Hvordan oppfylle hovedkravene i personopplysningsloven?

- En veiledning for kommuner og fylkeskommuner

IKA KONGSBERG
Interkommunalt arkiv for Buskerud, Vestfold og Telemark IKS

Forord

Med personopplysningsloven med forskrift har kommunene fått et økt ansvar med tanke på behandling av personopplysninger. Hvilke oppgaver er nye, hvordan skal kommunene forholde seg til det nye lovverket. Hvilke praktiske konsekvenser får denne, og hvordan oppfyller man kravene på best mulig måte. Etter at loven med forskrift trådte i kraft 1. januar 2001 har disse spørsmålene fra kommunene meldt seg.

For å hjelpe kommunene våre og for å styrke egen kompetanse, ble det satt ned en arbeidsgruppe som kunne samarbeide ut i fra ovennevnte problemstillinger.

Arbeidet med veiledningen startet sommeren 2003. Arbeidsgruppa har bestått av Torill Sveberg, Horten kommune, Ann Kristin Marumsrud, Tinn kommune, Anna-Brita Bakken, Buskerud fylkeskommune, Gunhild Solheim, Hole kommune samt June Wahl fra IKA Kongsberg. Tore Somdal-Åmodt, Oslo Byarkiv, har stilt opp som referanseperson for gruppa, og kommet med tilbakemelding på dokumentet underveis.
Møteaktiviteten har ikke vært stor, men via e-post og telefoner har vi kommet i havn med produktet vi hadde for øye å få til.

På arkivlederdagen 29. oktober ble veiledningen lagt frem for de deltagende arkivlederne, hvor vi hadde en gjennomgang og diskusjon rundt denne. Det var udelt positiv mottagelse og vi konkluderte med at dette var i høyeste grad et produkt vi så nytten av.

Målet med veiledningen har vært å lage en kort oversikt over hva som er nytt, samt tips til hva man må sette seg inn i og jobbe med for å kunne tilfredsstille kravene i loven.

Vi håper at dette målet er nådd, og på vegne av arbeidsgruppa og IKA ønsker vi dere lykke til med utfordringene som venter.

Kongsberg 9. januar 2004

June Wahl
Rådgiver, IKA Kongsberg

Innhold

Innledning

I 2001 trådte personopplysningsloven (pol) i kraft. Med denne loven har vi fått en del nye bestemmelser, mens gamle bestemmelser i personregisterloven har falt bort.

Tanken bak denne veiledningen er å gi en oversikt for kommunene i hva som er nytt i forhold til personregisterloven, hvordan ta fatt på de nye bestemmelsene og hvordan oppfylle hovedkravene i loven rent praktisk.

Kort definisjon av sentrale begrep, se pol § 2:
- Personopplysninger,
  opplysninger og vurderinger som kan knyttes til en enkeltperson
- Sensitive personopplysninger,
  personopplysninger som er underlagt et strengere vern enn andre personopplysninger, se § 2, nr 8.
- Behandlingsansvarlig,
  den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes
- Behandling,
  enhver bruk av personopplysninger, som f.eks innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter
- Databehandler,
  den som behandler personopplysninger på vegne av den behandlingsansvarlige

De viktigste bestemmelsene jfr. personopplysningsloven:
- Samtykke
- Informasjonssikkerhet og internkontroll
- Utvidet innsyns- og informasjonsrett
- Retting og sletting av opplysninger
- Meldeplikt og konsesjonsplikt

Behandlingsansvarlig:
Den som har bestemmelsesrett over personopplysningene, som bestemmer formålet med behandlingen og hvilke hjelpemidler som skal brukes for å oppnå formålet. Det daglige behandlingsansvaret kan i en kommune delegeres til en underliggende etat, skole eller helseinstitusjon. Lederen i dette underliggende organet får dermed et selvstendig ansvar for at personoppysningslovens regler blir fulgt. Kommunenes ledelse kan imidlertid ikke fraskrive seg sitt "rettslige" behandlingsansvar ved delegering. Ved eventuelle lovbrudd er det kommunen, representert ved ordføreren, som er rettslig ansvarlig og som kan saksøkes og pådra seg straffeansvar.

1. Samtykke

Pol §8
Forskriftens §§ 3-1, 7-14, 7-15, 7-16, 7-25, 8-4

Som hovedregel skal man alltid ha et samtykke før man starter behandling av personopplysninger. Et samtykke skal være frivillig, uttrykkelig og informert. Dette kan gis både muntlig og skriftlig, evt. elektronisk. Vi anbefaler skriftlig samtykke så langt dette lar seg gjøre. Her bør kommunen ha et standard skjema til utfylling.

Husk at i en persons kontakt med forvaltningen ligger det gitt et samtykke til behandling av personopplysninger.

Særskilt samtykke er ikke nødvendig å innhente dersom behandlingen er nødvendig for a) å oppfylle en avtale med den registerte, eller for å utføre gjøremål etter den registrertes ønske før en slik avtale inngås, b) at den behandlingsansvarlige skal kunne oppfylle en rettslig forpliktelse, c) å vareta den registrertes vitale interesser, d) å utføre en oppgave av allmenn interesse, e) å utøve offentlig myndighet, eller f) at den behandlingsansvarlige eller tredjepersoner som opplysningene utleveres til kan vareta en berettiget interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen.
Her kan det også finnes annet lovverk som tilsier at behandlingen skal skje.

1.1 Informert samtykke

Samtykket skal være informert. Den som skal registreres må få tilstrekkelig informasjon til å forstå hva samtykket gjelder og hvilke konsekvenser det kan få. Informasjonen til den registrerte skal minst omfatte:
- navn og adresse på den behandlingsansvarlige
- hva opplysningene skal brukes til
- om opplysningene vil bli utlevert til andre, og eventuelt hvem som er mottager
- om det er frivillig å gi fra seg opplysningene
- informasjon som gjør den registrerte i stand til å bruke sine rettigheter etter personopplysningsloven på best mulig måte, som f.eks om retten til å kreve innsyn, retting og sletting
- hvor lenge personopplysningene vil bli behandlet eller oppbevart

1.2 Frivillig samtykke

Et frivillig samtykke er et samtykke som ikke er avgitt under tvang, verken fra den behandlingsansvarlige eller fra andre.

Det er ikke alltid lett å se om samtykket er frivillig. Eksempler på dette kan være når en virksomhet stiller et samtykke som vilkår for å tilby en eller annen tjeneste eller for å ansette en person. Vil man ha jobben eller forsikringen, må man samtykke. Spørsmålet om samtykket er frivillig eller ikke må avgjøres konkret i det enkelte tilfelle: Hva spørres det etter? Hvor belastende vil et samtykke være? Er konsekvensene uforholdsmessige om man ikke samtykker?

1.3 Uttrykkelig samtykke

Samtykket skal være uttrykkelig. Når virksomheten ønsker å behandle opplysninger om en person, må personen foreta seg noe aktivt for å samtykke, som å sende inn en svarslipp eller liknende.

1.4 Hvordan skal samtykket gis

Den som skal registreres kan samtykke muntlig eller skriftlig, elektronisk eller på papir. Det må imidlertid gå klart og utvetydig fram:
- at den registrerte samtykker
- hvilke behandlinger samtykket omfatter

- hvilke behandlingsansvarlige samtykket rettes til

Den behandlingsansvarlige skal kunne sannsynliggjøre at samtykket er gitt. Dette er lettere dersom samtykket er gitt skriftlig.
Et eksempel kan være: samtykke gitt i form av medlemskap i en fagforening.

1.5 Kan samtykket gis av umyndige?

Som hovedregel kan bare myndige personer samtykke. Vergen må samtykke for mindreårige og umyndiggjorte. Samtykke fra mindreårige må likevel kunne oppfylle samtykkekravet i loven. Dette gjelder dersom det ikke dreier seg om sensitive personopplysninger, og man kan forvente en tilstrekkelig modenhet til å overskue hva et samtykke innebærer. Annen lovgivning kan bestemme andre aldersgrenser.

2. Informasjonssikkerhet og internkontroll

Pol §§13 og 14
Forskriftens kap 2, 3 og 8

Hjemmel for informasjonssikkerhet: Personopplysningsloven (pol)
Personopplysningsforskriften (forskriften)

Loven stiller av personvernhensyn krav til informasjonssikkerhet og internkontroll. Andre lover kan ha bestemmelser som også stiller krav til sikkerhet, av andre grunner. Som eksempel nevnes *Sikkerhetsloven av 20 mars 1998 nr 10*. Her er det både den enkeltes rettssikkerhet som beskyttes - i tillegg til rikets selvstendighet, sikkerhet og nasjonale sikkerhetsinteresser.

- Informasjonssikkerhet vil si å sikre kommunenes behandling av personopplysninger.

  Begrepet informasjonssikkerhet omfatter:
  - sikring av *konfidensialitet*, dvs. beskyttelse mot at uvedkommende får innsyn i opplysningene
  - sikring av *integritet*, dvs. beskyttelse mot utilsiktet endring av opplysningene
  - sikring av *tilgjengelighet*, dvs. sørge for at tilstrekkelig og relevante opplysninger er til stede

- Internkontroll vil si at kommunen må ha et system som sikrer at det man er pålagt i loven utføres på best mulig måte.

  Internkontroll innebærer at behandlingsansvarlig skal ha:
  - kjennskap til gjeldende behandlingsregler
  - tilstrekkelig og oppdatert dokumentasjon for gjennomføring av rutinene
  - ha denne dokumentasjonen tilgjengelig for innsyn

2.1 *Informasjonssikkerhet og ansvar*

Som kommunens rettslige representant har ordføreren det øverste ansvaret (dvs. behandlingsansvaret) for at kommunen etterlever kravene til informasjonssikkerhet og internkontroll.

Ansvar kan ikke delegeres, men oppgavene kan. Kommunen må – ved delegasjon – sørge for lovlig delegasjonsvedtak til for eksempel administrasjonen ved rådmannen, som igjen – etter alminnelige delegasjonsregler – kan videredelegere til aktuelle sektorledere. Det er viktig at informasjonssikkerhet forankres i ledelsen innenfor alle forvaltningsgrenene.

I kommuner av en viss størrelse bør det være to sikkerhetsansvarlige:

Kontrollerende ansvar:
- ansatt med ansvar for utarbeidelse av retningslinjer, oppdatering av rutiner, tilsyn, informasjon til ledelse og ansatte

Utøvende ansvar:
- IKT-enheten

Alle ledere har ansvar for sine sektorer og alle saksbehandlere har ansvar for sine oppgaver. Sikkerhet er et ledelsesansvar så vel som et fellesansvar.

Behandlingsansvarlig er pålagt å sørge for tilfredsstillende informasjonssikkerhet. For å oppnå dette må man kunne dokumentere informasjonssystemet og sikkerhetstiltakene, jfr.§ 13. Da må man foreta flere vurderinger, som:

Risikovurdering:
- krav til sikkerhet vil være forskjellige for de ulike typer behandling – behandlingsansvarlige må vurdere konkret hvert tilfelle (risikovurdering). Hvilke personverntrusler kan opplysningene være utsatt for? Risikoen for ikke tilfredsstillende behandling iht lovens krav om sikkerhet.
- risikovurderingen skal ta utgangspunkt i behandlingens formål og personopplysningenes omfang og art.
- hvilke krav til konfidensialitet/tilgjengelighet/integritet som gjelder i kommunen
- vurdere risikoen for at kravene i loven ikke kan oppfylles og sannsynligheten for sikkerhetsbrudd som en følge av dette
- fare for trusler som for eksempel menneskelige feil, innbrudd/hacking, feil i programvare, temperaturpåvirkning, vanninntrenging osv.

Tiltaksvurdering (svar på risikovurdering):
Nødvendige tiltak for å oppfylle lovens krav til informasjonssikkerhet er bl.a.
- Tekniske tiltak
- brannmur
- passord
- automatisk back-up
- skriveres plassering

Organisatoriske tiltak:
- klare ansvars- og myndighetsforhold
- kompetanse hos ansatte
- gradering av tilgang til personopplysninger
- grunnlaget for valg av tiltak finnes under avsnittet internkontroll (se nedenfor).

Behandlingsansvarlige må skriftlig dokumentere sikkerhets- og tiltaksvurderingen. Dersom det skjer endringer i behandlingen som influerer på sikkerhet/ansvar/tiltak, må det foretas ny

vurdering. Denne dokumentasjonen skal være tilgjengelig for ansatte, Personvernnemnda og Datatilsynet.

Det skal legges vekt på å sikre at opplysningenes kvalitet er gode nok i forhold til formålet med behandlingen.

2.2 Oversikt over hva kommunen bør ha på plass for å etterleve kravene i §§ 13 og 14:

- Sikkerhetsledelse / sikkerhetsorganisasjon
- Sikkerhetsinstruks
- Sikkerhetsrevisjon
- Risikovurdering av systemer, rom, teknologi, personer og rutiner og beskrivelse av akseptabelt risikonivå
- Tiltaksanalyse – prioritering av tiltak
- Avviksbehandling ved sikkerhetsbrudd og opptreden i strid med gjeldende instrukser /rutiner

2.2.1 Dokumentasjon

Ved utarbeidelse av dokumentasjon bør kap 2 i forskriften brukes samt Datatilsynets "Sikkerhetsbestemmelser i personopplysningsforskriften med kommentarer".

Eksempler på dokumentasjon:

Styrende dokumenter

Sikkerhetsinstruks
- sikkerhetsmål
- sikkerhetsstrategi
- sikkerhetsansvar

Oversikt over organisasjons- og konfigurasjonsstrukturen

"Daglige" dokumenter:

Hendelsesregistrering
Rutinebeskrivelser
Rapporter
Taushetserklæring
Oppfølging av styringssystemet
- Avviksbehandling
- Risikovurdering
- Ledelsesgjennomgang
- Sikkerhetsrevisjon

Sikkerhetstiltak, jfr. tiltaksanalysen
- Personell/fysiske tiltak
- Konfidensialitet
- Tilgjengelighet
- Integritet

2.3 Hvordan skal kommunen gå frem for å etablere internkontroll

På Datatilsynets hjemmesider er det lagt ut en del veiledninger og retningslinjer som er til god hjelp i arbeidet:
- Retningslinjer for informasjonssikkerhet
- Etablering av internkontroll
- Sikkerhetsbestemmelsene i personopplysningsforskriften (se Datatilsynets veiledning)*
- Risikovurdering av informasjonssystem
- Utkast til veiledning i informasjonssikkerhet

Annet:
- Forskrift til personopplysningsloven, klikk her
- Personopplysningsloven – en håndbok, Line M. Coll og Claude A. Lenth
- Personopplysningsloven, kommentarutgave av Wiik Johansen, Kaspersen og Bergseng Skullerud. Universitetsforlaget.

2.3.1 Internkontroll

Internkontrollen skal:
- sikre at personopplysningene har tilstrekkelig kvalitet (korrekte, fullstendige, oppdaterte og relevante for formålet med behandlingen § 11 stiller krav til kvalitet)
- være nødvendighetsvurdert (hvilke tiltak må oppfylles for å oppfylle kravene til behandling samt sikre opplysningenes kvalitet)

Dette danner grunnlaget for valg av organisatoriske og tekniske tiltak.

2.3.2 Systemkartlegging

Eget skjema bør utarbeides i kommunen. (se forslag til skjema - klikk her)
Skjemaet skal inneholde bl.a.:
- type system
- hva det brukes til
- sikkerhets- og kontrollrutiner (er dette utarbeidet)
- tilgangskontroll

Alle enheter/sektorer skal fylle ut skjemaet – helhetlig oversikt. Det enkelte system/program må vurderes mht meldeplikt.

Konfigurasjonskart utarbeides (hvordan datanettet er bygget opp).

Sikkerhetsrevisjon (forskriftens § 2-5):
Informasjonssystemer skal gjennomgås jevnlig slik at man er sikker på
- hensiktsmessighet mht kommunens behov
- sikkerhetsstrategien er tilfredsstillende

*Sikkerhetsbestemmelsen har kommentarer til alle paragrafene i kap 2 og forklarer og utdyper disse på en instruktiv måte og tydeliggjør hva som må være med i en slik instruks. Risikovurdering av ny programvare og nye systemer må alltid foretas.

Lukket nett/åpent nett (internt åpent) – hvor ligger opplysningene. Vurdering av hva som faktisk er sensitive opplysninger bør foretas.

3. Utvidet innsyns- og informasjonsrett

Pol §§18, 19 og 20
Forskriftens kap 3, 4 og 8

Kommunen må ha god oversikt over behandlingene de foretar i tilegg til gode rutiner for å gi informasjon. Alle som ber om det, har krav på såkalt grunninformasjon om hvilke behandlinger behandlingsansvarlig foretar.

Er man registrert har man i tillegg krav på å bli informert om:
- hvilke opplysninger som er registrert om en selv
- hvordan opplysningene er sikret
- til hvilket formål opplysningene behandles
- til hvem opplysningene utgis

Kommunen skal informere på eget initiativ. Kommunen har informasjonsplikt både når personopplysningene samles inn direkte fra den det gjelder, og når de samles inn fra tredje part (andre enn den registrerte selv) – her finnes flere unntak, se § 23.

4. Retting og sletting av opplysninger

Pol §§27 og 28
Forskriftens §§ 5-3 og 8-4

Som hovedregel skal ikke arkivmateriale slettes med mindre det finnes klar hjemmel for dette i arkivloven. Sletting etter personopplysningsloven kan bare skje etter at Riksarkivaren har fått anledning til å uttale seg.

Behandlingsansvarlig har plikt til å rette og slette opplysninger når disse er klart feilaktige, mangelfulle eller unødvendige. Dette gjøres på eget initiativ eller etter anmodning.
Å rette personopplysninger gjøres ved at man markerer og legger til korrekte opplysninger. Dersom et dokument blir klart misvisende ved retting av personopplysninger skal hele dokumentet slettes.

Alle kommuner er pliktige til å bevare dokumentasjon som nevnt i de retningslinjer for arkivbegrensning og kassasjon i kommunale arkiv, se Forskrift om Riksarkivarens arkivbestemmelser V, gitt med hjemmel i forskrift av 11. desember 1998 nr 1193 om offentlige arkiv § 3-21 og § 5-8.
Er kommunen i tvil om hva som skal bevares bør dette tas opp skriftlig med IKA Kongsberg.

5. Meldeplikt og konsesjonsplikt

Pol §§ 31 og 32
Forskriftens kap 7

Hovedregelen er at all behandling av personopplysninger, som behandles med elektroniske hjelpemidler, er meldepliktig, mens behandling av sensitive personopplysninger er konsesjonspliktig.

Kommuner som ønsker å sette i gang en behandling av personopplysninger skal melde til Datatilsynet senest 30 dager før behandlingen starter. Dette gjøres på eget meldeskjema. Skjemaet finnes på Datatilsynets internett sider. Datatilsynet foretrekker at meldingen sendes elektronisk. Kommunen mottar så en kvittering fra Datatilsynet. Dette er kun en kvittering på at meldingen er mottatt, ikke på at behandlingen tilfredsstiller kravene i loven.
Ny melding må sendes tilsynet om formålet endres eller det blir en ny juridisk person som overtar ansvaret for behandlingen.

Hovedregel:
- Meldeplikt for sensitive manuelle personregistre og elektroniske behandlinger av personopplysninger
- Konsesjonsplikt for elektroniske behandlinger av sensitive personopplysninger
- Men: Mange generelle og spesielle unntak.

Behandlingsansvarlig har krav på å få vite i forkant om en behandling er konsesjonspliktig av Datatilsynet.

Følgende behandling av personopplysninger i kommunen som har hjemmel i egen lov, er unntatt konsesjonsplikt, § 33, men underlagt meldeplikt, § 31.
Herunder nevnes følgende:
- Barnevern
- Sosialtjenesten
- PP-tjenesten
- Grunnskolen
- Videregående skole og fagopplæring
- Pleie og omsorg
- Familievernkontorer
- Kontantstøtteregister
- Kommunehelsetjenestens pasientjournaler / pasientadministrasjon innen rammen av helsepersonelloven § 26
- Fylkestannlegens pasientjournaler / pasientadministrasjon innen rammen av helsepersonelloven § 26

Behandlinger som er unntatt både konsesjonsplikt og meldeplikt:
- kommunale og private barnehager
- personellregistre, så sant de er innenfor rammen av personopplysningsforskriften § 7-16

Dette er i hovedsak de registrene som er unntatt konsesjonsplikt og meldeplikt, men det kan også være flere typer registre. Det anbefales da å ta kontakt med Datatilsynet.

Vær bevisste på hva dere faktisk legger av opplysninger og dokumentasjon i mappene, dette er avgjørende for om behandlingen er meldepliktig eller konsesjonspliktig. Husk formålet!

Systemnr.
XX

tilbake

Kommune-våpen	IT-sikkerhet NN kommune **Virksomhet …….**

Kartleggingsskjema

Formålet med dette skjemaet er å kartlegge alle de systemene som går inn under NN kommunes ansvarsområde, for å finne ut hvor det finnes sensitiv informasjon.

Vennligst fyll ut skjemaet nedenfor for hvert av de systemene du kjenner til innenfor din virksomhet. Bruk ett skjema per system.

1. Systemet (Applikasjonen)	
Systemnavn	_____

2. Sted:	
Avdeling eller institusjon som har ansvaret for systemet:	
Maskinnavn hvor systemet er installert:	
Nettsegment maskinen er plassert:	
Hvilke avdelinger / brukere er det på systemet	

3. Ansvar:	
Systemansvarlige:	
Telefonnummer:	
Faksnummer:	
E-postadresse:	

4. Konsesjon/meldeplikt (Hvor det ikke finnes hjemmel i særlov):	
Foreligger det konsesjon/meldeplikt for dette systemet/denne maskinen? (kryss av)	☐ *Søknad er under behandling* ☐ Konsesjon foreligger ☐ ☐ Meldt til datatilsynet Ingen konsesjon
Dersom konsesjon foreligger, hvilket konsesjonsnummer har systemet/maskinen?	(*Om hjemmel i særlov, angi denne)*

5. Beskrivelse av systemet:

a) Hva brukes systemet til? *Skriv kort om bruksområde*	
b) Hvilke personopplysninger lagres i systemet ? *Vennligst gi utfyllende opplysninger, bl a om formålet med behandlingen av personopplysningene*	
c) Annen relevant informasjon om systemet:	

6. Leverandørinfo:	
Leverandørnavn:	
Leverandøradresse:	
Telefon-/faxnummer:	
E-postadresse:	
Kontaktperson teknisk	

7. Dette skjemaet er utfylt av:	
Navn:	
Stilling:	
Tilhører virksomhet:	
Telefonnummer:	
Faksnummer:	
E-postadresse:	
Sted og dato:	