Begrepet «folkehelse» skal fortolkes slike det er definert i Europa-Parlamentets og Rådet forordning (EF) nr. 1338/2008. Det er altså ikke slik at nasjonale myndigheter står fritt til å definere hvilke typer behandlinger og lover som er nødvendig ut fra dette formålet.

5.7. Genetiske opplysninger mv.

Forordningens artikkel 9 nr.1 angir hvilke personopplysninger som er å anse som «særlige kategorier av personopplysninger», altså det som gjerne omtales som sensitive personopplysninger. Artikkel 4 nr. 13 og 15 gir definisjoner de sensitive opplysningene genetiske data, biometriske data og helseopplysninger. Artikkel 9 nr. 4 åpner opp for at det i nasjonal rett kan fastsettes ytterligere vilkår og begrensninger for behandling av genetiske opplysninger, biometriske opplysninger og helseopplysninger. Departementet legger til grunn at gjeldende nasjonale særregler som begrenser behandling av slike opplysninger kan videreføres, og viser til helseregisterloven, helseforskningsloven, pasientjournalloven, bioteknologiloven mv.

Vi bemerker at helseregisterloven, helseforskningsloven og pasientjournalloven baserer seg på en utvidet definisjon av begrepet helseopplysning.⁶¹ Det vil si at begrepet omfatter personopplysninger som muligens ikke kan anses som helseopplysninger etter forordningen. De norske lovene definerer for eksempel også *andre personlige forhold* som helsepersonell får vite om i egenskap av å være helsepersonell som helseopplysninger. Vi antar likevel at det er innenfor forordningens rammer at også slike typer opplysninger gis et særskilt vern. Det kan vurderes etter artikkel 6 nummer 1 bokstav c og e og eventuelt artikkel 9 nummer 2. Artikkel 29-gruppen har dessuten uttalt at *alle* opplysninger som er relevant for behandlingen av en pasient er å anse som sensitive personopplysninger. De påpeker at [h]vis de ikke er

⁶⁰ Se Prop.72 L 82013-2014). Punkt 3.2 inneholder kun en generelle gjennomgang av direktivet.

⁶¹ Se helseregisterloven § 2 bokstav a og helsepersonelloven § 21.

relevante for behandlingen af pasienten, ville og burde de ikke være medtaget i lægejournalen.»⁶²

Vi gjør oppmerksom på at artikkel 9 nummer 4 inneholder et viktig handlingsrom med hensyn til at det i medlemsstatenes lovgivning kan gi forbud mot bruk av samtykke. Datatilsynet mener departementet burde bedt om innspill fra høringsinstansene om de mener om et slikt handlingsrom bør benyttes. Datatilsynet opplever for eksempel allerede i dag et press fra forsikringsbransjen på ulike typer overvåking av kunder, for eksempel helseovervåking. Det kan også dreie seg om særlig inngripende behandlinger og bruk av samtykke fra mindreårige. Se i den forbindelse punkt 14.1 nedenfor om vurdering av videreføring av personopplysningsloven § 11 tredje ledd.

6. Behandling av sensitive personopplysninger for arkiv, forskning og statistiske formål

Departementet foreslår å videreføre bestemmelsen i gjeldende personopplysningslov § 9 første ledd bokstav h i forslag til ny lov § 6, men med visse ytterligere vilkår i lys av kravet til proporsjonalitet og egnede og særlige tiltak i forordnings artikkel 9 nr. 2. bokstav j.

Vi savner en nærmere redegjørelse for hvilke typer behandlinger departementet mener omfattes av disse kategoriene av behandlinger. Arkiv- og statistikkformål kan være begrenset til det offentliges behandlinger, men det kan også omfatte andre typer interesser.

Betegnelsen «forskning» må tolkes vidt, og i tillegg til konkrete forskningsprosjekter kan det også omfatte befolkningsundersøkelser, opprettelse og behandling av opplysninger i helseregistre, kvalitetssikring og overvåking av befolkningens helsetilstand mv. For disse formålene behandles det sensitive personopplysninger i et meget stort omfang, og i de fleste tilfellene uten at det innhentes samtykke fra de registrerte. Slike behandlinger må regnes som inngripende, og kravet til lovhjemmel bør være strengt, se kapittel 3 om prinsipper og kapittel 4 om behandlingsgrunnlag.

Vi er enige med departementet om at det for det offentliges statistikk- og arkivformål i hovedsak finnes særlovgivning, men det må presiseres at det er behov for å gjennomgå denne lovgivningen for å sikre at den gir rettigheter og beskyttelse av den enkeltes personvern i tråd med forordningen.

Datatilsynet mener at det foreslåtte bestemmelsen i § 6 er for vidt formulert og at det er grunn til å tro at den ikke oppfyller kravene til klarhet i hjemmelsgrunnlaget som følger av lovlighetsprinsippet og forordningens artikkel 6 nr. 1 bokstav e og artikkel 6 nr. 3, samt kravene til garantier i artikkel 89. Når garantien forhåndsgodkjenning (krav om konsesjon) nå bortfaller, blir behovet for en klar lovhjemmel enda sterkere.

⁶² Se WP punkt 2.

Datatilsynet mener at det er et stort behov for en særlov for forskning, hvor det fremgår hvilke organisatoriske og tekniske tiltak som må være på plass for å oppfylle kravet om nødvendige garantier. Loven må samtidig sikre at de grunnleggende kravene i art 5, 6 og 9 er oppfylt. Se nærmere om det nedenfor.

6.1. Våre merknader til lovforslaget § 6

Som nevnt over mener vi at bestemmelsen er for vidt formulert. Slik vi leser forslaget til bestemmelse er den ment å gi hjemmel for behandling av alle kategorier av sensitive personopplysninger etter forordningens artikkel 9 nr. 1, altså et svært vidt formål som vil omfatte svært mange forskjellige typer situasjoner.

Bestemmelsen er avgrenset til å gjelde sensitive opplysninger, mens det i realiteten ofte skjer behandling av opplysninger som ikke er sensitive til disse formålene. Disse behandlingene må også omfattes av lovforslagets § 6, ettersom artikkel 89 og artikkel 6 gjelder alle former for opplysninger, ikke bare sensitive. Bestemmelsen er derfor trolig også ment å gi nødvendig rettslig grunnlag etter artikkel 6 nr. 1 bokstav e og nr. 3, men det er ikke presisert i høringsnotatet.

Så langt vi kan forstå forslaget åpner bestemmelsen opp for omfattende og inngripende behandlinger som griper inn i retten til privatliv etter EMK, det forutsetter i seg selv en klar lovhome. Ut fra det som står i høringsnotatet er det uklart hvilke vurderinger departementet har gjort med hensyn til lovlighetsprinsippet, kravene til rettslig grunnlag som følger av forordningens artikkel 6, samt de øvrige krav og prinsipper som følger av forordningen. Som vi har påpekt flere steder ovenfor må en nasjonal bestemmelse være i tråd med forordningens krav til nødvendighet, proporsjonalitet og formålsbegrensning.

Slik vi ser det må denne bestemmelsen vurderes i nær sammenheng med at konsesjonsinstituttet avvikles og at den garanti som Datatilsynets forhåndsgodkjenning for forskningsformål nå utgjør blir borte.

Etter dagens system må denne typen behandling av personopplysninger gjennom en forhåndsvurdering og godkjenning etter litt ulike systemer. Enkelte typer forskning og annen sekundærbruk av data er, fordi de er særlig inngripende, regulert i forskrift eller lov. Helseregisterloven gir generelle bestemmelser for bruk av helseopplysninger til sekundære formål, men den tilsvarer i hovedsak innholdet i personopplysningsloven. Enkelte bestemmelser gir særlige rettigheter og plikter sammenlignet med den generelle personopplysningsloven.

Helseforskningsloven regulerer medisinsk og helsefaglig forskning, og de Regionale Etske Komiteene (REK) vurderer behandlingens lovighet knyttet til bestemmelser om taushetsplikt, personvern og informasjonssikkerhet, i tillegg gjør de en etisk vurdering av prosjektet. Intern kvalitetssikring i forbindelse med helsehjelp er ansett å ha hjemmel i helsepersonelloven og pasientjournalloven, og har ikke vært gjenstand for eksterne forhåndsgodkjenninger.

Norge har ingen generell sektorlovgivning som regulerer behandlingsformålet forskning, selv om enkelte typer forskning og eller enkelte typer registre altså delvis er regulert i særlovgivning. Forskning og opprettelse av registre som ikke omfattes av særlige ordninger blir vurdert av Datatilsynet i forbindelse med konsesjonsbehandling etter helseregisterloven og personopplysningsloven. Datatilsynets konsesjoner til sekundærbruk av data omfatter alle formål og alt fra prosjekter av forskjellig størrelse, befolkningsundersøkelser, kvalitets- og forskningsregistre. Prosjektene er avgrenset i omfang og tid, mens registre gjerne har større rekkevidde, lenger varighet og flere formål. Registerne skal også som hovedregel utlevere opplysninger til bruk i forskningsprosjekter.

Selv om REK godkjenner behandling av opplysninger i medisinske og helsefaglige forskningsprosjekter, må alle registre må ha konsesjon fra Datatilsynet. Kvalitets- og forskningsregistre er per i dag nesten utelukkende basert på samtykke fra de registrerte, mens prosjekter ofte er basert på alternative behandlingsgrunnlag.

Etter Datatilsynet syn har de rettslige kravene og systemene for forhåndsgodkjenning (konsesjon) av såkalt sekundærbruk av data fungert som en viktig garanti for at de registrertes rettigheter og friheter har blitt tilstrekkelig ivaretatt. Selv om vi sjelden avslår søknader om konsesjon, skjer det ofte tilpasninger av behandlingen underveis i søknadsbehandlingen, og det stilles ofte vilkår i vedtakene om konsesjon, jf. personopplysningsloven § 35.

Med forordningen forsvinner kravet om forhåndsgodkjenning i form av konsesjon eller vedtak fra REK.⁶³ Ivaretagelsen av de enkelte registrertes rettigheter og friheter ved forskning, vil dermed i hovedsak være avhengig av den behandlingsansvarlige følger regelverket, og at vi har andre virkemidler som gir de nødvendige garantier enn forhåndsgodkjenning.

Det er et vilkår for å kunne gjøre unntak fra forbudet mot behandling av opplysninger i artikkel 9 nr. 2 bokstav j at behandlingen av opplysninger skjer i samsvar med artikkel 89. Artikkel 89 stiller krav om nødvendige garantier som innebærer at man har innført tekniske og organisatoriske tiltak for å særlig sikre prinsippet om dataminimering. Eksempler på slike tiltak er pseudonymisering og anonymisering. Etterlevelse av artikkel 89 er også en forutsetning for at flere andre vilkår i forordningen er oppfylt, for eksempel artikkel 5, 9 og 14.

Datatilsynet er tvilende til at de foreslåtte garantiene og tiltakene for å verne om den enkeltes grunnleggende interesser som oppstilles i forslag til § 6 kan anses å være tilstrekkelige etter forordningens artikkel 9 nr. 2 bokstav j og artikkel 89 nr. 1.

Vi kan ikke se at *bokstav a* innebærer en særlig garanti, da den ikke gjør annet enn å beskrive en situasjon hvor det er nødvendig å ha et annet hjemmelsgrunnlag. Den legger til en viss grad opp til at man må foreta en vurdering av om innhenting av samtykke er umulig eller uforholdsmessig vanskelig, og det kan synes som om man mener at det som en hovedregel

⁶³ Jf. helseforskningsloven §§ 9 og 33 om forhåndsgodkjenning

skal innhentes samtykke. Innen forskningsformål vil det svært ofte vil være umulig eller i alle fall uforholdsmessig vanskelig å innhente samtykke. Dette gjelder særlig når datagrunnlaget omfatter mange registrerte. Det er i tillegg et klart påtrykk fra sentrale myndigheter om at det i større grad skal tas i bruk reservasjonsrett fremfor samtykke i medisinske kvalitetsregistre. Bestemmelsens bokstav a gir etter Datatilsynets oppfatning derfor liten anvisning på tiltak som kan fungere som garantier for at personvernet ivaretas.

Vi mener også at kravet om interesseovervekt i *bokstav b* gir liten garanti. Ansvar for å gjøre disse vurderingene overlates til den databehandlingsansvarlige, som selv sagt har en stor egeninteresse i å gjennomføre sin behandling. Den vurderingen som bokstav b pålegger ansvarlige å gjøre, følger i stor grad av de øvrige kravene i forordningen, blant annet gjennom prinsippene i artikkel 5 og i unntaket fra forbudet i artikkel 9 j. Det har derfor liten tilleggsverdi å presisere plikten til å gjøre en slik avveining i bokstav b.

Lovforslaget § 6 *bokstav c* er i all hovedsak en kopi av teksten i forordningen. Departementet viser til at «et slikt vilkår vil delvis overlappe det generelle kravet om «nødvendige garantier» i artikkel 89 nr. 1, men kan også innebære strengere krav der dette er påkrevd i lys av opplysningenes sensitiv». Slike krav til garantier må konkretiseres gjennom nasjonal lovgivning og at det således ikke er riktig å si at de overlapper det som følger av forordningen. Dette er også lagt til grunn i den danske utredningen. Helt konkret mener vi at kravene i artikkel 89 om garantier må spesifiseres i nasjonal rett, herunder kravet til å vurdere anonymisering og pseudonymisering. Bokstav c gir derfor liten tilleggsverdi, og kan ikke sies å være en garanti for ivaretagelse av forskningsdeltakeres personvern.

Forslag om tilråding fra personvernrådgiver i *bokstav d* kan slik vi ser det heller ikke anses tilstrekkelig for å anse kravet i artikkel 89 oppfylt, se nærmere om det nedenfor.

For å oppsummere, slik lovforslaget er utformet gir det for liten anvisning på hva som skal til før kravet til nødvendige garantier anses etterlevd. Slik vår fremstilling over viser at bokstavene a til c ikke knyttet noen ekstra plikter til vurderinger, utover det som allerede følger av forordningen selv. Bestemmelsen skiller heller ikke mellom de forskjellige formålene som artikkel 89 dekker, noe som i seg selv er problematisk.

Det vil i tillegg være en svært vanskelig oppgave for Datatilsynet å kontrollere etterlevelse av artikkel 89, utover at de formelle beslutningsprosessene er fulgt.

6.2. Særlig om § 6 første ledd bokstav d, tilråding fra personvernrådgiver

I forslag til § 6 først ledd bokstav d foreslår departementet at det skal være et vilkår om at «den behandlingsansvarlige har utpekt personvernrådgiver og personvernrådgiveren har tilrådd behandlingen»

Dette vilkåret er problematisk, av flere grunner.

En *tilråding* for gjennomføringen av et forskningsprosjekt vil kreve en rekke andre kvalifikasjoner av en personvernrådgiver, i tillegg til at oppgavene vil bli betydelig flere for de rådgiverne som er tilknyttet virksomheter som driver med forskning og annen sekundærbruk av data. Se punkt 13.3 og 13.4 når det gjelder utvidelse av plikten til utpeke personvernrådgiver og utvidelse av oppgavene til personvernrådgiver.

Begrepet «tilråding» er for øvrig brukt i dagens unntak fra konsesjonsplikt som følger av personopplysningsforskriften § 7-27. Etter denne bestemmelsen kan personvernombud tilrå mindre forskningsprosjekter, uten at det søkes Datatilsynet om konsesjon. I praksis vil forslaget i § 6 bokstav d innebære at man viderefører og utvider et unntak fra en konsesjonsplikten man ikke viderefører med ny personopplysningslov. Dette kan fremstå som noe underlig. Datatilsynet mener det er hensiktsmessig å vurdere begrepsbruken dersom man går videre med den foreslåtte ordningen.

Departementet viser til ordningen med NSD som personvernombud, og sier at det er ønskelig å videreføre denne også med nytt regelverk. Datatilsynet vil påpeke at § 6 først ledd bokstav d vil gjelde *alle typer behandling* av opplysninger etter bestemmelsen, uavhengig av hvilke typer ombud som skal vurdere en tilråding. Bestemmelsen vil altså ikke bare være rettet mot virksomheter som NSD, men også omfatte interne personvernrådgivere i virksomheter som driver med forskning. Som eksempler nevnes helseforetakene, Folkehelseinstituttet og Helsedirektoratet. De vil ikke nødvendigvis ha den samme type erfaring og kompetanse til å foreta de nødvendige vurderingene.

Datatilsynet mener det er en risiko for at forslaget i § 6 legger opp til en løsning som i praksis vil bli vanskelig å gjennomføre for virksomhetsinterne personvernrådgivere, særlig i kombinasjon med andre oppgaver som de også forventes å gjøre. Dette kan medføre at virksomheter som driver med forskning vil bli nødt til å tilknytte seg eksterne som gjennomfører disse oppgavene for seg. Dette kan igjen føre til at forordningens intensjon om å bygge ned byråkratiet og ordninger med forhåndsgodkjenning undergraves.

I tillegg stiller vi spørsmål ved om oppgaven er forenelig med øvrige oppgaver og den posisjonen et ombud skal ha i en virksomhet. Selv om personvernombudet etter forordningen skal ha en uavhengig rolle, er det ikke vanskelig å se for seg at vedkommende vil kunne oppleve det som et press dersom gjennomføring av store og viktige prosjekter står og faller på hva han eller hun «tilrår».

For de profesjonelle ombudene savner vi også en vurdering av hvordan forutsetningen om at denne rollen til en viss grad skal være beskyttet i sin stilling kan løses når relasjonen er basert på en kontrakt og ikke gjennom en arbeidsavtale med vedkommende.

Det må for øvrig tas stilling til ved hva en slik tilråding skal inneholde og i hvilken form den skal gis. En annen problemstilling er forholdet mellom personvernrådgiverens tilråding og godkjenninger fra REK som gis i tråd med helseforskningsloven. Den foreslåtte bestemmelsen tar ikke høyde for at det kan foreligge formelle godkjenninger fra andre instanser, og det bør vurderes hvordan disse forskjellige vedtakene skal vurderes mot hverandre.

6.3.Behov for lovregulering av behandling av data til forskningsformål

Departementet ber i høringsnotatets punkt 7.1.2 om behandlingsgrunnlag om innspill på hvorvidt det vil være behov for en lovregulering av behandling av data til forskningsformål. Det vises til at en slik løsning utredes i Sverige forbindelse med innføringen av personvernforordningen⁶⁴.

Som vi skriver over mener Datatilsynet at en norsk særregulering av dette behandlingsformålet er absolutt å anbefale.

Vi mener det er grunnlag for å si at personvernet er under særlig press på dette området. Vi har i Norge store samlinger av data om borgernes liv, skole, arbeid og helse som trolig ikke finnes andre steder i verden⁶⁵ og som for mange aktører anses svært nyttige og verdifulle. Hensynet til forskning og hensynet til personvern oppleves ofte å stå i motsetning til hverandre og det er ofte vanskelige avveininger. I tillegg er det klare signaler fra helsemyndighetene og forskningsmiljøene om at man i større og større grad ønsker å benytte reservasjonsrett framfor samtykke, at man ønsker mer effektiv tilgang og bedre bruk av eksisterende registre osv. I tillegg er det stort press på å gjenbruke data som er innsamlet til andre forskningsformål.

Videre er det et klart voksende ønske om å bruke våre tilgjengelige registre til å gjennomføre BigData-analyser og analyser basert på algoritmer og kunstig intelligens. Det er også flere nasjonale prosesser som har som formål å påvirke økt bruk av eksisterende data og mer effektiv tilgjengeliggjøring og gjennomføring av slike behandlinger⁶⁶.

Dersom den skjønsmessige og krevende personvern vurderingen av behandlingen skal foretas av behandlingsansvarlige (oftest forskningsansvarlige) selv, uten annet enn de generelle bestemmelsene i forordningen og lovforslaget § 6 å se hen til, mener vi at den generelle risikoen for personvernbrudd vil bli for høy. Det er derfor helt nødvendig med en mer detaljert og sektorspesifikk regulering som angir hvordan disse skjønsmessige vurderingene skal foretas.

Reguleringen bør særskilt omhandle de tiltakene artikkel 89 angir, slik at det blir krav om å særskilt vurdere om behandlingen av opplysninger kan skje med pseudonyme eller anonyme data. Disse tiltakene har tidligere vært utredet i Norge, blant annet gjennom Boe-utvalget i 1993⁶⁷. Reguleringen må selvsagt også ivareta kravene til rettslig grunnlag som finnes i artikkel 6 og 9 i forordningen.

⁶⁴ SOU 2017:50 Personuppgiftsbehandling för forskningsändamål

⁶⁵ <https://www.aftenposten.no/meninger/kronikk/i/p3x7G/Helsedata-kan-bli-det-nye-arvesolvet--Jon-Harald-Kaspersen>

⁶⁶ Helsedatautvalget, Helsedataprogrammet osv.

⁶⁷ Boe-utvalget i NOU 1993: 22 Pseudonyme helseregistre

Som nevnt over mener Datatilsynet at slik forslaget i § 6 er formulert tilfredsstillende det neppe kravene i forordningen (artikkel 5, 6, 9 og 89). Datatilsynet mener videre at det ikke er hensiktsmessig at det gis en hjemmel som gjelder et såpass avgrenset område i den generelle personopplysningsloven Personopplysningsloven bør heller gi føringer for hva en slik hjemmel bør inneholde, og overlate til særlovgivningen å gi relevante hjemler for å oppfylle forutsetningene i forordningen.

7. Samtykke

Samtykke er et av de alternative grunnlagene til behandlingsgrunnlag i forordningen artikkel 6 nr. 1 bokstav a og artikkel 9 nr. 2. bokstav a. Forordningen viderefører i det vesentlige gjeldende rett, samtidig som kravene er noe utdypet og presisert. Et krav om stilltiende og presumert/hypotetisk samtykke er åpenbart ikke et gyldig samtykke etter forordningen.

Selvbestemmelsesrett er en svært sentral del av personopplysningsretten. I hvilken grad den enkelte borger selv er gitt rett til å bestemme over bruken av egne opplysninger, er derfor sentralt i vurderinger som gjelder om en bestemt behandlingen kan bygge på et annet rettslig grunnlag enn samtykke, og også i vurderingen av om det kan gjøres unntak fra forbudet i artikkel 9 nr. 1 om behandling av sensitive personopplysninger. Som eksempel viser vi til Artikkel 29-gruppens redegjørelse om respekt for selvbestemmelsesretten ved behandling av sensitive personopplysninger i elektroniske pasientjournalssystemer som ikke er basert på samtykke.⁶⁸ Dette kan kanskje nevnes i proposisjonen.

Det er også verdt å merke seg at samtykke brukes både som *unntak fra de alminnelige regler om taushetsplikt* og som *rettslig grunnlag* etter personvernretten, uten at det nødvendigvis oppstilles samme krav til gyldig samtykke, se for eksempel forvaltningsloven § 13 a og helsepersonelloven § 21. Også på dette området er det behov for en gjennomgang av sektorlovgivningen for å se på behovet for justering av lovtekst og/eller praksis. Dette kunne med fordel vært omtalt i høringsbrevet.

Departementet kunne i høringsnotatets punkt 9.3 også pekt på at samtykke brukes i ulike varianter som rettslig grunnlag for behandling av personopplysninger i sektorlovgivningen. Vi legger til grunn at ansvarlige departementet på sine sektorområde likevel foretar en gjennomgang av hvorvidt slike behandlinger reelt sett er basert på et gyldig samtykke etter forordningen eller om det er nødvendig med lovhjemmel.

8. De registrertes rettigheter

Som departementet skriver i høringsnotatet er bestemmelsene i forordningen i stor grad en videreføring av gjeldende rett. Alle rettighetene fra direktivet er i all hovedsak videreført i

⁶⁸ Se WP 131 punkt III.

forordningen, men med noen presiseringer og utdypinger.⁶⁹ Videre er det tilføyet flere nye rettigheter i forordningen, som retten til å bli glemt i artikkel 17, retten til begrensning i artikkel 18, samt retten til portabilitet i artikkel 20.

Slik vi ser det har gjeldende personopplysningslov regler som både gir bedre og dårligere rettigheter enn direktivet. Eksempel på det første er at personopplysningsloven § 18 første ledd om innsynsrett til enhver går lenger enn den tilsvarende bestemmelsen i direktivet. Personopplysningsloven § 22 gir også mer rett til informasjon om automatiserte avgjørelser enn den tilsvarende bestemmelsen i direktivet.⁷⁰

På den andre siden er det verdt å merke seg at Norge har utelatt å gjennomføre en sentral rettighet i personopplysningsloven. Det vil si retten til innsigelse etter direktivets artikkel 14 bokstav a. Rettigheten er en sentral del av selvbestemmelsesretten.⁷¹ Departementets begrunnelse i forarbeidene for å utelate rettigheten er etter vår mening noe tvilsom.⁷² Artikkel 29-gruppen har spesielt pekt på at retten til innsigelse er sentral når det kommer til behandlinger av personopplysninger som er basert på artikkel 7 bokstav e og f, (som er gjennomført i personopplysningsloven § 8 bokstav d, e og f.⁷³)

Selv om det i hovedsak er snakk om å videreføring av rettigheter, er det behov for å foreta en kartlegging av om det må foretas endringer av rettighetsbestemmelser i sektorlovgivningen. Vi kan nevnte enkelte eksempler på lover innen helsesektoren hvor vi antar at det er behov for tilpasninger; helsepersonelloven, pasientjournalloven, helseregisterloven med forskrifter, pasient- og brukerrettighetsloven og helseforskningsloven. Håndtering av disse rettighetene er på flere områder overført til andre myndigheter enn Datatilsynet. Etter forordningen kan kontroll og tilsyn med rettighetene etter forordningen ikke uten videre foretas av andre myndigheter enn Datatilsynet. Se nedenfor om dette, under omtale av tilsynsmyndighetenes organisering.

Behovet for endringer i sektorlovgivningen burde vært omtalt i høringsnotatet. Vi legger til grunn at den nærmere kartlegging av behovet for endringer foregår i de ansvarlige departementer og at det således ikke hører hjemme i omtale av den alminnelige personopplysningsloven. Men siden dette verken er omtalt i høringsnotatets kapittel 8 om de registrertes rettigheter eller i kapittel 9 om tilpasninger i særlovgivning, er det trolig vanskelig for høringsinstanser å identifisere behovet for endringer. Departementet bør omtale dette nærmere i proposisjonen.

⁶⁹ Se Peter Blume «Den nye persondataret» side 90.

⁷⁰ Se direktivets artikkel 15. Se også Schartum og Bygrave 2010 om «Personvern i informasjonssamfunnet» side 114.

⁷¹ Den ble opprinnelig utviklet i Frankrike av CNIL, og ble adoptert inn i direktivet artikkel 14, se «Analysis and impact study on the implementation of Directive EC 95/46 in Member States» side 21.

⁷² Justisdepartementet støttet seg på utvalgets begrunnelse. Utvalget begrunnelse er for det første at «[m]ed de begrensninger som ligger i bestemmelsen, blir imidlertid regelen svært lite praktisk.» I tillegg fremheves det blant annet av utvalget at direktivbestemmelsen er «tilstrekkelig gjennomført at lovforslaget gir den enkelte rettigheter (se for eksempel lovforslaget §§ 25 og 26 om retten til å kreve opplysninger slettet) og dels ved at slike beføyelser kan utledes fra ulovfestede personvernprinsipper (se for eksempel [Rt-1952-1217](#)).» («To mistenkelige personer»- dommen).

⁷³ Se uttalelse 6/2014 side 23.

8.1. Unntak fra retten til informasjon og innsyn

Forordningens artikkel 23 bygger på direktivets artikkel 13. En vesentlig forskjell mellom forordningen og direktivet er at forordningens artikkel 23 nr. 2 oppstiller ytterligere krav til eventuelle nasjonale regler som gjør unntak fra rettighetene. Dette er en viktig endring med forordningen, som vi kommer tilbake til nedenfor.

Slik vi leser høringsnotatet foreslår departementet å videreføre gjeldende rett i ny lov § 13, så langt forordningen åpner for det. Departementet har ikke foretatt en nærmere vurdering av om den gjeldende bestemmelsen er i tråd med forordningen. Dette mener vi er problematisk.

Også på dette området må det ses hen til EU-retten. Forordningens foralepunkt 73 viser til at begrensninger må være i overensstemmelse med EU-pakten og EMK. Etter EU-retten må begrensninger av personopplysningsvernet være i tråd med EU-pakten artikkel 52 nr.1. Vilkår for begrensninger i charterets artikkel 52 nr. 1 ligger nokså tett på forordningens artikkel 23 nr. 1. EU-domstolen tolket avveiningen av grunnleggende interesser, hvor retten til informasjon og innsyn er veiet opp mot andre samfunnsmessige interesser. Domstolen har i flere saker uttalt at begrensninger i personopplysningsvernet skal holdes innenfor det «strengt nødvendige».⁷⁴ Kriteriet «nødvendig» og «forholdsmessig» i artikkel 2 må tolkes i lys av EMK og EMDs praksis.⁷⁵ For kriteriet «nødvendig» innebærer det et krav om at begrensningen adresserer et påtrengende samfunnsmessig behov («pressing social need».)⁷⁶ Videre har EMD klargjort at lovene som innskrenker personopplysningsvernet må være tydelige, presise og forutsigbare.⁷⁷

Videre har EU-domstolen fattet flere avgjørelser om tolkning av direktivets artikkel 13.⁷⁸ Domstolen har påpekt at medlemslandene ikke har anledning til å fastsette unntak som går utover opplistingen i artikkel 13 nr.1. Bestemmelsen gir imidlertid medlemsstatene mulighet til å fastsette et eller flere unntak som er innenfor rammene i opplistingen i artikkel 13 nr.1.⁷⁹

For å kunne videreføre gjeldende rett i ny lov § 13 må det altså foretas en konkret vurdering av om de foreslåtte unntakene er tydelige, presise og forutsigbare nok til at de kan anses i tråd med forordningen. Det fremgår ikke i høringsnotatet at departementet har gjort en slik vurdering. Vi savner en redegjørelse for hvert enkelt unntak i § 13, med henvisning til hvorvidt de er innenfor ordlyden i et eller flere av grunnlagene i artikkel 23 nr.1. Departementet har så langt vi kan se av høringsnotatet heller ikke foretatt noen nærmere

⁷⁴ Se for eksempel C-73/07 punkt 56 og C-473/12 punkt 37.

⁷⁵ I «Håndbok om den europæiske databeskyttelseslovgivningen» punkt 1.2 er det også redegjort for avveining av personopplysningsvern mot andre rettigheter og pekt på relevant praksis fra EMD vedrørende beskyttelse av personopplysninger.

⁷⁶ I Schartum og Bygrave «Personvern i informasjonssamfunnet» 2010 side 165 legges et slikt kriteriet til grunn for begrepet «nødvendig» i EMK artikkel 8 ut fra EMD praksis.

⁷⁷ Leander v Sverige, application no 9248/81, 26 mars 1987.

⁷⁸ Se for eksempel C-473/12 og C-201/14.

⁷⁹ C-473/12 punkt 37.

vurdering av hvorvidt unntakene er «strengt nødvendige» og «forholdsmessige», selv om det kort slås fast at de er proporsjonale (forholdsmessig).

Ettersom departementet foreslår å i stor grad videreføre reglene i personopplysningslov § 23, kan det relevant å se hen til hvilke vurderinger som ble gjort ved utarbeidelsen av denne bestemmelsen, med hensyn til om den er innenfor rammene i direktivets artikkel 13. I forarbeidene til § 23 omtales forholdet til artikkel 13 kun i en bisetning.⁸⁰ Det foretas ingen vurdering av unntakene i § 23 opp mot direktivets artikkel 13. Det er derfor vanskelig å se hva slags tilknytning flere av unntakene har til unntakene i artikkel 13 i direktivet. Det foretas heller ingen vurdering i forarbeidene av om unntakene er i overensstemmelse med direktivets krav til klarhet, nødvendighet og forholdsmessighet.

Videre mener vi at departementet foretar en for overfladisk vurdering av kravene som følger av artikkel 23 nr. 2 om krav til særlige bestemmelser.

Det bør i proposisjonen vurderes for hvert unntak opplistet i § 13 om det er momenter i artikkel 23 nr.2 som er relevante å ta inn i bestemmelsen. Vi mener behovet for tydelige, presise og forutsigbare unntakshjemler blir desto viktigere når departementet ønsker å basere den norske gjennomføringen på svært generelle unntakshjemler. Spesifisering av momenter i lovtekst kan være helt avgjørende for hvordan avveiningen av interesser slår ut. For eksempel har praksis fra EU-domstolen og EMD særlig pekt på viktigheten av særlige garantier mot misbruk i vurderingen av nasjonale regler.⁸¹

Departementet viser til at når det fastsettes unntak fra retten til informasjon og innsyn av generelle karakter, blir det ikke relevant for departementet å gi nærmere bestemmelser om alle de forhold som nevnes i artikkel 23 nr. 2. Deretter vises det til at § 13 regulerer omfanget av begrensningene i artikkel 23 nr. 2 bokstav c og at kravet om skriftlig begrunnelse tar sikte på å motvirke misbruk av unntakene jf. bokstav d, og å sikre at den registrerte blir underrettet, jf. bokstav h.

Vi er ikke enig med departementet i at den foreslåtte § 13 inneholder «særlige bestemmelser» om «omfanget av begrensningene som er innført» jf. artikkel 23 nr.2 bokstav c. Tvert imot mener vi at de fleste av unntakene i § 13 omfattes av flere av unntak i artikkel 23 nr. 1. Det er også vanskelig å se at departementet har foreslått tilstrekkelige garantier mot misbruk, sett opp mot hvor omfattende unntakene er, jf. artikkel 23 nr. 2 bokstav d. Slik vi ser det vil krav om begrunnelse etter § 13 tredje ledd kun være relevant i de tilfeller hvor den registrerte faktisk er klar over at det behandles opplysninger om vedkommende. Dette vil ikke være tilfellet for mange av de situasjoner som kommer inn under unntakene. Da blir garantien fort en papirrettighet uten særlig praktisk betydning.

Vi er imidlertid positive til at unntaket i personopplysningsloven § 23 første ledd bokstav e ikke videreføres. Vi er enige med departementet i at dette unntaket favner videre enn det som

⁸⁰ Se Ot.prp.nr 92 (1998-1999) side 121-122. Det vises spesielt til følgende setning: «Bestemmelsen oppstiller felles unntak fra plikten til å gi informasjon om behandlingen, jf. direktivet artikkel 13.»

⁸¹ Leander v Sverige para 60-67.

anses som nødvendig og forholdsmessig i artikkel 23 nr. 1. For øvrig mener det samme kunne vært sagt om gjeldende bestemmelse og forholdet til direktivets artikkel 13.

Flere av de andre grunnlagene i § 13 er problematiske, og særlig bokstav e. Vi går gjennom dette nedenfor.

8.2.Nærmere om unntakene som er foreslått i lovforslaget § 13

Lovforslaget § 13 bokstav a om utenrikspolitiske interesser eller nasjonale forsvars og sikkerhetsinteresser

Bokstav a gjør unntak for opplysninger som» er av betydning for Norges utenrikspolitiske interesser eller nasjonale forsvars og sikkerhetsinteresser, når slike opplysninger kan unntas etter offentleglova §§ 20 og 21».

Forslaget bygger i stor grad på gjeldende personopplysningslov § 23 bokstav a. Det fremgår av forarbeidene til denne bestemmelsen at den tilsvarer unntaket i offentlighetsloven § 6 første ledd og peker på at tolkningspraksis vedrørende denne vil være veiledende ved anvendelsen av dette unntaket.⁸² Lovforslaget knytter seg direkte til vilkårene i offentleglova §§ 20 og 21, på samme måte som forvaltningsloven § 19 første ledd bokstav a.

Det er grunn til å stille spørsmål ved hvorfor unntak som er knyttet til *allmennhetens* behov for innsyn alltid vil være nødvendig og forholdsmessig når det gjelder unntak fra de rettigheter den *registrerte* har etter forordningens artikkel 13, 14 og 15.

Vi savner en klargjøring av hvilke unntak i artikkel 23 nr. 1 bestemmelsen bygger på. Vi antar at dette unntaket i alle fall tilknytning til artikkel 23 nr.1 bokstav a, b og c, men muligens også bokstav e. Vi savner også en vurdering knyttet til spesifisering av flere momenter i artikkel 23 nr. 2. Det vil blant annet si hvilke offentlige og private virksomheter som er omfattet av bestemmelsen og, særlig viktig, hvilke garantier som kan gis mot misbruk av unntaket.

Datatilsynet vil trolig ikke ha mulighet til å kontrollere praksis omkring dette unntaket, og i hvert fall i begrenset grad. Spørsmålet er da hvilke(n) instans som eventuelt skal gjøre dette istedenfor. Garantien i personopplysningsloven § 13 tredje ledd vil ha liten reell verdi hvis ingen tilsynsorgan kan overprøve vurderingen til den behandlingsansvarlig. I tillegg vil den registrerte ofte ikke engang være klar over at det behandles personopplysninger om vedkommende. Se for øvrig vårt innspill vedrørende lovens saklige virkeområde og unntak som gjelder rikets sikkerhet i punkt 10.2.

En garanti som bør vurderes er plikt om underretning om behandlingen når hensynene som taler imot hemmelighold ikke lenger gjør seg gjeldende. En annen garanti er klare regler for oppbevaringsperioder, og garantier som særlig tar hensyn til behandlingens karakter, omfang og formål, jf. artikkel 23 nr. 2 bokstav f. Også krav om underretning om unntaket må

⁸² Ot.prp.nr92 (1998-1999) side 121.

vurderes, med mindre det kan skade formålet unntaket er relevant å vurdere, jf. artikkel 23 nr. 2 bokstav h.

Lovforslaget § 13 bokstav b om straffbare handlinger

Bokstav b gjør unntak når «det er påkrevd å hemmeligholde av hensyn til forebygging, etterforskning, avsløring og rettslig forfølgning av straffbare handlinger».

Unntaket er en direkte videreføring av personopplysningsloven § 23 bokstav b. I forarbeidene til bestemmelsen er det uttalt at det med etterforskning menes det som reguleres av straffeprosessloven kapittel 18.⁸³ Forarbeidene peker også på at bestemmelsen åpner for unntak for å avdekke straffbare forhold i andre *kontrolletaters virksomhet*, jf. for eksempel Toll- og ligningsvesenet.

Vi savner en klargjøring av hvilke grunnlag i artikkel 23 nr. 1 unntaket er knyttet til. Vi antar at det i hvert fall har tilknytning til artikkel 23 nr.1 bokstav d, men det kan også favne over bokstav g og h.

Vi savner også en redegjørelse om hvorfor det er nødvendig og forholdsmessig å utforme et slikt generelt unntak. Politiets behandling av personopplysninger er unntatt forordningens saklige virkeområde, jf. forordningen artikkel 2. Vi antar at kontrolletaters virksomhet i stor grad er nærmere regulert i sektorlovgivningen, se for eksempel folketrygdloven kapittel 21 om saksbehandling i trygdesaker.

Vi antar at unntaket dekker offentlig kontrolletaters virksomhet. Dersom departementet mener unntaket skal tolkes videre enn dette, bør det som et minimum klargjøres hvilke andre kategorier av behandlingsansvarlige som er omfattet, jf. artikkel 23 nr. 2 bokstav e. Det bør også klargjøres hvilke grunnlag i artikkel 23 nr. 1. som er aktuelle for eventuelle andre kategorier av behandlingsansvarlige.

De forslag til garantier mot misbruk som det redegjort for ovenfor under unntaket i § 13 bokstav a, også er relevante for dette unntaket, se artikkel 23 nr. 2 bokstav d, f og h. Som et minimum bør det gis garanti om informasjonsplikt når hensynene for hemmelighold ikke lenger gjør seg gjeldende. Det vil typisk være når etterforskningen er avsluttet og det ikke lenger er bevisforspillelsesfare.

Lovforslaget § 13 bokstav d om taushetsplikt

Bokstav d gjør unntak for opplysninger når det «i lov eller i medhold av lov er underlagt taushetsplikt».

Unntaket er en videreføring av personopplysningsloven § 23 bokstav d. I forarbeidene til bestemmelsen pekes det på at bokstav d henviser til lovbestemmelser om taushetsplikt, og gjør det klart at slik taushetsplikt går foran personopplysningslovens bestemmelser om informasjonsplikt og innsynsrett.

⁸³ Ot.prp.nr92 (1998-1999) side 121.

Forordningen gir ikke grunnlag for å unnta fra retten til informasjon ut fra alminnelige regler om taushetsplikt i medlemslandene. Taushetsplikten må være knyttet til et av grunnlagene i artikkel 23 nr.1. Vi ber departementet klargjøre hvilke formål i artikkel 23 nr. 1. unntaket er knyttet til, og gi en begrunnelse for hvorfor det er nødvendig og forholdsmessig.

Lovforslaget § 13 bokstav e om åpenbare og grunnleggende private og offentlige interesser

Bokstav d gjør unntak når «det vil være i strid med åpenbare og grunnleggende private og offentlige interesser å informere om, herunder hensynet til den registrerte».

Unntaket er en videreføring av personopplysningsloven § 23 bokstav f. I forarbeidene til bestemmelsen er det angitt at dette er et generelt utformet unntak og at vilkårene for å gjøre unntak er strenge jf. de kvalifiserte kravene som kommer til uttrykk i «åpenbare» og «grunnleggende».⁸⁴

Vi er kritiske til dette unntaket videreføres, og mener at gjeldende bestemmelse er i strid med våre forpliktelser etter direktivet. Vi deler ikke lovforarbeidenes oppfatning om at vilkårene for å gjøre unntak er strenge. Tvert imot at det er vanskelig å se hvilke offentlige og private interesser i forordningen artikkel 23 nr1. som unntaket *ikke* favner over.

Etter sin ordlyd kan unntaket dessuten favne over interesser som ikke engang er opplistet i artikkel 23 nr. 1. Det kan synes som om at kravet til «åpenbare» innebærer et klarhetskrav, altså at det med en viss grad av klarhet må kunne identifisere en grunnleggende privat eller offentlig interesse. Vi mener imidlertid forordningen stiller langt strengere klarhetskrav enn det. Heller ikke unntaket oppfyller forordningens krav til å være nødvendig og forholdsmessig. Formuleringen om at det må konstateres «strid» mellom retten til personopplysningsvern og en slik interesse er også problematisk. Det kan synes som om det er tilstrekkelig å konstatere «strid mellom personopplysningsvern og en annen grunnleggende interesse for at førstnevnte interesse må vike.

På bakgrunn av det ovenfor nevnte mener vi unntaket nokså klart bryter med krav til lovhjemmel, nødvendighet og forholdsmessighet etter forordningens artikkel 5 bokstav a og artikkel 23.

Når det gjelder krav til klarhet og spesifisering tilføyer vi at det er vanskelig å se hvilke momenter i artikkel 23 nr. 2 som *ikke* er relevante for å bringe klarhet i regelen, samt hvilke rammer som gjelder for avveiningen av personopplysningsvernet mot andre interesser. For dette unntak mener vi at garantien i § 13 tredje ledd om krav til skriftlig begrunnelse åpenbart ikke er tilstrekkelig. Vi ber derfor om at departementet gir en begrunnelse for hvorfor ingen momentene i artikkel 23 nr. 2 anses relevant.

⁸⁴ Ot.prp.nr 92 (1998-1999) side 122.

9. Tilpasninger i særlover som følge av forordningen

I høringsnotatets kapittel 36 foretar departementet en overordnet vurdering av behovet for tilpasninger i særlovgivningen. Det pekes innledningsvis på at forordningen på mange områder i det vesentlige viderefører gjeldende rett, og særlig de mange grunnleggende reglene og prinsipper om behandling. Derfor er det mange bestemmelser som kan videreføres uendret. Deretter foretas det en overordnet gjennomgang av behandling av personopplysninger i særlovgivningen. Departementet nevner ikke at forordningen innebærer en forpliktelse til å endre rettighetsbestemmelser i sektorlovgivningen, jf. forordningens kapittel III.

Ut fra høringsnotatet kan det se ut som det per i dag ikke er foretatt en grundig vurdering av om sektorlovgivningen er innenfor de rammer som følger av forordningen i forkant av høringen. Det vises til at departementet en rekke steder ber om høringsinstansenes syn på behovet for endringer. Som vi har vært inne på tidligere mener vi at gjennomgangen av kravene i forordningen som er gjort i høringsnotatet er så kortfattede at vi er usikre på om høringsinstansene har fått et godt nok utgangspunkt for å kunne vurdere behovet for endringer i sektorlovgivningen.

Den norske gjennomføringen av direktivet er også sentral når det kommer til etterlevelse av forordningen. Dette er fordi forordningen på mange områder viderefører eller bygger på bestemmelser i direktivet. Det er i den forbindelse verdt å merke seg den utbredte oppfatning i norsk rett er at det gjeldende personverndirektivet er et *minimumsdirektiv*.⁸⁵ Det vil si at direktivet angir minstekrav som medlemslandene må overholde, og at medlemslandene kan innføre en høyere grad av personopplysningsvern enn minstekravet. Det følger imidlertid av praksis fra EU-domstolen at personverndirektivet i prinsippet innebærer en totalharmonisering.⁸⁶ Domstolen har for eksempel uttalt:

«at direktiv 95/46 [...] har til formål at gjøre beskyttelsen af det enkelte menneskes rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger ensartet i alle medlemsstater. [...] [A]t tilnærmelsen af de nationale lovgivninger, der finder anvendelse på området, ikke må medføre en forringelse af den beskyttelse, disse yder, men at den tværtimod skal have til formål at sikre et højt beskyttelsesniveau inden for Unionen. [...] [H]armoniseringen af de nævnte nationale lovgivninger [er] ikke begrænset til en minimumsharmonisering, men fører til en harmonisering, der i princippet er fuldstændig.»

Medlemsstatene har derfor kun «begrænset manøvfrihed, når de gennemfører direktivet».⁸⁷

⁸⁵ Se for eksempel Stortingsmeldingen «Personvern og utfordringer» (Meld. St. 11 (2012-2013) side 21 eller NOU 2009: 1 Individ og integritet side 58.

⁸⁶ EU-domstolen tar allerede i *Österreichischer Rundfunk*. 20. mai 2003 stilling til harmoniseringsspørsmålet. Se også EU-domstolen ASNEF & FECEMD (C-468/10 og C-469/10).⁸⁶ Der ble det påpekt at «medlemsstatene hverken kan tilføje nye prinsipper vedrørende grundlaget for behandling af personoplysninger i artikel 7 i direktiv 95/46 eller fastsette supplerende krav, som ændrer rækkevidden af et av de seks principper, der er fastsat i denne artikel»

⁸⁷ Håndbog om europæisk databeskyttelseslovgivning punkt 1.1.3 om den nevnte dom.

EU-domstolen har i sin praksis også tydeliggjort de krav som stilles til harmonisering av nasjonal lovgivning etter direktivets artikkel 5 og 7.⁸⁸ Domstolen har i flere saker kommet til at medlemsland ikke har gjennomført artikkel 7 på en korrekt måte i nasjonal lovgivning.⁸⁹

Til tross for at den norske gjennomføringen av direktivet bygger på en oppfatning av at direktivet er et minimumsdirektiv, er det både gitt regler som gir bedre og dårligere vern i den gjeldende personopplysningsloven enn det som følger av direktivet. Avvik som gir dårligere vern avhjelpes ved at gjeldende lov nå erstattes med en ny lov. Når det gjelder sektorlovgivningen, blir problemet at den bygger på gjennomføringer og tolkninger i personopplysningsloven.

Vi har allerede ovenfor beskrevet avvikende norsk gjennomføring av direktivet i gjennomgangen av forordningens artikkel 5, 6 og 9 i kapittel 3, 4, 5 og 6, samt kapittel 8 om rettigheter. Etter vår vurdering avviker for eksempel praktiseringen av grunnlaget «fastsatt i lov» i personopplysningsloven § 8 og 9 fra direktivets artikkel 7 og 8. Når det gjelder rettigheter vises det for eksempel til at retten til innsigelse ikke er gjennomført i personopplysningsloven.

Det er i denne forbindelse verdt å merke seg at Norge ikke er alene om å ha avvikende gjennomføringer av direktivet. I forarbeidene til nytt personvernregelverk i 2012 ble det gjennomført en undersøkelse blant medlemsstatene.⁹⁰ Der ble gjennomføringen av blant annet artikkel 6, 7 og 8 vurdert. Det viste seg at gjennomføringen av direktivbestemmelsene varierte betydelig blant medlemsstatene. Vi er ikke kjent med at EFTA-statenes gjennomføring av direktivet var gjenstand for undersøkelsen, men en del av kritikken rammer utvilsomt også den norske gjennomføringen av direktivet.⁹¹ Kommisjonen pekte i nevnte undersøkelse blant annet på at enkelte medlemsland har⁹²

«... general, and more relaxed, rules which allow for processing whenever this is “authorised by law” or by “special provisions” in or even adopted under any law.»

I vurderingen av om det er nødvendig med justeringer av særlovgivning mener vi det er relevant å se på om lovgiver har gjort vurderinger av relevante rammer i direktivet. Dette gjelder spesielt direktivets artikkel 6 og 7, som i stor grad videreføres i forordningen artikkel 5 og 6. En viktig kilde til å belyse dette er lovens forarbeider. Dersom det ikke er spor av vurderinger av slike rammer eller at de er mangelfulle, medfører ikke det i seg selv at bestemmelsene strider mot krav i forordningen. Vi mener imidlertid at risikoen for brudd er større i slike tilfeller.

⁸⁸ Se for eksempel C-101/01, C-468/10, C-469/10, C-683/13 og C-582/14.

⁸⁹ Se for eksempel dom i sak C-468/10 og C-469/10, samt C-582/14.

⁹⁰ Se dokumentet «Analysis and impact study on the implementation of Directive EC 95/46 in Member States»

⁹¹ Spørsmålet om riktig gjennomføring av direktivet er ikke ukjent i praksis. I sak PVN-2014-01 pekte klager på at sensitive personopplysninger var gitt en videre definisjon i § 2 nr 8 bokstav b (opplysninger om straffbare forhold) enn i direktivets artikkel 8, samt at direktivet ikke er et minimumsdirektiv, men et fullharmoniseringsdirektiv. Nemnda la norsk lov til grunn at det er en lovgiversak om lovens innhold skal endres

⁹²

Uriktig gjennomføring av personverndirektivet innebærer at ryddejobben blir større ved innføringen av forordningen. Lovgiver og departement bør ha et kritisk blikk på om norske regler som presumeres å være i samsvar med direktivet virkelig er det. En videreføring av en regel i direktivet til forordningen vil ikke nødvendigvis innebære at norsk rett er i samsvar med de forpliktelser som følger av forordningen.

10. Lovens saklige virkeområde

Departementet foreslår at personopplysningsloven, og forordningen som inkorporeres gjennom loven, som et utgangspunkt skal gis generell anvendelse. Det vil si at disse reglene skal gjelde også utenfor rekkevidden av EØS-avtalen.

Datatilsynet støtter denne tilnærmingen. Vi er enige i at det å operere med forskjellige regelsett avhengig av om man er innenfor eller utenfor EØS-avtalens virkeområde ville ha bydd på vanskelige grensedragninger.

Samtidig er det ikke til å komme forbi at spørsmålet om man er innenfor eller uten EØS-avtalens virkeområde vil kunne oppstå og være relevant fra tid til annen. Det kan være viktig å vite hvor grensen går mellom der man materielt sett er EØS-rettslig forpliktet til å følge forordningen og der man materielt sett ikke har en forpliktelse til å følge forordningens regler.

Etter lovforslagets § 2 og § 5 vil loven og forordningen gjelde med mindre noe annet er bestemt i eller i medhold av lov. Som departementet redegjør for vil situasjonen her kunne være forskjellig alt ettersom man er utenfor eller innenfor rekkevidden av EØS-avtalen. Er man innenfor kan det oppstå spørsmål knyttet til lovgivning på et område hvor forordningen krever eller gir adgang til nærmere nasjonal regulering. I så fall må reguleringen være i henhold til forordningens regler og rammeverk. Er man utenfor rekkevidden av EØS-avtalen vil man stå friere, i den forstand at man ikke står overfor en EØS-rettslig forpliktelse.

Det er viktig at disse forholdene i størst mulig utstrekning behandles og avklares i forbindelse med lov- og forskriftsregulering som direkte eller indirekte berører behandling av personopplysninger. Det bør derfor utarbeides veiledning om grensedragningen, enten i utredningsinstruksen eller på annet vis, som kan brukes i den forbindelse.

10.1. Riksrevisjonens behandling av personopplysninger

Departementet foreslår å ikke videreføre gjeldende personopplysningsforskrift § 1-1 ettersom den er overflødig ved siden av riksrevisjonsloven § 17 annet ledd. Etter disse reglene gjelder det unntak fra retten til innsyn og retting, samt reglene om meldeplikt og konsesjon. De to sistnevnte vil bortfalle med forordningen og reiser ingen spørsmål.

Vi antar imidlertid at unntakene fra innsyn og retting etter forordningen artikkel 15 og 16 er tenkt videreført i riksrevisjonsloven § 17 annet ledd. I så fall mener vi det bør foretas en

fornyett vurdering av om det er adgang etter forordningen artikkel 23 til å opprettholde disse unntakene i såpass vidtrekkende form og på en så kategorisk måte.

Vi kan her vise til personopplysningsforskriften § 1-1 i sin tid ble gitt på basis av innspill fra Justiskomiteen i Innst. O. nr. 51 (1999-2000) side 9 og 10. Komiteen begrunnet sitt syn med at

«Riksrevisjonens kontrollvirksomhet innebærer midlertidig behandling av andre instansers personopplysninger i det øyemed å kontrollere den aktuelle instansens arbeid. Komiteen viser til at reglene i loven er utformet med sikte på primærinstansens ansvar, og mener det er grunnlag for å unnta Riksrevisjonen fra reglene om innsyn, retting (...) der Riksrevisjonen behandler opplysninger innhentet fra andre instanser som del av sin kontrollvirksomhet.»

På bakgrunn av disse merknadene forutsatte komiteen at departementet i forskrift ville gjøre unntak fra innsyn og retting inntil ny lov om riksrevisjon, som var under arbeid, kom på plass.

Den begrunnelsen som ble gitt da er neppe holdbar nå for å begrense innsynsretten og adgangen til å kreve retting i samsvar med artikkel 23. Regelen synes i realiteten å være begrunnet med at rettighetene kan begrenses fordi det (1) bare er tale om midlertidig behandling og at (2) retten til innsyn og retting kan skje hos primærinstansen (som det noe misforstått legges til grunn er det primære siktemålet for reglene for behandling av personopplysninger) siden Riksrevisjonen får opplysningene derfra.

Ved å gjøre kategorisk unntak fra innsynsretten har man i realiteten undergravet gjennomsiktighetsprinsippet i forholdet mellom den registrerte og Riksrevisjonen. I praksis fratar man samtidig den registrerte mulighet til å utøve andre rettigheter, for eksempel rett til å fremme innsigelser etter artikkel 21 eller gjøre krav på sletting av personopplysninger. Dette er rettigheter som fort blir illusoriske dersom det ikke er noen gjennomsiktighet.

Det bør det på denne bakgrunn spilles inn overfor Stortinget på egnet måte at riksrevisjonsloven § 17 bør revideres, siden det er Stortinget selv som er ansvarlig for denne loven.

10.2. Behandling av personopplysninger som er nødvendig av hensyn til rikets sikkerhet

Departementet foreslår å videreføre personopplysningsforskriften § 1-2 om begrensning i Datatilsynets myndighet til å kreve informasjon og gjøre andre undersøkelser der man står overfor behandling av personopplysninger som er nødvendig av hensyn til rikets sikkerhet mv.

Det er forslått å ta denne begrensningen inn i ny lov § 19, som står i kapittelet om tilsynsmyndigheten. Dette innebærer at behandling av personopplysninger som er nødvendig av hensyn til rikets sikkerhet mv., som et utgangspunkt er omfattet av personopplysningslovens og forordningens materielle virkeområde, så langt ikke noe annet følger av annen lov.

For organer som PST og E-tjenesten, som klart nok behandler personopplysninger begrunnet i hensynet til rikets sikkerhet mv., vil man være utenfor det materielle virkeområde til personopplysningsloven. For PST gjelder politiregisterloven, og for E-tjenesten vil det ifølge høringsnotatet gis regler om behandling av personopplysninger i etterretningstjenesteloven. Vi forstår det slik at disse reglene skal bli helhetlige slik at ingen deler av personopplysningsloven/forordningen skal gis virkning overfor E-tjenesten. Overfor disse organene finnes det også en egen tilsynsordning gjennom EOS-utvalget.

EOS-utvalget kontrollerer også Nasjonal sikkerhetsmyndighet og Forsvarets sikkerhetsmyndighet, så langt det gjelder disse organenes tjenester som har til formål å ivareta rikets sikkerhet. Om disse organenes behandling av personopplysninger til dette formålet faller innunder personopplysningslovens/forordningens materielle virkeområde, er det ikke sagt noe om i høringsnotatet. Et eksempel her er sikkerhetsloven.

Datatilsynet mener at forslaget til ny personopplysningslov § 19 tredje ledd er uheldig fordi den skaper mye uklarhet. Gjeldende regulering (personopplysningsforskriften § 1-2) har skapt tilsvarende uklarhet.

Etter ordlyden er det *selve behandlingen* av personopplysninger som anses nødvendig av hensyn til rikets sikkerhet mv. som skal unntas fra forordningens artikkel 58 nr. 1. Det betyr at dersom man står overfor en slik type behandling, uavhengig av hvem som er involvert, skal Datatilsynet ikke ha myndighet til å gjøre undersøkelser.

Forordningen artikkel 58 nr. 1 regulerer Datatilsynets myndighet til å gjøre undersøkelser overfor behandlingsansvarlige eller databehandlere. Lovforslagets § 19 tredje ledd begrenser imidlertid myndigheten Datatilsynet har til å gjøre undersøkelser av en viss type behandling, nemlig den som er begrunnet i hensynet til rikets sikkerhet mv. Her kan man tenke seg at en rekke ulike behandlingsansvarlige/databehandlere involvert. Vi illustrerer dette med et par eksempler:

- PST samler inn/mottar informasjon fra en rekke ulike kilder som ledd i sitt arbeid. Det kan være formelle prosesser, men kanskje også på mer uformelt vis. Sett ut fra forordningens/personopplysningsregelverkets system kan vi stå overfor en rekke behandlingsansvarlige utover PST. Skal Datatilsynet for eksempel kunne undersøke de som gir informasjon til PST?
- Ifølge merknadene til personopplysningsforskriften § 1-2 (kongelig resolusjon av 15.12.2000) vil hensynet til rikets sikkerhet også omfatte «beredskapshensyn som har sammenheng med rikets sikkerhet». Her kan for eksempel såkalt objektsikring komme inn, altså det å beskytte sentrale institusjoner som Stortinget og Regjeringskvartalet. Her vil det kunne være flere behandlingsansvarlige involvert, for eksempel vaktelskaper, som behandler personopplysninger som ledd i sitt arbeid med å beskytte institusjonene. Skal Datatilsynet her kunne kontrollere hvordan personopplysninger behandles?

Vi mener ikke at vi skal eller bør være tilsynsorgan i tilknytning til behandling av personopplysninger begrunnet i rikets sikkerhet. Slik reglene er utformet er det imidlertid grunn til å frykte at det finner sted behandling av personopplysninger som henger sammen med rikets sikkerhet og andre vitale nasjonale sikkerhetsinteresser, og som både faller utenfor både EOS-utvalgets og Datatilsynets myndighet til å undersøke. Da står man i så fall i en situasjon med begrensede kontroll- og tilsynsmekanismer, hvilket er problematisk.

Vi mener grensen her, som et utgangspunkt, bør trekkes ut fra hvem som skal være tilsynsmyndighet. Utgangspunkt her kan tas i at Datatilsynet er tilsynsmyndighet der EOS-utvalget ikke er det.

Forslaget til personopplysningsloven § 19 tredje ledd er også problematisk av andre grunner. Etter sin ordlyd begrenses bare Datatilsynets kompetanse etter artikkel 58 nr. 1 altså vår undersøkelsesmyndighet. Vår kompetanse etter artikkel 58 nr. 2 til å treffe såkalte korrigerende tiltak, er imidlertid i behold. Det gir ikke god mening at Datatilsynet har vidtgående beføyelser, i alle fall på papiret, til å treffe tiltak mot lovstridig behandling, samtidig som vi ikke har noen myndighet til undersøke saken for å bringe faktum på det rene.

I forlengelsen av dette kan vi peke på at den registrertes rett til å klage etter artikkel 77 vil bestå, men denne retten blir jo illusorisk i slike tilfeller fordi tilsynsmyndigheten ikke har kompetanse til å undersøke det påklagde forholdet. Lovforslaget § 19 tredje ledd har altså rekkevidde utover at den setter artikkel 58 nr.1 om undersøkelsesmyndighet til side.

Vi kan her også vise til lovutkastet § 13 første ledd bokstav a, som gjør unntak fra informasjon og innsyn for opplysninger som er av betydning for blant annet nasjonale sikkerhetsinteresser. Dersom den registrerte blir nektet innsyn under henvisning til denne bestemmelsen, er det forordningens system at den registrerte skal kunne klage til Datatilsynet som kan undersøke rettmessigheten av dette. Med forslaget til § 19 tredje ledd står vi imidlertid i en situasjon hvor Datatilsynet ikke kan kontrollere. Det fremstår ikke som holdbart, særlig hvis det ikke finnes andre mekanismer for kontroll. Se nærmere om dette i punkt 8.2.

Videre vil jo reglene om vurdering av personvernkonsekvenser og forhåndsdrøftelser, jf. artikkel 35 og 36, fremdeles gjelde. Den som behandler personopplysninger som henger sammen med rikets sikkerhet mv., og som materielt sett må følge personopplysningslovens/forordningens regler, må da etter omstendighetene konsultere Datatilsynet og gi oss nødvendig informasjon. Hvis tanken med forslaget til § 19 tredje ledd er at Datatilsynet ikke bør få tilgang til gradert informasjon, må nok reglene her få en annen innretning.

Datatilsynet mener det er viktig at departementet her vurderer de overnevnte problemstillingene knyttet til behandling av personopplysninger som er begrunnet i hensynet til rikets sikkerhet mv. nærmere.

10.3. Behandling av personopplysninger i rettspleien

Departementet foreslår å videreføre personopplysningsforskriften § 1-3 i lovutkastet § 2 annet ledd:

Loven gjelder ikke for saker som behandles eller avgjøres i medhold av rettspleielovene (domstoloven, straffeprosessloven, tvisteloven og tvangsfullbyrdelsesloven)

Ordlyden knytter unntaket fra lovens anvendelsesområde til *saker* som behandles eller avgjøres i medhold av rettspleielovene. Dette har i praksis medført uklarhet. Poenget her er at det i tilknytning til saker som behandles etter rettspleielovene vil være mange forskjellige aktører involvert. Foruten domstolen, kan det være sakens parter, prosessfullmektiger, rettsoppnevnte sakkyndige, politi og påtalemyndighet mv. Man står med andre ord overfor mange ulike behandlingsansvarlige i relasjon til personopplysningsbehandling.

Ordlyden gir ingen anvisning på hvilke organer eller aktører som i sin befatning med rettspleien er omfattet av unntaket. Se til sammenlikning advokatlovutvalgets utredning om ny advokatlov NOU 2015:3 punkt 16.4.2 om advokatvirksomhet og forholdet til personopplysningsloven, der utvalget vurderer advokaters behandling av personopplysninger i tilknytning til saker i rettspleien.

Det bør klargjøres i proposisjonen hva dette unntaket er ment å dekke.

Det også andre sider ved denne regelen som er problematisk. Departementet legger til grunn, uten nærmere begrunnelse, at «behandling av saker i medhold av rettspleielovene ligger utenfor EØS-avtalens saklige virkeområde og at Norge ikke er bundet av forordningen på dette punkt». Vi mener det er tvilsomt om dette er riktig, iallfall ikke sånn helt uten videre.

Forordningen, og personverndirektivet, har som et sentralt formål å sikre fri flyt av personopplysninger på tvers av landegrensene. Å ha felles regler og rammeverk for behandling av personopplysninger er ment forbedre betingelsene for det indre markedet. Tanken er at ulik standard – altså ulike regler – på kryss og tvers av landegrensene vil kunne føre til hindringer i utviklingen av det indre markedet.

Praksis fra EU-domstolen viser at unntakene fra det materielle virkeområdet må tolkes snevert, også med tanke på hva som er relevant opp mot en indre markedssammenheng og de grunnleggende friheter (de fire friheter).

Et eksempel her er sakene C-465/00, C-138/01 og C-139-01 (Österreichischer Rundfunk)⁹³. Saken gjaldt den Østerrikske riksrevisjonens behandling av personopplysninger, nærmere bestemt opplysninger om ansattes lønn og navn. Behandlingen fant sted i forbindelse revisjon og kontroll av offentlig pengebruk. Østerrike anførte at man var utenfor personverndirektivets virkeområde fordi riksrevisjonens undersøkelser av offentlig pengebruk falt utenfor

⁹³ Sakene slått sammen til en sak.

fellesskapsretten. Videre ble det pekt på at kontrollen ikke virket som en hindring på fri flyt av arbeidskraft.

EU-domstolen forkastet dette synspunktet. Etter å ha understreket at formålet med direktivet er å sikre fri flyt gjennom harmonisering av reglene for vern av personopplysninger og at reglene er gitt for å sikre betingelsene for utviklingen av det indre markedet, uttalte domstolen (avsnitt 42):

(...) Directive 95/46 cannot depend on whether the specific situations at issue in the main proceedings have a sufficient link with the exercise of the fundamental freedom guaranteed by the Treaty, in particular, in those cases, the freedom of movement of workers. A contrary interpretation could make the limits of the field of application of the directive unsure and uncertain, which would be contrary to its essential objective of approximating the laws, regulations and administrative provisions of the Member States in order to eliminate obstacles to the functioning of the internal market deriving precisely from disparities between national legislation.

Under henvisning til dette, og blant annet at behandlingen for øvrig ikke falt innunder unntakene som eksplisitt er nevnt i direktivets artikkel 3 nr. 2, slik som nasjonal sikkerhet, forsvar mv., fant EU-domstolen direktivet anvendelig.

Den danske utredningen har for øvrig behandlet det materielle virkeområdet utførlig, blant annet i lys av rettspraksis. Det er lagt til grunn at for eksempel behandling av personopplysninger i forbindelse med direkte beskatning faller innenfor, selv om direkte beskatning som sådan ikke er en del fellesskapsretten.

Departementet synes å legge til grunn at innenfor EU vil forordningen gjelde for domstolen. Dette er vi enig i. Danmark har også lagt dette utvetydig til grunn i sin utredning. Dette følger for så vidt også av artikkel 55 nr. 3, som sier at datatilsynsmyndighetene ikke skal ha myndighet til kontrollere domstolenes behandling av personopplysninger under utøvelsen av domsmyndighet. Denne bestemmelsen ville vært unødvendig dersom man uansett var utenfor regelverkets materielle virkeområde.

Konsekvensene av det standpunktet departementet inntar er at i relasjon til rettslig prosess i Norge er vi ikke en del av det harmoniserte vernet av personopplysninger som er forordningens intensjon. Strengt tatt vil da Norge, sett fra EU-landenes side, ikke uten videre kunne anses som et trygt land å overføre opplysninger til. Det skaper usikkerhet sett fra et fri flyt perspektiv. Dette er som ikke er helt upraktisk, tatt i betraktning at deltakelse i rettslige prosesser på kryss og tvers av landegrensene i EØS, hvor personopplysninger må kunne flyte, ikke er uvanlig. For eksempel bør selskaper og borgere hjemmehørende i EU-land kunne delta i rettslig prosess i Norge, og følgelig overføre personopplysninger hit i den forbindelse, og samtidig være trygg på at standarden for vern av personopplysninger er den samme.

I forlengelsen av dette kan vi også peke på at forordningen selv gir den registrerte rett til anlegge erstatningssøksmål mot behandlingsansvarlige og databehandlere for brudd på reglene, og som hovedregel skal søksmål anlegges i det land hvor foretaket er etablert.

Ettersom mye personopplysningsbehandling i dag foregår i sammenheng med handel/tjenester på kryss av tvers av landegrensene, vil det kunne være slik at en EU-borger kommer i tvist med en behandlingsansvarlig i et annet land, for eksempel Norge. Ved rettslige prosess vil personopplysninger etter omstendighetene måtte krysse landegrenser, og vi har vanskelig for å se det annerledes enn at harmoniserte regelverket for vern av personopplysninger må gjelde. Et motsatt syn vil skape uklarhet og usikkerhet.

Basert på dette mener vi at departementet bør foreta en mye grundigere vurdering enn det som er gjort i høringsnotatet. Dersom standpunktet opprettholdes bør det gis en begrunnelse.

Vårt syn er at forordningen *som utgangspunkt* må gis virkning på behandling av personopplysninger i forbindelse med rettslig prosess. Det betyr ikke at forordningen alltid skal gjelde fullt ut. For eksempel er man for politiets behandling i forbindelse med irettføring utenfor idet man er over i politiregisterloven. For domstolene gjelder uansett unntaket i forordningen med hensyn til Datatilsynets tilsynsmyndighet.

11. Behandling av personopplysninger om straffedommer og lovovertrедelser

Forordningens artikkel 10 kommer til anvendelse ved behandling av opplysninger om straffedommer og lovovertrедelser eller tilknyttede sikkerhetstiltak.

Datatilsynet er enig i at det ikke er helt klart akkurat hva slags type opplysninger som omfattes. Verken forordningens ordlyd eller fortale bringer fullstendig klarhet i dette, og det samme gjelder direktivet. Vårt inntrykk er at dette er et område hvor det har vært ulik innfallsvinkel fra land til land. Også den svenske og danske utredningen viser dette.

Den engelske forordningsteksten bruker ordene «criminal convictions and offences». Etter vårt syn vil det dekke både informasjon som knytter en person til en straffedom og informasjon som knytter en person til en handling som er straffbar uten at det har ført til noen straffedom.

Etter vårt skjønn er det antakelig også grunn til i praksis å oppstille noen kvalitative krav til opplysningene for at de skal være omfattet. For eksempel kan opplysninger som knytter en person til en straffbar handling være mer eller mindre sikker. Der det ikke foreligger en straffedom, kan det være mer eller mindre sikkert at personen faktisk har vært involvert i et straffbart forhold. Terskelen her kan ikke ligge for høyt, for eksempel ved å si at bestemmelsen omfatter bare opplysninger om et straffbart forhold der det er på det rene at personen har begått forholdet. På annen den annen side er det grunn til å avgrense mot eksempelvis opplysninger knyttet til at person angivelig har gjort noe straffbart som er av en slik karakter at de ikke er egnet til å hefte ved personen – for eksempel ubegrunnede påstander.

Departementet legger til grunn at straffeprosessuelle avgjørelser vil falle innunder begrepet «tilknyttede sikkerhetstiltak». Det er vi enig i. For eksempel bør en opplysning om at en person er varetektsfengslet eller ilagt besøksforbud være omfattet.

11.1. Behov for supplerende bestemmelser?

Departementet viser til at en rekke bestemmelser gir i dag hjemmel for å behandle opplysninger om straffedommer mv., og ber om høringsinstansenes syn på om det behov for supplerende bestemmelser.

Det er her fornuftig å skille mellom behandling av slike opplysninger som foretas av offentlige organer og private.

Artikkel 10 tar utgangspunkt i at behandling av opplysninger om straffedommer mv. bare skal skje under offentlig myndighets kontroll. Så lenge det er tilfellet, vil artikkel 10 i seg selv ikke stille seg i veien for det. Offentlige myndigheters behandling av slik informasjon må imidlertid være i samsvar for forordningen for øvrig. Blant annet kan man bare behandle slik informasjon så langt det ligger innenfor hva som er lovlig etter artikkel 6. I det vesentlige vil vi tro at behandling av slik informasjon her henger sammen med utførelsen av oppgaver i allmenhetens interesse eller utøvelsen av offentlig myndighet, jf. artikkel 6 nr. 1.bokstav e, og det må da foreligge nærmere nasjonale lovregler i samsvar med artikkel 6 nr. 2 og nr. 2.

Etter vår mening bør man i relasjon til offentliges organers behandling av opplysninger om straffedommer mv. bestrebe seg på å ha konkret lovgivning om dette i den spesifikke sektorlovgivningen som gjelder for de ulike organer. For eksempel bør NAVs adgang til å behandle slik type informasjon reguleres i det regelverket som gjelder særskilt for NAV, og det samme gjelder for eksempel for skattemyndighetene eller tollmyndighetene.

For private er utgangspunktet et annet etter artikkel 10. De kan ikke behandle slik informasjon med mindre det er tillatt i nasjonal lovgivning. Slik lovgivning må gi tilstrekkelig garantier for rettighetene og frihetene til de registrerte. Dersom det ikke er gitt slike nasjonale regler, så vil det være brudd på artikkel 10 om den private behandler opplysningene. I denne forbindelse representerer altså artikkel 10 et selvstendig vern.

Etter vår forståelse betyr det at den behandlingsansvarlige her ikke falle tilbake på de alminnelige rettsgrunnlagene i artikkel 6, slik som ivaretagelse av en berettiget interesse (bokstav f) eller nødvendig for å gjennomføre en avtale (herunder levere en tjeneste). Antakelig kan man heller ikke falle tilbake på samtykke, men mindre det er nærmere bestemt i nasjonal rett at man kan bygge på samtykke i konkrete tilfeller.

Vår erfaring er at private aktørers behandling av opplysninger om straffedommer og lovovertridelser mv. kan være uoversiktlig. Fra vår praksis kan vi nevne arbeidsgivers behov/ønske om å behandle slike opplysninger i ulike sammenhenger – for eksempel bakgrunnsjekk eller i tilknytning til at en ansatt har begått en straffbar handling på jobben. Arbeidsmiljøloven eller annen lovgivning kommer her etter vår forståelse litt til kort.

Et annet eksempel er såkalte IDD-prosesser (Integrity Due Diligence) eller liknende. Dette er undersøkelser som foretas i forbindelse med oppkjøp eller ulike former for samarbeid i næringslivet der man undersøker for eksempel om det foreligger tilknytning til korrupsjon eller annen alvorlig kriminalitet. Her har Datatilsynet valgt i gi tillatelser etter personopplysningsloven § 9 tredje ledd, idet vi har ansatt at det foreligger viktige samfunnsinteresser i bunn. Denne bestemmelsen videreføres ikke i sin nåværende form i ny lov. Her savner vi nærmere nasjonale regler og ber om dette avklares i proposisjonen.

Også i relasjon til private bør man bestrebe seg på å ha konkrete lovregler i tilknytning til lovgivningen som gjelder på ulike områder.

12. Vurdering av personvernkonsekvenser

Personvernforordningen artikkel 35 pålegger behandlingsansvarlige å gjennomføre en generell vurdering av personvernkonsekvenser før behandlingen iverksettes. Denne plikten vil i utgangspunktet også gjelde for offentlige organer.

I forordningens art 35 nr. 10 er det en særregel som gjelder behandling i henhold til artikkel 6 nr. 1 bokstav c (om rettslig forpliktelse) eller bokstav e (om offentlig myndighet) og som har hjemmel i lov. Dersom den aktuelle loven regulerer den eller de aktuelle spesifikke behandlingsaktivitetene, og det allerede er utført en vurdering av personvernkonsekvenser i forbindelse med vedtakelse av loven, så er det ikke nødvendig å gjennomføre en ny vurdering ved igangsetting av aktivitetene. Medlemslandene kan imidlertid fastsette en plikt til å gjennomføre en ny vurdering av personvernkonsekvensene i nasjonal lovgivning. Departementet ber om høringsinstansenes innspill på om hvorvidt dette handlingsrommet bør benyttes, herunder om dette kan være hensiktsmessig for å unngå eventuelle uklare grensedragningspørsmål knyttet til rekkevidden av unntaksregelen i artikkel 35 nr. 10.

Datatilsynet er enig i dette unntaket har en snever rekkevidde, ettersom de lovregulerte behandlingene sjelden er underlagt spesifikke regler om behandlingsaktiviteter. Vi anbefaler likevel at det inntas en bestemmelse som pålegger vurdering av personvernkonsekvensene, selv om når vilkårene i 35 nr. 1 er til stede.

Datatilsynet mener at plikten til å vurdere personvernkonsekvensene bør være knyttet til hvor stor risiko for fysiske personers rettigheter og friheter den som behandlingen innebære, og ikke til hvilket behandlingsgrunnlag den har og uavhengig av hvilke vurderinger som ble gjort tidligere i lovarbeidet. Vi har erfaring for at det ganske ofte er personvernkonsekvenser av forslaget vært mangelfullt utredet. Det vil være uheldig om man fremover lener seg på disse mangelfull vurderingene i stedet for å gjøre nye vurderinger i tråd med forordningens krav. Behandlingsansvarlige vil uansett kunne ta utgangspunkt i forarbeidet som blir gjort som en del av lovarbeidet i den aktuelle vurderingen.

Den viktigste grunnen at det er behov for en slik bestemmelse er at man da vil unngå uklare grensedragningspørsmål og misforståelser omkring bestemmelsens rekkevidde. Datatilsynet har i møter med virksomheter og sektororganisasjoner om forordningens betydning gjentatte

ganger blitt møtt med holdninger som «forordningen unntar behandlingsansvarlige som behandler personopplysninger med hjemmel i lov fra plikten til å gjennomføre en vurdering av personvernkonsekvensen». Datatilsynet frykter at i mangel på en generell presisering om at plikten også gjelder behandlinger hjemlet i artikkel 6 nr. 1. bokstav c eller e, vil en slik utvidende forståelse av bestemmelsen feste seg.

En korrekt anvendelse av det snevre unntaket i artikkel 35 nr. 10 vil dessuten kreve at de behandlingsansvarlige dette gjelder evner å ta stilling til om en lovhjemmelen inneholder regler som er tilstrekkelig spesifikke, samt vurdere om redegjørelsen av personvernkonsekvensene som ble gjort som en del av lovarbeidet er tilstrekkelig. Vi mener det er grunn til å tro at mange behandlingsansvarlige ikke har tilstrekkelig kompetanse til å foreta slike vurderinger.

Datatilsynet mener videre at den vurderingen av personvernkonsekvenser som gjøres som en del av lovarbeidet er av en vesentlig forskjellig karakter og detaljnivå enn det som behandlingsansvarlige er pålagt etter forordningens artikkel 35. Utredningen i tråd med utredningsinstruksen involverer i liten, hvis noen, grad de registrerte. Det fremstår for øvrig for oss som at konsekvensvurderingen som utredningsinstruksen legger opp til verker er eller omfattes som obligatorisk eller risikobasert, og den munner ut i en liste med anbefalinger og ikke pålegg⁹⁴.

Datatilsynet mener videre at en slik regel vil kunne fungere som et viktig pedagogisk grep og minne om viktigheten av å klargjøre personvernkonsekvenser. Det vil også kunne være en rettsikkerhetsgaranti i en situasjon med press fra ulike aktører om å foreta endringer i regelverket uforsvarlig raskt.

Når det gjelder høringsnotatets kapittel 13 om behandlingsansvarlig og databehandler for øvrig, er det, som departementet skriver, lite nasjonalt handlingsrom knyttet til de aktuelle bestemmelse. Vi har derfor ingen merknader knyttet til dette.

Vi støtter departementets forslag om å innta en forskriftshjemmel som kan brukes til nærmere regulering av plikten til forhåndsdrøftinger.

For øvrig har vi en kommentar knyttet til forordningen artikkel 36 nr. 4 om forhåndsdrøftelser. Det følger av denne bestemmelsen at

«medlemsstatene skal rådføre seg med tilsynsmyndigheten ved utarbeidelse av forslag til et lovgivningsmessig tiltak som skal treffes av et nasjonalt parlament eller av et reguleringsstiltak som er basert på slik lovgivningsmessige tiltak, og som er knyttet til behandling»

Datatilsynet forstår denne bestemmelsen som en forpliktelse til å rådføre seg med Datatilsynet, utover den plikten som følger av utredningsinstruksen til å sende lov- og forskriftsendringer på høring. I fortalepunkt 96 er dette nærmere begrunnet. Det vises til at

⁹⁴ Se veileder til utredningsinstruksen kapittel 3, særlig punkt 3.3.6

tilsynsmyndigheten bør rådspørres i det forberedende arbeidet med et lovgivningsmessig tiltak «for å sikre at den tiltenkte behandlingen oppfyller kravene i denne forordningen og særlig for å redusere risikoen den medfører for de registrerte»

Dersom Datatilsynet først blir involvert på høringstidspunktet vil det være begrenset hva vi kan komme med av innspill og det vil være vanskelig å komme med forslag som faller utenfor det som er foreslått i høringen. På hvilken måte Datatilsynet bør involveres i forkant av høringen vil blant annet komme an på hvor inngripende den aktuelle behandling av personopplysninger er.

Vi ber om at dette presiseres i proposisjonen.

13. Personvernråd giver

Datatilsynet har merknader knyttet til begrepet personvernråd giver, krav til personvernråd giver i offentlig sektor, utvidelse av plikten til å utpeke personvernråd giver, utvidelse av personvernråd giverens oppgaver og eventuell videreføring av ordning med Norsk senter for forskningsdata (NSD) som personvernråd giver.

Datatilsynet støtter departementets forslag til taushetspliktsbestemmelse og har ingen merknader til departementets forslag til bestemmelse.

13.1. Begrepet personvernråd giver

Departementet foreslår å oversette begrepet «*data protection officer*» (DPO) til «personvernråd giver» og ikke «personvernombud», og endrer på denne måten et begrep som har blitt innarbeidet i norsk praksis og regelverk gjennom mer enn 15 år. Departementet begrunner ikke denne foreslåtte endringen, ut over å konstatere at man ved å endre til personvernråd giver får samme begrep som i den norske oversettelsen av direktivet om behandling av personopplysninger i straffesakskjeden, altså begrepet som er brukt i politiregisterlov- og forskrift.

Datatilsynet er uenig i denne endringen og anbefaler på det sterkeste at begrepet «personvernombud» beholdes som den norske oversettelsen av «*data protection officer*». Vi vil i det følgende begrunne vårt standpunkt.

«Personvernombud» er et godt innarbeidet begrep både i Norge og Sverige. Nær 600 norske virksomheter har oppnevnt «personvernombud», som igjen forholder seg til mange tusen egne ansatte og enda mange flere registrerte. Til sammenligning er det per i dag kun et titalls personvernråd givere innen politiet og ordningen med personvernråd givere innen politiet har bare eksistert i noen få år. Disse har også har en mindre selvstendig rolle enn samme rolle etter personvernforordningen.

Slik vi ser det er det derfor heller ikke problematisk å videreføre ordningen med to begreper, altså å benytte begrepet «personvernrådgiver» på politiområdet, men beholde «personvernombud» på forordningens område.

Departementet bemerker i høringsbrevet at den danske versjonen av forordningen benytter begrepet «databeskyttelsesrådgiver», mens den svenske versjonen benytter begrepet «dataskyddsbud». Det er grunn til å anta at Sverige, med sine mer enn åtte tusen «personuppgiftsombud», har foretatt erfaringsbaserte vurderinger når de har bestemt seg for å videreføre begrepet «ombud». Danmark har på sin side ingen erfaring med ordningen.

Et svært viktig moment er at en endring av rollens betegnelse vil signalisere en svekkelse av rollens uavhengighet, selvstendighet og autoritet, sammenlignet med dagens betegnelse. Begrepet «rådgiver» gir ikke de riktige assosiasjonene til innholdet i stillingen og oppgavene til DPO, slik dette er beskrevet i forordningen. Dette omfatter vi som et paradoks, siden en tydelig og markant styrking av rollen som DPO er en vesentlig endring i forordningen.

Begrepet «rådgiver» brukes i svært mange andre sammenhenger, for eksempel sikkerhetsrådgiver eller HR-rådgiver. Hvis man går for «personvernrådgiver» mener vi at det vil være mindre intuitivt at dette er en lovfestet rolle med spesifikke oppgaver og plikter, som ikke skal motta instruksjoner om utførelsen av sine oppgaver. «Rådgiver», spesielt i offentlige virksomheter, viser til en nøytral stillingsbeskrivelse, som kun unntaksvis vil være i samsvar med forventningene til selvstendighet og plassering i organisasjon som uttrykkelig er fastsatt i forordningens artikkel 38 nr. 3.

Det vises videre til at det også i andre sammenhenger benyttes betegnelsen «ombud» på medarbeidere som er ansatt i den aktuelle virksomheten, men som likevel innehar en uavhengig rolle med det formål å sikre etterlevelse av et spesifikt regelverk. «Pasientombud» og «verneombud» er eksempler på dette.

Dette er ikke bare Datatilsynets oppfatning, flere av de eksisterende personvernombudene har tatt opp dette temaet med oss og uttrykker bekymring knyttet til å gå bort fra betegnelsen «personvernombud». De mener at dette vil signalisere en uheldig «nedgradering» av deres rolle og posisjon i virksomheten.

Vi siterer for øvrig en tilbakemelding vi har fått fra Språkrådet, etter å ha konferert med dem når det gjelder forståelse av begrepene «ombud» og «rådgiver»:

«Vi støtter tankegangen i vurderingene av de to orda og konklusjonen om at personvernombud bør beholdes. Det er grunn til å legge stor vekt på at betegnelsen personvernombud er innarbeidd gjennom over 15 år med en liknende ordning. Dette spørsmålet ligger innenfor Datatilsynets fagfelt, og vurderingene fra dere bør veie tungt.....»

13.2. Personvernrådgiver i offentlig sektor

Datatilsynet har allerede begynt å motta spørsmål om hvor langt plikten til å ha personvernombud i det offentlige strekker seg, eksempelvis om et interkommunalt selskap som drifter et knippe kommuners IT-systemer må ha personvernombud. Dette er spørsmål som det ofte er vanskelig å svare på. Artikkel 29-gruppen skriver følgende i sin veiledning om Data Protection Officers:

«The GDPR does not define what constitutes a ‘public authority or body’. The WP29 considers that such a notion is to be determined under national law.»

Det er trolig ikke behov for å avklare dette i loven, men det vil være svært nyttig dersom det i proposisjonen gis god veiledning om hva som i en norsk kontekst skal forstås som offentlige myndigheter og organer i relasjon til plikten til å ha personvernombud. Slik vi ser det må dette ses i sammenheng med hensynene bak det at offentlig sektor skal ha personvernombud. Det handler både om at offentlige organer ofte behandler store mengder og ofte sensitive personopplysninger, og ikke minst om at enkeltmennesket i møte med det offentlige ofte har liten makt over om, og hvordan, deres personopplysninger behandles.

I høringsnotatet beskrives virkeområdet for den pålagte ordningen om personvernombud i offentlig sektor slik:

«Etter departementets vurdering tilsier en alminnelig språklig forståelse av forordningen at de organer som omfattes av offentliglova § 2 første ledd bokstav a, må ha personvernrådgiver, mens rettssubjektene i offentliglova § 2 første ledd bokstav b til d faller utenfor.»

Vi er enig i at de organene som omfattes av offentliglova § 2 første ledd bokstav a må omfattes av plikten til personvernrådgiver i forordningen. Avgrensningen om at rettssubjekter som er omfattet av offentliglova § 2 første ledd bokstav b til d er ikke forpliktet til å ha personvernrådgiver er imidlertid uheldig. Dette vil trolig gjøre forståelsen av begrepet «offentlig myndighet eller offentlig organ» i forordningens forstand for snever, både ut fra formålet med forordningen og det vi mener er en naturlig språklig forståelse av ordlyden. Vi presiserer at *ikke* alle organer som omfattes av § 2 første ledd bokstav b til d nødvendigvis bør være forpliktet til å ha personvernrådgiver, men det er uheldig dersom det i lovens forarbeider inntas et så kategorisk standpunkt.

Utfordringen, så langt vi kan se, ligger særlig i kommunal sektors utskillelse av deler av sin drift i egne selskaper, eventuelt i samarbeid med andre kommuner. Utskillelse av deler av driften skjer i stor skala og ofte på en måte som innbyggerne verken tenker over eller merker noe til. Etter det vi forstår, vil altså mange av virksomhetene som er skilt ut i kommunal sektor *ikke* falle inn under offentliglova § 2 første ledd bokstav a, men eksempelvis bokstav c for interkommunale selskaper eller bokstav d for stiftelser. Her må det ses hen til at formålet med offentlighetsloven og personvernregelverket er helt forskjellig, og at hensynene som ligger bak offentliglova og hensynet til personvern i noen tilfeller kan være i konflikt med hverandre.

Slik vi ser det, bør virksomheter som er eid av det offentlige, og som utfører oppgaver vi forbinder med det offentlige – som typisk fatter vedtak eller gir offentlige tjenester – ha personvernombud. Det blir også urimelig hvis en kommunes måte å organisere sitt ansvar og sine oppgaver på skal få betydning for om en aktuell bruk av personopplysninger er omfattet av plikten til å opprette et personvernombud eller ikke. Etter vårt syn kan det ikke legges stor vekt på at obligatorisk personvernombud blir for byrdefullt. Kommunene må uansett ha personvernombud, og man må vurdere om kommunens personvernombud også skal ha ansvar for de forskjellige utskilte selskapene.

Grensedragningen i offentlighetsloven mot virksomheter som, på tross av offentlig eierskap, fungerer som markedsaktører i konkurranse med private, er trolig hensiktsmessig også etter personvernregelverket. Disse bør ikke ha en plikt til å ha personvernombud etter artikkel 37 nr. 1 bokstav a.

For å oppsummere, Datatilsynet mener at det er for snevert å avgrense plikten til å ha personvernrådsgiver til organet som omfattes av offentleglova bokstav a. En kategorisk avgrensningen mot organer som omfattes av § 2 første ledd bokstav b til d er uheldig. Dette er imidlertid en kompleks problemstilling og vi har per i dag ikke en klar anbefaling til hvor grensene for artikkel 37 nr1 bokstav a bør gå. Dette krever inngående kunnskap om offentlighetsloven, kommunal organisering og kjennskap til andre lovverk der begrepet offentlig myndighet er brukt. Samtidig er dette noe vi får mange spørsmål om og som må avklares forholdsvis raskt.

Vi ber derfor departementet, som også er ansvarlig for offentleglova, se nærmere på hvordan bestemmelsen i forordningen om personvernombud i offentlig sektor bør forstås. Dersom det viser seg vanskelig å finne en naturlig grense med utgangspunkt i offentleglova, bør man vurdere å benytte mer kvalitative beskrivelser av hvilke offentlige virksomheter kravet gjelder for.

13.3. Utvidelse av plikten til å utpeke personvernrådsgiver

Etter departementets vurdering bør det ikke på nåværende tidspunkt gis nasjonale regler som utvider plikten til å utpeke personvernrådsgiver utover det som følger av artikkel 37 nr. 1.

Datatilsynet er enig i denne vurderingen. Vi mener likevel at gjennom forslaget til § 6 første ledd bokstav d i ny personopplysningslov foretar departementet en de facto utvidelse av plikten til å ha personvernombud.

Kravet om tilråding fra personvernombud gjelder, ifølge forslaget, alt forskning på sensitive personopplysninger, som ikke er regulert i lov. Dette omfatter både samtykkebasert forskning, og forskning der samtykke fra de registrerte ikke foreligger, jf. forslag til § 6 andre ledd. Særskilt regulering av bruken av sensitive personopplysninger i forskningsaktiviteter finner vi per i dag bare i helseforskningsloven. Som nevnt over er det, utover dette, personopplysningsloven og helseregisterloven som setter rammene for behandling av (sensitive) personopplysninger til forskningsformål.

Departementets forslag innebærer at institusjoner som ønsker å iverksette forskning som innebærer bruk av sensitive personopplysninger, og som ikke omfattes av helseforskningsloven, i praksis må ha personvernrådgiver for å få gjennomført dette. Dette selv om en vurdering av de generelle vilkårene i artikkel 37 nr. 1. bokstav a til c ikke skulle tilsi en slik plikt, for eksempel fordi behandlingen av sensitive personopplysninger ikke er «stor skala» eller «kjernevirksomhet» eller fordi ikke virksomheten er offentlig.

Datatilsynet stiller spørsmål ved om departementets forslag til § 6 første ledd bokstav d i praksis vil innebære at alle forskningsinstitusjoner må ha personvernrådgiver. Dette bør i så fall synliggjøres i form av nasjonal regulering, slik forordningens artikkel 37 nr. 4 krever.

13.4. Utvidelse av personvernrådgiverens oppgaver?

Departementet skriver i høringsnotatet at de er i tvil om forordningens artikkel 39 nr. 1 åpner for å pålegge personvernrådgivere ytterligere plikter ved nasjonal lovgivning, men kan uansett ikke se at det skulle være behov for en slik utvidelse.

Datatilsynet støtter denne vurderingen. Artikkel 39 nr.1, sett i sammenheng med artikkel 38 nr. 6 (plikten databehandler eller behandlingsansvarlig har til å sikre at andre oppgaver eller plikter ikke fører til interessekonflikt), ikke kan forstås slik at det er adgang til å utvide pliktene til personvernrådgivere gjennom nasjonal lovgivning, men at den muligheten eventuelt ligger innenfor arbeidsgivers styringsrett i konkrete tilfeller.

Datatilsynet er likevel usikker om departementets forslag i § 6 bokstav d er forenlig med denne konklusjonen. Slik vi ser det er tilråding av forskningsprosjekter en ny type oppgave, som ikke kan utledes av personvernrådgiverens øvrige plikter etter artikkel 39 nr. 1.

I tillegg til at oppgavene vil bli betydelig flere for rådgivere som er tilknyttet virksomheter som driver med forskning, vil krav om tilråding for gjennomføringen av et forskningsprosjekt kreve en rekke andre kvalifikasjoner av en personvernrådgiver enn det som følger av forordningen. Se nærmere i kapittel 6 om vårt syn på dette forslaget.

13.5. Videreføring av ordning med Norsk senter for forskningsdata (NSD) som personvernrådgiver

I høringsnotatets punkt 8.3.6, om behandling av sensitive opplysninger for arkiv, statistikk og forskningsformål, ber departementet om innspill på hvordan ordningen der NSD er personvernrådgiver for en rekke forskningsinstitusjoner kan videreføres, herunder hvorvidt en funksjonsdeling der en institusjon har flere personvernrådgivere som dekker ulike deler av institusjonens aktivitet, kan være en hensiktsmessig løsning.

Datatilsynet er enig i departementets vurdering at Norsk senter for forskningsdata (NSD) sin rolle som personvernombud for en rekke forskningsinstitusjoner har fungert godt. NSD har bygd seg opp et av de beste kompetansemiljøene for å vurdere personvernkonsekvensene av

forskningsprosjekter i Norge. Datatilsynet ser imidlertid ikke at forordningen åpner for at det er mulig å ha flere personvernombud i en virksomhet.

Datatilsynet har gått igjennom forordningsteksten, veiledningen om personvernombud fra Artikkel 29-gruppen, samt underlagsdokumentene som ble brukt under forhandlingene mellom Kommisjon, Parlament og Råd uten å finne noen holdepunkter til støtte for en tolkning i retning av at det kan være flere personvernombud i en virksomhet. Selv om forholdet ikke uttrykkelig er omtalt i disse dokumentene, peker innretning og oppbygning samt ordlyden i tekstene entydig mot at det kun er mulig å ha ett ombud i hver virksomhet. Tilsynene i Sverige, England og Tyskland, som alle har lang erfaring med personvernombudsordningen, tolker også forordningsteksten slik at det i utgangspunktet skal være ett personvernombud i en virksomhet.

Forordningsteksten referer konsekvent til personvernombudet og Artikkel 29-gruppens veileder peker i samme retning. Blant annet står i punkt 2.1 i veilederen at hvis man utnevner et personvernombud skal dennes oppgaver gjelde alle behandlingene i en virksomhet. Datatilsynets erfaring med ordningen viser også at det er utfordrende for virksomheter å trekke klare og tydelige ansvarslinjer mellom ulike type behandlinger som ligger innenfor ansvarsområdet til ulike personvernombud. Også i utførelsen av ombudets oppgave som går på å ha kontakt med og veiledning til de registrerte etter forordningens artikkel 38 nr. 4, er det helt klart mest praktisk at de registrerte forholder seg til en person.

Regelverket åpner imidlertid for at personvernombudet kan være ekstern eller intern, og at vedkommende kan ha en gruppe med medarbeidere rundt seg, samt innhente sakkyndige uttalelser fra andre. Kunnskapen som NSD har opparbeidet kan benyttes gjennom at virksomhetens ombud innhenter råd og uttalelser fra NSD, som dermed kan fungere som et kompetansesenter for slike oppgaver.

14. Melde- og konsesjonsplikt

Etter dagens regelverk er det som hovedregel et vilkår for behandling av personopplysninger at det meldes fra til Datatilsynet. Behandling av sensitive opplysninger krever som hovedregel forhåndsgodkjenning. Slik godkjenning gis i form av konsesjon fra Datatilsynet, og i noen tilfeller gjennom godkjenning med hjemmel i helseforskningsloven fra Regional Etisk komite (REK) eller i form av tilråding fra personvernombud i tråd med personopplysningsforskriften § 7-27.

Meldeplikten er ikke videreført i forordningen. Forordningen legger heller ikke opp til at behandling av sensitive opplysninger må ha forhåndsgodkjenning. I stedet legges det opp til en rekke alternative virkemidler som skal sikre etterlevelse. Behandling av sensitive personopplysninger som hovedregel sikres gjennom å ilegge et tydeligere og større ansvar for den behandlingsansvarlige. I artikkel 36 nr. 5 åpnes det imidlertid opp for at det gjennom nasjonal lovgivning kan settes krav om forhåndsgodkjenning fra tilsynsmyndigheten for enkelte typer behandlinger av allmenn interesse, for eksempel innen områdene sosial trygghet

eller folkehelse. Artikkel 9 nr. 4 åpner også opp for å regulere behandling av visse typer opplysninger.

Departementet drøfter i høringsnotatet hvorvidt konsesjonsplikten bør videreføres, i den grad det er adgang til det innenfor forordningens nasjonale handlingsrom. Departementet foreslår at som hovedregel skal det ikke være et krav om forhåndsgodkjenning, men gir i lovutkastet § 11 forskriftshjemmel til å kunne gjeninnføre konsesjonsplikt, dersom dette viser seg nødvendig av personvern hensyn.

Datatilsynet støtter departementets forslag om å som hovedregel ikke videreføre konsesjonsplikt.

Slik praksis i Datatilsynet er i dag varierer betydningen av konsesjoner fra fagområde til fagområde. På flere områder benyttes såkalte standardkonsesjoner, for eksempel innen bank, forsikring og kredittopplysningsvirksomhet. Den reelle saksbehandlingen i forbindelse med søknader i disse sakene er begrenset, men det er en omfattende prosess å utforme og revidere disse standardkonsesjonene. Bruken av standardkontrakter er med på sikre lik praksis i disse bransjene. På andre fagområder krever en søknad om konsesjon betydelig ressurser til saksbehandling hos Datatilsynet, for eksempel ved konsesjoner for behandling av opplysninger til sekundære formål som omfatter blant annet samfunnsforskning, som vurderes etter personopplysningsloven § 33 og befolkningsundersøkelser, registre og prosjekter som vurderes etter helseregisterloven § 6.

Datatilsynet har gjennomgått sin konsesjonspraksis på ulike områder, sett i sammenheng med de alternative virkemidlene i ny forordning. Vi er enig i at for å gjennomføre det vi oppfatter som grunntanken med ny forordning, nemlig å flytte enda mer ansvaret over på den behandlingsansvarlige, bør det være krav om konsesjon der det er strengt nødvendig.

Slik vi ser der er det imidlertid en forutsetning for at «det nye regimet», uten bruk av forhåndskontroller og standardkonsesjoner, at de øvrige pliktene og tiltakene i forordningen etterlevs. For eksempel at det bes om forhåndsdrøftelser med Datatilsynet og at de alternative strategiene for etterlevelse av regelverket, herunder adferdsregler og bransjenormer, rent faktisk tas i bruk. Dilemmaet er at dette vil ikke vite før det har gått noe tid og det bør derfor vurderes om det er behov for overgangsordninger. Se nærmere om dette nedenfor.

Når det gjelder forskning og sekundærbruk av data mener Datatilsynet som nevnt over at det bør utarbeidetes særlovgivning, se våre synspunkter i kapittel 6. Som det fremgår her er vi bekymret for at det mangler garantier for ivaretagelse av personvernet slik det kreves i artikkel 89 nr. 1.

Når det er sagt, Datatilsynet legger til grunn at det vil foreligge en plikt til forhåndsdrøfting med Datatilsynet for de mest inngripende behandlingene, jf. forordningen artikkel 36.

14.1. Om lovforslagets § 7 – konsesjon til behandling som er nødvendig av hensyn til viktige samfunnsinteresser

I høringsnotatet punkt 15.3.2.2 redegjør Justisdepartementet for dagens anvendelse av personopplysningsloven § 9 tredje ledd. Denne bestemmelsen åpner for at Datatilsynet kan gi behandlingsgrunnlag i særlige tilfeller dersom de andre alternativene i lovens § 9 ikke kan anvendes. Departementet foreslår å videreføre denne adgangen i forslag til ny personopplysningslov § 7, men påpeker at den bør være snevrere enn i dag og forbeholdt «særlige tilfeller».

Departementet viser til at Datatilsynet har gitt en rekke tillatelser med hjemmel i de gjeldende bestemmelsen, blant annet for behandling av opplysninger i forbindelse med antidopingarbeid ved treningssentre, oppreisingsordninger og til det som departementet omtaler som «samfunnsforskningsprosjekter».

Det synes som om departementet har lagt til grunn at Datatilsynet benytter personopplysningsloven § 9 tredje ledd i en større utstrekning enn det som er tilfelle. Behandlingsgrunnlag til forskning (herunder samfunnsforskningsprosjekter) vil alltid vurderes etter personopplysningsloven § 9 h. Denne bestemmelsen gir behandlingsgrunnlag når behandlingen er nødvendig for historiske, statistiske eller vitenskapelige formål, og samfunnets interesse i at behandlingen finner sted klart overstiger ulempene den kan medføre for den enkelte. Bestemmelsen har imidlertid blitt anvendt dersom behandlingen *ikke* kan karakteriseres som forskning, for eksempel til behandling av opplysninger av 22. juli Kommisjonen og til håndteringen av tsunamien i Asia for noen år tilbake.

Datatilsynet er usikker på om det er adgang etter forordningen til å adgang til å ha en slik hjemmel i nasjonal lovgivning.

Bestemmelsen i personopplysningsloven § 9 tredje ledd gjennomfører den tilsvarende bestemmelse i personverndirektivet, artikkel 8 nr. 4. Denne generelle adgangen for medlemsland til å fastsette ytterligere unntak fra forbudet til å behandle sensitive personopplysninger er ikke videreført i forordningen. Dette tror vi neppe er tilfeldig.

Behandling av sensitive personopplysninger utenfor reglene i artikkel 9 nr. 2, det vil blant annet si behandling uten samtykke og uten lovhjemmel, er i praksis forbudt etter forordningen. Siden det ikke lenger en klar hjemmel for nasjonal handlingsrom for å supplere listen med unntak fra forbudet mot behandling av sensitive personopplysninger i forordningens artikkel 9 nr. 2, mener Datatilsynet at det er grunn til å tro at det ikke er adgang til å videreføre bestemmelsen i personopplysningsloven § 9 tredje ledd slik departementet foreslår. Vi mener også at det er uheldig å overlate dette til Datatilsynet. En konsesjon gir ikke de samme mulighetene til å innhente de registrertes synspunkter som ved en offentlig høring ved forskriftsendring.

Dersom departementet kommer til at det er adgang til slik regulering, bør denne adgangen gjøres svært snever. Hvis ikke er vi redd for at Datatilsynet vil få mange henvendelser om dette og det vil kunne oppfattes som en «nødløsning».

14.2. Gjeldende konsesjoner – overgangsregler

Departementet ber om høringsinstansenes syn på behovet for overgangsregler som skal sikre at allerede igangsatte behandlinger av personopplysninger, som Datatilsynet har forhåndsgodkjent gjennom konsesjon, kan fortsette, samtidig som forordningens regler overholdes. Fortalepunkt 171 åpner opp for at tidligere gitte forhåndsgodkjenninger kan fortsette å gjelde inntil de endres, oppheves eller erstattes.

Som nevnt over er det i en forutsetning for at «det nye regimet», uten bruk av forhåndskontroller og standardkonsesjoner, at de øvrige pliktene og tiltakene i forordningen etterleves. Hvordan dette vil fungere vil man ikke vite før det har gått noe tid. Som det også fremgår ovenfor er det store variasjoner mellom samfunnsområder og bransjer med hensyn til hvilken form og betydning bruk av konsesjoner har. Slik vi ser det vil det være behov for overgangsregler, men det vil være stor variasjon mellom ulike typer konsesjoner med hensyn til hvor lenge dette behovet for overgangsordning vil vare.

Der særlovgivning ikke i tilstrekkelig grad ivaretar kravet til supplerende rettsgrunnlag for behandlingen slik forordningen krever, mener Datatilsynet at videreføring av eksisterende konsesjoner kan utgjøre en nødvendig garanti for ivaretagelse av personvernet inntil lovgivning er på plass. Dette vil gjelde for eksempel for etablering av helseregistre i helsesektoren, der de fleste konsesjonene som Datatilsynet gir inneholder vurdering av konkrete tiltak og tilleggskrav til hvordan behandlingen av personopplysninger skal skje, hvordan samtykke skal innhentes eller informasjon skal gis.

Datatilsynet foreslår at det settes en absolutt grense for gjeldende konsesjonenes gyldighet på to år, men med en mulighet for Datatilsynet å oppheve slike tillatelser tidligere, etter en konkret vurdering.

Datatilsynet vil da kunne vurdere de ulike gruppene av konsesjoner særskilt. Innen bank- og finanssektoren mv. kan det være konkurransemessige hensyn som tilsier at overgangsperioden bør begrenses til det som er helt nødvendig. Datatilsynet kan da, i samarbeid med de aktuelle bransjene, komme frem til hva som må være på plass før gjeldende konsesjoner oppheves.

En slik tilnærming vil, slik vi ser det, ivareta hensynet til likebehandling og forutsigbarhet for de behandlingsansvarlige, samtidig som det gir nødvendig insentiv for å få på plass tiltak som gjør at forordningen etterleves.

Det vil også gi de ansvarlig fagdepartementer et incentiv til å få på plass lovhjemler for behandlingen av personopplysninger som ikke har tilstrekkelig behandlingsgrunnlag etter bortfallet av konsesjon.

Dersom departementet ønsker et mer utfyllende innspill på dette punktet kan vi eventuelt komme tilbake til dette.

15. Overføring av personopplysninger til tredjestater

Datatilsynet støtter forlaget om å gi en forskriftshjemmel i forslag til lov §10 andre ledd for kunne å regulere overføringer til utlandet nærmere på et senere tidspunkt, i den grad det er anledning til det innenfor det nasjonale handlingsrommet.

Det kan stilles spørsmål ved om ordlyden i hjemmelen er for vid, den kan gi inntrykk av at det er adgang til å regulere overføring til utlandet som sådan, mens det i realiteten dreier seg om å utnytte handlingsrommet som følger av artikkel 49 nr. 5.

Vi har for øvrig ingen merknader til høringsnotatets kapittel 16 om overføring av personopplysninger til tredjestater.

16. Tilsynsmyndighetenes organisering

Departementet foreslår å videreføre Datatilsynet som det organet som skal håndheve personvernregelverket og ivareta de oppgavene forordningen pålegger tilsynsmyndigheten. Departementet mener at Datatilsynets myndighet også bør omfatte særlovgivningen som faller utenfor EØS-avtalen. Hovedregelen vil derfor være at Datatilsynet har den myndighet som fremgår av forordningen artikkel 57 og 58 for *all behandling* av personopplysninger.

Datatilsynet deler departementets vurderinger av de krav som forordningen stiller tilsynsmyndigheten, slik de er beskrevet i forordningens kapittel VI.

Vi savner imidlertid en omtale i høringsbrevet av hvilke konsekvenser en slik plassering av ansvar eventuelt vil få for *andre myndigheter og organer* som i dag er tillagt oppgaver knyttet til ivaretagelse av personvernet. Et forhold som særlig kunne vært nevnt er at helseforskningsloven gir REK (Regionale komiteer for medisinsk og helsefaglig forskningsetikk) adgang til å forhåndsgodkjenne medisinske og helsefaglige forskningsprosjekter⁹⁵.

Denne forhåndsgodkjenningen omfatter flere forhold, men det er klart at den også omfatter behandlingen av personopplysninger. Med helseforskningsloven ble oppgaver som tidligere lå

⁹⁵ «Forslaget til ny helseforskningslov innfører et nytt, tredje hjemmelsgrunnlag for behandling av helseopplysninger. Et forskningsprosjekt eller en undersøkelse som faller inn under helseforskningslovens virkeområde, skal vurderes i forhold til bestemmelsen om hva som kreves for behandling av opplysninger (behandlingsgrunnlag) i § 33 og øvrige bestemmelser i denne loven.

Det vil være svært positivt at det unngås dobbeltbehandling av forskningsprosjektene i disse sakene, og departementet foreslår derfor at REK også skal være eneste forhåndsgodkjenningsinstans for forskningsprosjekter som involverer helseopplysninger. Imidlertid må REK kunne forelegge store, kompliserte saker for Datatilsynet etter behov. Dette vil særlig være aktuelt der det er de rent datatekniske løsningene for å ivareta personvernet som er vurderingstemaet» (Ot prp. nr. 74 (2006-2007) Helseforskningsloven)

til Datatilsynet flyttet til REK, med blant annet det formål å forenkle saksbehandlingen ved slike prosjekter. Det vil i mange tilfeller være overlappende vurderinger mellom godkjenning av behandling av personopplysninger og andre typer godkjenninger som REK gjør, for eksempel de etiske vurderingene. De delene som gjelder behandlingen av personopplysninger må foretas i tråd med de nye kravene i personvernforordningen.

For de deler av REKs vurderinger som er «rene» forhåndsgodkjenninger etter personvernregelverket, må det vurderes om det er ønskelig og mulig å videreføre ordningen med forhåndsgodkjenninger. Dersom behovet for forhåndsgodkjenninger fortsatt er tilstede, må det vurderes om forordningen åpner for at REK kan fortsette å være den instansen som foretar disse forhåndsgodkjenningene, jf. ordlyden i artikkel 36 nr. 5. som tillegger denne oppgaven til «tilsynsmyndigheten». Etter forordningen kan kontroll og tilsyn med rettighetene etter forordningen altså ikke uten videre foretas av andre myndigheter enn Datatilsynet. Der en stat har flere tilsynsmyndigheter, må alle oppfylle alle krav som fremgår av artikkel 51-54 og ha den kompetansen som fremgår av artikkel 57. Vi er usikker på om disse kravene oppfylles av REK eller andre instanser som i medhold av særlovgivningen har oppgaver som knytter seg til å kontrollere etterlevelse av personvernregelverket.

Et annet eksempel er at flyttingen av kompetanse og regulering om direkte markedsføring til markedsføringsloven og Forbrukerombudet. Dette var tidligere regulert i personopplysningsloven § 26, som gjennomførte direktivets artikkel 14 bokstav b, og Datatilsynet var tilsynsorgan.⁹⁶ Datatilsynet er tilsynsmyndighet når det gjelder etterlevelse av forordningens artikkel 21 nr. 2 om direkte markedsføring. Det kan stilles spørsmål ved om dagens regelverk kan videreføres i sin nåværende form, herunder om Forbrukerombudet kan inneha denne kompetansen.

Vi nevner også til helsepersonelloven § 43 som gir Fylkesmannens myndighet til å behandle klager på avslag på anmodning om sletting av opplysninger i pasientjournaler.

Vi legger til grunn at dette avklares i ansvarlige departement.

17. Domstolsprøving

Når det gjelder Datatilsynets adgang til å bringe saker inn for retten, viser vi til det som er sagt over i forbindelse med klage over Datatilsynets vedtak. Som nevnt fremstår det for oss usikkert om tvisteloven § 1-4 gir Datatilsynet adgang til å bringe en sak inn for domstolen for å sikre etterlevelse av forordningen, jf. forordningen artikkel 58 nr.5.

Det er videre nødvendig å gi regler knyttet til Datatilsynets posisjon i rettslig prosess der vi er involvert. Vi tenker her på partsevne eller utøvelsen av partsrollen. Dette er relevant både ved søksmål over Datatilsynets vedtak (gyldighetssøksmål) og ellers der Datatilsynet måtte opptre i rettslig prosess.

⁹⁶ Se nærmere om bakgrunn i Ot.prp.nr.55 (2007-2008) side 85.

Datatilsynet er et statlig organ, og når ikke noe annet er sagt er det staten som er rett part i rettslig prosess. Videre vil det i mangel av annen regulering være departementet som er stedfortreder og som utøver statens partsstilling i saken, jf. tvisteloven § 2-5 jf. domstoloven § 191. Dette har vi erfart i praksis etter gjeldende rett der søksmål mot Datatilsynet måtte rettes mot Staten v/kommunal- og moderniseringsdepartementet. Dette fordi det ikke er sagt noe i personopplysningsloven om hvem søksmål skal rettes mot når det gjelder Datatilsynet eller noe om vår partsevne, i motsetning til det som er uttrykkelig sagt når det gjelder Personvernemnda. Dette er prinsipielt sett ikke heldig fordi det da er departementet som formelt sett utøver partsrollen og direkte eller indirekte er med å bestemme hvilken posisjon staten skal innta i saken og til de rettsspørsmål den reiser. Det mener vi kan rokke ved Datatilsynets uavhengighet.

Vi mener derfor at Datatilsynet må gis selvstendig partsevne, jf. tvisteloven § 2-1 (1) bokstav f, eller i det minste at det må gjøres klart at Datatilsynet er stedfortreder og følgelig utover statens partsstilling på selvstendig grunnlag.

18. Datatilsynets og Personvernemndas taushetsplikt og tilgang til opplysninger

18.1. Om bestemmelsen som gjelder taushetsplikt

Departementet har foreslått en uttrykkelig bestemmelse om taushetsplikt ved varsling om mulig regelbrudd.

Vi er enig i at det må foreligge en slik taushetsplikt, men vi mener at taushetsplikten må forsterkes. Det sentrale poenget med taushetsplikten her er å beskytte varslere, noe som igjen kan bidra til å motivere de som sitter på informasjon om mulige regelbrudd til å komme frem. Det underliggende, i tillegg til å beskytte varsleren, er altså å legge til rette for at informasjon om mulige regelbrudd kan komme tilsynsmyndigheten for øre.

Departementet skriver at forvaltningslovens regler for unntak fra taushetsplikten skal gjelde. Dette medfører at taushetsplikten ikke gjelder for sakens parter, jf. § 13 b første ledd nr. 1.

Dette er ikke tilfredsstillende. Vi viser i den forbindelse til arbeidsmiljøloven § 2 A-4, som er en ny bestemmelse som pålegger taushetsplikt ved varsling fra en arbeidstaker. Denne taushetsplikten gjelder også overfor sakens parter og den gjelder tilsynsorganer generelt, og ikke bare Arbeidstilsynet. Taushetsplikten her beskytter imidlertid bare arbeidstakeren i relasjon til arbeidsgiver, idet formålet er å bedre vilkårene for varsling i arbeidslivet. Varslere overfor Datatilsynet kan imidlertid være andre enn ansatte, for eksempel tidligere ansatte, som også har behov for beskyttelse. Vi viser til taushetsplikten for Konkurransetilsynet i konkurranseloven § 27 hva gjelder tipsers identitet. Den gjelder helt generelt og også overfor sakens parter.

Det bør inntas en bestemmelse om at taushetsplikten også skal gjelde overfor sakens parter og deres representanter. I forlengelsen av dette peker vi også på at taushetsplikten med hensyn til varslere antakelig også bør gjelde overfor Personvernemnda. Der er her nærliggende å sammenlikne med prøving av saken for domstolene, hvor utgangspunktet er at taushetsplikten gjelder. Som et utgangspunkt kan vi ikke se at det er behov for å avsløre varsleren overfor nemnda.

18.2. Tilgang til opplysninger for Personvernemnda

Departementet har foreslått at forordningen artikkel 58. nr.1 bokstav a og e skal gis tilsvarende anvendelse overfor Personvernemnda. Det vil si at nemnda skal ha oppfattende undersøkelseskompetanse, herunder kunne gjennomføre stedlig kontroll (on sight inspections). Etter vårt syn kan det være betenkeligheter knyttet til dette. Vi kan her trekke en linje til det vi har sagt over om innretningen på den administrative klageordningen, og at nemnda bør ha mer karakter av å være et slags domstolliknende organ med mer partsprosess.

At en behandlingsansvarlig/databehandler som klager til Personvernemnda kan risikere at «det dømmende organet» bestemmer seg for selv å etterforske saken, herunder foreta stedlige kontroller, er kanskje ikke helt heldig.

19. Klage over Datatilsynets vedtak

Departementet foreslår å videreføre Personvernemnda som uavhengig klageorgan og at medlemmene av nemnda skal utnevnes av Kongen. Det vurderes å redusere antallet nemndsmedlemmer fra 7 til 5. Personvernemnda skal i utgangspunktet kunne behandle klager over alle vedtak Datatilsynet fatter. Et viktig unntak her er imidlertid saker som behandles i henhold til forordningens regler om samarbeid og konsistens.

Datatilsynet er enig at det bør være en administrativ klageordning. Videre er vi enig i avgrensningen mot saker som er behandlet etter samarbeid- og konsistensmekanismen. Vi finner imidlertid grunn til å reise spørsmål om *innretningen på den administrative klageordningen*.

Etter vårt syn bør klageordningen innrettes mer mot Personvernemnda som et domstolliknende organ, med mer innslag av partprosess. Nemnda bør for eksempel bare ha anledning til å behandle saker *etter klage*, og ikke ha adgang til å gripe inn i saken på eget initiativ med omgjøring etter forvaltningsloven § 35. Det kan stilles spørsmål ved om det er forenlig med forordningen at det etableres et administrativ klageorgan, med medlemmer utnevnt av regjeringen (Kongen), som på eget initiativ har rett til å gripe inn overfor Datatilsynets avgjørelser. Å kunne gripe inn på eget initiativ fremstår som noe mer enn «administrative remedy» for berørte parter, som er det som forordningen åpner for.

I denne sammenheng kan det gis særskilte saksbehandlingsregler, for eksempel slik som for Markedsrådet og Konkurransenemnda som blant annet har innslag av muntlig behandling. Etter omstendighetene reiser sakene på området for personopplysningsvern mange og

kompliserte spørsmål hvor ren skriftlig saksbehandling i klagerunden har vesentlige begrensninger. Saker som gjelder store overtredelsesgebyr er for eksempel kanskje ikke egnet for rent skriftlig overprøving basert på oversendelse av sakens dokumenter og merknader fra partene.

Det er videre grunn til å understreke at mange av klagesakene i realiteten dreier seg om tvisteløsning. Det gjelder særlig saker der det er den registrerte som har klaget til Datatilsynet. For eksempel saker om innsyn – der den registrerte mener å ha innsynsrett mens behandlingsansvarlig bestrider dette – eller saker om sletting. Selv om klagen over Datatilsynets vedtak gjeler en overprøving av vår avgjørelse, er det i realiteten tvisten mellom den registrerte og behandlingsansvarlige som skal behandles i nemnda i annen instans. Situasjonen her minner mer om anke over dom enn forvaltningsprosess i tradisjonell forstand. Vi opplever at de alminnelige reglene for klagebehandling i forvaltningsloven ikke treffer så godt her.

I slike trepartsforhold, hvor man har den registrerte og den behandlingsansvarlige (som tvisten egentlig står mellom) og Datatilsynet (hvis avgjørelse er påklaget), er vår erfaring at man mister litt av syne hvem tvisten egentlig står mellom i klagerunden. Saken blir ikke behandlet med dem i sentrum, men istedenfor med utgangspunkt i den som har klaget på den ene siden og Datatilsynet på andre. I svært mange saker fra nemnda er vedtaket bygget opp omkring klagers anførsler og Datatilsynets merknader, mens den reelle motparten har blitt litt borte.

Et eksempel her er PVN-2014-08, som gjaldt ileggelse av overtredelsesgebyr. Datatilsynet hadde kommet til at det ikke var grunnlag for overtredelsesgebyr og avsluttet saken. Dette ble påklaget av den registrerte, som mente at det forelå regelbrudd av en slik karakter at det burde reageres med overtredelsesgebyr. Nemnda kom til at gebyr skulle ilegges, og sendte saken tilbake til Datatilsynet for fastsettelse av gebyrets størrelse. Beslutningen om at gebyr skulle ilegges ble imidlertid tatt uten at kommunen det var tale om å sanksjonere, ble trukket inn i saken og hørt for nemnda.

Nevnte sak illustrer for øvrig behovet for å gi mer presise regler for nemndas behandling, herunder hva nemnda kan og ikke kan behandle. Etter vårt syn bør det klart være slik at nemnda ikke skal ha kompetanse til å ilegge overtredelsesgebyr i første instans. Nemndas rolle her må avgrenses til å behandle klager der gebyr er ilagt.

Vi mener videre at Datatilsynets rolle/posisjon i relasjon til den administrative klageordningen bør klargjøres. Slik vi ser det bør Datatilsynet betraktes som en slags part i saken, med partsrettigheter. Det er mest forenlig med den rolle og funksjon datatilsynsmyndigheten er ment å ha etter forordningen. Det tradisjonelle forvaltningsrettslige system med overordnet og underordnet organ som forvaltningsloven alminnelige klage regler er bygget på, passer ikke helt. For eksempel har vi opplevd at saken, etter at vi har sendt den over til nemnda, har blitt ytterligere opplyst av klager, uten at vi er gjort kjent med dette eller har fått anledning til å gi våre innspill. Vi har blitt møtt med at det ikke er nødvendig fordi vi ikke er part i saken.

I forlengelsen av dette mener vi at Datatilsynet må gis uttrykkelig adgang til å angripe nemndas vedtak for domstolene. Datatilsynet har en særlig interesse i hvordan regelverket utvikles og fortolkes i praksis. Nemnda kan ikke alltid ha siste ord vis a vis Datatilsynet. For eksempel kan det være slik at saken reiser prinsipielle og uavklarte spørsmål, eller nemndas avgjørelse kolliderer med praksis og avklaringer som er blitt til gjennom samarbeid- og konsistensmekanismen, og følgelig går mot den harmoniseringen som er forordningens grunntanke og som tilsynsmyndighetene har en særskilt oppgave med å fremme. Det å kunne bringe saker inn for rettsapparatet for å søke rettslig avklaring, er etter omstendighetene viktig og nødvendig. Viktige avklaringer blant annet gjennom praksis fra EU-domstolen har kommet nettopp fordi «noen» har tatt initiativ til å få prøvd spørsmålet. Denne «noen» må etter omstendighetene kunne være tilsynsmyndigheten.

Under punktet om domstolsprøving har departementet kort lagt til grunn tvisteloven § 1-4 gir Datatilsynet mulighet til å reise sak for domstolene, og det er tilstrekkelig etter forordningen artikkel 58. nr. 5. Det følger imidlertid av forarbeidene til § 1-4 at «bestemmelsen vil ikke ha selvstendig betydning for tilsynsorganer i forhold til den lovgivningen de har som oppgave å håndheve». Følgelig synes det å være behov for uttrykkelig regulering her for å gjøre det klart at Datatilsynet kan ta saker for retten.

Dersom Datatilsynet skulle ta saken for retten etter at Personvernemnda har fattet sin avgjørelse stiller vi spørsmål ved om det er riktig at søksmål i så fall skal rettes mot Staten ved Personvernemnda. Det vil etter omstendighetene gi liten mening om saken prøves for domstolene med Staten på begge sider av bordet – henholdsvis Staten ved Personvernemnda og Staten ved Datatilsynet – i en sak som i realiteten dreier seg om en behandlingsansvarlig/databehandler skal pålegges en plikt.

Vi har for øvrig ingen merknader til at antallet medlemmer av Personvernemnda reduseres til fem og endringen som innebærer det at Kongen alene skal oppnevne medlemmene til nemnda.

Hvilke vedtak som kan påklages

Det følger av lovforslaget at det er Datatilsynets vedtak som kan påklages til Personvernemnda. Vi regner med at det med vedtak menes vedtak i forvaltningslovens forstand, og at det da er enkeltvedtak som kan påklages, jf. forvaltningslovens § 28.

Vi har erfaring med at det etter omstendighetene er vanskelig å si om man står overfor et enkeltvedtak eller ikke. Som eksempel kan vi nevne PVN-2014-08 hvor vår beslutning om å ikke ilegge overtredelsesgebyr overfor den behandlingsansvarlige ble påklagd av den registrerte. Det er så langt vi kan forstå tvilsomt om en slik avgjørelse er et enkeltvedtak i relasjon til den registrerte ettersom den ikke er bestemmende for hans eller hennes rettigheter etter personopplysningsregelverket.

Et annet eksempel som kan by på vanskeligheter er for eksempel en klage fra en registrert som mener at det er samlet inn opplysninger om vedkommende ulovlig. Dersom Datatilsynet etter å ha undersøkt og vurdert saken kommer til at det ikke foreligger brudd på loven og følgelig avslutter saken på det grunnlag, kan det spørres om en slik avgjørelse er

bestemmende for den registrertes rettigheter. Til sammenlikning kan vi vise til Rt. 2015 side 1313 som gjaldt søksmål om gyldigheten av en avgjørelse fra Likestillings- og diskrimineringsnemnda om at en person ikke var utsatt for ulovlig diskriminering.

Ankeutvalget avviste saken med den begrunnelse at en avgjørelse som går ut på at det ikke foreligger brudd på diskrimineringsloven, er en avgjørelse uten rettsvirkninger. Det rettslige kjennetegnet ved vedtak var ikke til stede. Personen som mente seg diskriminert, og som følgelig var uenig i nemndas vurdering, måtte i så fall saksøke arbeidsgiveren.

På bakgrunn av dette mener vi det bør vurderes å gi mer presise bestemmelser med hensyn til hva som kan påklages. Vi viser her også til vårt brev til Justisdepartementets lovavdeling av 19.01.2016, som så langt vi kan se ikke er besvart.

20. Overtredelsesgebyr

Som departementet skriver i høringsnotatet kapittel 2,3 gir gjeldende personopplysningslov hjemmel for at Datatilsynet kan ilegge overtredelsesgebyr ved brudd på personopplysningsregelverket, forordningen hever imidlertid maksimumsbeløpet betraktelig.

Datatilsynet har ingen merknader til lovforslagets § 21 første ledd, som åpner for å ilegge overtredelsesgebyr for forordningens artikkel 10 og 24. Vi støtter forslaget om å presisere i § 21 andre ledd at Datatilsynet kan ilegge offentlige myndigheter overtredelsesgebyr.

20.1. Foreldelse av adgangen til å ilegge overtredelsesgebyr

Departementet ber om høringsinstansenes syn på om det bør innføres en foreldelsesfrist for adgangen til å ilegge overtredelsesgebyr og eventuelt hva som skal være fristens varighet. Ut fra det som står i høringsnotatet har departementet ikke gjort nærmere vurderinger når det gjelder dette spørsmålet.

Datatilsynet mener at det bør være en foreldelsesfrist for adgangen til å ilegge overtredelsesgebyr etter forordningen og anbefaler at dette utredes nærmere. Spørsmålet om foreldelsesfrist reiser en rekke prinsipielle, komplekse og praktiske spørsmål. Vi har ikke hatt mulighet til å gå grundig inn i dette i denne omgang, så vi har ikke noe konkret forslag til hvordan en slik bestemmelse i så fall skal utformes. Vi har likevel noen tanker om dette som departementet kan ta med i det videre arbeidet.

Slik vi ser det er de viktigste problemstillingen å ta stilling til *når fristen begynner å løpe fra, varighet og når fristen avbrytes*.

Til sammenlikning viser vi til at konkurranselovens § 29 fjerde ledd regulerer adgangen til å ilegge overtredelsesgebyr for brudd på lovens bestemmelser. Bestemmelsen fastsetter to ulike frister avhengig av overtredelses natur. I tillegg regulerer bestemmelsen at fristen avbrytes idet tilsynsmyndigheten tar formelle skritt for å undersøke mistanken om lovbrudd eller meddeler foretaket at et er mistenkt eller at det er truffet vedtak for brudd av loven.

Personopplysningsloven har som kjent ikke tilsvarende regler om foreldelse. I europeisk sammenheng har imidlertid foreldelse vært et viktig spørsmål, som medlemsland, ofte etter inspirasjon fra nasjonal særlovgivning på andre område, har løst på ulike måter. Konkurranselovgivning trekkes ofte frem av mange som en lov det er relevant å sammenligne med. I følge mange av våre kollegaer i europeiske tilsyn bør man ved fastsettelse av foreldelsesfrister for adgangen til å ilegge overtredelsesgebyr se hen til både *hvilken* bestemmelse som er overtrådt og *hvordan* den er overtrådt.

I forsøk på å finne en harmonisert tilnærming til overtredelsesgebyr på personvernområdet har kommisjonens prosedyre for fastsettelse av overtredelsesgebyr for brudd på konkurransereglene vært mye omtalt⁹⁷. Diskusjoner i Artikkel 29-gruppen har gått på at en bør se hen til overtredelsens natur, med henvisning til den trinnvise tilnærmingen i artikkel 83 nr. 4, 5 og 6 og hva overtredelsen faktisk består i. Det ses hen til om det snakk om et lite, formell brudd, som ikke påvirker kjernen i rettighetene, eller er det snakk om en grov, systematisk eller villet handling. Slike forhold kan ha betydning ikke bare for utmåling av gebyrets størrelse, men gir en også indikasjon om hvor alvorlig bruddet er og hvor lett eller vanskelig for tilsynet er å avdekke det straffbare forholdet.

En slik tilnærming skiller seg fra straffelovens kapittel 15, som kun viser til den høyeste lovbestemte fengselsstraffen i det straffebudet som er overtrådt. Forordningen definerer imidlertid ikke like tydelig som straffeloven hvilken adferd som utgjør brudd på konkrete bestemmelser i forordningen, annet å vise til den aktuelle pliktbestemmelsen som er overtrådt.

For eksempel vil brudd på artikkel 34, altså informasjon til den registrerte om avvik, kunne innebære en rekke ulike forhold, der iblant at fristen til å gi informasjon er oversittet med noen få timer, at opplysningene som er gitt er ufullstendige, at opplysningene ikke ble sent til alle registrerte som er berørt, at opplysningene ble sent til feil mottaker og at Datatilsynet bestrider vurderingen som er gjort av hvorvidt plikten til å informere de registrerte inntreffer.

21. Administrativ inndragning

Personopplysningsloven har ikke regler om inndragning. Det er heller ingen regler om det i forordningen, men artikkel 58 nr.6 åpner for at tilsynsmyndighetene kan få utvidet kompetanse, herunder rett til å ilegge administrative reaksjoner. Departementet ber om høringsinstansenes syn på om Datatilsynet bør gis rett til administrativ inndragning.

Datatilsynet har ingen særlige synspunkter knyttet til inndragning.

Ut fra vår praksis og erfaring har vi liten grad stått overfor tilfeller hvor inndragning hadde vært et ønsket virkemiddel, eller særlig egnet eller proporsjonalt for den slags skyld. Det måtte kanskje være tilfeller av ulovlig kameraovervåking eller liknende overvåkingstilfeller hvor det å inndra utstyret kunne være nødvendig. For eksempel bruk av overvåkingsutstyr

⁹⁷ [http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52006XC0901\(01\)&from=EN](http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52006XC0901(01)&from=EN)

som er laget for å være skjult og hvor man rett og slett av hensyn til effektiv håndheving ikke kan la den behandlingsansvarlige få beholde utstyret fordi det er fare for gjentakelser.

Mer praktisk enn inndragning kan imidlertid være muligheten for å *ta beslag* i bevissikringsøyemed. Det bør vurderes å gi Datatilsynet bedre bevissikringsmuligheter slik som for eksempel Konkurransetilsynet, jf. konkurranseloven § 25.

22. Straffebestemmelser

Det følger av forordningens artikkel 84 at det i nasjonal rett skal fastsettes nærmere regler om straff som kommer til anvendelse ved overtredelse av forordningen. Artikkel 84, sammenholdt med fortalen punkt 148, 149 og 152, viser at det enkelte land har handlingsrom til å vurdere og avgjøre hvor det kan være behov for straff, definere hvilke handlinger som skal kunne straffes og i så fall hva slags reaksjon som skal kunne benyttes. Siktemålet med slike regler er å styrke håndhevingen av reglene og, til syvende og sist, styrke personopplysningsvernet.

Departementet har bedt høringsinstansene om innspill på om brudd på personopplysningsloven bør være straffbart, og i så fall hvilke overtredelser som skal være straffbare.

Departementet har, slik vi ser det, ikke selv utredet spørsmålet om straff i nevneverdig grad, og høringsinstansene har dermed ikke et godt underlag for å vurdere straff som et virkemiddel. I høringsnotatet er det kort lagt til grunn at overtredelsesgebyr, eventuelt sammenholdt med administrativ inndragning slik det er foreslått, vil ha den nødvendige avskrekkende effekt, og at straff dermed ikke vil ha ytterligere allmennpreventiv eller individualpreventiv effekt.

Etter vår forståelse blir dette en for enkel vurdering av tiltak som kan sikre effektiv etterlevelse og håndheving av reglene, noe som er en sentral målsetning bak forordningen. For eksempel bør man også se hen til at politiet, med sine ressurser og hjemler for å etterforske en sak, etter omstendighetene kan bidra til å oppklare regelbrudd. Vi mener således at det kan ligge en avskrekkende virkning at man kan risikere politietterforskning, tatt i betraktning at Datatilsynet er et relativt lite organ. Det er vel også grunn til å hevde at trusselen om fengselsstraff vil kunne ha ekstra avskrekkende virkning overfor de personer som har det øverste ansvaret. Forordningen legger opp til ansvarliggjøring og at personopplysningsvern skal opp på det høyeste nivået hos behandlingsansvarlig, og trusselen om straff kan bidra til at slike personer tar personopplysningsvernet på største alvor.

Vi mener derfor at spørsmålet om straff burde vært utredet bedre. Der departementet viser til at det i Sverige er foreslått å ikke fastsette noen straffebestemmelser, kan vi vise til at det i Danmark er det foreslått fengsel og/eller bøter for en rekke overtredelser. Vi kan også vise til at i Tyskland er det fastsatt straffebestemmelser for mer konkrete handlinger, slik som for

eksempel ulovlig utlevering til tredjepart, gjort forsettlig, av personopplysninger til et stort antall personer for kommersielle formål.⁹⁸

Etter vårt skjønn bør en utredning og vurdering av straff være mer innrettet mot type handlinger som anses som særlig skadelig/straffverdig, fremfor en vurdering av hvilke lovbestemmelser som bør belegges med straff. For eksempel kan det være vanskelig å knytte straff til overtredelse av artikkel 13 og 14 om informasjonsplikt generelt. Men grove brudd, hvor det ikke er gitt noe informasjon overhodet og det hele har karakter av skjult behandling av personopplysninger, kunne vært skilt ut som en straffbar handling.

23. Tvangsmulkt

Etter personopplysningsloven § 47 kan Datatilsynet fastsette tvangsmulkt ved pålegg etter flere av lovens bestemmelser. Forordningen har ikke særskilte regler om dette, men departement legger til grunn at de er adgang til å videreføre dagen regler med hjemmel i forordningens artikkel 58 nr. 6.

Datatilsynet er enig i departementets vurdering når det gjelder å videreføre tvangsmulkt.

24. Behandling i journalistisk, akademisk, kunstnerisk og litterær virksomhet

Departementet foreslår i lovutkastet § 3 å videreføre gjeldende rett slik at behandling av personopplysninger for kunstnerisk, litterær og journalistisk formål er unntatt fra storparten av forordningens regler. Tilsvarende unntak skal også gjøres for akademiske yringer.

Datatilsynet støtter forslaget om å regulere dette særskilt, men har noen merknader basert på de utfordringer vi ser ved praktisering av gjeldende bestemmelse.

Forslaget er basert på at forordningens artikkel 85 gir medlemsstatene handlingsrom til å gjøre unntak fra visse av forordningens regler dersom det er nødvendig for å forene retten til personvern med retten til ytringsfrihet og informasjonsfrihet. Disse grunnleggende rettighetene skal også avveies mot hverandre etter EMK artikkel 8 og 10, og tilsvarende etter EU-pakten artikkel 8 og artikkel 11. Nasjonale unntak fra forordningen sikrer at man i enkelte tilfeller fritt kan behandle personopplysninger uten at reglene om behandlingsgrunnlag i artikkel 6 begrenser lovligheten av behandlingen. Videre innebærer handlingsrommet at andre plikter etter forordningen ikke urettmessig setter hindringer for bearbeiding og videreformidling av informasjon som er vernet av ytrings- og informasjonsfriheten.

⁹⁸ En engelsk oversettelse er tilgjengelig her:

http://www.bmi.bund.de/SharedDocs/Downloads/EN/Gesetzestexte/datenschutzanpassungsumsetzungsgesetz.pdf?__blob=publicationFile

Etter forordningen er det rom for å avveie hensynet til databeskyttelse mot hensynet til ytrings- og informasjonsfrihet i to sammenhenger: Ved at den aktuelle behandlingen er unntatt fra forordningens regler, i tråd med nasjonale særregler hjemlet i artikkel 85, og ellers, i øvrige tilfeller, ved vurdering av behandlingsgrunnlag og innsigelsesrett etter artikkel 6 nr. 1 bokstav f og 21 nr. 1.

Artikkel 85 første ledd gir medlemsstatene handlingsrom til å fastsette særregler som forener personvern og ytringsfrihet, *herunder* når formålet med en behandling er journalistisk, kunstnerisk, litterært eller akademisk. Handlingsrommet synes dermed å åpne for en mer generell henvisning til ytrings- og informasjonsheten generelt. Departementet mener at en slik henvisning vil bli for åpen og skjønnsmessig.

Datatilsynet er enig i departementets vurdering. Vi viser for øvrig til fortalepunkt 153 og EU-domstolens praksis, som slår fast at «journalistisk» skal tolkes vidt, slik at også ikke-erhvervsmessig meningsytring kan falle innenfor unntaksregelen. Datatilsynets erfaring med den tilsvarende, eksisterende unntaksregelen i personopplysningsloven § 7 er at den er tilstrekkelig fleksibel og egnet til å verne ytringer som Grunnloven § 100 er ment å beskytte. Dette forutsetter imidlertid at personopplysningsloven § 7 og Grunnloven § 100 tolkes harmoniserende.

Når det gjelder hvilke bestemmelser i forordningen som det i lovforslaget gjøres unntak fra har Datatilsynet ingen merknader.

Vi vil for øvrig bemerke at Norge har et nasjonalt handlingsrom til å vurdere mer *utfyllende sektorlovgivning* om unntaket for behandlinger for journalistisk, akademisk, kunstnerisk eller litterært formål. Fordelen med en mer utfyllende regulering av unntak er at en vil trenge mindre juridisk ekspertise for å tolke forholdet mellom de grunnleggende interesser, samtidig som man utnyttet handlingsrommet til å balansere rettighetene mer konkret ut fra norsk rettstradisjon.

Mer utfyllende sektorlovgivning kan for eksempel gis der i dag er klart at ytringsfriheten skal veie tyngst. Dette kan typisk være nyhetsdekning innenfor de redaktørstyrte mediene. Vi viser i denne sammenheng til Danmark, som både i nåværende og foreslått persondatalov for eksempel har gjort unntak for behandlinger som omfattes av lov om massemediers informationsdatabaser. Dette kan blant annet være relevant for Norge å se på i forbindelse med ny medieansvarslov.

24.1. Utfordringer ved lovforslaget

Den foreslåtte regelen i ny personopplysningslov § 3 kan fremstå som «enkel», men vurderingene etter dagens personopplysningsloven § 7 har vist seg å være sammensatte og komplekse i praksis. Den foreslåtte regelen er en videreføring av den gjeldende bestemmelsen vil den i liten grad skape bedre forutberegnelighet for de ulike partene og bli enklere å praktisere for Datatilsynet.

Datatilsynets erfaring er at tolkningen av hvorvidt en behandling av personopplysninger skjer for utelukkende journalistiske, litterære eller kunstneriske formål, i praksis er svært utfordrende. Forarbeidene til dagens personopplysningslov § 7 sier at i denne vurderingen er *arten av og hensikten* med ytringen avgjørende. Siden det ikke gjelder noen formkrav for hva som skal anses som en journalistisk, litterær eller kunstnerisk ytring, og det heller ikke bør gjøre det, er det imidlertid vanskelig å vurdere ytringens art. Videre er det er krevende, om ikke umulig, for Datatilsynet å fastslå for eksempel hvilken hensikt en enkeltpersons ytring på internett har. Det er heller ikke lett å avgjøre hvorvidt enkeltpersoner som ytrer seg på nett gjør det med et *utelukkende* journalistisk formål, eller om vedkommende gjennom omtalen samtidig ønsker å sanksjonere personen som omtales.

Datatilsynets sak om nettsiden offentlig.info er et godt eksempel på problemstillingene som oppstår i praksis. På siden omtales navngitte offentlige ansatte i forbindelse med en arbeidsrettssak mot nettsidens innehaver. Mens innehaveren har uttalt at hensikten med siden er å sette forvaltningen i kritisk søkelys, har de omtalte personenes arbeidsgiver anført at hensikten er å henge ut personene som hevn. For Datatilsynet er det vanskelig å avgjøre hva hensikten er. Siden skiller seg vesentlig fra etablerte nyhetsmedier både når det gjelder form og ordelag, men også meningsytringer i andre formater og språkformer kan ha «journalistiske formål», og dermed er det vanskelig å fastslå hva som ligger i «journalistisk art». Derfor gir heller ikke dette kriteriet god veiledning.⁹⁹

Dette gjør blant annet er at det ofte er vanskelig for Datatilsynet å gripe inn når offentlige ansatte eller andre henges ut på internett, selv om departementet tidligere har ment Datatilsynet kan og bør kunne pålegge opphør av slik behandling, se Prop. L (2011–2012) punkt 4.6. Dette er et aktuelt problem som neppe vil bli mindre i fremtiden.

Unntak i den grad det er *nødvendig*

Som departementet har pekt på, oppstiller artikkel 85 annet ledd to nødvendighetsvurderinger. Medlemsstatene kan innføre enkelte unntak i den grad det er *nødvendig* av hensyn til yttrings- og informasjonsfrihet, og hvilke unntak man velger å gjøre, kommer også an på en nødvendighetsvurdering.

Når det gjelder hvorvidt man skal gjøre unntak, har departementet gått inn for å ikke innta en henvisning til nødvendighetsvurderingen i lovteksten. I stedet vil unntaket gjelde alle behandlinger der formålet utelukkende er journalistisk, akademisk, litterært eller kunstnerisk. Som begrunnelse viser departementet til uttalelsene i Prop. 47 L (2011–2012) og Ot.prp. nr. 92 (1998–1999), der det blant annet sies at utelatelsen er ment å gjøre det lettere for rettsanvenderen.

Datatilsynets erfaring med den eksisterende, tilsvarende unntaksregelen i personopplysningsloven § 7 tilsier at unntaket av henvisning til proporsjonalitetsregelen har gjort det *vanskeligere* å anvende regelen. Regelen fremstår som mekanisk og kategorisk, noe som undertiden kan resultere i et uforholdsmessig unntak fra retten til privatliv og

⁹⁹ Se PVN-2017-06. Personvernemnda opphevet Datatilsynets vedtak på grunn av formelle feil. Saken er ennå ikke avgjort.

personvern. Dette skaper særskilte lovanvendelsesspørsmål i praksis når regelen skal anvendes.¹⁰⁰

Vi ber derfor departementet vurdere igjen om det likevel er mulig og hensiktsmessig å innta noe om nødvendighetsvurderinger i lovforslaget. Hvis ikke, er det ønskelig at det i proposisjonen til ny personopplysningslov oppstiller gode vurderingstemaer og at det gis veiledning med hensyn til hvordan disse temaene skal vurderes.

Det er for øvrig også viktig at det er tilstrekkelig godt utredet hvorvidt den foreslåtte regelen er innenfor handlingsrommet forordningen oppstiller.¹⁰¹

Vi viser til EU-domstolens praksis i saker som omhandler avveining av personvern mot ytrings- og informasjonsfrihet etter tilsvarende, någjeldende regler. Domstolen har gjennomgående uttalt at mens «journalistisk» må tolkes vidt, må eventuelle unntak holdes innenfor det som er «strengt nødvendig», slik at man oppnår en god *balanse* mellom de to menneskerettighetene.¹⁰² Dersom unntaksregelen ikke åpner for å vurdere nødvendigheten i den enkelte sak, kan eventuelle unntak fra personvernet vanskelig sies å holde seg innenfor hva som er «strengt nødvendig».

Vi viser også til at etter EMK er retten til ytringsfrihet og retten til privatliv sidestilte rettigheter. Inngrep i ytringsfriheten må kunne la seg forsvare etter EMK artikkel 10 annet ledd. Dersom en ytring som innebærer behandling av personopplysninger blir tillatt, kan dette innebære et inngrep i retten til privatliv. Slike inngrep må tilsvarende kunne la seg forsvare etter artikkel 8 annet ledd. Den europeiske menneskerettsdomstolen har behandlet flere saker der artikkel 8 og artikkel 10 har måttet avveies mot hverandre. Domstolen har i slike avveininger lagt vekt på hva slags ytring det er, hvilken kontekst den fremgår i og hvorvidt ytringen bidrar til en debatt av generell samfunnsinteresse.¹⁰³

¹⁰⁰ Se også Datainspektionens uttalelse av 4. september 2017, *Remittering av betänkandet SOU 2017:39 Ny dataskyddslag*. I Sverige er det foreslått en regel som kan innebære at tryckfrihetsförordningen og yttrandefrihetsgrundlagen gis forrang fremfor personverndirektivet. Datainspektionen redegjør for hvordan retten til personvern og retten til ytrings- og informasjonsfrihet må avveies mot hverandre – altså at den ene ikke ukritisk kan gå foran den andre. Selv om uttalelsen gjelder en annen regel, er uttalelsen likefremt relevant her.

¹⁰¹ EFTA Surveillance Authority (ESA) stilte i brev 28. november 2002 også spørsmål om dagens personopplysningslov § 7 går for langt i forhold til personverndirektivet artikkel 9, siden proporsjonalitetsprinsippet ikke er uttrykkelig inkorporert i § 7. Ved utelatelsen av en slik formulering syntes ESA å anta at den norske bestemmelsen åpner for en urettmessig vektlegging av hensynet til ytringsfriheten på bekostning av personvernhensyn. I svarbrev til ESA 18. februar 2003 ga departementet uttrykk for at direktivet ikke kan forstås slik at medlemsstatene er forpliktet til å inkorporere nevnte formulering i unntaksbestemmelsen. Departementet mente heller at de unntak som fastsettes av medlemsstatene måtte være et resultat av en tilstrekkelig proporsjonalitetsvurdering. Det ble videre gitt uttrykk for at det til en viss grad må være opp til medlemsstatene å avstemme hensynet til personvern og ytringsfrihet opp mot hverandre. I den prosessen må statene ta i betraktning sine internasjonale forpliktelser i henhold til EMK. Bestemmelsene i § 7 må dessuten ses i samsvar med de begrensninger som følger av andre lover og yrkesetiske kodekser.

¹⁰² Se for eksempel sak C-73/07, *Tietosuoja- ja valtuutus v Satakunnan Markkinapörssi Oy, Satamedia Oy*, avsnitt 56.

¹⁰³ Schartum, Dag Wiese og Bygrave, Lee A., *Utredning av behov for endringer i personopplysningsloven*, Justis- og politidepartementet, 2006, s. 74.

Poenget her er at behandlinger av personopplysninger kan falle innenfor den foreslåtte unntaksregelen selv om den aktuelle ytringen i liten grad er egnet til å bidra til debatt av generell samfunnsinteresse og personvernkonsekvensene er betydelige. Inngrepet i retten til privatliv kan da potensielt fremstå som uforholdsmessig. Dette kan medføre at Norge ikke overholder sine plikter etter EMK artikkel 8, noe som igjen kan stride mot lovlighetsprinsippet i forordningen artikkel 5 første ledd bokstav a.

Et eksempel på manglende forholdsmessighetsvurdering finner vi i Personvernemndas sak PVN-2010-11, som departementet har kritisert i Prop L (2011–2012) punkt 4.6. Saken omhandlet publisering av informasjon om beredskapshjem og illustrerer hvordan dagens regel kan gi mekaniske utslag som fremstår som lite proporsjonale. Som reaksjon på saken ble lovens ordlyd endret ved at formuleringen «herunder opinionsdannende» ble fjernet. Etter Datatilsynets syn var det ikke der problemet lå – sakens kjerne var ikke nødvendigvis hvorvidt publiseringen kunne nyte et visst vern etter ytringsfriheten, men heller hvordan ytringsfriheten skulle avveies mot retten til personvern i det konkrete tilfellet.

I slike situasjoner har Datatilsynet to muligheter: Tilsynet kan innfortolke en forholdsmessighetsvurdering i strid med lovgivers vilje, eller tilsynet kan tolke «journalistisk», «akademisk», «litterært» og «kunstnerisk» mindre vidt enn det som ellers hadde vært ønskelig. Denne formen for harmoniserende tolkning vil ofte fremstå som kunstig eller vanskelig tilgjengelig for utenforstående. Dette er uheldig av hensyn til ytrings- og informasjonsfriheten.

Følgelig er Datatilsynet av den oppfatning av en henvisning til nødvendighetsvurderingen vil være positivt for ytrings- og informasjonsfriheten fordi det kan tillate Datatilsynet en praksis der «journalistisk», «akademisk», «litterært» og «kunstnerisk» tolkes tilstrekkelig vidt. Dersom anvendelse av unntaksregelen er uforholdsmessig, vil selve nødvendighetsvurderingen i lovteksten garantere at de registrertes rettigheter varetas i tilstrekkelig grad.

Datatilsynet understreker at en henvisning til nødvendighetsprinsippet i de fleste saker neppe vil medføre en praksisendring, siden behandling av personopplysninger som skjer for utelukkende journalistiske, akademiske, litterære og kunstneriske formål som hovedregel vil være vernet av ytrings- og informasjonsfriheten.

25. Offentlighet og innsyn

Departementet skriver følgende om forordningen artikkel 86 og forholdet mellom allmennoffentlighet og personopplysningsvern:

«Etter forordningen artikkel 86 kan personopplysninger utleveres etter nasjonale regler om allmennoffentlighet, og det er tilstrekkelig at utleveringen er «i samsvar med» de nasjonale reglene. Ettersom artikkel 86 ikke stiller andre krav til utleveringen av personopplysningene enn at den er «i samsvar med» reglene om allmennoffentlighet, går forordningen på dette punktet noe lenger i retning av offentlighet enn

unntaksregelen i dagens lov. Mens unntaksregelen i personopplysningsloven § 6 første ledd kun gjelder ved innsynsrett etter offentleglova, omfatter unntaket i forordningen art. 86 også de tilfellene der offentleglova bare gir adgang, og ikke plikt, til å gi innsyn, jf. offentleglova § 11 om meroffentlighet.»

Og videre:

«Når forordningen artikkel 86 avklarer forholdet til offentleglova, og forordningen vedtas som norsk lov, anser departementet det som overflødig å lovfeste en ytterligere presisering av at forordningen ikke er til hinder for innsyn etter offentleglova. Departementet foreslår derfor ingen lovregulering av forholdet til offentleglova tilsvarende gjeldende personopplysningslov § 6 første ledd. Departementet understreker at dette ikke medfører noen innskrenkning av innsynsretten etter offentleglova sammenlignet med dagens regler.»

Vi er enig i at en bestemmelse tilsvarende personopplysningsloven § 6 første ledd ikke er nødvendig. Den vil heller ikke ha noen rettslig funksjon. Den fremstillingen departementet gir er imidlertid, etter vårt syn, ikke treffende for forholdet mellom personopplysningsvern og offentlighet. Tvert imot er den misvisende.

For det første etterlater fremstillingen et inntrykk av at artikkel 86 er en unntaksregel som begrenser eller setter til side retten til personopplysningsvern i relasjon til offentlighetsprinsippet. Eller sagt på en annen måte, at artikkel 86 er en slags forrangsbestemmelse i favør den offentlighet som måtte følge av nasjonale regler.

Videre gis det et inntrykk av at det avgjørende, og det eneste som er relevant, er utelukkende om utlevering skjer i henhold til nasjonale regler om offentlighet, underforstått at så lenge det er tilfellet så spiller det ingen rolle hvordan reglene om offentlighet er utformet og hvor godt offentliggjøringen er balansert mot retten til personopplysningsvern.

Dette bygger i så fall neppe på riktig forståelse.

25.1. Nærmere om forholdet mellom offentlighet og personopplysningsvern

Artikkel 86 sier at utlevering *kan* skje i medhold av nasjonal lov som offentlige organer er underlagt

«for å bringe retten til innsyn i offisielle dokumenter i samsvar med retten til vern av personopplysninger i henhold til denne forordning» («in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.»).

Dette er utdypet nærmere i fortalen punkt 154:

«Denne forordning gir mulighet for at det ved anvendelse av denne forordning kan tas hensyn til prinsippet om innsyn i offisielle dokumenter. Innsyn i offisielle dokumenter kan anses for å være i allmennhetens interesse. Personopplysninger i dokumenter som oppbevares av en offentlig myndighet eller et offentlig organ, bør kunne offentliggjøres av nevnte myndighet eller organ dersom dette er fastsatt i unionsretten eller medlemsstatenes nasjonale rett som den offentlige myndigheten eller det offentlige organet er underlagt. Nevnte lovbestemmelser bør bringe innsyn i offisielle dokumenter og viderebruk av informasjon fra offentlig sektor i samsvar med retten til vern av personopplysninger, og kan derfor inneholde bestemmelser om det nødvendige samsvaret med retten til vern av personopplysninger i henhold til denne forordning.»

Poenget er at forordningen anerkjenner allmenhetens tilgang til informasjon som en behandling i allmenhetens interesse (public interest) og den anerkjenner følgelig at utlevering kan skje i samsvar med nasjonal regler om dette. Imidlertid er det en forutsetning at den nasjonale loven forener hensynet til allmenhetens tilgang til informasjon med personopplysningsvern. Disse skal bringes i samsvar med hverandre. Det avgjørende er således ikke bare om man opptrer i samsvar med nasjonale regler, men også om de nasjonale reglene for offentlighet er tilfredsstillende balansert med retten til vern av personopplysninger.

EU-domstolen har avsagt flere avgjørelser som berører forholdet mellom hensynet til allmenhetens tilgang til informasjon (public access) og personopplysningsvern. Se for eksempel sakene C-92/09 og C-93/09, den såkalte Schecke-dommen, C-465/00, C-138/01 og C-139/01, den såkalte Österreichischer Rundfunk dommen, og C-28/08, den såkalte Bavarian Lager-dommen.

Schecke-dommen omhandler allmenn tilgjengeliggjøring av informasjon om mottakere av landbruksstøtte. EU domstolen undersøkte om publiseringen og reglene for dette var forenlig med retten til personopplysningsvern.

Domstolen tok det utgangspunkt at offentliggjøring av personopplysninger innebar et inngrep («interference») i retten til privatliv og personopplysningsvern (avsnitt 64). Ettersom det forelå et inngrep var det avgjørende om inngrepet kunne rettferdiggjøres. Domstolen slo først fast at utlevering av informasjonen var i samsvar med loven og forfulgte et legitimt formål. Dette var imidlertid ikke tilstrekkelig idet domstolen fant at det ikke forelå en tilfredsstillende balanse («proper balance»).

Domstolen fremholdt blant annet at «*No automatic priority can be conferred on the objective of transparency over the right to protection of personal data*». Dette gjaldt selv om gjennomslukt med tanke på offentlig pengebruk er tungtveiende. Videre må utgangspunkt tas i at begrensningene i personopplysningsvernet bare skal skje så langt det er strengt nødvendig («*strictly necessary*»). Konkret kom Domstolen til at begrunnelsen for reglene om tilgjengeliggjøring av informasjon om mottakere av landsbruksstøtte ikke på tilfredsstillende måte viste hvorfor det var nødvendig av hensyn til formålet man søkte å oppnå. Herunder var det ikke tilfredsstillende påvist hvorfor ikke alternative måter å være gjennomslukt på, som

samtidig skjermet personopplysninger noe mer, ikke var tilstrekkelig. Reglene om tilgjengeliggjøring ble derfor ansett ugyldig.

Vi nevner også Bavarian Lager-dommen, som gjaldt innsyn i et møtereferat der navnene på enkelte deltakere var sladdet. Spørsmålet var om man urettmessig holdt tilbake opplysninger etter reglene om offentlighet, eller om sladding var rettmessig av hensyn til reglene om personopplysningsvern.

EU-domstolen i første instans kom til at det ikke var grunnlag for sladding. Begrunnelse for dette var at navnet på de som var i møtet, og som var sladdet, kun berørte dem i relasjon til utøvelsen av sitt profesjonelle virke og at det ikke forelå et inngrep av nevneverdig betydning i retten til privatliv. Man var altså ikke over terskelen for beskyttelse. Forholdet til personopplysningsvern og de reglene som er laget for å gi dette vernet, ble da ikke aktualisert.

EU-domstolen i annen instans (storkammer) kom derimot til at dette bygget på feil forståelse. Det kan ikke gjøres et slikt skille mellom behandling av personopplysninger som samtidig medfører et inngrep i privatlivet og behandling som ikke medfører slikt inngrep. Retten til personopplysningsvern kommer inn idet det behandles personopplysninger, og første instans hadde da kommet i skade for vurdere saken uten å ta hensyn til reglene som gjelder vern av personopplysninger.

Domstolen (storkammer) kom derfor til at «Whether under the former system of Directive 95/46 or under the system of Regulations Nos 45/2001 and 1049/2001, the Commission was right to verify whether the data subjects had given their consent to the disclosure of personal data concerning them.» Underinstansen avgjørelse ble satt til side.

Slik vi ser det kan det ikke legges ukritisk til grunn at offentleglova er forenlig med personopplysningsvern, i betydningen at man har sørget for «a proper balance» og at utleveringen av personopplysninger ikke går utover det som er «strictly necessary» for det/de formål man søker å ivareta. Offentlighetsloven har ikke vært gjenstand for en systematisk vurdering med tanke på personopplysningsvern slik dette vernet har utviklet seg til å bli en moderne og selvstendig rettighet.

Ved gjennomføringen av personverndirektivet tok man tvert imot motsatt utgangspunkt – personopplysningsregelverket skulle ikke røkke ved allmenhetens tilgang til informasjon – istedenfor å stille seg spørsmålet og undersøke om offentlighetsloven på tilstrekkelig vis er brakt i samsvar med personopplysningsvernet.

For eksempel kan man spørre seg hvor godt taushetspliktbestemmelsen i forvaltningsloven treffer som en grensegang mellom hva slags personopplysninger som skal være offentlig tilgjengelig og hva som skal beskyttes. Ved å knytte vernet til «personlige forhold» har man reelt sett innført en terskel som i Bavarian Lager-dommen over, og nærmest kategorisk unntatt personopplysninger som ikke faller innunder denne nokså diffuse og vanskelige kategorien fra vern. Her kan vi jo også peke på at fødselsnummer i seg selv ikke er taushetsbelagt, men man fra et personopplysningsvern ståsted må man spørre hvorfor det virkelig er nødvendig og proporsjonalt å levere ut den type informasjon til allmenheten ut fra

de formål man søker å oppnå. Det er også en ulogisk sammenheng mellom på den ene siden det ekstra vernet man forsøker å oppstille gjennom særskilte regler for bruk av slik informasjon i personopplysningsregelverket og på den andre siden reglene om offentlighet.

Etter vårt syn er det nødvendig med økt forståelse for forholdet mellom offentlighetsprinsippet og retten til personopplysningsvern. Det synes å være en ganske utbredt forståelse at reglene om offentlighet lever sitt eget liv separat fra reglene som er laget for å gi personopplysningsvern. For eksempel forekommer frasen «offentlighetsloven går foran» ganske ofte. Men det er ikke snakk om «å gå foran», det er snakk om å balansere.

26. Fødselsnummer og andre entydige identifikasjonsmidler

Departementet foreslår å videreføre gjeldende rett om vilkårene for behandling av fødselsnummer og andre identifikasjonsnummer. Med grunnlag i forordningen artikkel 87 foreslås det å fastsettes en regel om at fødselsnummer og andre entydige identifikasjonsmidler bare kan benyttes når det er saklig behov for sikker identifisering og bruken av slikt nummer er nødvendig for å oppnå slik identifisering.

Vi støtter forslaget om særskilt regulering av bruk av slike typer opplysninger. Slike personopplysninger har et særlig misbrukspotensiale. Personvernundersøkelsen 2013/2014 viste at fødselsnummer var den personopplysninger flest anså som svært viktig å beskytte.¹⁰⁴ Antallet henvendelser Datatilsynet mottar om temaet viser at det opptar svært mange. Når det gjelder biometri er vi enige i at nasjonal regulering er helt nødvendig, i alle fall inntil man har utredet dette nærmere.

Det ble i 2008, på oppdrag av Justisdepartementet, skrevet en omfattende utredning om fødselsnummer, fingeravtrykk og annet bruk av biometri i forbindelse med lov om behandling av personopplysninger § 12.¹⁰⁵ Siden det er foreslått å videreføre gjeldende rett, mener vi at denne utredningen fremdeles er relevant. Datatilsynet var i all hovedsak positive til de vurderinger og forslag som fremkom i utredningen da den var på høring.¹⁰⁶ Det er uklart for oss om departementet har vurdert de anbefalinger som følger av denne utredningen siden den ikke er nevnt i høringsnotatet. Vi anbefaler at departementet vurdere anbefalingene i rapporten, dersom det ikke allerede er gjort.

Utredningen tar blant annet for seg forskjellen på å bruke denne typen opplysninger til identifisering og autentisering, noe som ikke er omtalt i høringsnotatet. Vi sier noe kort om det nedenfor. Videre kommer vi inn på at vi savner en nærmere vurdering av hvilke garantier som kan gis mot misbruk av fødselsnummer og andre biometriske opplysninger, jf. artikkel 87. Dette knytter vi opp mot videreføring av forskriftsbestemmelser. Vi har også en merknad til begrepet «saklig behov».

¹⁰⁴ <https://www.datatilsynet.no/globalassets/global/om-personvern/planer-strategier/personvernundersokelsen/samlerapport-personvernundersokelsen.pdf>, sist åpnet 2.10.17

¹⁰⁵ <https://www.regjeringen.no/no/dokumenter/utredning-om-fodselsnummer-fingeravtrykk/id534749/>

¹⁰⁶ Se vår høringsuttalelse om etterkontroll av personopplysningsloven av 30. oktober 2009 punkt 14.

Identifisering, autentisering og faren for ID-tyveri

Fødselsnummer og andre nasjonale identifikasjonsnumre brukes til identifisering, det vil si å utpeke et bestemt individ i en gruppe eller skille en person fra andre personer på en entydig måte. Fødselsnummer sikrer at man snakker om det samme, bestemte individet på tvers av systemer. Fødselsnummer og andre nasjonale identifikasjonsnumre er ikke alene egnet til autentisering, altså å verifisere identiteten til vedkommende. Årsaken er at det er velkjent at andre enn den registrerte kjenner til eller kan skaffe seg tilgang til vedkommendes fødselsnummer.

På tross av dette har Datatilsynet inntrykk av at fødselsnummer brukes til autentisering. Når virksomheter uten videre stoler på at den som oppgir fødselsnummeret, faktisk er rett innehaver av det, oppstår potensialet for ID-tyveri. Dersom man har skaffet seg tilgang til en persons fødselsnummer, kan man potensielt bestille abonnements- og kredittjenester i vedkommendes navn.

Derfor foreslår Datatilsynet at det vurderes å gi et eksplisitt forbud mot at fødselsnummer og andre nasjonale identifikasjonsnumre blir brukt til autentisering. Dette synliggjør at virksomheter må bruke andre virkemidler for å verifisere at de oppgitte personopplysningene er korrekte, jf. forordningen art. 5 første ledd bokstav d og annet ledd.

Biometriske identifikatorer er, med få unntak, umulige å endre, og derfor medfører behandling av slike personopplysninger en særlig risiko. Biometri kan brukes til både identifisering og autentisering. Derfor vil biometriske data ofte behandles på en annen måte enn fødselsnummer. Videre vil ulike hensyn gjøre seg gjeldende ettersom de biometriske dataene brukes til identifisering eller autentisering. På denne bakgrunn ber Datatilsynet departementet vurdere behovet for en separat bestemmelse om biometri.

Vi viser til den nevnte utredningen som understøtter og konkretiserer forslagene.

Nødvendige garantier og videreføring av særregler i personopplysningsforskriften

Vi savner en nærmere vurdering av hvilke garantier som kan gi vern mot misbruk av fødselsnummer og andre entydige identifikasjonsmidler – både i offentlig og privat sektor. Det foreslåtte forbudet mot bruk av fødselsnummer til autentisering er et eksempel på dette.

En annen garanti finnes i dagens personopplysningsforskrift § 10-2. Vi er enig med departementet i at regelen også kan følge av forordningens artikkel 5 og 32. Regelen er imidlertid praktisk, og vi foreslår derfor at bestemmelsen likevel videreføres av pedagogiske årsaker.

Når det gjelder elektronisk overføring av fødselsnummer, forbyr personopplysningsforskriften § 2-11 tredje ledd eksplisitt at fødselsnummer sendes i klartekst på vanlig e-post. I praksis skjer dette likevel ofte, og Datatilsynet erfarer at dette skuldes manglende kunnskap om sikkerheten ved e-post hos de behandlingsansvarlige. Svært mange tar kontakt med Datatilsynet for råd om hvilke regler som gjelder for elektronisk oversendelse av fødselsnummer.

Regelen i § 2-11 tredje ledd har i denne sammenheng vært svært praktisk og hatt stor betydning. For behandlingsansvarlige synliggjør den en plikt, mens den er til hjelp for enkeltpersoner som ønsker å ta opp et konkret brudd med den behandlingsansvarlige. Samtidig er den en garanti mot misbruk, og det er foreløpig noe usikkert hvilket vern art. 32 i forordningen vil oppstille i praksis. Vi foreslår derfor at denne regelen videreføres tilsvarende innenfor det konkrete handlingsrommet som artikkel 87 gir.

På samme måte bør det oppstilles garantier mot misbruk av biometriske opplysninger. For eksempel kan biometriske opplysninger lagres på medarbeiderens personlige ID-kort og ikke i et sentralt register.¹⁰⁷ Man kan også vurdere særregler om sikkerhet ved trådløs avlesning av biometriske data, for eksempel fra RFID-brikker.

Begrepet «saklig behov»

I forarbeidene til dagens personopplysningslov ble det uttalt at dagens bestemmelse skulle hindre bruk av fødselsnummer i utrengsmål.¹⁰⁸ Datatilsynet opplever imidlertid at fødselsnummer brukes i økt utstrekning, blant annet av næringsdrivende. Samtidig er det særnorske begrepet «saklig behov» vanskelig å tolke, dels fordi ordet «saklig» har blitt brukt flere steder i loven og forskriften med ulik betydning og praksis,¹⁰⁹ og dels fordi begrepet i seg selv gir få holdepunkter for hvor terskelen ligger.

Videre erfarer Datatilsynet at behandlingsansvarlige ikke alltid forstår at i § 12 er ment å oppstille tilleggsvilkår til §§ 8, 9 og 11.

Derfor foreslår Datatilsynet å erstatte «saklig behov» med «særskilt behov». Dette er ment å synliggjøre at fødselsnummer og andre entydige identifikasjonsmidler kun kan benyttes når behandlingsansvarlige faktisk har et behov for identifisering ut over det alminnelige, altså der forveksling kan ha betydelige eller alvorlige konsekvenser for den registrerte. Datatilsynet mener ikke at dette skal heve terskelen for adgang til bruk i forhold til hva lovgiver mente i forarbeidene til dagens personopplysningslov.

Forholdet til særlovgivning

Avslutningsvis vil vi bemerke at vi er usikre på om departementet mener at det bare er den foreslåtte § 9 som bygger på forordningen artikkel 87, om reguleringen av fødselsnummer og andre entydige identifikasjonsmidler som i dag er hjemlet i *sektorlovgivningen* også skal vurderes etter artikkelen, eller om sektorlovgivningen skal vurderes etter forordningens alminnelige regler i artikkel 6 og 9. Dette kan med fordel klargjøres.

¹⁰⁷ Se Artikkel 29-gruppens uttalelse 06/2014 side 68.

¹⁰⁸ Ot.prp. nr. 92 (1998–1999) s. 114.

¹⁰⁹ Se personopplysningsloven § 11 første ledd bokstav b og personopplysningsforskriften §§ 4-3 og 8-4.

27. Unntak fra den registrertes rettigheter ved behandling for arkivformål i allmenhetens interesse, vitenskapelig eller historisk forskning eller for statistiske formål

Datatilsynets merknader knytter seg til lovforslaget § 14, om unntak fra den registrertes rettigheter ved behandling for arkivformål i allmenhetens interesse, vitenskapelig eller historisk forskning eller for statistiske formål og de vurderinger som er gjort i den forbindelse.

Våre merknader til denne bestemmelsen vil i stor grad være de samme som vi har til lovforslagets §13 og til § 6, se punkt 8 og 4. Som det fremgår her mener vi at både lovforslagets § 6 og 13 er problematiske, sett hen til de forpliktelser som følger av forordningen når det gjelder krav til nasjonale lovbestemmelser og avveining av retten til personopplysningsvern mot andre interesser.

Vi mener videre at departementet i høringsnotatets punkt 31.3 gjør en for overfladisk vurdering av de krav til unntak som følger av artikkel 89 nr. 2 og 3 og artikkel 23. Unntakene i § 14 blir dermed for generelle, ut fra de krav som følger av forordningen artikkel 89 nummer 2 og 3, samt artikkel 23. En unntaksbestemmelse bør utformes mer kasuistisk. Vi anbefaler at det gjøres konkrete vurderinger av hvilke tilfeller som ikke er tilfredsstillende dekket i sektorlovgivningen, og at det eventuelt gjøres tilpasninger der. Vi viser først og fremst til arkivloven og statistikkloven, samt en eventuell ny forskningslov. En slik gjennomgang vil klargjøre om det er strengt nødvendig å utforme et slikt generelt unntak og om det er forholdsmessig.

Vi anbefaler altså at unntaket i § 14 ikke vedtas i sin nåværende form. Vi har også noen særskilte merknader til departementets forslag.

27.1. Lovforslaget § 14 første og annet ledd

Bestemmelsen har implementert enkelte av rammene for unntak som følger av artikkel 89 nummer 2 og 3. Det vises her til kravene i forordningen om at rettighetene sannsynligvis må gjøre det umulig eller i alvorlig grad hindre oppfyllelse av de spesifikke formålene som er nevnt i artikkel 89 nummer 1. Departementet har ikke omtalt at kravet om at slike unntak må være nødvendige for å oppfylle formålene. Det er heller ikke gjort noen vurdering av de krav til garantier som følger av bestemmelsen nr. 1. Den norske regelen kan dermed synes å være mer liberal enn det som følger av rammene for unntak i forordningens artikkel 89 nr. 2, 3 og 4. Den kan også neppe sies å være mer spesifikk enn de alminnelige rammene i forordningen.

Det er uklart for oss hva som skal til før en behandling er innenfor unntakene i § 14. Kriteriene for å kunne gjøre unntaket gjeldende, er for det første at behandlingens formål blir «umulig» å nå. Dette må anses som en meget høy terskel, og det er vanskelig å forestille hvilke tilfeller dette skulle vært begrunnelsen. Det er også vanskelig å fastslå hvilke konkrete situasjoner de ulike rettighetene i «alvorlig grad» vil hindre oppfyllelse av formålene. Rekkevidden av bestemmelsen kan derfor neppe sies å være tilstrekkelig konkretisert.

Det er også helt uklart hvilke kategorier av behandlingsansvarlige som kan omfattes av bestemmelsen. Det er heller ikke gitt noen garantier mot misbruk av unntaket. Dette kunne for eksempel vært krav til oppbevaringsperioder før sletting, eller krav om informasjon om unntaket når dette ikke lenger i alvorlig grad vil hindre oppfyllelse av formålet. En viktig garanti som kunne berettiget unntak fra rettighetene er innføring av krav om pseudonymisering og anonymisering i § 6, jf. artikkel 89 nr. 1. Slik behandling har også en sammenheng med forordningens artikkel 11 om behandling som ikke krever identifikasjon.

27.2. Lovforslaget i § 14 tredje ledd

Unntaket i § 14 tredje ledd bygger ikke på artikkel 89 nummer 2 og 3, men artikkel 23 nummer 1 bokstav e. Vi utelukker ikke at artikkel 89 nummer 2 og 3 ikke er uttømmende når det kommer til adgangen til å gjøre unntak fra sentrale rettigheter. Vår innvending er også her den mangelfulle vurderingen av de krav som følger av artikkel 23.

Krav til nødvendighet er ikke omtalt, men det opplyses at det som følger av kravet til proporsjonalitet oppstilles et tilleggsvilkår om at det vil kreve en uforholdsmessig stor innsats å gi innsyn.

Det foretas ingen vurdering av de krav som følger av artikkel 23 nummer 2. Når det gjelder krav til klarhet, spesifisering og garantier mener vi det er vanskelig å se hvilke momenter som ikke er relevante for den norske bestemmelsen. Vi savner en begrunnelse for hvorfor ingen av momentene i artikkel 23 nummer 2 er vurdert.

Vi vil bemerke at behandlingen av slik bruk av data, altså såkalte sekundære formål, kun i sjeldne tilfeller vil ha direkte betydning for den registrerte. Dette unntaket oppfattes dermed som meget vidt, og det vil i praksis innebære en betydelig svekkelse av den enkelte borgers personopplysningsvern. Retten til informasjon og rett til å vite om behandlinger av sine egne opplysninger, er å anse som en høyt beskyttelsesverdig rettighet, til tross for at man ikke har bestemmelsesrett over behandlingen i noen annen form.

Det andre kriteriet er at det blir uforholdsmessig vanskelig å gi innsyn. Etter dagens praksis, legger Datatilsynet til grunn at det med dagens teknologi og med alle nasjonale tjenester for kommunikasjon som utvikles, kun i sjeldne tilfeller gjøres unntak fra informasjonsplikten. Unntakene begrunnes ofte i at det ikke behandles identitetsopplysninger, at det er et stort antall deltakere eller at det er meget kostbart. I tilfeller hvor det er et høyt antall registrerte, stiller vi som regel vilkår om at informasjonen gis kollektivt gjennom for eksempel en nettside eller i lokalaviser. Hovedregelen er imidlertid at de registrerte skal informeres individuelt.

28. Behandling av barns opplysninger

Departementet viser i høringsnotatets punkt 32.3.1 til at forordningen ikke gir adgang til å videreføre någjeldende bestemmelse i personopplysningsloven § 11 tredje ledd om personopplysninger som gjelder barn.

Vi er enige med departementet i at bestemmelsen ikke kan videreføres i sin nåværende form. Vi ber likevel departementet vurdere om bestemmelsen kan videreføres i en annen form, for eksempel som en spesifikk begrensning for behandling av sensitive personopplysninger etter artikkel 9 nr. 4. Vi bemerker også at Artikkel 29-gruppen har lagt til grunn at prinsippet om «barnets tarv også kan klassifiseres som en samfundsmæssig interesse» etter direktivets artikkel 7 bokstav e.¹¹⁰ Vi legger derfor til grunn at tilsvarende gjelder for forordningens artikkel 6 nr. 1 bokstav e, og at det derfor foreligger et nasjonalt handlingsrom etter dette grunnlaget.

Når det gjelder barns samtykke ved informasjonstjenester foreslår departementet en bestemmelse i ny personopplysningslov som setter en aldersgrense på 13 år. Det er viktig at slike aldersgrenser ses i sammenheng med barns fysiske og psykiske modenhet, og at de fra en viss alder er i stand til å ta stilling til spørsmål som gjelder dem.¹¹¹ Aldersgrensen på 13 år er i tråd med Datatilsynets praksis, og vi støtter departementets forslag.

29. Kameraovervåking

Personopplysningsloven kapittel VII og personopplysningsforskriften kapittel 8 inneholder særlige bestemmelser om kameraovervåking. Kapittelet regulerer kameraovervåking *generelt* og har derfor et bredt anvendelsesområde. Forordningen inneholder ingen særskilte bestemmelser om kameraovervåking.

Vi er enig med departementet i at forordningen ikke åpner for å videreføre de gjeldende generelle reglene om kameraovervåking. Som departementet skriver i høringsnotatet vil de alminnelige bestemmelsene i forordningen derfor komme til anvendelse.

I forbindelse med vurdering av nasjonalt handlingsrom og regulering i forordningen på dette området er det imidlertid en bestemmelse i forordningen vi savner omtale av i høringsbrevet. Det fremgår av forordningens artikkel 10 at

«behandling av personopplysninger om straffedommer og lovovertrедelser eller tilknyttede sikkerhetstiltak på grunnlag av artikkel 6 nr. 1 skal bare utføres under kontroll av offentlig myndighets kontroll eller med hjemmel i lov som sikrer egnet vern av de registrertes rettigheter og friheter».

En stor del av kameraovervåkingen som foregår, skjer nettopp for å avdekke kriminelle handlinger, og når dette skjer, behandles «personopplysninger relatert til lovovertrедelser», da i regi av private.

I den svenske utredningen om kameraovervåking¹¹² er det lagt til grunn at artikkel 10 ikke gjelder iakttagelse av straffbare handlinger, men bare idømte forhold. Datatilsynet mener det

¹¹⁰ Se WP 160 side 9.

¹¹¹ Se WP 160 side 9 om vurdering av barns samtykkekompetanse.

¹¹² SOU 2017:55 s.121

er grunn til å tro at denne tolkningen er feil. Artikkel 10 nevner både «straffedommer» og «lovovertrедelser» som alternative vilkår. På engelsk «Convictions and offences». Meningsinnholdet av «straffbare handlinger» mener vi må derfor tolkes separat fra «straffedommer».

Vi ber departementet om å klargjøre anvendelse av forordningens artikkel 10, sett i sammenheng med reglene om kameraovervåking. Artikkel 10 oppstiller i realiteten en plikt til lovhjemmel, samt mulighet/handlingsrom for tilpasninger.

Departementet foreslår å fastsette nasjonale bestemmelser om kameraovervåking på arbeidsplass og bruk av uekte kameraovervåkingsutstyr. Bestemmelsene er langt på vei en videreføring av dagens regulering på disse områdene. Vi har imidlertid noen merknader til forslaget, se punkt 29.2. Andre merknader som gjelder kameraovervåking følger av punkt 29.3 og 29.4.

29.1. Kameraovervåking på arbeidsplass

Datatilsynet støtter departementets forslag om å fastsette nasjonale regler om kameraovervåking på arbeidsplass. Vi har imidlertid noen merknader.

Lovforslagets § 1 regulerer kapittelets virkeområde. Her fremgår det at «*Kapittelet gjelder for kameraovervåking på arbeidsplass*». Datatilsynet ber om at det i lovproposisjonen avklares hva som menes med «arbeidsplass», helst at begrepet defineres i lovteksten, men i det minste at begrepet det omtales i merknadene. Slik forslaget er fremstilt i høringsbrevet er det uklart hvilke områder av en arbeidsplass reglene gjelder. Svært mange steder i samfunnet vil være en arbeidsplass for noen. Dette kan være både lukkede områder som et kontor, eller offentlig tilgjengelige områder slik som butikklokaler, restauranter og legevakt. For eksempel er Oslo S en arbeidsplass for blant annet vektere og rengjøringspersonell.

Slik vi leser det skal dette kapittelet gjelder for kameraovervåking av *alle steder* på en arbeidsplass. Det betyr at reglene gjelder uavhengig av hvilke områder på arbeidsplassen som fanges opp.

I lovforslagets § 2 fremgår det at:

«Kameraovervåking av sted på arbeidsplass hvor en begrenset krets av personer fredes jevnlig, er bare tillatt dersom det ut fra virksomhetens er behov for å forebygge at farlige situasjoner oppstår og ivareta hensynet til ansattes eller andres sikkerhet eller det for øvrig er et særskilt behov for overvåkingen.»

Datatilsynet mener det ikke fremstår som klart i lovforslaget om departementet mener at § 2 skal være *et tilleggsvilkår* for overvåking av slike områder på en arbeidsplass, eller om departementet mener at *hele kapittelet* gjelder kameraovervåking av slike områder på en arbeidsplass. Dersom departementet mener at § 2 skal være et tilleggsvilkår tilsvarende det personopplysningsloven § 38 er i dag, bør dette synliggjøres ved at overskriften til

bestemmelsen endres til «Tilleggsvilkår ved overvåking av sted hvor en begrenset krets av personer ferdes jevnlig».

Datatilsynet mener at det bør inntas en egen bestemmelse som henviser til forordningens øvrige bestemmelser. Selv om departementet skriver i høringsnotatet at dette kapittelet ikke er ment som uttømmende regulering, bør det av pedagogiske grunner fremgå av selve teksten også. Det er særlig nødvendig å vise til forordningens artikkel 6 første ledd bokstav f, som er behandlingsgrunnlaget for kameraovervåking på arbeidsplass. Særlig er dette viktig dersom § 2 skal forstås som et tilleggsvilkår.

Dette kan løses ved å innta en ny bestemmelse mellom § 1 om «kapittelets virkeområde» og § 2 om «kameraovervåking av sted på arbeidsplass hvor en begrenset krets av personer ferdes jevnlig» om alminnelige vilkår. Denne kan utformes ganske likt som dagens § 37 første og tredje ledd. § 37 understreker at personopplysningslovens øvrige bestemmelser også gjelder for kameraovervåking, samtidig som den konkretiserer hva man skal legge vekt på i vurderingen av personopplysningsloven § 8 f som tilsvarer forordningens § 6 f.

Datatilsynet opplever ofte at kameraer på arbeidsplasser fanger opp større områder enn det som er nødvendig ut i fra formålet. Vårt inntrykk er at arbeidsgivere antar at kameraovervåkingen er tillatt – selv om den fanger opp unødvendige områder – forutsatt at formålet med overvåkingen er saklig.

Vi foreslår derfor at departementet inntar en egen bestemmelse som sier at et kamera ikke kan fange opp andre områder enn det som er strengt nødvendig for å oppnå formålet med overvåkingen. En slik bestemmelse vil gi klare føringer til arbeidsgivere om at det ikke er tillatt å overvåke utover det som er nødvendig. Dette er i tråd med minimeringsprinsippet, og kan trolig bidra til at ansatte i større grad enn i dag har «friområder» der de ikke blir overvåket.

Varsel om at overvåking finner sted

Datatilsynet støtter forslaget om å inntas en bestemmelse om varslingsplikt i form av skilting «eller på annen måte», men mener at den bør utvides.

Vårt inntrykk er at arbeidstakere ofte får for dårlig informasjon om kameraovervåking på arbeidsplassen, som regel kun ved at arbeidsgiver henger opp et skilt. Vi mener at det å sette opp et skilt ikke er tilstrekkelig til at informasjonsplikten ovenfor overfor arbeidstakere kan anses oppfylt. Arbeidsgivere har plikt til å gi mer utfyllende og presis informasjon om kameraovervåking for å skape derfor større forutsigbarhet for berørte arbeidstakere og skape gjennomsiktighet, som er et viktig personvernprinsipp. Kameraovervåking vil også være et kontrolltiltak etter arbeidsmiljøloven, med de konsekvenser det har.

Slik bestemmelsen er formulert fremstår det som at skilting er tilstrekkelig for å oppfylle kravet om informasjon. Vi foreslår derfor at det inntas en mer utfyllende bestemmelse om informasjonsplikt overfor arbeidstakere før kameraovervåking tas i bruk. Bestemmelsen bør inneholde plikt til å gi informasjon om blant annet formålet med kameraovervåkingen, om det skjer monitorering eller opptak og lagringstiden. I det minste bør det inntas en henvisning til

informasjonsplikten i forordningen og informasjons- og drøftingsplikten etter arbeidsmiljøloven kapittel 9 om kontrolltiltak.

Sletting av opptak gjort ved kameraovervåking

Departementet gir i lovutkastets § 5 bestemmelser som fastsetter konkrete slettefrister for opptak gjort ved kameraovervåking på arbeidsplass. Av lovforslagets første ledd fremgår det at *«Opptak skal slettes senest en uke etter at opptaket er gjort. Hvis det er sannsynlig at opptaket vil bli utlevert til politiet i forbindelse med etterforskning av straffbare handlinger eller ulykker, kan opptakene oppbevares inntil 30 dager»*. Denne bestemmelsen er langt på vei en videreføring personopplysningsforskriften § 8-2 annet ledd.

I lovforslagets § 5 annet ledd følger det at *«opptak gjort på utsalgsteder som benytter betalingskort, eller i post- eller banklokaler, skal slettes senest tre måneder etter at opptakene er gjort.»* Dette innebærer en utvidet lagringsadgang sammenlignet med første ledd. For utsalgsteder representerer dette også en utvidelse i forhold til gjeldende rett, hvor lagringstiden følger hovedregelen om syv dager.

Regler om lagring av opptak gjort på utsalgsteder som benytter betalingskort, eller i post- eller banklokaler er slik, vi oppfatter det, begrunnet i avvergelse av skimming. Det kan stilles spørsmål ved om artikkel 88 gir grunnlag for å regulere sletteregler for banknæringen. Trolig inngår dette i «vern av arbeidsgiverens eller kundens eiendom» i artikkel 88, men departementet kan vurdere å presisere dette i proporsjoner.

Om ordlyden «Opptak gjort på utsalgsteder som benytter betalingskort»

Det er uklart om den utvidede lagringstiden gjelder for opptak fra kameraer gjort på en arbeidsplass som har et utsalgsted som benytter betalingskort som sådan, eller om den utvidede lagringstiden bare gjelder de kameraene som er rettet mot et betalingspunkt. Dette må avklares.

Slik bestemmelsen er formulert kan den forstås som at arbeidsplasser med betalingspunkter automatisk omfattes av bestemmelsen. Dette innebærer i prinsippet at all kameraovervåking i f.eks. en butikk lagres i tre måneder. Dette vil i så fall være fullstendig uproporsjonalt, tilfeldig og lite personvernvennlig. Arbeidstakere vil kunne oppleve det som svært belastende at arbeidsgiver lagrer opptak av arbeidshverdagen tre måneder tilbake i tid. Det er derfor svært viktig at departementet presiserer i lovteksten at utvidet lagringstid bare gjelder kamera som er rettet mot selve betalingspunktet. Å begrense bruk av utvidet lagringstid til slike kamera vil være i tråd med minimeringsprinsippet og hovedbegrunnelsen bak bestemmelsen, nemlig avvergelse av skimming. Det er videre viktig å presisere at bestemmelsen ikke åpner for overvåking av de ansatte i tre måneder.

For øvrig er ikke alle betalingspunkter like utsatt for skimmingrisiko. Vanlige betalingspunkter i utsalgsteder er vanligvis under oppsyn av ansatte, og i slike tilfeller er det vanskelig å forsvare utvidet lagring. Derimot ser vi at ubetjente betalingspunkter og liknende kan være utsatt for særlig risiko, og dette kan begrunne utvidet lagringstid. Vi stiller derfor spørsmål ved om bestemmelsen er for vidt formulert. Departementet bør derfor vurdere å oppstille en slags nedre grense for når det er tillatt med utvidet lagring. Uten en slik

presisering blir konsekvensen at alle som har kameraovervåking rettet mot et betalingspunkt lagrer opptak i tre måneder, uavhengig av om det er behov for det eller ikke.

«Opptak gjort i post- eller banklokaler»

Av ordlyden fremgår det at «opptak gjort i post- eller banklokaler, skal slettes senest tre måneder etter at opptaket er gjort». Dette er en videreføring av dagens regelverk. Datatilsynet vil på peke at «post i butikk» og «bank i butikk» faller etter dagens praksis utenfor denne bestemmelsen. Disse områdene har allerede tillatelse fra Datatilsynet, jf.

personopplysningsforskriften § 8-4 sjette ledd, til å lagre opptak av kassapunkt og kontantsafe i tre måneder, men Datatilsynet må ved enkeltvedtak gi ny tillatelse for hvert nye lokale. Slike områder bør inkluderes i regelen, eller så bør det presiseres i proposisjonen at regelen er ment å omfatte også slike områder.

Dispensasjoner gitt etter gjeldende rett

Etter nåværende personopplysningsforskrift § 8-4 siste ledd kan Datatilsynet gjøre unntak fra slettereglene ved særlig behov. Denne regelen er foreslått videreført i § 5 siste ledd.

Datatilsynet ser at det kan være hensiktsmessig med en overgangsregel som sier at allerede gitte dispensasjoner, som knytter seg til reglene om arbeidsliv, fortsatt skal være gyldige etter nytt regelverk.

29.2. Bruk av uekte kameraovervåkingsutstyr

Departementet ber høringsinstansenes syn på om forslaget om å innta en bestemmelse om bruk av uekte kameraovervåkingsutstyr.

Datatilsynet støtter forslaget om å ha en bestemmelse om uekte kameraovervåkingsutstyr, men har et par merknader.

I lovforslaget fremgår det at uekte kameraovervåkingsutstyr kun kan *«benyttes der bruken oppfyller vilkårene i personvernforordningen artikkel 6 nr. 1»*. Slik bestemmelsen er utformet kan den oppfattes som at også privatpersoner som ønsker å montere et dummykamera som dekker eget hus eller hage må oppfylle vilkårene i artikkel 6 første ledd nr. 1. Dersom kameraet er ekte, vil imidlertid forordningen ikke gjelde siden unntaket for «private formål» i forordningens artikkel 2 nr. 2 bokstav c kommer til anvendelse. Konsekvensen av dette vil i så fall være at privatpersoner får større adgang til å montere ekte kameraer enn dummykameraer innenfor rammene av sin husholdning. For å unngå uklarheter omkring dette, bør det komme klart fram av bestemmelsen at unntaket i forordningen art 2. annet ledd bokstav c gjelder tilsvarende, eventuelt at det presiseres at bestemmelsen ikke gjelder for personlige eller andre private formål.

Datatilsynet er videre av den oppfatning at skilting av om at et område er overvåket, selv om det i realiteten ikke finnes overvåkingsutstyr på stedet, må likestilles med bruk av uekte kameraløsninger. Det er plikt til slik skilting i dag, jf. personopplysningsloven § 40, jf. § 36 første ledd siste punkt. Følelsen av å bli overvåket vil i like stor grad gjøre seg gjeldende når

det informeres om at området er kameraovervåket som når det faktisk er det. Det kan vurderes å innta et punkt om dette i bestemmelsen eller omtalen i proposisjonen.

29.3. Andre merknader knyttet til kameraovervåking

Vi har merknader knyttet til behandling av sensitive personopplysninger, politiets bruk av kameraovervåking og behovet for andre nasjonale regler om kameraovervåking, herunder særlig forbud mot kameraovervåking i undervisningstiden på skoler og barnehager.

Behandling av sensitive personopplysninger, jf. art 9

Kameraovervåking innebærer ofte en behandling av sensitive personopplysninger. Dette var bakgrunnen for § 37 annet og fjerde ledd i personopplysningsloven. Bestemmelsen sier at kameraovervåking kun skal anses som behandling av sensitive personopplysninger der slike utgjør en vesentlig del av opplysningene som overvåkingen omfatter.

Datatilsynet har tolket bestemmelsen som at det må foreligge en systematisk eller formålsrettet registrering av sensitive opplysninger for at vesentlighetskravet er oppfylt. Vi har lagt stor vekt på hvilke områder som blir overvåket, blant annet med henvisning til forarbeidene til personopplysningsloven (Prop 47 L.(2011-2012) side 43-44) som sier at

«..overvåkingskamera i nærheten av sykehus, apotek, helsestasjoner etc. i stor utstrekning vil kunne få med opplysninger om personers helsesituasjon. Vesentlighetskravet vil da lett være oppfylt».

Vi har blant annet vurdert at kameraovervåking hos en spesialisthelsetjeneste som hovedregel oppfyller vilkåret. Det er overveiende sannsynlig at personer på et venterom hos en onkolog har kreft. Samtidig har vi ment at overvåking på en rutebuss ikke oppfyller vilkåret, selv om kameraet kan fange opp både personer med brukket ben og personer med religiøse plagg.

Det er i prinsippet gode grunner for å videreføre en lignende regel da den i de fleste tilfeller forbyr kameraovervåking som i stor grad fanger opp sensitive personopplysninger. Personverninngrepet er som regel svært stort på slike steder. Eksempler på dette er religiøse arenaer og spesialisthelsetjenester. Vi kan imidlertid ikke se at det er nasjonalt handlingsrom for å videreføre § 37 fjerde ledd etter forordningen.

Å ikke ha en slik lovbestemmelse å forholde seg til fremover vil i praksis reise mange tolkningsspørsmål. Forordningen artikkel 9 vil, etter en ren ordlydfortolkning, som hovedregel forby bruk av kameraovervåking som innebærer behandling av sensitive personopplysninger. Det kan imidlertid ikke være formålet med bestemmelsen å avskjære *all* bruk av kameraovervåking. Det vil være en stor fordel om det i proposisjonen klargjøres i hvilke tilfeller artikkel 9 forbyr bruk av kameraovervåking.

Det er naturlig og formålstjenstlig at kameraovervåking som hovedregel er forbudt når *formålet* er å fange opp sensitive personopplysninger. Dette er i tråd med Artikkel 29-gruppen gruppens uttalelse i 11759/02/EN som sier at det bør være forbudt å kameraovervåke hvis formålet kun er å fange opp sensitive personopplysninger. Dette vil medføre at

diskriminerende og trakasserende bruk av kameraovervåking vil være er forbudt. Et klart standpunkt i proposisjonen vil gjøre regelverket enklere å praktisere enn tidligere, både for de behandlingsansvarlige og for Datatilsynet.

En slik avklaring vil også innebære at det blir tillatt å overvåke steder der sensitive personopplysninger tilfeldigvis vil bli fanget opp. Dette forutsetter selvfølgelig at det foreligger et saklig behov og formål, og at behovet overstiger personvern hensynet, jf. art 6 bokstav f. Dette betyr at sykehus, apotek eller andre lignende virksomheter ikke er avskåret fra å benytte kameraovervåking på grunn av art 9.

Vi presiserer at det uansett må foreligge et behandlingsgrunnlag i art 6 for kameraovervåking på slike steder, og at dette bør presiseres i proposisjonen. På slike steder gjør personvern hensyn seg gjeldende i stor grad, og der kameraovervåking er basert på artikkel 6 første ledd bokstav f, skal det derfor tungtveiende grunner til for at kameraovervåking er tillatt.

Politiets bruk av kameraovervåking

Det har tidligere vært lagt til grunn at politiets bruk av kameraovervåking i forebyggende øyemed reguleres av personopplysningsloven og ikke av politiregisterloven. Politiregisterloven regulerer som kjent politiets og påtalemyndighetens behandling av opplysninger for øvrig. Det antas imidlertid at politiets og «andre kompetente myndigheters» kameraovervåking faller *utenfor* forordningens virkeområde, jf. artikkel 2 (2) (d) og fortalen punkt 19, og at det tilsvarende vil falle *innenfor* direktiv 2016/680.

Etter direktivets artikkel 8 må behandling av personopplysninger ha hjemmel i lov for å være lovlig. Politiets legitime bruk av kameraovervåking kan ikke hjemles i regler om gjelder overvåking på arbeidsplass. Slik vi ser det, foreligger det ikke hjemmel for politiets bruk av kameraovervåking i forebyggende øyemed i politiregisterloven heller. Uten slik hjemmel vil ikke politiet kunne iverksette kameraovervåking etter at forordningen trer i kraft. Til orientering har Sverige i sin utredning konkludert med at det er direktiv 2016/680, og ikke forordningen, som gjelder på dette området.^[1]

Datatilsynet har behandlet flere saker som gjelder politiets kameraovervåking etter dagens personopplysningslov. Erfaringer fra disse sakene viser at det er et stor behov for en spesifikk regulering av politiets adgang til å iverksette kameraovervåking.

Vi mener departementet må utrede dette nærmere og enten gi hjemmel til politiets kameraovervåking i politiregisterloven, eller ved en uttrykkelig bestemmelse i personopplysningsloven, dersom man kommer til at det er adgang til det.

Andre nasjonale regler om kameraovervåking, herunder særlig forbud mot kameraovervåking i undervisningstiden på skoler og barnehager

Departementet ber om høringsinstansenes syn på om det bør fastsettes nærmere regler om kameraovervåking innenfor det nasjonale handlingsrommet. Datatilsynet har per i dag ingen

^[1] SOU 2017:55 s. 242 flg.

konkrete forslag her, men det kan være aktuelt å komme tilbake til dette ved en senere anledning.

Departementet ber særlig om høringsinstansenes syn på om det bør fastsettes forbud mot kameraovervåking i undervisningstiden på skoler og barnehager, i den utstrekning forordningen åpner for dette. Selv om ikke forordningen uttrykkelig gir barn et særskilt vern, er det klart at dette en gruppe som både lovgiver og Datatilsynet må være særlig oppmerksom på.

Datatilsynet ser at det er mange gode argumenter for å gi et slikt forbud. Datatilsynet erfarer at det er svært enkelt å ty til kameraovervåking som virkemiddel. Kameraovervåking er synlig, konkret og lite kostbart, og det kan være enkelt å ty til for å vise at man har gjort noe når det av en eller annen grunn er behov for tiltak. Datatilsynet har eksempler både fra skoler og barnehager der kameraovervåking har blitt tatt i bruk, med den konsekvens at barn har blitt filmet gjennom sin barnehage- og skolehverdag.

Barn bør kunne leke og utfolde seg fritt i barnehagen og skolen uten at dette fanges opp av et overvåkningskamera. Kameraovervåking av barn i skole og barnehage kan bidra til å sende uheldige signaler om hva som er akseptabelt når det kommer til overvåking videre i livet. Barn kan komme til å oppfatte at dette er en normalsituasjon. Dersom det iverksettes kameraovervåking i skolens fellesområder vil det i verste fall bety at et barn blir overvåket gjennom hele sin skoledag.

Datatilsynet er imidlertid usikker om en regelen ligger innenfor vårt nasjonale handlingsrom, det må i så fall utredes nærmere. I tillegg har Datatilsynet erfaring med at det unntaksvis kan være et velbegrunnet behov for slik kameraovervåking, sånn at et *absolutt* forbud er trolig ikke hensiktsmessig.

30. Arbeidsgiveres innsyn i e-postkasse mv.

Departementet foreslår i stor grad å videreføre reglene om innsyn i e-post mv, som følger av gjeldende personopplysningsforskrift kapittel 9.

Vi støtter forslaget om å videreføre særskilte regler om innsyn i e-post og filer. Spørsmålet om arbeidsgivers adgang til å gjøre innsyn i ansattes e-post og filer har utgjort en stor andel av antallet henvendelser til Datatilsynet de senere årene. Bestemmelsene skaper forutberegnelighet for både arbeidsgiver og arbeidstaker.

Vi støtter imidlertid ikke forslaget om at bestemmelsene også skal gjelde innsyn i aktivitetslogger. Vi mener bestemmelsene, som i hovedsak er beregnet på innsyn i e-post, i liten grad er egnet til å skape forutberegnelighet på dette området. Se nærmere om det i punkt.28.1

Det fremgår ikke av høringsnotatet hvilke nærmere vurderingen departementet har gjort med hensyn til handlingsrommet i artikkel 88. Det slås kun fast at forordningens artikkel 88 åpner

for at de norske reglene i hovedsak kan videreføres. Vi mener artikkel 88 neppe åpner for å gjøre unntak fra sentrale krav i forordningen som artikkel 5 om prinsipper, kapittel III om rettigheter, samt de nye pliktene som følger av artikkel 25 og 35. Vi antar at departementet er enig i dette, men dette er i liten grad belyst i høringsnotatet.

30.1. Behov for separate bestemmelser for innsyn og overvåking

Den teknologiske utviklingen de senere år har medført at arbeidsgivere har helt nye muligheter til å overvåke sine ansatte enn da personopplysningsforskriften kapittel 9 ble vedtatt. Forslaget til bestemmelser bør avgrenses til å bare regulere adgangen til innsyn i e-post, altså at de ikke skal gjelde for overvåkingstiltak (aktivitetslogg). Departementet kan eventuelt utforme utfyllende regler om overvåking i tillegg.

Bakgrunnen for forslaget er at vi mener at de foreslåtte bestemmelsene i så liten grad klargjør grensene for lovlig overvåking at det er enklere for å forholde seg til de alminnelige reglene i forordningen. Det er åpenbart stor forskjell på bruk av e-post som kommunikasjonsmiddel og iverksetting av overvåkingstiltak og det er derfor ikke hensiktsmessig å ha like regler om dette.

Artikkel 29-gruppen har utarbeidet en uttalelse om overvåking av elektronisk kommunikasjon og slik vi har forstått det vil en ny uttalelse bli publisert om ikke altfor lang tid.¹¹³ Disse uttalelsene vil samlet sett gi grundig veiledning om regelverket på dette området. Artikkel 29-gruppen omtale spesielt krav til gjennomsiktighet, rettslig grunnlag, nødvendighet, formålsbegrensning og proporsjonalitet for å kunne *innføre* overvåkingstiltak. Det kan også være tale om så inngripende overvåkingstiltak at det kreves klare nasjonale regler. Artikkel 29-gruppen har dessuten pekt på at de ikke anser overvåkingsaktiviteter som er direkte rettet mot behandling av sensitive opplysninger om ansatte som berettigede eller akseptable etter personverndirektivet, med mindre det er tillatt ifølge nasjonale lovbestemmelser som fastsetter nødvendige garantier.¹¹⁴

Forslag til § 2 og 3 gir liten veiledning med hensyn til sentrale krav for innføring av et overvåkingstiltak. Bestemmelsene regulerer etter sin ordlyd vilkår og prosedyrer ved innsyn som gjøres i aktivitetslogger som *allerede* er innført.

Innsyn i aktivitetslogg kan dermed være ulovlig etter de alminnelige reglene i forordningen, mens vilkårene for innsyn og prosedyrekrav i §§ 2 og 3 isolert sett er oppfylt. For eksempel kan formålet med innsyn være uforenelig¹¹⁵ med det opprinnelige formålet med aktivitetsloggen. På dette området blir for øvrig det foreslåtte regelverket mer uklart enn det gjeldende, siden departementet har fjernet formålsbegrensningen i dagens § 9-2 jf. 7-11. Det vil si at adgangen til overvåking ikke lenger er avgrenset til administrasjons- og sikkerhetsformål.¹¹⁶ Departementet har ikke begrunnet dette i høringen.

¹¹³ Se WP 55.

¹¹⁴ Se WP 55 side 17.

¹¹⁵ Se artikkel 5 nummer 1 bokstav b.

¹¹⁶ Se personopplysningsforskriften § 9-2 annet ledd jf 7-11. Henvisningen til sistnevnte bestemmelse har vært tolket og praktisert som en formålsbegrensning.

Det foreslåtte kapittelet får heller ikke frem de sentrale krav til gjennomsiktighet som gjelder ved *innføringen* av slike typer overvåkingstiltak. Det vises her til forordningens artikkel 13 og 14, som er de sentrale bestemmelsene arbeidsgiver må oppfylle.

Krav om sletting av opplysninger fra aktivitetslogg er heller ikke særlig regulert i § 4. Dermed må arbeidsgivere i all hovedsak forholde seg til de alminnelige reglene i forordningens artikkel 5 nummer 1 bokstav e og artikkel 17 om sletting.

Regler om overvåking av ansatte kan ta utgangspunkt i ILOs adferdskodeks om beskyttelse av arbeidstakers personopplysninger (1997) punkt 6.14. Se spesielt de krav som er stilt til gjennomsiktighet og proporsjonalitet:

«(1) Hvis arbeidstagere overvåges, bør de på forhånd underrettes om begrunnelsen for overvågingen, tidsplan, metode og anvendte teknikker samt om de opplysninger, der skal indsamles, og arbeidsgiveren bør begrense sin indtrængen i arbeidstagernes privatliv til et minimum.

(2) Hemmelig overvåging bør kun tillades,:

a) hvis det er i overensstemmelser med national lovgivning, eller

b) hvis der er begrundet mistanke om straffbare handlinger eller andre alvorlige uregelmæssigheder.

(3) Fortsat overvåging bør kun tillades, hvis det af sundheds- eller sikkerhedsmæssige grunde eller med henblik på beskyttelse af ejendom er nødvendigt (...).»

30.2. Merknad til § 2 om vilkår for innsyn

Gjeldende personopplysningsforskrift § 9-2 i stor grad er en konkretisering av direktivet artikkel 7 bokstav f. Vi antar også at § 9-2, ut fra krav til harmonisering etter direktivet, er innenfor det handlingsrom medlemsstatene har til å utforme særskilte bestemmelser etter direktivets artikkel 5 og artikkel 7 bokstav f.

Slik vi ser det angir derfor vilkårene som er oppstilt i forslag til § 2 bokstav a og b på tilsvarende måte en konkretisering av de tilfeller som også vil gi grunnlag for innsyn etter forordningens artikkel 6 nummer 1 bokstav f.

30.3. Merknad til § 3 om prosedyrer ved innsyn

Vi er positive til mange av de prosedyrekrav som er foreslått i § 3 ved innsyn i e-postkasse mv. Vi trekker i den forbindelse spesielt frem § 3 tredje ledd. Vi er enige med departementet at arbeidstakeren bør ha informasjon i de tilfeller hvor vedkommende ikke har vært tilstede.

Vi mener imidlertid at også arbeidstakeren bør ha en *innsigelsesrett* etter § 3 første ledd og ikke bare en rett til å uttale seg om innsynet. Vi viser her til forordningens artikkel 21 nr. 1. Denne bestemmelsen gjelder etter sin ordlyd behandlinger etter artikkel 6 nr. 1 bokstav e og f, og viser ikke uttrykkelig til artikkel 88. Ordlyden i artikkel 88 taler for at en slik rett også bør

gjelde i de tilfeller hvor medlemsstatene fastsetter mere spesifikke bestemmelser for å sikre beskyttelse av arbeidstakers rettigheter.

Vi savner en klargjøring i tilknytning til § 3 om dataminimerings/proporsjonalitetsprinsippet gjelder ved innsyn i arbeidstakers e-postkasse og ved overvåking av arbeidstaker.

Som det fremgå av kapitel 8 er vi kritiske til det generelle unntaket fra retten til informasjonsplikt i § 13. På dette området mener vi departementet burde ha vurdert spesifikke unntak. I praksis er det tidsaspektet og bevisforspillelsesfare som gir grunnlag for unntak. Vi foreslår at departementet heller utformer særskilte grunnlag for unntak fra retten til informasjon, og ikke viser til de svært generelle unntaksbestemmelsen i lovforslagets § 13.

30.4. Merknad til § 4 om sletting av opplysninger ved opphør av arbeidsforholdet

Vi støtter en videreføring av bestemmelsen om sletting av opplysninger fra e-postkassen ved opphør av arbeidsforholdet. Bestemmelsen er i stor grad en konkretisering av prinsippet om lagringsbegrensning etter forordningens artikkel 5 nr. 1 bokstav e.

Vi vil imidlertid påpeke at begrepet «daglige driften» er uklart allerede i dag. Dersom departementet ønsker å videreføre dette begrepet bør det gis noe veiledning på hva som nærmere ligger i det. Merknadene til § 9-4 er ikke helt klargjørende på dette i dag.

31. Økonomiske og administrative konsekvenser

Ettersom forordningen, etter departementets oppfatning, i betydelig grad viderefører gjeldende personopplysningsregelverk, «antar departementet at det ikke vil medføre betydelige økonomiske og administrative konsekvenser». Datatilsynet går nedenfor gjennom konsekvensene for Datatilsynet, men vil understreke at gjennomføringen vil medføre betydelig omkostninger også for de behandlingsansvarlige.

De pålegges en lang rekke nye plikter, blant annet plikten til å bygge systemer på innebygd personvern, utnevne personvernombud og plikt til å forhåndsdrøfte behandlinger med Datatilsynet. Også en forsterket rett til å få data slettet, og ikke minst retten til dataportabilitet vil ha betydning. Det pågår nå storstilte endringsprosjektet i mange norske virksomheter for å etterleve loven når den trer i kraft.

Det er viktig å understreke at noe av ånden i forordningen er at man skal jobbe systematisk og kontinuerlig for ikke bare å etterleve loven den 25. mai 2018, men også i 2019 og årene som følger. Dette krever etablering av nye systemer, rutiner og i en del tilfeller også ansettelse av nye folk. Dette er selvsagt ressurskrevende. Etter vår oppfatning undervurderer departementet i betydelig grad de økonomiske og administrative konsekvensene forordningen vil ha for de behandlingsansvarlige.

Departementet ber om høringsinstansenes innspill til økonomiske og administrative konsekvenser av personvernforordningen, men skriver samtidig at de nærmere konsekvensene for Datatilsynet vil bli utredet nærmere. Vi vil komme tilbake med en detaljert utredning av dette spørsmålet, men vil i høringen gi en kort og skjematisk oversikt over de nye oppgavene vi vil bli pålagt som følge av forordningen.

Vi kommenterer kun de nye oppgavene vi blir pålagt, og der vi ser at eksisterende oppgaver vil kreve vesentlig mer ressurser.

Forhåndsdrøftelser

Folks personopplysninger er en viktig ingrediens i nær sagt alle utviklingsprosjektet i offentlig og privat sektor. Tre eksempler kan nevnes:

- Helseplattform i Trøndelag, som skal være pilot for det større målbildet om «en innbygger, en journal».
- Velferdsteknologisk plattform i Oslo, og tilsvarende utviklingsprosjekter i andre kommuner.
- Telenors visjon om å levere tjenesteplattform, og «vite mer om kundens behov enn kunden vet selv».
- NAVs satsing på big data for å avdekkes svindlere, og enklere matching av arbeidssøker og arbeidsgiver.
- Utkontraktering av datadrift og lagring.

Kanskje disse, og en lang rekke tilsvarende prosjekter, vil ha betydelig risiko, og vil trolig måtte forhåndsdrøftes med Datatilsynet, noe som vil svært ressurskrevende.

Vi behandler i dag et stort antall konsesjoner, men denne ordningen er foreslått avvirket ved innføringen av forordningen. Det alt vesentlig av konsesjonsbehandlingen gjelder helseforskning, og andre konsesjoner på helsesektoren. Det er imidlertid mange av sakene som tidligere krevde konsesjon som vil falle inn under den kategorien av behandlinger som krever forhåndsdrøftelse med Datatilsynet etter forordningen art. 36. Vi antar derfor at bortfallet av konsesjonsinstituttet ikke vil føre til noen ressursbesparelse innen denne sektoren.

Økt antall kontroller

En bærende prinsipp i forordningen er å erstatte forhåndskontroll med etterkontroll, herunder å avvikle konsesjonsbehandlingen. Det innføres en rekke systemplikter som i sum skal føre til etterlevelse av regelverket. Dette fordrer imidlertid aktiv tilsynsinnsats fra Datatilsynets side. Kontrollene vil bli stadig mer krevende, særlig på felt hvor ny teknologi tas i bruk. For å oppfylle kravene i forordningen, må Datatilsynet derfor gjennomføre flere kontroller enn tilfellet er i dag.

Bransjenormer

Datatilsynet skal oppfordre til å etablere bransjenormer og skal i tillegg godkjenne slike normer. Vi forventer stor pågang fra bransjer som vil etablere bransjenormer. Vi har allerede

mottatt mer enn ti henvendelser fra bransjer om dette. Noen av disse arbeidene vil være svært ressurskrevende.

Personvernombud/personvernrådgivere

Det vil bli en mangedobling av antall personvernombud. I offentlig sektor alene kan det dreie seg om 12 – 1500. Datatilsynet skal ikke godkjenne, og heller ikke drive aktiv opplæring av ombudene. Det er imidlertid helt klart at svært mange av ombudene vil be om råd og veiledning hos oss.

Avvikshåndtering

Datatilsynet behandler også i dag avviksmeldinger, men etter forordningen skal langt flere avvik meldes inn til oss. Vi venter en mangedobling i antall avviksmeldinger, og har allerede sett en vesentlig økning.

Behandle saker etter konsistensmekanismen

Et sentralt del av forordningen er å etablere en enhetlig praksis i saksbehandlingen, på tvers av landegrensene. Vi vil bli trukket inn i mange enkeltsaker der norske selskaper er involvert, enten som ledende tilsynsmyndighet eller vi vil bli hørt i saken.

Bidra i internasjonalt arbeid, i EDPB og i informasjonskampanjer

European Data Protection Board blir etablert som et sentrale EU-organ, og det er svært viktig med aktiv deltagelse fra det norske Datatilsynet. Som ikke-medlem er det også viktig at vi bygger uformelle nettverket utenfor de formelle møtene, særlig med våre nordiske kollegaer. I tillegg til diskusjon av enkeltsaker, får EDPB en rekke andre oppgaver der det er viktig å delta aktivt.

Flere rettssaker som følge av høye overtredelsesgebyr

Datatilsynet gis mandat til å ilegge betydelig høyere overtredelsesgebyr enn i dag, da maks gebyr er på 10 G. Dette vil utvilsomt føre til en enda større grad av rettsliggjøring av våre saker. Det er all grunn til å tro at flere av våre forvaltningsvedtak vil bli bragt inn for retten, med den ressursbruk det medfører.

Komplisert, teknisk rådgivning, særlig knyttet til innebygd personvern

Det blir en plikt å bygge systemer etter prinsippene for innebygd personvern. Dette er komplisert, og Datatilsynet vil få en svært sentralt rolle som rådgiver i slike spørsmål. Dette vil for eksempel gjelde når tekniske løsninger skal forhåndsdrøftes med tilsynet.

Opprette og føre liste over DPIA, og hvem som ikke trenger DPIA

Det innføres en plikt for mange virksomheter til å gjennomføre utredning av personvernkonsekvenser, som blant annet skal inkludere identifikasjon av risiko, og risikoreduserende tiltak. Datatilsynet pålegges en ny plikt om å føre en liste over slike utredning, og hvilke behandlinger der det ikke er nødvendig.

Mer rapportering – for eksempel oversikt over typer overtredelser og hvilke tiltak som er truffet.

Det pålegges å rapportere på en lang rekke aktiviteter til EDPB, for eksempel skal tilsynet lage oversikt over hvilke type overtredelser vi har behandlet, og hvilke tiltak vi har truffet.

Mer informasjonsaktiviteter

Forordningen er til dels meget uklar og fortalen gir liten hjelp i fortolkningen av reglene. Vi forventer (og har allerede klart merket) en betydelig økning i pågangen fra virksomheter og borgere. Dette gjør det nødvendig med en vesentlig satsing på informasjonsaktiviteter. Forordningen legger også opp til særlig fokus på informasjonsaktiviteter rettet mot barn og unge.

Som nevnt i innledningen vil Datatilsynet komme med en grundig utredning av hva de nye oppgavene vil utløse av behov for økt bemanning og økte utgifter til utvikling av nye, digitale tjenester. Vi kan imidlertid konkludere med at vesentlig av budsjettet er nødvendig for å kunne utføre de oppgavene vi blir pålagt.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Jørgen Skorstad
avdelingsdirektør

Kopi: Kommunal- og moderniseringsdepartementet
v/Statsforvaltningsavdelingen
Postboks 8112 Dep, 0034 Oslo