FORNYINGS- OG
ADMINISTRASJONSDEPARTEMENTET

Veileder til utredningsinstruksen

Vurdering av personvern-konsekvenser

Innhold

I Innledning/formål

Hensikten med denne veilederen er å bidra til at statlige etater på en god måte kan utrede de personvernmessige konsekvensene av sine forslag.

Utredningsinstruksen[1] fastslår at hver sak skal inneholde en konsekvensutredning som skal bestå av analyse og vurdering av antatte vesentlige konsekvenser av den beslutning som foreslås truffet. Det samme gjelder ved utredningsarbeid som er et forarbeid til departementets arbeid med saken.

Til utredningsinstruksen er det utarbeidet en generell veileder i utredningsarbeid. Det går fram av denne veilederen pkt. 11.3 at personvern er et område hvor det kan være aktuelt med konsekvensvurderinger. Dersom saken har personvernmessige konsekvenser, skal disse utredes som et ledd i den ordinære utredningsprosessen.

Dette dokumentet er et supplement til den generelle veilederen i utredningsarbeid. Den er generelt utformet, og er ment til bruk på tvers av ulike sektorer. Veilederen er ment som et hjelpemiddel ved:

1. vurdering av i hvilke saker personvernkonsekvenser bør utredes, se kapittel IV
2. fremgangsmåte ved utredning av personvernmessige konsekvenser, og analysens/utredningens innhold, se kapittel V og VI

Personvernhensyn tar sikte på å beskytte enkeltmenneskets personlige integritet og privatlivets fred. En avveining av personvernmessige konsekvenser mot andre interesser vil bidra til å skape tillit hos borgerne som kan gjøre iverksettingen av tiltaket eller beslutningen enklere, eventuelt etter justeringer for å ivareta personvernet på en bedre måte.

1 Instruks om utredning av konsekvenser, foreleggelse og høring ved arbeidet med offentlige utredninger, forskrifter, proposisjoner og meldinger til Stortinget (fastsatt ved kongelig resolusjon 18. februar 2000, revidert 24. juni 2005, se Utredningsinstruksen - regjeringen.no)

En utredning av personvernkonsekvenser skal bidra til et godt beslutningsgrunnlag for tiltaket, herunder om det faktisk er nødvendig å innhente personopplysninger, og om ev. personvernulemper oppveies av andre gevinster ved tiltaket. Arbeidet med utredningen vil også gi grunnlag for å vurdere om man kan oppnå målsetningen på en annen, og mindre personverninngripende måte.

Veilederens hoveddel er å finne i kapittel IV, V og VI. Som bakteppe for disse kapitlene er det gitt en kort oversikt over personvernretten og målsettinger i personvernarbeid i avsnitt II og III. Vi antar disse avsnittene er særlig nyttige for personer uten erfaring med personvernarbeid.

II Hva er personvern/ definisjoner

Det er nyttig å ha noe teori som bakteppe når man skal foreta vurdering av om en sak har personvernmessige konsekvenser.

Et sentralt element i personvernet er den enkeltes rett til og reelle mulighet for å bestemme over bruk av egne personopplysninger.

Personvern er et område som ikke så enkelt kan gis et målbart uttrykk. Det hører til sjeldenhetene at personvernkonsekvenser kan måles og tallfestes. Dessuten oppleves interessen i personvern forskjellig fra individ til individ. Personvernreguleringen er nært knyttet til enkeltindividers behov og muligheter for privatliv, selvbestemmelse (autonomi) og selvutfoldelse. Retten til privatliv følger bl.a. av den europeiske menneskerettskonvensjon (EMK) artikkel 8 og står sentralt i EUs personverndirektiv (95/46/EF).

Relevant regelverk

Relevant regelverk på personvernområdet er i første rekke personopplysningsloven (14.04.2000 nr. 31) med forskrifter som gjennomfører EUs personverndirektiv [2] i norsk rett. I tillegg har vi en rekke spesiallover og spesialbestemmelser om personvern, så som lov om helseregistre og behandling av helseopplysninger, og lov om Schengen informasjonssystem. Mange særlover har også enkelte personvernrelaterte bestemmelser, som for eksempel taushetsbestemmelser eller innsynsbestemmelser. Forvaltningsloven § 13, som etablerer taushetsplikt om "noens personlige forhold", er også et eksempel på en personvernbestemmelse utenfor personvernlovgivningen.

Personopplysninger

Personopplysninger er i personopplysningsloven definert som "opplysninger og vurderinger som kan knyttes til en enkeltperson". Eksempler på personopplysninger er navn, fødselsdato, yrke og opplysninger om hvor en person har vært på et bestemt tidspunkt. Opplysningene kan foreligge i forskjellige former, for eksempel i tekst, bilde, lyd (stemme), fingeravtrykk og genetiske kjennetegn.

Et sentralt vilkår i definisjonen er at opplysningene "kan knyttes til en enkeltperson". Også opplysninger som *indirekte* kan knyttes til en person, vil være personopplysninger. Dette gjelder selv om det må benyttes en nøkkel, for eksempel i form av en tallkode (fødselsnummer, bilregistreringsnummer, telefonnummer, organisasjonsnummer), for å knytte forbindelse mellom opplysningen og den bestemte personen. Dersom man ved hjelp av nøkkelen (tallkoden) kan finne ut hvem opplysningen gjelder, kaller man opplysningene for *avidentifiserte*. I en del større registre er opplysningene pseudonymiserte. Dette innebærer at personopplysningene er kryptert eller skjult på annet vis, men likevel individualisert slik at det lar seg gjøre å følge enkeltpersoner uten at identiteten røpes. Av sikkerhetshensyn oppbevares pseudonymiseringsnøkkelen hos en tredjepart.

I vurderingen av om en person er identifiserbar, skal alle hjelpemidler som med rimelighet kan tenkes benyttet i identifikasjonsprosessen, tas i betraktning. I denne vurderingen vil det være relevant både å se på hvilken ressursinnsats som kreves for å identifisere personen, og hvor stor motivasjon det vil være for å knytte opplysningen til en bestemt person. Etter omstendighetene vil for eksempel en IP-adresse kunne være en personopplysning.

Opplysninger om døde personer kan være personopplysninger, i den grad de sier noe om levende personer, for eksempel om vedkommendes etterkommere.

2 direktiv 95/46/EF om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger

Et eksempel her kan være genetiske opplysninger.

Opplysninger om juridiske personer vil være personopplysninger dersom de "kan knyttes til" (sier noe om) fysiske personer. Typisk vil informasjon om enkeltmannsforetak kunne være opplysninger som også sier noe om eieren, for eksempel om eierens økonomi.

Behandling av personopplysninger

Behandling av personopplysninger er et vidt begrep og omfatter etter definisjonen i personopplysningsloven "enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller kombinasjoner av slike bruksmåter". Behandlingen kan skje manuelt eller ved hjelp av elektroniske hjelpemidler. Manuell behandling av personopplysninger er bare omfattet av personopplysningsloven når opplysningene inngår eller skal inngå i et personregister. Personopplysningsloven gjelder som hovedregel all behandling med elektroniske hjelpemidler, fordi dette legger til rette for omfattende bruk av opplysninger også til andre formål enn de ble innsamlet for. Risikoen for uønsket spredning av opplysninger og skadepotensialet blir da større.

Personopplysningsloven §§ 8, 9 og 11 oppstiller visse grunnkrav til behandling av personopplysninger. Disse kravene må oppfylles for at behandlingen skal være lovlig. I tillegg oppstiller personopplysningsloven § 13 krav til sikring av de registrerte personopplysningene. God informasjonssikkerhet er sentralt i godt personvern. Som ledd i informasjonssikkerhetsarbeidet kan det blant annet være aktuelt å vurdere ulike personvernfremmende teknologier. Som navnet sier, brukes personvernfremmende teknologi for å ivareta de registrertes personvern. Dette kan være f.eks. bruk av krypterings- eller autentiseringsløsninger som hindrer at uvedkommende får tilgang til personopplysninger. Også elektroniske innsynsløsninger som gjør det enkelt for de registrerte å få tilgang til de personopplysningene som er lagret om dem, er eksempel på personvernfremmende teknologi.

Mer om behandling av personopplysninger finnes i kap. IV i denne veilederen.

Sensitive personopplysninger og andre beskyttelsesverdige personopplysninger

Personopplysningsloven har definert visse opplysninger som "sensitive personopplysninger", se personopplysningsloven § 2 nr. 8. Dette er opplysninger som av lovgiver er vurdert som særlig beskyttelsesverdige. For disse gjelder enkelte særregler, som skjerpet hjemmelskrav til behandlingsgrunnlaget og som hovedregel konsesjonsplikt. Mer om hvilke opplysninger som er sensitive etter personopplysningsloven, og behandlingen av disse, finnes i personopplysningsloven § 2 nr. 8, og § 9 jf § 8 og 11.

Forskjellige rapporter og undersøkelser har vist at befolkningen til en viss grad har en avvikende oppfatning av hvilke typer personopplysninger det er viktig å beskytte mot innsamling og videre bruk. Mange oppfatter for eksempel økonomiske opplysninger, som kredittopplysninger og ligningsopplysninger, som særlig beskyttelsesverdige, selv om disse opplysningene ikke er sensitive etter personopplysningsloven § 2 nr. 8. Ved utredning av personvernmessige konsekvenser må det derfor foretas en konkret vurdering av hvor beskyttelsesverdige de aktuelle personopplysningene er. Sentrale momenter i denne konkrete vurderingen vil være om opplysningstypen er sensitiv i lovens forstand, og hvor beskyttelsesverdige de registrerte eller befolkningen for øvrig oppfatter de aktuelle opplysningene.

Kontaktinformasjon som navn, adresse og telefonnummer er informasjon som er alminnelig tilgjengelig for de fleste menneskers vedkommende. Dette kan tale for at det ikke er store personvernulemper knyttet til behandling av disse. Unntak vil gjelde for eksempel for personer som har hemmelig adresse. Videre vil kilden til opplysningene være relevant, herunder om kilden som dataene er hentet fra kan røpe følsom eller sensitiv informasjon, for eksempel når opplysningene kommer fra politiet, kriminalomsorgen eller krisesentre. Typiske eksempler er dersom adressen røper at den registrerte er innsatt i fengsel (straffbare forhold, personopplysningsloven

§ 2 nr. 8 bokstav b) eller innlagt på psykiatrisk behandlingsinstitusjon (helseforhold, personopplysningsloven § 2 nr. 8 bokstav c). Til sammenlikning vil informasjon om at bostedsadressen er et aldershjem ikke være en sensitiv opplysning i personopplysningslovens forstand, siden denne opplysningen ikke nødvendigvis sier noe om personens helse.

Et annet eksempel på en opplysningstype som mange oppfatter som beskyttelsesverdige, er biometriske kjennetegn. Biometri er uløselig knyttet til den registrerte, og er derfor som regel godt egnet til legitimasjonsformål, men opplysningen er ikke i seg selv sensitiv.

Det vil ha betydning om opplysningene er avgitt frivillig eller pliktig, og bakgrunnen for at opplysningene ble avgitt. Opplysningskvaliteten og presisjonen vil også ha betydning. Det er i regelen større personvernkonsekvenser ved behandling av detaljerte opplysninger eller uverifiserte tips enn ved behandling av overordnede, objektive opplysninger.

Også spredningspotensialet vil være relevant for om opplysningene oppfattes som beskyttelsesverdige. Eksempelvis vil det kunne være betydelige personvernkonsekvenser ved Internettpublisering av ellers trivielle personopplysninger. Det vil blant annet ikke være mulig å garantere fullstendig sletting av opplysningene, siden man mister kontroll over hvor de er lagret, og således heller ikke vet hvor man skal foreta sletting. Dessuten vil muligheten for sammenstilling med andre opplysninger, som igjen kan gi grunnlag for å utlede nye opplysninger, bli enorme og oppleves som en integritetstrussel.

III Målsettinger i personvernarbeid

Beskyttelse av privatlivets fred er et sentralt hensyn bak personvernreguleringen. For å konkretisere hva som ligger i personvern og i de overordnede hensyn knyttet til å beskytte enkeltmenneskets personlige integritet og privatlivets fred, er det i teorien utviklet ulike innfallsvinkler. På et overordnet nivå kan man se personvernet ut fra tre ulike fokus:

Først har man det *integritetsfokuserte personvernet*, som er et uttrykk for borgernes ønske om å ha kontroll over opplysninger om seg selv og ha en sirkel av privatsfære som ingen har rett til å trenge innenfor, uten tillatelse eller en god og legitim grunn. Taushetspliktsbestemmelser er et uttrykk for det integritetsfokuserte personvern.

Dernest snakker man om det *maktfokuserte personvernet*, som framhever at personlige opplysninger kan forrykke maktbalansen mellom enkeltpersoner og offentlige eller private aktører. Personvernet kan ses som et uttrykk for beskyttelse mot det som kan oppleves som overdreven markedsmakt, offentlig (og privat) myndighetsutøvelse eller arbeidsgivermakt. Regulering av bruk av informasjon samlet inn gjennom automatisk trafikkontroll er et uttrykk for det maktfokuserte personvern.

For det tredje har man det *beslutningsfokuserte personvernet*, som tar utgangspunkt i at personopplysninger brukes som grunnlag for beslutninger i offentlig og privat virksomhet (f eks banker og forsikringsselskap). For at beslutningene skal bli riktige og rettferdige, må opplysningene være korrekte, relevante og tilstrekkelige i forhold til formålet.

I norsk teori snakker man dessuten gjerne om ulike personverninteresser. Personverninteressene gir uttrykk for en del hensyn som ligger til grunn for personvernregelverket. Ved å ta utgangpunkt i de forskjellige personverninteressene kan det bli mer konkret hvilke personvernmessige konsekvenser som kan gjøre seg gjeldende ved ulike tiltak. Den såkalte interessemodellen kan derfor være en nyttig innfallsvinkel og et godt utgangpunkt når personvernmessige konsekvenser skal utredes.

I interessemodellen beskrives personvernet som et knippe ideelle interesser som tilligger enkeltmennesker. De grunnleggende personverninteressene omfatter

- Interessen i selvbestemmelse
- Interessen i innsyn og kunnskap
- Interessen i opplysnings- og behandlingskvalitet
- Interessen i forholdsmessig kontroll og begrenset overvåkning (beskyttelse av intimitetssfæren)
- Interessen i brukervennlighet og en borgervennlig forvaltning (nært knyttet til rettssikkerhetsvurderinger)
- Interessen i et robust samfunn

Personverninteressene kan være innbyrdes motstridende, og hvordan de enkelte interessene skal vektlegges, må alltid vurderes konkret. Dette kan variere fra område til område, og fra sak til sak.

Mer om både de ovennevnte innfallsvinklene og interessemodellen kan man finne i diverse personvernlitteratur. Se for eksempel NOU 1997:19 Et bedre personvern, pkt. 3.3 og 3.4.

IV I hvilke saker bør personvernkonsekvenser utredes?

Utredningsinstruksen knytter et "vesentlighetskrav" til når det skal gjennomføres konsekvensutredning, se pkt 2.1 første setning:

> "Hver sak skal inneholde en konsekvensutredning som skal bestå av analyse og vurdering av antatte vesentlige konsekvenser av den beslutning som foreslås truffet."

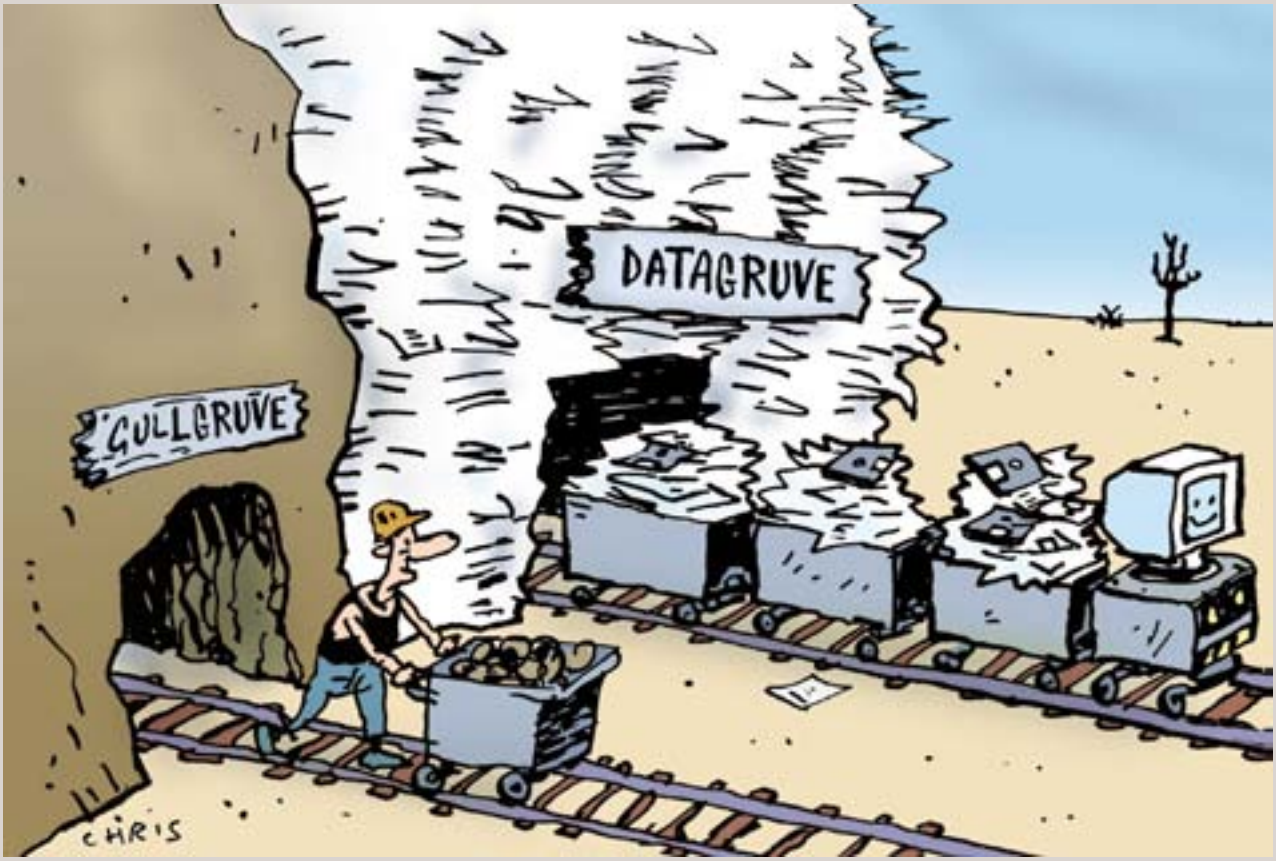
"Antatte vesentlige konsekvenser" innebærer at det innledningsvis må foretas en overordnet vurdering av *om* tiltaket har vesentlige personvernkonsekvenser. Denne innledende vurdering vil ikke være så grundig som selve utredningen av personvernkonsekvenser, jf. kapittel V, selv om vurderingstemaet for så vidt er det samme (den innledende vurdering kan regnes som en forenklet konsekvensvurdering).

Vi vil her redegjøre for vesentlighetsvurderingen, blant annet ved å liste opp noen momenter som trekker i retning av at vesentlige personvernkonsekvenser foreligger, og gi noen eksempler på situasjoner hvor det vil være krav til utredning av personvernkonsekvenser.

Ved innføring av nye former for behandling av personopplysninger må det alltid foretas en vurdering av tiltakets konsekvenser for de berørtes personvern, med sikte på å avgjøre om konsekvensene er vesentlige. Som eksempel kan nevnes innføring av biometriske kjennetegn i norske pass. Også tiltak som endrer premissene for pågående behandling av personopplysninger, f.eks. overgang fra avidentifiserte opplysninger til en behandling av direkte identifiserbare personopplysninger, må konsekvensutredes.

Type personopplysninger og omfanget av opplysninger som berøres, har betydning for konsekvensutredningen, se kap. II. For eksempel vil det kunne være av betydning for vesentlighetsvurderingen om behandlingen gjelder en begrenset krets av personer, eller om den omfatter behandling av opplysninger om store deler av befolkningen. En omfattende kartlegging og registrering av hele befolkningen vil ha et større misbruks- og skadepotensial enn behandling av opplysninger om en begrenset krets, og vil således kunne ha vesentligere konsekvenser for personvernet. Dette har betydning for om det skal foretas konsekvensutredning, og hvor omfattende denne evt. skal være.

En beslutning som berører sensitive personopplysninger vil normalt ha større konsekvenser for



personvernet enn behandling av mer trivielle opplysninger, og nødvendiggjør derfor grundigere konsekvensutredning. Men man bør se på både opplysningstype og opplysningsverdier. Som nevnt i kapittel II kan for eksempel kontaktopplysninger i seg selv inneholde sensitiv informasjon.

Undersøkelser[3] har dessuten vist at befolkningen ofte er mer opptatt av å beskytte andre opplysninger enn de personopplysningsloven definerer som sensitive. For eksempel mener de fleste at kredittopplysninger og andre økonomiske opplysninger er svært beskyttelsesverdig informasjon, selv om opplysningene ikke er sensitive etter personopplysningslovens definisjon. Tiltak som innebærer behandling av opplysninger som store deler av befolkningen oppfatter som beskyttelsesverdige, bør alltid ha grunnlag i en vurdering av personvernmessige konsekvenser ved tiltaket.

For øvrig må spørsmålet om personvernkonsekvensene ved et tiltak er vesentlige, vurderes på bakgrunn av personverninteressene som omtalt ovenfor i kapittel III. Behandlingens formål, innhold og omfang vil stå sentralt i denne vurderingen. Som eksempel kan nevnes bruk av biometriske kjennetegn for identifikasjons- og autentiseringsformål. Biometriske kjennetegn er knyttet til kroppen, og kan for eksempel være fingeravtrykk eller irismønster. Den viktigste grunnen til å være varsom med bruk av biometri, er at biometriske kjennetegn unikt identifiserer det enkelte individ, og er uløselig knyttet til dette individet. Slike kjennetegn er i seg selv ikke en sensitiv opplysning, og brukt riktig kan biometri være et godt og effektivt verktøy for sikkerhet. Men dersom opplysningene misbrukes, fins det ingen mulighet for offeret til å skaffe seg et nytt biometrisk kjennetegn til erstatning for det som er misbrukt. De fleste vil derfor være opptatt av at opplysningene behandles og beskyttes på behørig vis.

Også risikoen for utilsiktet utlevering og andre sikkerhetsbrudd, basert på en vurdering av sannsynligheten for skader og hvilke konsekvenser skadene vil ha, er vesentlig. Hvis mulige konsekvenser av f.eks.

3 TØI rapport 789/2005

en utilsiktet utlevering av opplysninger er tilstrekkelig alvorlige, selv om sannsynligheten for at det skal skje vurderes som liten, er det grunn til å vurdere alternative tiltak for å oppnå det ønskede målet.

Det bør også legges vekt på at selv om hvert enkelte inngrep isolert sett kanskje ikke har store personvernmessige konsekvenser, vil mange slike inngrep samlet sett medføre at personvernet svekkes gradvis over tid. I offentlige utredninger kan det derfor være på sin plass også å gi rom for overordnede vurderinger knyttet til viktigheten av å ivareta personvernet som en ideell interesse i samfunnet og forsøke å sette personvernaspektet i den konkrete saken i en større sammenheng. En utredning av personvernmessige konsekvenser vil bidra til et bredere grunnlag for den beslutningen som skal fattes, og vil slik sett alltid være et gode, også når man er usikker på om konsekvensene vil være vesentlige eller ikke.

Nedenfor følger en liste over momenter som gir indikasjoner på om personvernkonsekvensene ved et tiltak bør utredes

- inngripende behandling
  - opplysningenes art (intime, sensitive, stigmatiserende)
  - opplysningskvalitet (tips, mer eller mindre kvalifiserte vurderinger vs. objektive forhold)
  - opplysningenes detaljeringsgrad

- omfattende behandling
  - antall registrerte personer
  - antall opplysninger om den enkelte
  - koblingsrisiko
  - planlagt formål
  - andre legale formål – fare for "function creep" (dvs bruk til andre utilsiktede formål)

- fare for feil
  - dårlig datakvalitet, jf. beslutningsfokusert personvern

- fare for misbruk (bruk til andre formål)
  - andre legale formål
  - ulovlige formål, f eks kriminalitet

- lav grad av selvbestemmelse
  - behandlingen er obligatorisk
  - behandlingen er frivillig, men basert på avmelding (opt-out), ikke frivillig samtykke

- liten grad av opplysthet
  - den registrerte vil i liten grad være kjent med behandlingen

Eksempler på behandlinger med vesentlige personvernkonsekvenser:

- biometriske pass (obligatorisk, varige/unike opplysninger om den enkelte, fingeravtrykk forbindes av mange med kriminalitet – straffedømte/åstedsundersøkelser)
- bompengepasseringer (kartlegger bevegelsesmønster)
- automatisert behandling av lånesøknader (automatisering av skjønn)

V Prosess – fremgangsmåte ved utredning av personvernmessige konsekvenser

Fremgangsmåten ved utredning og vurdering av personvernmessige konsekvenser er den samme som ved vurdering av alle andre konsekvenser ved tiltaket. Utredningsprosessen er grundig beskrevet i veilederen til utredningsinstruksen. Her vil vi nøye oss med å minne om at det er Justisdepartementet og Fornyings- og administrasjonsdepartementet som er ansvarlige for henholdsvis personopplysningsloven og personopplysningsforskriften. Det vil imidlertid være det enkelte fagdepartement som selv er ansvarlig for å utrede de personvernmessige konsekvensene av et tiltak på sitt ansvarsområde. Justisdepartementet og Fornyings- og administrasjonsdepartementet må konsulteres og involveres i prosessen i den grad dette følger av utredningsinstruksen. Det kan også være naturlig å be om innspill fra Datatilsynet mens en sak er under utredning.

VI Analysens/utredningens innhold

Når det er besluttet at personvernmessige konsekvenser skal utredes, kan mandatet gi pålegg om forhold som konsekvensutredningen skal omfatte i den konkrete saken. Personvernmessige konsekvenser skal analyseres og vurderes for alle alternativer som utredningen omfatter.

Fokuset ved utredning av personvernmessige konsekvenser vil særlig være rettet mot tre forhold:

- tiltakets virkninger i forhold til de grunnleggende personverninteressene
- eventuelle trusler som tiltaket medfører for personvernet
- hva som kan gjøres for å avhjelpe eventuelle trusler

Konsekvensutredningen anbefales gjennomført i følgende fire trinn:

a. Kartlegging
b. Analyse
c. Vurdering
d. Oppsummering og konklusjon

Trinnene kan gå noe over i hverandre – særlig trinnene "analyse" og "vurdering". En trinnvis fremgangsmåte er likevel å anbefale fordi det bidrar til å strukturere arbeidet. I det følgende gis innspill til hva de forskjellige trinnene i utredningsprosessen bør inneholde.

a) Kartleggingsfasen

1. *Innebærer tiltaket behandling av personopplysninger?*
   - Dersom enkeltpersoner kan identifiseres, er svaret sannsynligvis ja, se omtale i kapittel II.

2. *Hvis ja på 1, hvilke endringer innebærer tiltaket i forhold til nåværende situasjon*
   - Ny behandling av personopplysninger
   - Endringer i eksisterende behandlinger, eventuelt angivelse av type endringer

3. *Hvilke typer personopplysninger skal behandles*
   - Ikke sensitive personopplysninger
   - Sensitive personopplysninger, jf personopplysningsloven § 2 nr. 8
   - Opplysninger som ikke er sensitive etter personopplysningsloven, men som store deler av befolkningen likevel oppfatter som beskyttelsesverdige
   - Opplysninger som er taushetsbelagte, jf. for eksempel forvaltningsloven § 13 eller særlovgivning

4. *Hvis tiltaket ikke direkte omfatter ny behandling av personopplysninger, har det likevel personvernkonsekvenser?*

Selv om tiltaket ikke direkte innebærer en ny behandling av personopplysninger, kan det ha personvernkonsekvenser. Typisk vil endringer i datamaskinbaserte systemer kunne få konsekvenser for de personopplysningene som behandles i systemet. Særlig synlig er dette dersom endringene gjelder sikkerheten i systemet. Også endrede tilgangsrutiner som medfører at flere personer får tilgang til personopplysninger, kan ha personvernmessige konsekvenser ved at det blant annet innebærer en økt spredning av opplysningene og dermed økt skadepotensial.

5. *Hvem, herunder hvor mange, blir berørt av tiltaket?*

Om tiltaket innebærer behandling av opplysninger om en begrenset krets av personer eller om det vil berøre hele eller en stor del av befolkningen, vil ha betydning for den videre utredningen av tiltakets personvernrelaterte konsekvenser.

6. *Planlagt bruk, risiko for misbruk*

Hva er formålet med tiltaket, herunder behandlingen av personopplysninger? Hvorfor behandles personopplysningene?
   - Er behandlingsformålet tilstrekkelig presist angitt til at man kan vurdere om opplysningene og behandlingen tilfredsstiller lovens krav?
     – Eks: "Forskning" som formålsangivelse vil ikke være tilstrekkelig. Det må presiseres hvilken type forskning og hva man forventer å oppnå.
   - Vil opplysningene også kunne brukes til andre lovlige formål? Det må ses både på andre offentligrettslige formål (eks. passeringsopplysninger kan benyttes i kontrolløyemed – kontroll av næringsdrivendes transportutgifter; fartskontroll – gjennomsnittsberegning; etterforskning av kriminalitet), kommersiell bruk (eks. kartlegging av reisemønster som grunnlag for alternative transporttilbud), annen privat bruk (overvåking av den enkelte – hvor var han når). Utnytting til kriminelle formål er også tenkelig, f.eks. kartlegging av reisemønster (fravær fra hjemsted som grunnlag for innbruddsraid), eller bruk til sladder.
   - Hvilke av disse formål ønskes det at opplysningene skal kunne brukes til? Hvilke regnes som uønsket? For eksempel kan det være relevant å kartlegge potensialet for kommersiell bruk av personopplysninger, som bruk av skattelistene som grunnlag for adressert markedsføring, og om slik bruk er forenelig med det opprinnelige innsamlingsformålet.
   - Hvor stor er skaden ved bruk til andre formål?

7. *Rettslig grunnlag for behandlingen*
   - Samtykke
   - Lovhjemmel
   - Nødvendighetsvurdering etter personopplysningsloven § 8 a) til f). § 8 bokstav f) gir for eksempel anvisning på en avveining mellom

gjennomføring av behandlingen for å ivareta en berettiget interesse og de registrertes interesse i personvern.

All behandling av personopplysninger må ha rettslig grunnlag. Dette kan f.eks. være hjemmel i lov, samtykke fra de registrerte eller behandlingen kan basere seg på en nødvendighetsvurdering jf personopplysningsloven § 8 a) til e), eller avveining mellom de registrertes interesse i personvern og den behandlingsansvarliges interesse i at behandlingen utføres jf personopplysningsloven § 8 f). En slik interesseavveining vil sette personvernhensyn i perspektiv i forhold til andre interesser, private eller offentlige.

Samtykke er det behandlingsgrunnlaget som i størst grad ivaretar hensynet til de registrerte, og det anbefales derfor at behandling av personopplysninger som hovedregel baseres på samtykke. Behandling av personopplysninger på andre grunnlag skal begrunnes særskilt.

8. Informasjon, innsyn

Vil den registrerte ha rett til å bli informert om hvilke opplysninger som behandles, generelt og konkret? Hvordan skal man eventuelt sikre at den registrerte blir kjent med behandlingen? Jo bedre informert de registrerte er, jo mindre vil ofte personvernulempene være (særlig relevant i et maktperspektiv).

9. Hvis endringene knytter seg til én eller flere konkrete behandlinger, hvem er eller skal være behandlingsansvarlig?

Det er den behandlingsansvarlige som må ha rettslig grunnlag for behandlingen, og som vil være ansvarlig for den behandling som utføres. I en offentlig eller privat virksomhet vil det være praktisk å knytte behandlingsansvaret opp mot en ledende funksjon i organisasjonen.

10. Hvor lenge skal opplysninger behandles/lagres?

Det er en viktig personverngaranti at opplysninger ikke lagres lenger enn det som er nødvendig for formålet. Det må derfor foretas en vurdering av lagringstid opp mot formål. Også den registrertes mulighet til å kreve opplysninger slettet, bør kartlegges og vurderes.

b) Analysefasen

11. Er det forholdsmessighet mellom behandling og formål?

Her må det vurderes om de tiltak som vurderes iverksatt er hensiktsmessige, tilstrekkelige og nødvendige for å oppnå formålet.

- Er det nødvendig å behandle personopplysninger, eller kan formålet oppnås på andre måter?

12. Analyse av hvilke personverninteresser som gjør seg gjeldende

- Hvilke personverninteresser gjør seg gjeldende?
- Sensitive eller ikke sensitive personopplysninger?
- Ved behandling av ikke sensitive opplysninger, kan behandlingen likevel oppleves som integritetskrenkende?

13. Sammenheng opplysningstyper og formål

- Er opplysningene relevante for formålet?
- Er opplysningene nødvendige for formålet?
- Redusere opplysningsomfanget for å begrense mengden overskuddsinformasjon?

14. Fins det alternative opplysningstyper og behandlingsmåter som kan ivareta det definerte formålet, men som representerer en mindre personverntrussel? Vurdere tiltak for å avhjelpe personverntrusler

- Anonymisering - er det nødvendig å behandle personidentifiserbare opplysninger?

- Avidentifisering – kan man fjerne de direkte identifiserende opplysningene?
- Pseudonymisering – kan det brukes et kryptert id-nummer hvor koblingen oppbevares av en pseudonymforvalter?
- Kortere lagringstid?
- Fødselsnummer - dersom bruk av fødselsnummer (11 siffer) vurderes, skal det foretas en analyse av om denne identifikatoren er nødvendig og/eller egnet for formålet. Fødselsnummer er normalt godt egnet til identifikasjonsformål (dvs. for å hindre sammenblanding av personer), men ikke egnet til legitimasjons- og autentiseringsformål (dvs. for kontroll av om en person virkelig er den vedkommende gir seg ut for å være).
- Sikring av personopplysninger
- Bruk av personvernfremmende teknologier (PET=Privacy Enhancing Technologies)

c) Vurderinger

Utredningsinstruksen krever at konsekvenser som utredes skal tallfestes så langt dette er mulig, se utredningsinstruksen pkt. 2.3. Personverninteressene som sådan, og verdien av å ivareta disse, er ideelle interesser og verdier som det i de aller fleste tilfellene ikke er mulig å gi en eksakt kroneverdi. Godt personvern er imidlertid i seg selv en positiv verdi som verdsettes høyt av mange. Taushetspliktsregler er et uttrykk for ivaretakelse av personvernhensyn. For eksempel er helsepersonells overholdelse av taushetsplikt grunnleggende for pasientenes tillit til helsevesenet. Taushetsplikt i helsevesenet har derigjennom en positiv verdi i seg selv, selv om verdien ikke kan tallfestes i kroner og øre.

Kostnadene ved tiltak som skal bidra til å ivareta personvernet vil imidlertid som oftest ha en kroneverdi. Dette kan for eksempel være administrative kostnader knyttet til en konsesjonsprosess eller kostnader knyttet til informasjonssikkerhetstiltak. Når man får kroneverdier bare på kostnadssiden, gir dette en risiko for at personvern blir ansett som "en utgift". Verdsetting i kroner vil ikke gi beslutningstagerne noe bedre og mer utfyllende bilde av tiltakets effekter, og kost-/nytteanalyser kan derfor som hovedregel ikke benyttes ved utredning av personvernmessige konsekvenser.

Selv om personvernmessige konsekvenser ikke kan gis en kroneverdi eller verdsettes i andre fysiske størrelser, må virkningene systematiseres slik at man kan vurdere dem. De personvernmessige konsekvensene må, ved motstrid, vurderes og veies mot hverandre. Personvernkonsekvensene må også veies mot andre effekter av det foreslåtte tiltaket. Dette kan for eksempel være en mer effektiv kriminalitetsbekjempelse eller oppfyllelse av andre grunnleggende interesser og verdier som personvernet må avveies mot. Vurderingene vil være med på å danne grunnlaget for en beslutning om tiltaket skal iverksettes og hvordan det i så tilfelle skal gjennomføres.

Momenter på personvernsiden i disse avveiningene kan være borgernes tillitt til staten/forvaltningen, borgernes tillit til ulike næringsdrivende som de er i kontakt med, å hindre overdreven overvåking og kontroll (herunder ivaretakelse av privatlivets fred), ivaretakelse av muligheten til å ferdes anonymt eller retten privat kommunikasjon. Fravær av overdreven overvåking og kontroll kan blant annet ha den positive effekt at borgerne i større grad tør ytre seg kritisk til ulike sider av samfunnet, noe som igjen bidrar til økt åpenhet og debatt. Alt dette er verdier som verdsettes i en rettsstat uten at de kan måles i kroner og øre.

15. Avveining av eventuelle motstridende personverntrusler

Av og til kan man oppleve at et tiltak har ulike personvernmessige konsekvenser som til en viss grad er innbyrdes motstridige. Ønsket om at den behandlingsansvarlige skal kjenne alle relevante og nødvendige opplysninger for å kunne fatte et vedtak kan medføre at det også innhentes noe overskuddsinformasjon, noe som igjen kan komme i konflikt med den registrertes ønske om mest mulig diskresjon. I slike tilfeller må de ulike personverninteressene veies mot hverandre.

16. Avveining mot andre hensyn

Når tiltakets konsekvenser for personverninteressene er systematisert, og risikoen knyttet til de ulike behandlinger av personopplysninger er kartlagt, må konsekvensvurderingen avsluttes med avveininger av personvernkonsekvenser mot andre hensyn knyttet til det foreslåtte tiltaket.

Et eksempel på et saksområde hvor denne type vurderinger er relevante, er samfunnets ønske om kontroll med bruk av trygdemidler. Dette kontrollønsket fører med seg omfattende innsamling og behandling av personopplysninger om trygdemottakerne, ofte fra andre offentlige etater og helsetjenesten, men også fra private virksomheter som forsikringsselskap. Slik utveksling av informasjon effektiviserer kontrollen, men svekker prinsippet om at opplysninger som hovedregel bare skal benyttes til det opprinnelige innsamlingsformålet (formålsbestemthetsprinsippet), et viktig personvernrettslig prinsipp. I slike saker må det foretas grundige vurderinger av myndighetens kontrollbehov opp mot borgernes behov for beskyttelse av deres personlige integritet. Som argument for kontroll og informasjonsutveksling finner vi effektivitetshensyn og økonomiske hensyn. På personvernsiden finner vi bl.a. hensynet til diskresjon, hensynet til tillitsforholdet mellom lege og pasient, og den registrertes behov for kontroll med flyt av egne opplysninger. I den enkelte sak må det foretas en konkret vurdering av de ulike argumentene mot hverandre. I tillegg må det vurderes tiltak som kan minske evt. personvernulemper til et minimum, så som informasjonstiltak, begrensinger i tilgangen til informasjonen internt i en etat og bruk av personvernfremmende teknologier (som for eksempel logging av tilgang til personopplysninger).

d) Konklusjoner

17. Konklusjon av personvernanalysen og begrunnelse for valgene

Basert på analysen gjort i samsvar med de ovenstående punktene skal man ende opp med det tiltaket som på best mulig måte er egnet til å realisere det målet man har satt seg samtidig som det ivaretar sentrale personvernhensyn og eventuelle andre hensyn som skal tas i betraktning. Det må gis en tilfredsstillende redegjørelse for resonnementene som ligger til grunn for de valg som gjøres.

VII Oppsummering/avslutning

Personvern kan oppsummeres som et knippe ideelle interesser individet har i beskyttelse av personlig integritet og privatlivets fred. Personvernlovgivningen er et virkemiddel for å ivareta disse interessene. Personvernreguleringen er sektorovergripende, og svært mange offentlige og private tiltak vil ha i seg elementer som tilsier at det foretas en vurdering av tiltakets personvernmessige konsekvenser.

Tiltak kan ha vesentlige personvernmessige konsekvenser som innebærer at de skal utredes i henhold til utredningsinstruksen. De personvernmessige konsekvensene bør vurderes på ulike stadier i utredningsprosessen for å sikre grundig utredning. Dersom personvernkonsekvensene viser seg å være vesentlige, skal de vies særskilt oppmerksomhet i høringsnotatet.

En vurdering av personvernmessige konsekvenser bør bestå av en vurdering av tiltaket i forhold til de ulike personverninteressene, og en forholdsmessighetsvurdering der både forholdet til andre aktuelle personvernhensyn og forholdet til øvrige hensyn som gjør seg gjeldende inngår. Det må blant annet vurderes om behandling av de aktuelle personopplysningene er nødvendig og egnet til å oppnå det ønskede formålet. I høringen av en sak som reiser vesentlige personvernspørsmål, vil det ofte være hensiktsmessig å invitere til innspill om nettopp disse spørsmålene, for på denne måten å sikre grundigst mulig behandling av spørsmålene.

VIII Informasjon på nett:

Artikkel 29-gruppen (EUs datatilsynsmyndigheter): http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

Datatilsynet: www.datatilsynet.no

Du Bestemmer: www.dubestemmer.no

EU Kommisjonens personvernsider: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

Nettvett: www.nettvett.no

NOU 1997:19 – Et bedre personvern: http://www.regjeringen.no/nn/dep/jd/Dokument/NOU-ar/1997/NOU-1997-19.html?id=140970

Personvern på nett: http://www.personvern.uio.no/pvpn/index.html

Personvernkommisjonen: www.pvk.no

Personvernnemnda: www.personvernnemnda.no

Stortingsmelding nr. 17 (2006-2007) Eit informasjonssamfunn for alle: http://www.regjeringen.no/nn/dep/fad/kampanjer/Eit-informasjonssamfunn-for-alle.html?id=445374&epslanguage=NO-NY

Teknologirådet: www.teknologiradet.no

Utredningsinstruksen: www.regjeringen.no/nb/dep/fad/dok/Lover-og-regler/reglement/2005/utredningsinstruksen.html?id=107582

IX Litteraturliste

- Apenes, Georg: Panoptikon – Vårt gjennomsiktige samfunn; Geelmunden.Kiese 2000
- Apenes, Georg: Fra tillit til kontroll – tolv samtaler om politikk, teknologi og personvern; PAX 2005
- Bing, Jon: Personvern i faresonen; Cappelen 1991
- Johansen, Kaspersen og Skullerud: Personopplysningsloven: Kommentarutgave; Universitetsforlaget, 2001
- Bygrave, Lee: Personvern i praksis: Justisdepartementets behandling av klager på Datatilsynets enkeltvedtak 1980-1996; Cappelen Akademisk Forlag 1997
- Schartum og Bygrave: Personvern i samfunnet; Fagbokforlaget 2004
- Coll og Lenth: Personopplysningsloven – en håndbok; Kommunerlaget 2000
- Engelschiøn, Ullrichsen og Nilsen: Helseregisterloven. Kommentarutgave; Universitetsforlaget 2002
- Djønne, Grønn og Hafli: Personregisterloven med kommentarer; TANO 1987

X Personopplysningsloven, forarbeider

- NOU 1997:19: Et bedre personvern – forslag til lov om behandling av personopplysninger
- Ot.prp. nr 92 (1998-1999): Om lov om behandling av personopplysninger
- Inst. O. nr. 51 (1999-2000): Innstilling om lov om behandling av personopplysninger

Utgitt av:
Fornyings- og administrasjonssdepartementet

Offentlige institusjoner kan bestille
flere eksemplarer fra:
Departementenes servicesenter
Post og distribusjon
E-post: publikasjonsbestilling@dss.dep.no
Faks: 22 24 27 86

Publikasjonskode: P-0949 B
Trykk: Lobo Media AS 10/2008 – opplag 2000