Direktoratet for forvaltning og IKT

Vår dato	Vår referanse
1.11.2009	2009/459
Deres dato	Deres referanse
3.7.2009	200904400 ES HAJ

Saksbehandler:
Jon Holden

Justisdepartementet
Postboks 8005 Dep
0030 Oslo

Høring – etterkontroll av personopplysningsloven

Vi viser til departementets høringsbrev av 3.7 om etterkontroll av personopplysningsloven.

Vårt høringssvar følger strukturen og nummereringen i departementets høringsnotat.

Direktoratet for forvaltning og ikt skal bidra til effektiv og brukerrettet e-forvaltning. Godt personvern, med klare regler for hvordan opplysningene skal behandles og god etterlevelse hos de behandlingsansvarlige, ser vi som forutsetninger for at e-forvaltningen skal lykkes. Klare og enkle regler vil være ressursbesparende. Difi har videre ansvar for koordinering og drift av felleskomponenter for e-forvaltningen, som Minside og MinID.

Vi har i vårt svar konsentrert oss om

- rettstekniske spørsmål, med sikte på at reglene skal være lettere å forstå,
- spørsmål som har betydning for e-forvaltning, herunder regulering av sikkerhet, fødselsnummer, nettpublisering og ansvarsspørsmål,

1.1 Begrepet personopplysninger

Kravet om identifikasjon

Departementet spør om begrepet "identifiserbar" bør tas inn i loven. Vi kan ikke se at begrepet i vesentlig grad gjør loven klarere, jf. at kravet i dag er at opplysninger "*kan* knyttes til en enkeltperson".

Derimot tror vi det med fordel kan presiseres hvor strengt identifikasjonskravet skal forstås. Avsnitt 26 i direktivets fortale kan danne utgangspunkt for en slik presisering, eksempelvis slik: "I vurderingen av om en enkeltperson kan identifiseres skal det tas hensyn til alle virkemidler som det med rimelighet kan tenkes at noen vil ta i bruk for å identifisere personen".

Artikkel 29-gruppens fyldige uttalelse 4/2007 om "begrepet personopplysninger" bør etter vårt skjønn kommenteres i forarbeidene, i alle fall dersom det legges opp til norske avvik fra den forståelse som gruppen legger opp til, jf. målet om rettsenhet på direktivets område.

Sensitive opplysninger

Utrederne foreslår i større grad å bruke uttrykket "opplysningstype" i bestemmelser om sensitive opplysninger., og viser til at man derved unngår at opplysningsverdiene blir avgjørende for vurderingen (eks. den ikke-sensitive opplysningstypen adresse inneholder den sensitive opplysningsverdien IIa fengsel).

Direktoratet for Forvaltning og IKT (Difi)
Postboks 8115 Dep, 0032 Oslo
Telefon: 22 45 10 00

Besøksadresse Oslo:
Sandakerveien 24C,
inngang D 9, 4. etasje
Telefaks Oslo: 22 45 10 01

Besøksadresse Leikanger:
Skrivarvegen 2
Telefaks Leikanger: 57 65 50 55

postmottak@difi.no
Org.nr.: NO 991 825 827
www.difi.no

Vi er i tvil om hensiktsmessigheten i forslaget. Personverndirektivet artikkel 8 setter vilkår for å kunne behandle opplysninger som *røper* ("revealing") sensitive forhold; eventuell forhåndsklassifiseringen av opplysningstypene er ikke avgjørende for vurderingen etter direktivet. Direktivets tilnærming fremstår som en løsning som bedre ivaretar den registrertes personvern – og som derved gir grunnlag for tillit til behandlingsregimet. Vi antar vurderingen bør ta utgangspunkt i hvorvidt sensitive forhold sannsynligvis vil kunne bli avslørt i den planlagte behandling (jf. dansk praksis slik det er redegjort for i notatet pkt 7.4.2.2)

1.2 – behandling av personopplysninger

Vi er enige med departementet i at begrepet behandling må avgjøres konkret.

Effektivitetshensyn kan tale for at operasjoner som henger sammen ses som én behandling. Muligens kan bestemmelsen gjøres klarere dersom man presiserer at begrepet avgenses av formål og behandlingsansvar: Operasjoner som bidrar til å realisere det samme formål hos den samme behandlingsansvarlige, er å regne som én behandling.

1.3 - registerbegrepet

Difi tiltrer Justisdepartementets oppfatning om at de to refererte avgjørelsene i PVN fra 2005 er uheldig. Det må være uten betydning for definisjonen av begrepet personopplysning om opplysningen benyttes eller ikke. Det må vel uansett antas at registreringen/lagringen og at det er å benytte opplysningen hvis det skulle vise seg nyttig.

Vi støtter departementets forslag til endret definisjon av begrepet, som gjør registerbegrepet enklere å forstå.

1.4 behandlingsansvarlig

Difi er også enige i forslaget om at det åpnes for å plassere behandlingsansvaret i lov eller forskrift. Det vil bidra til klarhet.

I personverndirektivets presiseres det at behandlingsansvaret blant annet kan legges til offentlig myndighet, institusjon eller organ (art 2 litra d). Datatilsynet og Personvernemnda synes i sin praksis å ha lagt til grunn en tilsvarende forståelse.

I forarbeidene og personvernteori er det lagt stor vekt på at ansvaret skal legges til juridiske eller fysiske personer.

Vi antar begrepet "behandlingsansvarlige" kan bli noe lettere tilgjengelig for offentlig sektor dersom en revidert lovbestemmelse – eventuelt forarbeidene – i større grad speiler direktivets definisjon av begrepet.

Helseregisterloven og personopplysningsloven bruker ulike navn på det sentrale ansvarssubjektet etter loven (databehandlingsansvarlig vs. behandlingsansvarlig). Vi ber departementet vurdere om begrepsbruken kan harmoniseres.

2.1 – virkeområdet, § 3 første ledd

Vi er enige med departementet i at elektronisk behandling gjerne skjer i samspill med menneskelig aktivitet, og at loven er ment å ramme slike behandlinger. Dette kommer etter vårt skjønn greit til uttrykk i § 3 ("*helt eller delvis* skjer med elektroniske hjelpemidler").

Begrepet "elektronisk" er godt innarbeidet i norsk regelverk som regulerer spørsmål knyttet til maskinell behandling av opplysninger, eksempelvis e-forvaltningsforskriften og e-signaturloven. Vi kan ikke se at bestemmelsen blir lettere å forstå ved at man innfører et tilleggskrav om at behandlingen skal skje mer eller mindre automatisert.

Vi vil også nevne at personvernutfordringene ikke utelukkende er knyttet til gjenfinningsmuligheter, men at også lagringsmuligheten (store mengder kan lagres effektivt) er relevant.

2.2 – personopplysningsloven § 3 annet ledd – behandling av opplysninger for private formål

Vi slutter oss til departementets forslag, som kan være klargjørende. Det kan være grunn til å gi nærmere veiledning i merknadene til bestemmelsen eksempelvis for hvor lovens grense skal trekkes mht. distribusjon i lukkede nettverk, som sosiale nettverk.

4 – kravet til rettslig grunnlag

Vi slutter oss til forslaget om å plassere bestemmelsen om grunnkravene (dagens § 11) foran bestemmelsene de ulike rettslige grunnlag (dagens §§ 8 og 9).

Utrederne foreslår i sitt radikale forslag en hierarkisk ordning av behandlingsgrunnlag, hvor dagens § 8f havner på tredje nivå. Konsekvensene ved det radikale utkastets endringer er imidlertid ikke så lett tilgjengelig. Vi savner en fremstilling av hvordan den foreslåtte § 8c vil gi andre resultater enn gjeldende rett, for eksempel for de situasjoner som PVN har lagt til grunn at § 8 f er anvendelig. Dagens § 8 f har etter vårt skjønn et viktig virkeområde, eksempelvis for meldinger til innbyggerne ex officio, som utsending av pin-koder.

Begrepet "frivillig har gjort alminnelig kjent" antar vi bør presiseres. I hvilken grad vil uttrykket ramme sensitive forhold som fremkommer i det offentlige rom, for eksempel gjennom utseende eller atferd – i hvilken grad kan disse gjengis i ubegrenset grad.

5 – overføring av opplysninger til utlandet

Utrederne har vurdert enkelte spørsmål knyttet til overføring av opplysninger til tredjeland uten tilfredsstillende personvernlovgivning.

Tilbud om bruk av databehandlere med globale leveranseapparat er en trend som møter både privat og offentlig sektor. Behandlingen av personopplysninger vil da dels skje i Norge, dels inær- og fjerntliggende land. Etter personopplysningsdirektivet kan overføring til tredjeland utenfor EØS baseres på "Binding Corporate Rules" for overføringer innen et multinasjonalt selskap, og mellom virksomheter kan standard kontraktsvilkår for overføringer benyttes.

Vi ber om at slike overføringer omtales kort i kommende lovarbeid, jf. at dette er praktisk viktige alternativer til overføring basert på samtykke. Overføringer som følger ovennevnte regler vil i henhold til EU-kommisjonens beslutning 2002/16/EF artikkel 4 kun i spesielle tilfeller kunne nektes av nasjonal datatilsynsmyndighet.

Departementet tar spesielt opp forholdet mellom §§ 29-30 og publisering av opplysninger på Internett.

Difi har ansvar for OEP-tjenesten (offentlig elektronisk postjournal), hvor postjournaler gjøres tilgjengelige over Internett.

Tjenesten vil legge til rette for lenking til dokumenter som forvaltningsorganene publiserer. I den grad slike dokumenter publiseres etter en meroffentlighetsvurdering, vil pol §§ 29-30 formodentlig regulere ev. nedlasting[1] fra tredjeland, jf. at pol § 6 bare unntar lovbestemt innsyns*rett* fra de nevnte bestemmelser.

Vi ber om at denne problemstilling vurderes i det videre arbeid, så det ikke oppstår rettslige uklarheter knyttet til bruken av denne tjenesten.

---

[1] I Lindqvist-dommen tok domstolen eksplisitt stilling til at *opplastingen* av personopplysninger til en webtjener i en medlemsstat ikke innebar overføring til tredjeland; dog presiserte domstolen at opplysningene ved opplastingen ble *tilgjengelige* i tredjeland.

Som illustrasjon til personvernproblemstillingen kan nevnes presseoppslag nylig om et norsk nettsted som tilbyr personsøketjenester som sammenstiller opplysninger fra ulike nettsteder. Datatilsynet har bedt om en redegjørelse for hjemmelsgrunnlaget for behandlingen[2]. En slik sammenstillingstjeneste kunne alternativt vært etablert utenfor EØS-området, og slik unngått norsk personvernregelverk.

10 – Andre spørsmål

10.1 - Henvisning til taushetspliktsregler

Justisdepartementet ber særskilt om merknader til § 8 i radikalt lovutkast, jf. forslagets presisering i litra a av at behandlingen av personopplysninger må skje innenfor rammen av taushetspliktsbestemmelser. Bestemmelsen har et pedagogisk formål.

Vi tror det kan være ønskelig at rettsanvenderne gjøres oppmerksom på sammenhengen mellom personopplysningsloven, offentlighetsloven og taushetspliktsregler – kanskje særlig knyttet til sensitive opplysninger. Muligens vil det være mer naturlig å plassere en slik pedagogisk bestemmelse i nærheten av dagens § 6. Det kan da presiseres at også sensitive opplysninger vil være omfattet av lovbestemt innsynsrett.

10.2 - Struktur

Vi slutter oss til forslaget om endret struktur på lovbestemmelsene.

10.4 – informasjonssikkerhet og internkontroll

Dagens informasjonssikkerhetsbestemmelse nevner tre sikkerhetsinteresser: konfidensialitet, integritet og tilgjengelighet. Dette er en vanlig definisjon av informasjonssikkerhet, som også benyttes i internasjonale standarder, som ISO NS 27002:2005 (pkt 2.5).

Vi kan ikke se at rapportene godtgjør at ivaretakelse av *kvalitetskrav* naturlig hører hjemme i informasjonssikkerhetsbestemmelsen, og anbefaler at dagens terminologi videreføres. Begrepsbruken fremstår som veloverveid i forarbeidene til gjeldende lov; i odelstingsproposisjonens merknader til § 13 presiseres det at "Kravet til integritet må ikke forveksles med krav til kvalitet som er knyttet til riktigheten av personopplysningene." (Uttalelsen kan formodentlig forstås som en forklaring på at personopplysningslovens uttrykk "integritet" avløste begrepet "kvalitet" som ble benyttet i personregisterforskriften).

At opplysningene skal ha høy kvalitet er avgjørende for at behandling skal gi godt personvern. Kravet til opplysningskvalitet er imidlertid etter vårt skjønn godt dekket i gjeldende lovverk. Pol § 11 litra d og e understreker at opplysningene må være korrekte og oppdaterte, tilstrekkelige og relevante. Dessuten er ansvaret for personopplysningenes kvalitet særskilt nevnt i internkontrollbestemmelsen, jf. pol § 14 første ledd i.f.

Ved revisjon av § 13 kan det for øvrig gjerne presiseres at den behandlingsansvarlige har det overordnede ansvaret for sikkerheten, jf. at han setter rammene for behandlingen og kriterier for akseptert risiko. Databehandler har ansvar for at sikkerheten er tilfredsstillende *innen de rammer* den behandlingsansvarlige setter.

10.5 Databehandleravtale

Vi slutter oss til forslaget om en noe mer utførlig regulering.

---

[2] http://www.datatilsynet.no/templates/Page____3017.aspx

10.8 Elektroniske spor

Utrederne foreslår at kontrollformål skal synliggjøres, jf. radikalt utkast til §§ 9 annet ledd og 18 første ledd bokstav b.

Difi er i tvil om rekkevidden av og hensiktsmessigheten ved disse forslagene.

Vi kan ikke se hvorfor "sammenstilling" bør være et selvstendig vilkår. Dels vil begrepet være vanskelig å avgrense mot bruk av enkeltopplysninger, dels er det vanskelig å se knytningen mellom dette vilkåret og motivet for bestemmelsen (vern mot bruk til kontrollformål).

Vi slutter oss til departementets og utredernes vurdering av at det ikke er grunn til å regulere dette særskilt.

10.9 Bruk av fødselsnummer, biometri

Personopplysningsloven § 12 regulerer i dag både autentisering og identifisering, jf. personvernnemndas praksis. Utrederne foreslår å regulere disse spørsmål hver for seg. Vi er enige i at det er fornuftig, jf. at identifisering og autentisering berører ulike personverninteresser.

Entydig identifisering er personvernmessig relevant for risikoen for muligheten til samkljøring av opplysniner (profilbygging). Krav til identitetskontroll (autentisering) er avgjørende for vernet av opplysningenes konfidensialitet (vern mot uberettiget innsyn) og for sikring av datakvaliteten (hvem er kilde for opplysningene).

Bestemmelsen om fødselsnummer og sikker identifisering

Begrepet "sikker identifisering" bør etter vårt skjønn ikke benyttes i bestemmelsen om fødselsnummer, ettersom "sikker" lett kan oppfattes uttrykk for at identifiseringen er korrekt, mao. at bestemmelsen regulerer autentisering. Vi vil foreslå at uttrykket "entydig identifisering" benyttes. Fødselsnummer er egnet til *entydig* identifikasjon, men ikke til *sikker* identifikasjon. Fødselsnummeret er egnet til å skille navnesøsken[3] fra hverandre, men det ligger ingen identitetskontroll i bruken av fødselsnummeret; identifiseringen kan være uriktig, selv om den er entydig.

For forvaltningen – som skal ivareta rettigheter og plikter – vil det normalt være behov for entydig identifikasjon. For å oppnå effektiv gjenbruk av registeropplysninger, for eksempel folkeregisteropplysninger, vil det også være behov for entydig identifikasjon av de registrerte hos dem som skal nytte folkeregisteret.

Når det gjelder risikoen for ulovlig samkjøring av registre (profilbygging) vil vi minne om at flesteparten av innbyggerne har unike navn, og det er derfor mulig å koble registre for disse personer *uten* bruk av fødselsnummer. Samkjøring vil imidlertid mislykkes for personer som har endret navn, og for navnesøsken vil det være nødvendig å basere koblingen på flere registrerte opplysninger, som fødselsdato eller adresseopplysninger.

Etter vårt skjønn bør vernet mot uønskede samkjøringer/profilbygging ikke alene baseres på en restriktiv holdning til bruk av fødselsnummer. Gode sikkerhetstiltak, tjenestedeling og desentralisert lagring er tiltak som er sentrale for å redusere risikoen for misbruk. På områder hvor entydig identifikasjon (herunder fødselsnummer) ikke er nødvendig, bør det også vurderes tiltak for å vanskeliggjøre samkjøring basert på navn eller øvrige opplysninger som unikt identifiserer den registrerte. Begrenset identifisebarhet kan oppnås ved å legge til rette for at brukeren kan benytte selvvalgte brukernavn eller pseudonymer. Det er på dette området mulig å lage personvernøkende elektroniske løsninger, hvor den registrerte gis mulighet til å velge

---

[3] Som navnesøsken regner vi her bare personer som har identiske navn, dvs. identiske kombinasjoner av fornavn, mellomnavn og etternavn. 80 % av befolkningen har unike navn iflg opplysninger fra SSB. 40 % av befolkningen har et beskyttet etternavn (inntil 200 bærere).

hvordan hun skal identifiseres overfor tjenesteeier, jf. våre merknader til personvernkommisjonens rapport.

Utrederne foreslår at det må foreligge en risikovurdering som viser behovet for bruk av fødselsnummeret.

Vi tror det er fornuftig å analysere behovet for bestemmelsen noe grundigere. Fødselsnummer er i dag en meget viktig koblingsnøkkel, som gjør det mulig med omfattende effektiv og rettssikker samhandling i og med offentlig sektor for *alle* innbyggere, og ikke bare dem med unike navn. Med mindre man ønsker en redusert bruk av fødselsnummer, kan vi ikke se behovet for denne endringen.

Difi vil understreke betydningen av at eventuelle endringer i bestemmelsen om fødselsnummer ikke må bli et hinder for effektiv og rettssikker e-forvaltning,. For effektiv samhandling i offentlig sektor er kobling basert på fødselsnummer i dag den beste løsningen.

Fornyings- og administrasjonsdepartementets presiserte i brev av 24.9.2007 til flere sentrale aktører at fødselsnummer ikke skal brukes til autentisering i Internettløsninger[4]. Siden har Posten (flyttemeldingen) og NAV (fastlegebytte) gått bort fra påloggingsløsninger hvor fødselsnummer ble brukt til autentisering. Begge løsninger vil benytte den felles påloggingsløsningen MinID, som Difi har ansvaret for. Vårt inntrykk er således at utviklingen på området synes å gå i riktig retning, og at misbruket av fødselsnummer til autentisering er på retur.

Vennlig hilsen
for Difi

Tone Bringedal
avdelingsdirektør

Jon Holden
seniorrådgiver

[4] http://www.regjeringen.no/nb/dep/fad/dok/andre-dokumenter/brev/utvalgte_brev/2007/bruk-av-fodselsnummer-i-internettlosning.html?id=481566