17 NOV 2009

Skattedirektoratet

Saksbehandler	Deres dato	Vår dato
Thomas Olsen	3. juli 2009	15. november 2009
Telefon	Deres referanse	Vår referanse
22077628	200904400 ES HAJ/mk	2009/529993

Justisdepartementet
Postboks 8005 Dep
0030 Oslo

JUSTISDEPARTEMENTET
20 NOV 2009
SAKSNR.: 200904400
AVD/KONT/BEH: LOV I 53 IHOLLE
DOK.NR. 56 ARKIVKODE:

Høring – etterkontroll av personopplysningsloven

Vi viser til høring av 3. juli 2009 vedrørende etterkontroll av personopplysningsloven. Skattedirektoratet har følgende kommentarer:

1 Lovens definisjoner

1.1 Begrepet "personopplysning"

Skattedirektoratet deler utredernes (Schartum og Bygrave) oppfatning om at det er hensiktsmessig at viktige vurderingskriterier som i dag kun fremgår av lovens forarbeider, forvaltningspraksis og personverndirektivet også inntas i personopplysningslovens sentrale definisjoner.

Direktoratet støtter utredernes forslag om å presisere at vurderingen av om det foreligger personopplysninger gjelder uavhengig av hvordan opplysningene kommer til uttrykk. I stedet for "eller andre signaler" kan formuleringen "eller på andre måter" benyttes.

Etter vår oppfatning er utredernes radikale forslag vedrørende opplysninger om døde personer for snever da den blant annet avgrenser mot økonomiske forhold som mange anser som ømfintelig. Departementets forslag synes som en hensiktsmessig klargjøring av i hvilke tilfeller opplysninger om døde personer skal anses som personopplysninger. Slik vi forstår presiseringen vil det være hensynet til den levende som opplysningene samtidig angår som begrunner unntaket om at opplysninger om døde personer også vernes av personopplysningslovens regler.

Etter direktoratets oppfatning vil "fysisk enkeltperson" være å foretrekke fremfor bare "fysisk person" fordi begrepet "enkeltperson" virker å være godt innarbeidet.

Direktoratet mener formuleringen "opplysninger og vurderinger" bør videreføres, siden den gjør det klart at også subjektive vurderinger og uverifiserte opplysninger anses som personopplysninger.

Direktoratet støtter departementets forslag til ordlyd vedrørende biologisk materiale.

Vi mener det kan være hensiktsmessig å innføre et identifiserbarhetskriterium som presiserer at definisjonen både omfatter opplysninger hvor det *er* foretatt en identifisering og hvor dette *potensielt* kan skje, jf departementets kommentarer i punkt 1.1.3.6 vedrørende

Postadresse
Postboks 9200 Grønland
0134 Oslo
skattedirektoratet@skatteetaten.no

Besøksadresse
Fredrik Selmers vei 4
Org. nr: 974761076

Sentralbord
800 80 000
Telefaks
22 17 08 60

Personvernnemndas avgjørelser i PVN-2005-12 og PVN-2005-13. Samtidig vil vi bemerke at Artikkel 29-gruppen i sin uttalelse nr. 4/2007 synes å legge til grunn at kjernen av identifiserbarhetskriteriet er å kunne skille enkeltpersoner fra andre i den aktuelle gruppe. Dette innebærer for det første at hva som skal til for å identifisere vil avhenge av konteksten, dvs. hvor stor den relevante gruppen av personer er. For det andre åpner Artikkel 29-gruppen for at det at en person er identifiserbar ikke nødvendigvis innebærer at man kan skaffe seg kjennskap til en persons alminnelig kjente navn.

Direktoratet ønsker å påpeke at Artikkel 29-gruppen i sin uttalelse tar til orde for et vidt personopplysningsbegrep og dermed et bredt virkeområde for lovens bestemmelser, men samtidig en fleksibel regelanvendelse i forhold til personvernrisikoen som behandlingen innebærer. Som Artikkel 29-gruppen og departementet er inne på vil behandling av pseudonymiserte opplysninger i mange tilfeller representere en mindre personvernrisiko som kan legitimere mindre streng anvendelse av reglene. Direktoratet deler oppfatningen om at det i enkelte tilfeller kan være mulig å finne frem til alternative behandlingsformer som innebærer en mindre personvernrisiko. Muligheten som ligger i å åpne for lempligere regler ved redusert personvernrisiko kan muligens gi den behandlingsansvarlige incentiver til å legge til rette for behandlingsformer som kan bidra til å fremme personvernet. Før den behandlingsansvarlige vurderer å pseudonymisere i utgangspunktet identifiserbare opplysninger, slik departementet nevner eksempel på, bør den behandlingsansvarlige vurdere om det i det hele tatt er behov for å samle inn og å behandle personidentifiserbare opplysninger for å oppnå formålet med behandlingen. Vi viser for øvrig til NOU 2009: 1 kap 10 og 16 hvor Personvernkommisjonen påpeker at arbeidet med pseudonyme helseregistre verken er forstått eller tilfredsstillende fulgt opp, og utredningen om personvernøkende teknologi og identitetsforvaltning som følger som vedlegg 4 til kommisjonens rapport.

Når det gjelder vurdering av hvilke opplysninger som skal anses som sensitive, er vår oppfatning at det utover de klare tilfeller hvor den opplistede opplysningstypen behandles må gjøres en konkret sensitivitetsvurdering av om opplysningene sier noe om de opplistede forhold. Departementets forslag "informasjon som sier noe om" gir anvisning på en slik sensitivitetsvurdering. Det er imidlertid grunn til å påpeke at det vil være behov for veiledning i forhold til hvor klart og direkte opplysningene må si noe om de opplistede forhold. Dette gjelder særlig hvor opplysninger sett i sammenheng med andre opplysninger eller i forhold til den aktuelle kontekst vil kunne gi utenforstående, dvs. personer utenfor den behandlingsansvarlige og den registrerte, forutsetninger for å trekke slutninger om forhold som er definert som sensitive. Vi viser her til den prinsipielle diskusjon vedrørende hvilke opplysninger som skal betegnes som "helseopplysninger" i forhold til registrering av betalingstransaksjoner i forarbeidene til lov 28. mai 2004 nr. 29 om valutaregister. Se Ot.prp. nr. 35 (2003-2004) punkt 6.4.3 (Datatilsynets høringssvar) og punkt 6.4.4. (Departementets vurderinger).

1.2 Begrepet "behandling av personopplysninger"

Skattedirektoratet mener det ikke er grunn til å endre definisjonen av "behandling av personopplysninger". Slik vi ser det er det i praksis sjelden tvil om håndtering av personopplysninger skal anses som behandling i lovens forstand og dermed faller inn under

lovens virkeområde. Hva som utgjør én behandling kommer imidlertid på spissen i forhold til reglene om behandlingsansvar siden enhver behandling forutsetter (minst) en behandlingsansvarlig. I tillegg er avgrensningen av ulike behandlinger sentralt i forhold til melde- og konsesjonsplikt, behandlingsgrunnlag, grunnkrav, samt gjennomføring av disse i internkontroll. Vår erfaring er at formålet med behandlingen er det viktigste vurderingsmomentet for å vurdere hvilke enkeltoperasjoner som samlet sett utgjør én behandling i forhold til disse reglene.

1.3 Begrepet "personregister"

Skattedirektoratet støtter departementets forslag til definisjon av personregister.

1.4 Begrepet "behandlingsansvarlig"

Skattedirektoratet deler oppfatningen om at definisjonen av behandlingsansvarlig har et uklart meningsinnhold og at begrepet er vanskelig å anvende i praksis.

Et av de grunnleggende problemene med begrepet behandlingsansvarlig er at det benyttes både om den behandlingsansvarlige virksomheten *som sådan*, om den eller de som *representerer* virksomheten og av og til om *interne roller* i den behandlingsansvarlige virksomhet med særlige oppgaver for å sørge for etterlevelse av lovens forpliktelser. Viktigheten av å sondre mellom den behandlingsansvarlige virksomhet, hvem som skal representere virksomheten og interne roller aktualiseres etter vår oppfatning blant annet av de sanksjoner som kan gjøres gjeldende for overtredelse av lovens bestemmelser. Vi viser her til våre kommentarer i punkt 10.7 om straffebestemmelsen i § 48.

Etter vår oppfatning vil det være klargjørende om begrepet behandlingsansvarlig forbeholdes virksomheten som sådan.

I spørsmålet om hvem som skal representere den behandlingsansvarlige utad, evt. hvem som skal være kontaktperson i den behandlingsansvarlige virksomhet, bør man etter vår oppfatning være bevisst på om det er ønskelig å sondre mellom korrespondanse med Datatilsynet/Personvernnemnda og politi/påtalemyndigheter på den ene siden og de registrerte på den annen. Vi viser her til våre kommentarer i punkt 10.7 hvor det kommer frem at rollen som "daglig ansvarlig" i dag kun nevnes i bestemmelsene om meldeplikt (§ 32 første ledd c)) og innsynsrett (§ 18), mens rollen ikke er nevnt i lovens informasjonspliktregler (§§ 19 og 20).

I tilfeller hvor lovgiver vedtar lover som forutsetter registre mener vi det kan være hensiktsmessig at lovgiver også tar stilling til hvem som er behandlingsansvarlig. Et eksempel på dette har en i valutaregisterloven hvor Toll- og avgiftsdirektoratet er oppgitt som behandlingsansvarlig for registeret. Vi vil imidlertid understreke at slike bestemmelser ikke gir noen uttømmende regulering av spørsmålet om behandlingsansvar, siden eksterne aktører som mottar opplysninger vil bli behandlingsansvarlig (evt. databehandler) ved mottak av opplysninger fra registreret.

Ved samarbeid mellom flere foretak/offentlige etater om behandling av personopplysninger vil det behov for å klarlagt hvem som er behandlingsansvarlig. Et viktig spørsmål er da om disse skal anses som selvstendige behandlingsansvarlige, eller om det foreligger såkalt delt behandlingsansvar for hele eller deler av behandlingen. Skattedirektoratet mener det i mange tilfeller med nært samarbeid mellom virksomheter vil være behov for å klargjøre ansvarsforholdene, og at det etter omstendighetene vil kunne være behov for å formalisere partenes ansvar og oppgaver i en avtale. Vi er imidlertid usikre på om det er hensiktsmessig å innføre et *krav* om skriftlig avtale ved delt behandlingsansvar, jf radikalt forslag § 7 fjerde ledd. Bakgrunnen for dette er at det vil kunne være vanskelig å avgjøre om det foreligger delt behandlingsansvar for de involverte behandlinger, og i enkelte tilfeller vil aktørene antakeligvis også ha et visst slingringsmonn i forhold til hvordan de definerer sine roller. Det vil derfor etter vår oppfatning være stor usikkerhet knyttet til hvilke typer av samarbeid og behandlinger som krever avtale.

Etter vår oppfatning er det også grunn til å diskutere forslagets formulering, da den kan gi uttrykk for at de samarbeidende parter kan "dele" ansvaret for behandlingen seg i mellom. Slik vi ser det er det mer treffende å omtale det slik at det er flere behandlingsansvarlige som sammen bestemmer formål og hjelpemidler for den aktuelle behandling. I utgangspunktet vil alle behandlingsansvarlige ha en selvstendig plikt til å etterleve lovens bestemmelser, men det nære samarbeidet tilsier at oppgavene med etterlevelse må koordineres mellom partene. Koordineringen må blant annet omfatte forholdet til databehandlere og databehandleravtaler, melde/konsesjonsplikt og informasjonsplikten.

Skattedirektoratet har vanskelig for å forstå meningsinnholdet og rekkevidden av radikalt forslag § 7 tredje ledd om muligheten for å delegere utøvelsen av behandlingsansvaret. Tilsvarende gjelder forslaget om å innta formuleringen "i siste instans" i § 7 første ledd.

Når det gjelder radikalt forslag § 7a er vi skeptiske til å ta inn i loven ytterligere interne roller i den behandlingsansvarlige virksomhet. Vi viser her til våre kommentarer i punkt 10.7 om at rollen "daglig ansvarlig" har et uklart mandat og at rollen ikke er blitt viet oppmerksomhet i Datatilsynets praksis. Innføringen av nye interne roller må også sees i sammenheng med rollen "daglig leder" i personopplysningsforskriften § 2-3 som også synes å ha en noe uklar status.

2 Personopplysningslovens saklige virkeområde (§ 3)

2.1 Personopplysningsloven § 3 første ledd bokstav a

Skattedirektoratet støtter departementets forslag om ta inn formuleringen om at personopplysningsloven gjelder for behandling som "helt eller delvis" skjer automatisert med elektroniske hjelpemidler.

2.2 Personopplysningsloven § 3 annet ledd

Skattedirektoratet støtter departementets forslag til ordlyd. Etter vår oppfatning vil det imidlertid også være hensiktsmessig å ha med "familiemessige" aktiviteter som

eksemplifisering på hva som anses som privat og som gjelder en konkret og begrenset krets av personer.

Etter direktoratets oppfatning er det viktig med en presisering av hvordan § 3 annet ledd skal forstås og anvendes i forhold til tilgjengeliggjøring av personopplysninger på Internett.

3 Ytringsfrihet og personvern (§ 7)

Ingen merknader.

4 Krav til rettslig grunnlag for behandling av personopplysninger (§§ 8-11)

Etter Skattedirektoratets oppfatning er det ønskelig at behandling av personopplysninger så vidt mulig hjemles i enten lov eller samtykke fremfor de mer skjønnsmessige nødvendighetsgrunnene. Når det gjelder diskusjonen om samtykke skal anses som "hovedregelen" vil vi bemerke at kravet til frivillighet i Personvernnemndas praksis er blitt tolket strengt, noe som f. eks. på arbeidslivsområdet innebærer et stort innhugg i anledningen til å benytte samtykke som behandlingsgrunnlag. Se nærmere Peter Blume "Vurdering af personvernnemndas praksis 2001–2008", Complex 3/09, s. 13 og 14.

Skattedirektoratet støtter departementets forslag i punkt 4.3.6 om å flytte grunnkravene i dagens § 11 før vilkårene for behandling i §§ 8 og 9. Etter vår oppfatning er "grunnkravene" blitt et innarbeidet begrep om bestemmelsene i § 11 som i hovedsak omfatter behandlingsgrunnlag, formålsbestemthetsprinsippet og datakvalitet. Vi mener derfor det er grunn til å holde fast ved denne betegnelsen og *ikke* utvide grunnkravene til også å omfatte informasjonssikkerhet, internkontroll og databehandlerens rådighet slik utrederne forslår i det radikale forslaget kapittel II.

Når det gjelder forslaget til ny § 8a c) (radikalt forslag) – "opplysninger som de registrerte personer selv frivillig har gjort alminnelig kjent" – er vi oppmerksomme på at dette er en videreføring av § 9 d). Vi vil likevel bemerke at dette behandlingsgrunnlaget i lys av Internett og tjenester for søk og deling av informasjon kan legitimere meget vidtrekkende behandling som går ut over det den registrerte ønsket ved sin offentliggjøring.

Angående lovens formålsbestemthetsprinsipp mener vi det vil være klargjørende om kravet til angivelse av formål knyttes mer uttrykkelig til *innsamlingen* av opplysningene. Dette vil bringe personopplysningslovens ordlyd tettere opp mot personverndirektivets ordlyd og system, jf personverndirektivet artikkel 6 første ledd b) om at personopplysninger skal "*innsamles* til bestemte, uttrykkelig angitte formål samt at senere behandling ikke skal være uforenlig med disse formålene" (vår utheving).

5 Overføring av personopplysninger til utlandet (§§ 29-30)

Skattedirektoratet støtter forslaget om å presisere at den registrerte forut for avgivelsen av samtykket er gjort oppmerksom på den særlige risiko som overføringen kan innebære (§ 30 første ledd a)). Etter vår vurdering er det ellers naturlig å se hen til den informasjon som den behandlingsansvarlige uoppfordret plikter å oppgi ved innsamling av opplysninger fra den

registrerte og fra andre, jf pol §§ 18 og 19. Dette innebærer at det som et minimum må oppgis hvem som er behandlingsansvarlig og formålet med behandlingen.

Direktoratet gir også tilslutning til departementets forslag om å innta en bestemmelse i personopplysningsforskriften som slår fast at publisering av opplysninger på en hjemmeside som hovedregel ikke skal anses som en overføring til utlandet.

6 Melde- og konsesjonsplikten (§§ 31-35)

Skattedirektoratet er usikker på rekkevidden av radikalt forslag til § 31 andre ledd om at varsel om at melding er sendt skal gis til berørte personer, eller – i tilfeller det et stort eller ubestemt antall person er berørt – til relevante interesseorganisasjoner/allmenheten. Etter Direktoratets oppfatning reiser bestemmelsen uavklarte spørsmål om hvordan varselet skal gis, og vi mener en slik varslingsplikt kan bli tilnærmet umulig å overholde i praksis. Skattedirektoratet vil derfor sterkt fraråde forslaget.

Skattedirektoratet støtter radikalt forslag til ny § 31a som presiserer i hvilke tilfeller det er plikt til å sende fornyet melding.

Direktoratet støtter radikalt forslag til ny § 32 om at den behandlingsansvarlige i meldingen skal bekrefte at det foreligger dokumentasjon vedrørerende informasjonssikkerhet (§ 13) og internkontroll (§ 14).

Det gis støtte til radikalt forslag til ny § 33 om Datatilsynets rett til å kreve konsesjonsbehandling.

Radikalt forslag til ny § 33a om registrertes rett til å kreve konsesjonsbehandling fremstår som nærmest umulig å realisere i forhold til en massebehandlingsetat som skatteetaten.

Direktoratet mener det er hensiktsmessig, slik radikalt forslag § 33b legger opp til, at det i personopplysningsforskriften angis hvilke behandlinger som skal være konsesjonspliktig. Vi deler oppfatningen om at enkelte av opplysningskategoriene som er definert som sensitive, f. eks. fagforeningstilknytning, ikke nødvendigvis er av en slik art at de i alle tilfeller bør være underlagt konsesjonsbehandling.

Direktoratet oppfatter radikalt forslag § 33c grunnleggende sett som en videreføring av dagens § 33 fjerde ledd om unntak fra konsesjonsplikt når behandlingen har hjemmel i lov. Vi mener det er viktig å holde fast ved utgangspunktet i dagens § 33 fjerde ledd om at offentlige organers behandling av personopplysninger er unntatt konsesjonsplikt når behandlingen er hjemlet i egen lov.

I følge radikalt forslag § 33c andre punktum vil behandlinger som er "utvetydig forutsatt" i lov eller forskrift også være unntatt konsesjonsplikt. Dagens regel i pol § 33 fjerde ledd synes å stille noe strengere krav til uttrykkelighet for at behandlingen skal være unntatt konsesjonsplikt, noe som blant annet fremgår av Justisdepartementets uttalelser i Ot.prp. nr. 92 (1998-1999) s. 129:

> "For at et personregister skal være fritatt for konsesjon i medhold av denne bestemmelsen kreves det at det *eksplisitt* fremgår av loven at det skal eller kan føres et register. Det er ikke tilstrekkelig at en særlov hjemler en aktivitet som gjør opprettelse av et personregister nødvendig. Selv om et register er fritatt fra konsesjonsplikt i medhold av bestemmelsen her, vil personopplysningsloven supplere den aktuelle særloven hvis ikke noe annet uttrykkelig fremgår av denne, jf. § 5 i lovforslaget." (vår utheving).

Etter vår oppfatning er det usikkert om man med den foreslåtte formuleringen "utvetydig forutsatt" ønsker å senke kravet til uttrykkelighet. Vi ønsker i alle tilfelle en nærmere presisering av hvor klart lovgivningen må forutsette behandlingen for at regelen om unntak fra konsesjonsplikt kommer til anvendelse.

Slik vi ser det er det også ønskelig at lovgiver ser nærmere på sammenhengen mellom lov og forskrift som *hjemmelsgrunnlag* for behandling (dagens §§ 8 og 9), og som *vilkår* for at et unntak fra konsesjonsplikt skal komme til anvendelse (dagens § 33). Dersom det stilles større krav til uttrykkelighet i sistnevnte tilfelle (vilkår), enn i førstnevnte (hjemmelsgrunnlag), kan dette skape inntrykk av at konsesjon fra Datatilsynet kan reparere et haltende hjemmelsgrunnlag. Den rådende oppfatning, noe dagens utforming av konsesjonsskjemaet også bekrefter, er vel at den behandlingsansvarlige uavhengig av konsesjon må oppfylle alle grunnkravene til behandling av personopplysninger, herunder krav til behandlingsgrunnlag.

Dersom det er meningen at det stilles strengere krav til lov- eller forskriftshjemmel i reglene om unntak fra konsesjonsplikt (dagens § 33), enn reglene om behandlingsgrunnlag (dagens §§ 8 og 9), bør dette etter vår oppfatning presiseres. Problemstillingen kommer særlig på spissen der den behandlingsansvarlige har klar hjemmel i lov for sin egen behandling, men hvor eventuell utlevering til andre behandlingsansvarlige reiser spørsmål om loven også hjemler den aktuelle utlevering, og om mottaker har tilstrekkelig klar hjemmel for sin innsamling. I slike tilfeller er det for det første utfordrende å vurdere utleverende og behandlingsansvarliges respektive lovhjemler opp mot lovens krav til hjemmelsgrunnlag/vilkår for unntak fra konsesjonsplikt. Hvis man kommer til at kravet til uttrykkelighet ikke er oppfylt, oppstår dessuten spørsmålet om både den som utleverer og den som mottar opplysningene må ha konsesjon fordi en av partenes hjemmelsgrunnlag ikke oppfyller kravet til uttrykkelighet.

Skattedirektoratet har ikke erfart noen praktiske problemer med dagens meldesystem, men er generelt positiv til tiltak som kan effektivisere meldepliktsordningen, jf departementets merknader i punkt 6.3.2.

7 Fjernsynsovervåkning (§§ 36-41)

Ingen merknader.

8 Mindreåriges personvern

Ingen merknader.

9 Personvernombud

Ingen merknader.

10 Andre problemstillinger

10.1 Personopplysningsloven og særlovgivningen

Skattedirektoratet ser at det kan være hensiktsmessig å minne om at lov- og forskriftsbestemt taushetsplikt legger begrensninger på adgangen til å utlevere personopplysninger. Vi er imidlertid usikre på om det er heldig å plassere en slik bestemmelse i umiddelbar tilknytning til "grunnkrav til behandling av personopplysninger"/"rettslig grunnlag" slik det er gjort i radikalt forslag til ny § 8.

10.2 Personopplysningslovens struktur

Skattedirektoratet støtter utredernes forslag om å presisere i § 11 første ledd bokstav c) at både *lovhjemmel* og *samtykke* kan hjemle behandling til formål som er uforenlig med det som ble angitt ved innsamling av opplysningene. Etter vår oppfatning er dette en presisering av gjeldende rett, jf Ot.prp. nr. 92 (1998-99) s. 113.

Personopplysningsloven § 11 første ledd c) bør etter vår oppfatning formuleres slik at det kommer klart frem at uforenlighetsvurderingen må gjøres opp mot formålet angitt ved *innsamlingen* av opplysningene. Bokstav c) må sees i sammenheng med bokstav b) om at personopplysninger bare skal "nyttes til uttrykkelig angitte formål som er saklig begrunnet i den behandlingsansvarliges virksomhet". Også bokstav b) bør presisere at formålet skal angis ved innsamling, jf tilsvarende bestemmelse i personverndirektivet artikkel 6 (1) b) om at personopplysninger "skal *innsamles* til bestemte, uttrykkelig angitte og berettigede formål samt at senere behandling ikke skal være uforenlig med disse formålene" (vår utheving).

Skattedirektoratet mener det videre er grunn til å vurdere å flytte lovens informasjonspliktbestemmelser (§§ 19 og 20) foran reglene om innsyn (§ 18). Dette vil bringe loven i tråd med personverndirektivets systematikk. Vi mener også det vil bli bedre sammenheng i regelverket å *først* nevne den behandlingsansvarliges plikt til uoppfordet å gi informasjon ved innsamling av opplysninger, for *deretter* nevne den registrertes rett til innsyn i opplysningene. Behovet for å be om innsyn vil dessuten kunne begrenses dersom den behandlingsansvarlige klarer å realisere informasjonspliktreglene på en måte som gjør den registrerte oppmerksom på de sentrale sider ved behandlingen.

Etter vår oppfatning kan det også være grunn til å se nærmere på hvilken informasjon som skal formidles etter §§ 19 og 20, særlig ved oppfyllelse av informasjonsplikten ved Internettbaserte tjenester. Vi viser her til at Europakommisjonen i sin rapport "First report on the implementation of the Data Protection Directive" (2003) påviste flere uoverensstemmelser i den nasjonale gjennomføringen av direktivets artikkel 10 og 11. Kommisjonen fremhever det som særlig uheldig at enkelte nasjonale implementasjoner krever at all informasjon nevnt i bestemmelsene skal gis i alle tilfeller. Det påpekes at direktivet skiller mellom *grunnleggende* informasjon som skal gis i alle tilfeller (behandlingsansvarlig og formål), og *ytterligere* informasjon som skal gis når det i det

konkrete tilfellet er nødvendig for å gjøre behandlingen transparent for den enkelte. Etter kommisjonens oppfatning vil regler som påbyr å oppgi alle opplysningstypene kreve store ressurser uten å fremme de registrertes personvern. Kommisjonens uttalelser er senere fulgt opp av Art 29-gruppen i "Opinion on More Harmonised Information Provisions" (2004). Skattedirektoratet mener formålet med informasjonspliktreglene bedre vil kunne realiseres ved å endre personopplysningsloven i tråd med kommisjonens og Art 29-gruppens uttalelser.

10.3 Forholdet mellom personopplysningsloven og personopplysningsforskriften

Skattedirektoratet viser her til enkeltkommentarer om forholdet mellom loven og forskriften i enkelte av de andre punktene.

10.4 Informasjonssikkerhet og internkontroll

Skattedirektoratet mener det ikke er hensiktsmessig å ta inn "kvalitet" som element i informasjonssikkerheten. Datakvalitet, som i følge formålsbestemmelsen er et av de grunnleggende personvernhensyn loven skal fremme, er etter vår oppfatning tilstrekkelig ivaretatt i §§ 11 b) til e), 27 og 28. Disse bestemmelsene må etter vår oppfatning også hensyntas i informasjonssikkerhetsarbeidet. Et viktig aspekt ved datakvalitet er dessuten allerede omfattet av § 13 og kravet om tilfredstillende informasjonssikkerhet med hensyn til "integritet". I personopplysningsforskriften § 2-13 er sikring av integritet angitt som et krav om tiltak mot uautoriset endring av personopplysninger.

Direktoratet støtter departementets forslag om å konkretisere og utdype kravene til internkontroll i § 14. Etter vår oppfatning bør en konkretisering og utdyping av reglene om internkontroll ta sikte på å angi hovedelementene i internkontroll. Sælig bør oppmerksomheten rettes mot hvor omfattende internkontroll skal være med tydelige krav til hva som skal dokumenteres. Dagens regler oppfattes som vanskelig å gjennomføre i praksis, samtidig som dokumentasjon knyttet til internkontroll er svært viktig for Datatilsynets kontrollvirksomhet. Etter vår oppfatning vil departementets forslag til konkretisering av "systematiske tiltak" til styrende, gjennomførende og kontrollerende del bidra til å bringe § 14 nærmere Datatilsynets praksis knyttet til Internkontroll. Vi viser her til Datatilsynets veiledning "Internkontroll og informasjonssikkerhet", Veileder 07/01, Publisert 15.02.2007, http://www.datatilsynet.no/upload/Dokumenter/internkontrollfiler/ik-veileder.pdf.

Vi vil for øvrig påpeke behovet for å klargjøre sammenhengen mellom lovens og forskriftens regler om *informasjonssikkerhet* (pol § 13/pof kap 2) og *internkontroll* (pol § 14/pof kap 3). Slik vi opplever det er det enkelte uuttalte sammenhenger mellom disse reglene, noe som vanskeliggjør gjennomføringen og som i enkelte tilfeller fører til direkte misforståelser. Etter vår oppfatning skyldes dette særlig en uheldig rekkefølge og balanse mellom reglene. Reglene om internkontroll innebærer planlagte og systematiske tiltak som er nødvendige for å oppfylle *alle* kravene i eller i medhold av loven. Informasjonsikkerhet er bare en liten delmengde av lovens og forskriftens krav. Rekkefølgen på bestemmelsene og det faktum at etterlevelse av krav til informasjonssikkerhet etter § 13 forutsetter en internkontrollmetodikk, bidrar til å tilsløre sammenhengen mellom internkontroll og informasjonssikkerhet. Når forskriftens kapittel 2 om informasjonssikerhet er såpass detaljert med hensyn til systematikk skapes etter vår oppfatning et intrykk av at mye av

internkontrollarbeidet er unnagjort bare man etterlever reglene om informasjonssikkerhet. Kapittel 3 om internkontroll inneholder til sammenlikning lite veiledning om den metodikk som må til for å få på plass en helhetlig internkontroll som også omfatter informasjonsikkerhet.

10.5 Databehandlerens rådighet over personopplysninger

Skattedirektoratet mener dagens regulering i § 15 ikke byr på særlig tvil om i hvilke tilfeller det skal foreligge avtale mellom den behandlingsansvarlige og databehandleren. Etter vår erfaring skyldes eventuell tvil om det skal foreligge en databehandleravtale primært usikkerhet knyttet til om en aktør skal anses som selvstendig behandlingsansvarlig eller databehandler, jf om begrepet "behandlingsansvarlig" i punkt 1.4 i høringen.

Det er den behandlingsansvarlige som må oppfylle lovens grunnkrav og ha behandlingsgrunnlag for behandlingen, mens databehandlerens rådighet og rettslige grunnlag for å behandle personopplysningene følger av avtalen med den behandlingsansvarlige. Den behandlingsansvarlige har en viss handlefrihet med hensyn til valg av databehandler, men personverndirektivet artikkel 17 nr. 2 krever at nasjonal lovgivning stiller krav til at den behandlingsansvarlige bare kan *velge* en databehandler som kan sørge for tilstrekkelig informasjonssikkerhet, og den behandlingsansvarlige skal pålegges en plikt til å *påse* at dette overholdes.

Når det gjelder krav til innholdet i databehandleravtaler, er det grunn til å påpeke at personverndirektivet art 17 nr. 3 forutsetter at det i en kontrakt ("eller et annet juridisk bindende dokument mellom databehandleren og den behandlingsansvarlige") særlig skal være fastsatt "at databehandleren bare skal handle utelukkende etter *instruks* fra den behandlingsansvarlige", og at databehandleren har et selvstendig ansvar for informasjonssikkerhet. Selv om begrepsbruken er forskjellig er det grunn til å anta at pol § 15 første ledd om at databehandleren ikke kan behandle personopplysninger på annen måte enn det som er skriftlig avtalt tilfredstiller direktivets krav til at den behandlingsansvarlige utelukkende skal handle etter den behandlingsansvarliges instrukser. Direktivets krav om at databehandleren har et selvstendig ansvar for informasjonssikkerhet følger uttrykkelig av pol § 15 andre ledd.

Skattedirektoratet mener det kan være hensiktsmessig at § 15 gir noe mer veiledning i hva en databehandleravtaler etter omstendighetene bør inneholde. Vi vil i denne sammenheng understreke at behovet for detaljgrad og nærmere innhold vil variere sterkt avhengig av område, opplysningenes art og omfang, samt partenes kompetanse og forutsetninger. Selv om pol § 15 første ledd slår fast at databehandleren ikke skal behandle personopplysninger "på annen måte" enn det som er skriftlig avtalt med den behandlingsansvarlige, kan dette etter vår oppfatning ikke bety at avtalen nødvendigvis må foreskrive hver enkelt behandling i detalj. Datatilsynets årsmelding 2008 s. 23 går etter vår oppfatning langt i å kreve detaljregulering: "Avtalen må (...) inneholde et minimum av bestemmelser som ivaretar de registrertes rettigheter etter personopplysningsloven. All bruk av personopplysninger mellom start- og sluttidspunkt må reguleres av avtalen." Kravene til detaljregulering er tilsynelatende dempet noe i Datatilsynets veiledning "Databehandleravtaler" Veileder

26.05.2009, hvor det fremheves at det klart skal fremgå hva som er formålet med behandlingen og hva databehandler skal gjøre med opplysninger. Etter vår oppfatning kan det være hensiktsmessig at § 15 oppstiller krav om at avtalen skal angi et uttrykkelig formål for databehandlerens behandling. Formålet vil da være retningsgivende for å vurdere databehandlerens rådighet over opplysningene. Dette vil for øvrig være i tråd med Skaugeutvalgets forslag, jf NOU 1997: 19, forslag til § 13 på s. 143, om at databehandleren ikke skal anvende opplysningene til "*andre formål* enn det oppdraget gjelder" (vår utheving).

Også i forhold til informasjonssikkerhet kan det etter vår oppfatning være grunn til å presisere nærmere hva avtalen skal omfatte. Datatilsynet går i sin veiledning langt i oppstille detaljerte krav til avtalen på dette punktet, jf Datatilsynet "Databehandleravtaler" Veileder 26.05.2009, punkt 5 på s. 9. Slik vi ser det bør reglene ta hensyn til at databehandleren i mange tilfeller er den profesjonelle part som er valgt nettopp på bakgrunn av sin ekspertise på den aktuelle behandling. I mange tilfeller vil det da bli illusorisk å forvente at den behandlingsansvarlige skal ha kompetanse og forutsetninger for å detaljere kravene til informasjonssikkerhet. Databehandlerens selvstendige ansvar for informasjonssikkerhet innebærer etter vår oppfatning at databehandleren da må foreta en selvstendig vurdering av hva som er tilfredsstillende informasjonssikkerhet i forhold til behandlingen som skjer på vegne av den behandlingsansvarlige. For at den behandlingsansvarlige skal kunne følge opp og påse at databehandleren har tilfredstillende informasjonssikkerhet kan det være hensiktsmessig at avtalen pålegger databehandleren på forespørsel å utlevere dokumentasjon av sikkerhetstiltakene til den behandlingsansvarlige.

Av § 15 første ledd andre punktum følger det at opplysninger som nevnt i første ledd "kan heller ikke uten slik slik avtale overlates til noen andre for lagring eller bearbeidelse". Skattedirektoratet mener det kan være grunn til å vurdere om loven bør gi nærmere anvisning på hvilke krav som kreves for at databehandleren skal kunne benytte underleverandører. I Datatilsynets veiledning om databehandleravtaler punkt 3 er det lagt til grunn at databehandleren bare kan gjøre bruk av underleverandører i den grad dette klart fremgår av avtalen mellom databehandleren som ønsker å sette bort deler av oppdraget og den behandlingsansvarlige. Direktoratet mener det kan være grunn til å presisere denne forutsetningen for databehandlerens utsetting av oppdraget i lovteksten.

Etter skattedirektoratets oppfatning kan det videre være grunn til å se nærmere på sammenhengen i regelverket når det gjelder aktører som tilsynelatende verken er behandlingsansvarlige eller databehandlere – i loven og forskriften ofte omtalt som "andre". Bestemmelser som nevner slike "andre" er pol § 13 tredje ledd, § 15 første ledd andre punktum samt personopplysningsforskriften §§ 2-5 andre ledd og 2-15 ("kommunikasjonspartner og leverandører"). Vi gjør her oppmerksom på at personverndirektivet tilsynelatende gjør et klart skille mellom aktører som enten er behandlingsansvarlige eller databehandlere på den ene siden og såkalte tredjemenn på den annen, jf definisjonen av tredjemann i artikkel 2 f):

> ""tredjemann": enhver annen fysisk eller juridisk person, offentlig myndighet, byrå eller ethvert annet organ enn den registrerte, den behandlingsansvarlige, databehandleren og

> de personer som under den behandlingsansvarliges eller databehandlerens direkte myndighet har fullmakt til å behandle opplysningene."

Sett i lys av direktivets definisjon av tredjemann mener vi det er grunn til å sette spørsmålstegn ved om det er behov i personopplysningsloven for å operere med betegnelsen "andre" om aktører som verken er behandlingsansvarlige eller databehandlere, men som likevel tilsynelatende skal være underlagt reglene som gjelder for databehandlere.

Etter direktoratets oppfatning bør personopplysningsforskriften § 2-15 fjerde ledd andre punktum om at ansvars- og myndighetsforhold overfor kommunikasjonspartnere og leverandører skal beskrives "i særskilt avtale" sees i sammenheng med kravet til databehandleravtale etter § 15.

10.6 Automatiserte avgjørelser – personopplysningsloven § 22

Skattedirektoratet støtter forslaget om å innta en regel i § 22 om at den registrerte kan kreve overprøvning av fullt ut automatiserte avgjørelser.

10.7 Straffebestemmelsen i personopplysningsloven § 48

Skattedirektoratet støtter departementets forslag om å erstatte formuleringen "den behandlingsansvarlige" i pol § 48 tredje ledd med "vedkommende". Som departementet påpeker er hovedpliktsubjektet etter loven den behandlingsansvarlige. Enkelte bestemmelser, f. eks. § 13 om informasjonssikkerhet, retter seg dog også mot databehandleren. Bestemmelsen om informasjonssikkerhet i § 13 må naturligvis sees i sammenheng med de svært detaljerte reglene i forskriften kapittel 2 som også er straffesanksjonert, jf forskriften § 10-3.

Direktoratet deler departementets oppfatning om at personopplysningsloven § 48 ikke åpner for noen "delegering" eller "fordeling" av straffeansvar. Personopplysningslovens regler om innsyn (§ 18) og meldingsplikt (§ 32 c)) stiller krav til at den behandlingsansvarlige angir hvem som er "daglig ansvarlig" for å oppfylle den behandlingsansvarliges plikter. Informasjonspliktreglene oppstiller ikke noe slikt krav, og lovens øvrige regler gir heller ikke veiledning i rollens oppgaver og eventuelle straffeansvar. Av forarbeidene fremkommer det at hensikten var å knytte *gjennomføringen* av den behandlingsansvarliges plikter til en stilling (eller fysisk person) i virksomheten, mens det *formelle ansvaret* påhviler virksomhetens ledelse, jf Ot.prp. nr 92 (1998-99) s. 102 og NOU 1997: 19 s. 132.

Ot.prp. nr 92 (1998-99) s. 102:

> "Der den behandlingsansvarlige er en juridisk person, vil den juridiske personen representert ved dens ledelse være behandlingsansvarlig. Ledelsen må sørge for at loven etterleves, og som ledd i dette foreta en intern arbeidsfordeling slik at det er klart hvilken stilling det ligger til å sørge for at loven etterleves i praksis, jf § 18 første ledd bokstav b i lovforslaget. Funksjonen bør knyttes til en lederstilling slik at stillingsinnehaveren har reell daglig innflytelse på behandlingen som foretas"

NOU 1997: 19 s. 132:

> "Det formelle ansvaret for at pliktene som den behandlingsansvarlige pålegges oppfylles ligger hos ledelsen i den aktuelle virksomheten. Virksomheten skal imidlertid knytte gjennomføringen av pliktene som den behandlingsansvarlige pålegges til en stilling eller en fysisk person i virksomheten, jf forutsetningsvis lovforslaget § 16 nr 2. Funksjonen bør være knyttet til en bestemt stilling innen virksomheten slik at ansvarsforholdet er klart selv om enkeltpersoner i virksomheten skifter jobb, slutter etc. Funksjonen bør legges til en lederstilling knyttet til behandlingen av personopplysninger slik at stillingsinnehaveren har reell daglig innflytelse på de behandlingene som foretas (f eks daglig leder, eventuelt daglig leder i administrasjonsavdelingen)."

I praksis kan det synes som om rollen "daglig ansvarlig" ikke er blitt viet særlig oppmerksomhet. Det kan her nevnes at rollen ikke er nevnt i Datatilsynets veiledning om internkontroll og informasjonssikkerhet (jf henvisning i punkt 10.4) – en veiledning som vel nettopp tar sikte på å veilede virksomheter i å organisere arbeidet med å sikre gjennomføring av lovens forpliktelser.

Behovet for å klargjøre hvorvidt straffeansvaret kan gjøres gjeldende overfor interne roller kommer etter vår oppfatning også til syne i forhold til rollen "daglig leder" som etter personopplysningsforskriften § 2-3 har ansvaret for at bestemmelsene i forskriften kapittel 2 følges.

Skattedirektoratet ønsker for øvrig å gjøre oppmerksom på at pol § 46 andre ledd g) om vurderingsmomenter ved ileggelse av overtredelsesgebyr kan gi inntrykk av at *ansatte* hos den behandlingsansvarlige (eller databehandleren) kan bli ilagt straff etter § 48. I kommentarene til bestemmelsen, jf Ot.prp. nr. 71 (2007-2008) s. 12, uttales det:

> "Momentet i *bokstav g* – om andre reaksjoner som følge av overtredelsen blir ilagt overtrederen eller noen som har handlet på vegne av denne, blant annet om noen enkeltperson blir ilagt straff – kan få anvendelse blant annet når en ansatt hos den behandlingsansvarlige ilegges straff for den samme handlingen, eller når eieren selv, i et enkeltmannsforetak, ilegges en slik reaksjon" (vår understrekning).

Etter direktoratets oppfatning er det videre behov for en avklaring av forholdet mellom personlig straffeansvar og foretaksstraff etter § 48. Utrederne uttaler i forbindelse med straffebestemmelsen at det bør fremgå klart "at det her er tale om et personlig straffeansvar, og at virksomhetsstraff kan komme i tillegg til det personlige straffeansvaret". Det kunne være ønskelig med en nærmere avklaring av prioriteringen mellom ansvarene og om foretaksstraff er noe som er ment å komme "i tillegg til" det personlige straffeansvaret.

10.8 Elektroniske spor

Skattedirektoratet er enig i at det ikke er hensiktsmessig med egne bestemmelser om elektroniske spor.

10.9 Bruk av fødselsnummer, fingeravtrykk og annen biometri

Skattedirektoratet gir sin tilslutning til regulering av fødselsnummer og biometri i egne bestemmelser. Vi minner for øvrig om at Skaugeutvalgets forslag opprinnelig bare omfattet

fødselsnummer (se NOU 1997: 19, forslag til § 10 på s. 165), men at det i Ot.prp. nr. 92 (1998-99) s. 114 uten nærmere redegjørelse ble foreslått at bestemmelsen i tillegg til fødselsnummer også skulle omfatte "andre entydige identifikasjonsmidler".

Utredernes forslag til § 11 første ledd viderefører grunnvilkårene i dagens § 12 om at fødselsnummer bare kan brukes dersom det er "saklig behov for sikker identifisering og bruk av fødselsnummer er nødvendig for å oppnå slik identifisering". Begrepet "sikker identifisering" er av Personvernnemnda tolket til å omfatte både identifisering og autentisering i forbindelse med biometri, jf PVN-2006-10 og PVN-2006-11. Etter direktoratets oppfatning kan muligens "entydig identifisering" være et mer presist begrep som ikke gir så klare assosiasjoner til det å sannsynliggjøre riktigheten av en påstand om identitet (autentisering).

Skattedirektoratet mener forslaget til § 11 andre ledd om at bruk av fødselsnummer forutsetter en forutgående risikovurdering vil være vanskelig å gjennomføre i praksis. Etter vår oppfatning er det noe uklart hvilke risikoer som skal vurderes, og det er ingen nær sammenheng mellom risikovurderinger etter reglene for informasjonssikkerhet og de vurderinger hovedvilkårene for å benytte fødselsnummer legger opp til.

Forslaget til ny § 11 fjerde ledd om at fødselsnummer ikke skal benyttes for autentisering synes å være en presisering av gjeldende rett, jf NOU 1997: 19 s. 85, NOU 2001: 10 s. 53, juridisk teori (Schartum og Bygrave 2004 s. 170 og Johansen m.fl. Kommentarutgave 2001 s. 125) og Personvernnemndas praksis PVN-2002-7 og PVN-2003-6.

Slik forslaget er formulert gir det rom for tvil på to punkter. Er det meningen at fødselsnummer skal kunne benyttes til autentisering *sammen* med andre opplysninger? Hvis svaret er ja – hvilke tilleggsopplysninger kreves i såfall for at fødselsnummer skal ha en slik autentiseringseffekt. Hovedregelen om forbud mot bruk av fødselsnummer til autentisering vil etter direktoratets oppfatning undergraves av en unntaksbestemmelse som ikke gir klare holdepunkter for når slik bruk vil være tillatt.

Skattedirektoratet er klar over at fødselsnummer benyttes i enkelte innloggingsløsninger til Internett-tjenester. Etter vår oppfatning er det her viktig å skille mellom bruk av fødselsnummer som ren identifikator, og som autentiseringsmekanisme. Når fødselsnummer benyttes som *identifikator* ("brukernavn") har den som funksjon å "hente frem" brukerprofilen til den påberopte identiteten. Passordet (eller annen autentiseringsmekanisme som smartkort, pin-koder etc.) benyttes i slike tilfeller for å *autentisere* (underbygge/sannsynliggjøre) påstanden om at brukeren er den som er knyttet til den aktuelle identifikatoren.

Forslaget til ny § 49 tredje ledd om erstatning for skade som har oppstått ved uautorisert tilgang til fødselsnummer er etter vår oppfatning lite hensiktsmessig da det kan bidra til å underbygge den feilaktige oppfatningen om at fødselsnummeret kan benyttes til autentisering. Bestemmelsen trekker fokuset vekk fra det som egentlig er problemet, nemlig ulovlig *bruk* av fødselsnummeret.

Etter bestemmelsens ordlyd er det etter vår oppfatning uklart om det at fødselsnummer er kommet på "avveie" i seg selv skal anses som en erstatningsbetingende skade, eller om det er den etterfølgende og rettstridige bruk av fødselsnummer som må ha medført skade. Dersom det er den etterfølgende bruk som har medført skade vil dette i hovedsak skyldes at andre behandlingsansvarlige i strid med pol § 12 (ny § 11) har benyttet fødselsnummer til autentisering. Etter vår oppfatning vil det være urimelig å innføre et objektivt ansvar for skade som skyldes andre behandlingsansvarliges rettstridige bruk av fødselsnummeret. En slik regel vil dessuten by på vanskelige bevisspørsmål i forhold til å kunne knytte bestemte sikkerhetsbrister til senere "identitetsmisbruk".

Slik vi ser det er fødselsnummer og tilknyttede opplysninger allerede undergitt tilfredsstillende vern etter hovedreglen om informasjonssikkerhet etter pol § 13 og hovedregelen om erstatning etter pol § 49 (1). Skattedirektoratet fraråder derfor forslaget.

Med hilsen

Sven Rune Grem
direktør
Skattedirektoratet
Rettsavdelingen

Lars Nilsen

Kopi: Finansdepartementet