Datatilsynet

Kommunens Internkontroll

Verktøy for rådmenn

Et redskap for å kontrollere kommunens etterlevelse av personopplysningsloven

2012

Innhold

Til deg som er rådmann

Undersøkelser har vist at kommunal sektor har utfordringer i forhold til etterlevelse av bestemmelsene i personopplysningsloven[1]. For å hjelpe deg som rådmann å kartlegge situasjonen i egen kommune, har Datatilsynet laget dette verktøyet.

Verktøyet er lagt opp som en sjekkliste med 49 spørsmål, der kommunen ideelt sett skal svare ja på alle relevante spørsmål. Da etterlever kommunen personopplysningsloven på en god måte. For de spørsmål der svaret er nei, må kommunen sørge for å innføre tiltak, sikre dokumentasjon, eller bygge opp systemer for å sikre at loven etterleves. Datatilsynet anbefaler at rådmannen ber den eller de i kommunen som jobber med informasjonssikkerhet og personvernrelaterte oppgaver å bidra til å fylle ut sjekklisten.

Dersom kommunen, etter å ha gått gjennom sjekklista, har behov for videre hjelp til å komme i gang med arbeidet kan dere finne nyttige veiledere og maler på Datatilsynets hjemmeside[2]. Disse vil hjelpe kommunen i gang med arbeidet med å sikre etterlevelse av personopplysningsloven.

Hvordan dokumentet er bygd opp

Regelverket inneholder en rekke krav og påbud formulert for eksempel slik: ”behandlingsansvarlig skal…” og ”behandlingsansvarlig må…”. Det kan være vanskelig å tolke hva disse betyr ut av den juridiske konteksten. I sjekklisten er regelkravene omsatt til påstander som kommunen svarer ”ja” eller ”nei” på. Sjekklisten er delt inn i fire hoveddeler:

- **Styrende del** – av overordnet karakter. Retter seg hovedsakelig mot ledelsen.
- **Gjennomførende del** – mer praktisk orientert. Dreier seg om rutiner som sikrer at de ansatte følger regelverket.
- **Kontrollerende del** – gjelder kontrollrutiner som sikrer at kommunen etterlever regelverket.
- **Andre forhold** – tar for seg andre viktige elementer som taushetsplikt og forholdet til andre virksomheter.

Oppfølging av resultatet

Internkontroll er kommunens verktøy for å sikre etterlevelse av personopplysningsloven. Resultatene av sjekklisten gir rådmannen en oversikt over status for internkontroll. Dette gir et godt grunnlag for å vite eventuelt hvilke grep kommunen bør ta dersom det er behov for å bedre regeletterlevelsen. Dersom det er behov for å gjøre endringer anbefaler Datatilsynet at rådmannen for eksempel nedsetter en arbeidsgruppe som tar fatt i de kartlagte utfordringene. Datatilsynets veiledere vil være nyttige verktøy for en slik arbeidsgruppe.

[1] Se Datatilsynets rapport ”Kommuneundersøkelsen 2010-2011”.
[2] http://www.datatilsynet.no/informasjonssikkerhet

Styrende del

I denne delen av sjekklisten måles kommunen på om ledelsen er bevisst sitt overordnede ansvar, at behandling av personopplysninger skjer på tilstrekkelig juridisk grunnlag og at kommunens har kartlagt sine plikter i tilstrekkelig grad.

Ansvar og grunnlag for å behandle personopplysninger

En viktig forutsetning for å ivareta etterlevelse av regelverket er at ansvaret for og organiseringen av arbeidsoppgavene knyttet til internkontroll er tydelig for de ansatte. Først og fremst må kommunen være kjent med hvilke krav i regelverket som er gjelder dem. Når dette er etablert må kommunen kartlegge hvilke behandlinger av personopplysninger kommunen utfører.

Behandlingsansvar

1. Kommunen har en dokumentert oversikt over hvem som er ansvarlig for behandling av personopplysninger.

❍ *Ja* ❍ *Nei*

Kartlegging av personopplysninger som behandles

Kommunen bør ha en liste med oversikt over hvilke personopplysninger den behandler. Oversikten over behandlinger må blant annet inneholde det juridiske grunnlaget for og formålet med behandlingen. Dette skal også dokumenteres. Mange av kommunenes behandlinger er hjemlet i lov. Disse bør være med i listen.

I andre tilfeller behandler kommunen personopplysninger om innbyggerne etter deres samtykke. I listen må det fremgå tydelig hvilke behandlinger som kun gjøres med innbyggernes samtykke, og hvordan dette skal innhentes. Dersom det oppstår nye formål for behandling av personopplysningene, må kommunen sørge for at det foreligger et nytt juridisk grunnlag. Alle nye behandlinger skal også oppdateres i oversiktslistene.

Datatilsynet anbefaler at det enten lages en liste over alle behandlinger eller at listene over de ulike behandlingene sammenstilles, slik at det foreligger en samlet oversikt.

2. Kommunen har en skriftlig oversikt over hvilke personopplysninger som behandles.

❍ *Ja* ❍ *Nei*

3. Kommunen har avklart det rettslige grunnlaget for hver behandling

❍ *Ja* ❍ *Nei*

4. Kommunen har dokumentert hvilket formål de ulike opplysningene er samlet inn for.

❍ *Ja* ❍ *Nei*

Klarlegging av plikter

De fleste kommuner behandler mange ulike personopplysninger. Behandlingene vil samtidig gjøres for en rekke formål. Dette betyr at kommunen som en hovedregel må forholde seg til flere krav i personopplysningsloven enn andre virksomheter. For å sikre at kommunen har en oversikt over dette, bør oversikten over hvilke behandlinger som foretas også ha en kolonne for hvilke krav i regelverket som gjelder for hver enkelt behandling.

5. Kommunen har en oversikt over hvilke krav i personopplysningsloven og tilhørende forskrift som gjelder for den.

❍ *Ja* ❍ *Nei*

Rammer for informasjonssikkerhet

Loven krever at personopplysninger skal sikres på en tilfredsstillende måte. Det innebærer at kommunen skal ha en sikkerhetsstrategi som beskriver arbeidet med informasjonssikkerhet. Samtidig skal kommunen kunne dokumentere at det er god sikkerhet i valgte løsninger.

Den behandlingsansvarlige, det vil si kommunen, skal selv sette mål for sikkerhetsarbeidet gjennom sine sikkerhetsmål.

Gjennom å utforme sikkerhetsmål, sikkerhetsstrategi samt akseptkriterier fastlegges rammene for kommunes arbeid med informasjonssikkerhet. For å avgjøre om kommunen ligger innenfor selvdefinerte rammer må det gjennomføres en risikovurdering. Det vil som regel være IT-ekspertene i kommunen som utfører dette arbeidet. Datatilsynet har egen veileder om risikovurdering[3].

En kommune som gjennomfører en grundig vurdering av rammene for sikkerhetsarbeidet som resulterer i fastsetting av sikkerhetsmål og sikkerhetsstrategi, siker sine data på en kostnadsoptimal måte. Det er viktig at rammene fastsettes gjennom tett samarbeid mellom rådmannen og IT-faglig personell.

Etter å ha gjennomført en risikovurdering som er vurdert mot akseptkriterier, må kommunen etablere en fungerende sikkerhetsorganisasjon.

6. Kommunen har fastsatt sikkerhetsmål

❍ *Ja* ❍ *Nei*

7. Kommunens valg og prioriteringer i sikkerhetsarbeidet er beskrevet i en sikkerhetsstrategi

❍ *Ja* ❍ *Nei*

[3] http://www.datatilsynet.no/templates/article 888.aspx

8. Sikkerhetsmål og sikkerhetsstrategi blir gjennomgått jevnlig (for eksempel hvert år) for å klarlegge at strategiene dekker kommunens behov

   ❍ *Ja* ❍ *Nei*

9. Kommunen kan, basert på egne sikkerhetsmål og sikkerhetsstrategi, gi uttrykk for hva som er akseptabel risiko (det vil si hva som er kommunens akseptkriterier).

❍ *Ja* ❍ *Nei*

10. Kommunen har gjennomført en risikovurdering som dokumenterer at risikoen for sikkerhetsbrudd ligger innefor kommunens fastsatte akseptkriterier (som beskrevet i sikkerhetsmålene og sikkerhetsstrategien).

❍ *Ja* ❍ *Nei*

11. Kommunen har etablert og dokumentert en sikkerhetsorganisasjon hvor roller og ansvar for informasjonssikkerheter klart definert.

❍ *Ja* ❍ *Nei*

12. Kommunen har en skiftlig, samlet oversikt over informasjonssystemets utforming.

❍ *Ja* ❍ *Nei*

Gjennomførende del

I tilfeller der det juridiske grunnlaget, det vil si formålet, for behandlingen er fastsatt i lov eller forskrift, vil det som regel ikke være noen dialog mellom kommunen og den registrerte før personopplysningene behandles. I slike tilfeller er det tilstrekkelig at kommunen informerer om behandlingene på egne hjemmesider, for eksempel i sin personvernpolicy.

Dersom kommunen ikke har lovhjemlet grunnlag for behandlingen, vil behandlingen normalt være basert på samtykke fra den registrerte eller etter avtale. Kommunen må da forsikre seg om at et samtykke er innhentet eller avtale er inngått. Et samtykke skal være frivillig, uttrykkelig og informert.

Personopplysninger skal som hovedregel slettes når formålet med behandlingen er oppfylt. Innen kommunal sektor er det imidlertid en rekke unntak som pålegger kommunen å lagre opplysningene etter at de er behandlet, for eksempel en særlov som arkivloven. Det er kommunens ansvar fortløpende å ta stilling til hvilke personopplysninger som omfattes av unntakene og å sørge for at personopplysningene håndteres korrekt. For eksempel vil flere av kommunens behandlinger være melde- eller konsesjonspliktig til Datatilsynet. Kommunen må ha rutiner for å sjekke hvilke tilfeller de har slike plikter.

13. Kommunen har rutiner som sikrer at innbyggere og andre registrerte får informasjon om sine rettigheter til innsyn i, retting av feil informasjon og supplering av personlig informasjon ved behandling av personopplysninger der behandlingsgrunnlaget er fastsatt i lov eller forskrift.

❍ *Ja* ❍ *Nei*

14. Kommunen har rutiner som sikrer at det innhentes samtykke eller inngås avtale når det vil utgjøre det utgjør behandlingsgrunnlaget.

❍ *Ja* ❍ *Nei*

15. Kommunen har etablert rutiner for sletting av personopplysninger. Disse rutinene er avstemt mot relevante bestemmelser i personopplysningsloven og arkivloven.

❍ *Ja* ❍ *Nei*

16. Kommunen har rutiner for å kontrollere om behandlingen av personopplysninger er konsesjonspliktig før behandlingen tar til.

❍ *Ja* ❍ *Nei*

17. Kommunen har rutiner for å kontrollere om en behandling av personopplysninger er meldepliktig før den gjennomføres.

❍ *Ja* ❍ *Nei*

Daglig informasjonssikkerhet

For at kommunen skal opprettholde god informasjonssikkerhet i den daglige driften, må det innføres en kombinasjon av tekniske og organisatoriske rutiner. Det er viktig å sørge for at alle ansatte følger disse i sitt daglige virke.

Regler for å sikre den daglige informasjonssikkerheten sikrer at kommunens ansatte bruker informasjonssystemet innen de rammer som er bestemt. Formålet med rammene kan for eksempel være å redusere risiko for uønskede hendelser.

18. Kommunen har klare regler for de ansattes bruk av informasjonssystemet, det vil for eksempel si saksbehandlersystemet eller andre IT-ressurser som er tilgjenglig på IT-systemet.

❍ *Ja* ❍ *Nei*

19. Kommunen har sørget for å gjøre de ansatte oppmerksom på reglene.

❍ *Ja* ❍ *Nei*

20. Kommunen har god oversikt over brukerne av informasjonssystemet. Det er fastsatt gode rutiner for tildeling av rettigheter i systemet og for å oppheve slike når det er relevant (eksempelvis ved oppsigelse).

❍ *Ja* ❍ *Nei*

21. Kommunens informasjonssikkerhetssystem har logger som benyttes til å føre kontroll med eventuell misbruk av systemet.

❍ *Ja* ❍ *Nei*

22. Kommunens sikkerhetstiltak er begrenset til tiltak som medarbeidere ikke kan påvirke eller lett omgå.

❍ *Ja* ❍ *Nei*

23. Kommunen har et velfungerende system for sikkerhetskopiering.

❍ *Ja* ❍ *Nei*

24. Kommunens sikkerhetskopier blir testet jevnlig for å sikre at disse fungerer dersom originaldata skulle bli kompromittert.

❍ *Ja* ❍ *Nei*

25. De ansatte er kjent med og har undertegnet avtale om at kommunens internkontroll legges til grunn for eget arbeid. Det vil si at de må forholde seg til internkontrollen i sitt daglige virke.

❍ *Ja* ❍ *Nei*

26. En kommune skal ha rutiner som sikrer at ansatte opptrer riktig i sin arbeidshverdag. Rutinene viser de ansatte hvordan de skal opptre i gitte sammenhenger. Behovet for slike rutiner kan variere fra kommune til kommune. Gå gjennom listen under og svar på om kommunen har etablert rutiner for:

• Bruk av internett	❍ *Ja*	❍ *Nei*	❍ *Ikke relevant*
• Bruk av elektronisk post	❍ *Ja*	❍ *Nei*	❍ *Ikke relevant*
• Utskrift og kopiering	❍ *Ja*	❍ *Nei*	❍ *Ikke relevant*
• Makulering av dokumenter	❍ *Ja*	❍ *Nei*	❍ *Ikke relevant*
• Sikkerhet og orden på eget kontor	❍ *Ja*	❍ *Nei*	❍ *Ikke relevant*
• Adgangskontroll	❍ *Ja*	❍ *Nei*	❍ *Ikke relevant*
• Innleid personell og håndverkere	❍ *Ja*	❍ *Nei*	❍ *Ikke relevant*
• Bruk av hjemmekontor	❍ *Ja*	❍ *Nei*	❍ *Ikke relevant*
• Bruk av bærbare enheter	❍ *Ja*	❍ *Nei*	❍ *Ikke relevant*

Sikring av konfidensialitet

Sikring av konfidensialitet handler om å sikre data eller opplysninger fra uvedkommende. Hvilket behov opplysningene har for beskyttelse vil avhenge av hvilken type personopplysninger en har.

27. Kommunen har etablert tiltak for å sikre tilstrekkelig konfidensialitet for opplysningene som behandles i egne systemer.

❍ *Ja* ❍ *Nei* ❍ *Ikke relevant*

(Ikke relevant velges dersom kommunen har satt bort alle behandlinger til eksterne, det vil si databehandlere)

Sikring av tilgjengelighet

Å sikre tilgjenglighet handler om at personopplysninger skal være tilgjenglig for rette person til rett tid.

28. Kommunen har etablert tiltak for å sikre at ansatte har tilgang til alle relevante personopplysninger som er nødvendig for vedkommendes arbeid.

❍ *Ja* ❍ *Nei* ❍ *Ikke relevant*

Sikring av integritet

Sikring av integritet handler om at personopplysninger ikke skal kunne endres av andre enn personell som er autorisert til å gjøre dette. Hvis opplysninger ikke sikres mot dette, er det en risiko for at utro tjenere kan manipulere eller endre data til ulempe behandlingsansvarlig eller den registerte.

29. Kommunen har sikret seg at *endring av* personopplysninger i systemene kun kan gjøres av autorisert personell.

    ❍ *Ja* ❍ *Nei* ❍ *Ikke relevant*

30. Kommunen har etablert tiltak mot ødeleggende programvare, som for eksempel trojanere eller andre virus.

    ❍ *Ja* ❍ *Nei*

Sikkerhetshendelser

31. Kommunen har sikkerhetstiltak som hindrer uautorisert *bruk av* informasjonssystemet.

    ❍ *Ja* ❍ *Nei*

32. Kommunen har et system som gjør at forsøk på uautorisert bruk av informasjonssystemet blir registrert slik at det kan følges opp videre.

    ❍ *Ja* ❍ *Nei*

Kontrollerende del

Selv om kommunen har dokumenterte rutiner for internkontroll og gode rutiner for daglig informasjonsikkerhet, vil det kunne oppstå avvik. Det kan skyldes at ansatte ikke kjenner rutiner eller at de velger å overse rutinene. I slike tilfeller er det viktig å ha et system som fanger opp brudd. Et tilfredsstillende informasjonssikkerhetssystem forutsetter både jevnlig stikkontroller og at det meldes fra når avvik blir oppdaget. Kommunen skal ha et system for avvikshåndtering. Det betyr at kommunen har skjema både ansatte og ledere kan benytte for å melde fra dersom de oppdager handlinger som avviker fra fastsatt system. I tillegg til skjemaet må kommunen ha et system for hvem og hvordan slike meldinger mottas og følges opp.

33. Kommunen har rutiner for gjennomføring av regelmessige stikkontroller.

    ❍ *Ja* ❍ *Nei*

34. Kommunen har gjennomført stikkontroll av informasjonssikkerhetssystemet i løpet av de 12 siste månedene.

    ❍ *Ja* ❍ *Nei*

35. Kommunen skriver rapport med oppsummering av funn og ved behov forslag til tiltak etter stikkontroll.

    ❍ *Ja* ❍ *Nei*

36. Kommunen har rutiner for å følge opp tiltaksplan fra stikkontroll.

    ❍ *Ja* ❍ *Nei*

37. Kommunen har et system for hvordan avvik som oppstår i det daglige skal håndteres. Det betyr blant annet at de ansatte har mulighet til å rapportere avvik.

    ❍ *Ja* ❍ *Nei*

Sikkerhetsrevisjon av informasjonssikkerhetssystemet

I informasjonssikkerhet skilles det mellom fysisk og logisk sikring. Fysisk sikring omfatter adgangsbegrensning, adgangskontroll, låsing og så videre. Logisk sikring betyr datateknisk beskyttelse av personopplysninger. Eksempler på logisk sikring kan være tilgangsstyring, soneinndeling av datasystem og brannmurer.

En sikkerhetsrevisjon er en komplett revisjon av kommunens datasikkerhet. Revisjonen bør være praktisk orientert og skal gjennomføres regelmessig, for eksempel årlig. En revisjon skal blant annet inneholde kartlegging av kommunens organisering og sårbarhetsanalyse, kontroll og verifisering av sikkerhetstiltak, en konkret gjennomgang av alle relevante løsninger, og dersom kommunen benytter eksterne leverandører, en kontroll av leverandører.

38. Det gjennomføres regelmessige sikkerhetsrevisjoner i kommunen.

    ❍ *Ja* ❍ *Nei*

39. Sikkerhetsrevisjonen omfatter en vurdering av;

- Organisering ❍ *Ja* ❍ *Nei*
- Sikkerhetstiltak ❍ *Ja* ❍ *Nei*
- Bruk av kommunikasjonspartner ❍ *Ja* ❍ *Nei*
- Sikkerhet hos leverandører ❍ *Ja* ❍ *Nei*

40. Kommunen har rutiner for regelmessig gjennomgang av informasjonssystemets fysiske sikkerhet.

    ❍ *Ja* ❍ *Nei*

41. Kommunen har rutiner for regelmessig gjennomgang av den logiske sikringen av informasjon i informasjonssystemet.

    ❍ *Ja* ❍ *Nei*

42. Sikkerhetstiltakene kommunen har, hindrer uautorisert tilgang til annet utstyr av betydning for informasjonssikkerheten, for eksempel serverrom eller sentrale infrastrukturkomponeneter.

    ❍ *Ja* ❍ *Nei*

Andre forhold

I denne delen kartlegges andre forhold det er viktig å få en oversikt over for å ha fullstendig oversikt over informasjonssikkerhetssystemet, for eksempel ansattes taushetsplikt og forholdet til andre virksomheter.

Taushetsplikt

Loven sier at medarbeidere hos den behandlingsansvarlige skal være pålagt taushetsplikt for personopplysninger der konfidensialitet er nødvendig. I praksis betyr det at taushetsplikten normalt kommer til anvendelse i de tilfeller virksomheten behandler beskyttelsesverdige data. Ansatte som håndterer slike data bør undertegne en taushetserklæring.

43. Kommunen har rutiner for å sikre at taushetsplikt etterleves der dette er nødvendig, for eksempel må alle ansatte som behandler beskyttelsesverdige data undertegne en taushetserklæring.

    ❍ *Ja* ❍ *Nei*

44. De ansatte i kommunen har taushetsplikt for informasjon som har betydning for informasjonssikkerheten.

    ❍ *Ja* ❍ *Nei*

Databehandlere

Flere kommuner velger å sette ut hele eller deler av behandling av personopplysninger til andre virksomheter, såkalte databehandlere. En databehandler kan både være en annen kommune som opptrer som vertskommune for flere omkringliggende mindre kommuner eller private tilbydere av tilsvarende. Datatilsynet har utarbeidet en veileder til databehandleravtale som også inneholder et utkast til avtaleskisse. Dokumentene kan lastes ned fra Datatilsynets hjemmesider[4]:

45. Kommunen har oversikt over hvilke databehandlere den bruker, det vil si hvilke eksterne virksomheter som behandler personopplysninger kommunen har ansvar for.

    ❍ *Ja* ❍ *Nei*

46. Kommunen har inngått skriftlig databehandleravtale med alle eksterne virksomheter som behandler eller har tilgang til personopplysninger kommunen har ansvar for.

    ❍ *Ja* ❍ *Nei*

Dokumentasjon

47. Kommunen har skriftlige rutiner for hvordan informasjonssystemet skal brukes og hvordan informasjon med betydning for informasjonssikkerheten er dokumentert

    ❍ *Ja* ❍ *Nei*

[4] www.datatilsynet.no/databehandler

48. Når dokumentasjonen for oppbygging av informasjonssystemet, oppdateres eller erstattes sørger kommunen for at all dokumentasjon for det gamle informasjonssystemet lagres i frem år.

    ❍ *Ja* ❍ *Nei*

49. Kommunen lagrer registreringer av uautorisert bruk og forsøk på uautorisert bruk av informasjonssystemet i minst 3 måneder.

    ❍ *Ja* ❍ *Nei*

50. Kommunen lagrer registreringer av alle hendelser med betydning for sikkerheten i minst 3 måneder.

    ❍ *Ja* ❍ *Nei*

Oppsummering

Når spørsmålene er gjennomgått vil du som rådmann ha en oversikt over hvordan din kommune etterlever personopplysningsloven. For de relevante spørsmål kommunen har svart nei på, må kommunen følge opp videre for eksempel med å sikre dokumentasjon, bygge opp systemer eller på annen måte innføre tiltak for å sikre at lovens krav etterleves.

For å komme i gang med dette arbeidet foreslår Datatilsynet at kommunen benytter veiledningsmateriell og maler. Dette er tilgjenglig på tilsynets nettside: www.datatilsynet.no.