Alle one-pagere

Innhold

1. Behandlingsprotokoll

Behandlingsprotokoll (Del 2 punkt 8 i Datatilsynets rapport)

I brevkontrollen ba Datatilsynet om å få oversendt kommunenes behandlingsprotokoller.

Kommunen er behandlingsansvarlig for behandling av personopplysninger som skjer i kommunens regi. For kommunen som behandlingsansvarlig betyr dette at kommunen må føre en protokoll over alle behandlingsaktiviteter som omfatter behandling av personopplysninger, jf. personvernforordningen artikkel 30.

Det følger av artikkel 30 at protokollene skal være skriftlige og at de på anmodning skal gjøres tilgjengelige for tilsynsmyndigheten.

Protokollen skal blant annet inneholde informasjon om de ansvarlige, formålet med behandlingen, kategorier registrerte, kategorier personopplysninger, eventuelle utleveringer, overføring til tredjeland, om sletting og beskrivelse av sikkerhetstiltak.

Utfordringer/funn i brevtilsynet

Datatilsynet finner at kommunene har høy grad av bevissthet om plikten til å føre protokoll. Funnene i brevkontrollen viser imidlertid en svært varierende grad av modenhet blant kommune og Datatilsynet anslår at så mange som 25-30 prosent av kommunene mangler tilfredsstillende protokoller. Det er videre en utfordring at flere kommuner ikke var i stand til å tilgjengeliggjøre protokollene for tilsynet.

Datatilsynet påpeker at protokollen skal være oppdatert til enhver tid og at det er viktig å ha på plass gode rutiner for gjennomgang og vedlikehold av behandlingsprotokollene.

Veiledning og forslag til tiltak

Kommunene skal føre en skriftlig protokoll over behandlingsaktivitetene de har ansvar for, jf. personvernforordningen art. 30. Protokollen må kunne gjøres tilgjengelig for tilsynet og inneholde informasjonen det stilles krav om i artikkel 30.

Protokollen bør være lett tilgjengelig og forståelig. Kommunen bør ha rutiner for gjennomgang og vedlikehold av behandlingsprotokollene.

Eksempler/ressurser

- Foranalyse av eget ansvarsområde | Digdir
- Hva må jeg gjøre før jeg kan ta i bruk en ny digital tjeneste? - KS
- Slik sikrer du oppfølging av personvern og informasjonssikkerhet - KS
- Protokoll over behandlinger av helse- og personopplysninger i virksomheten (faktaark 13) - ehelse

Kommunedirektørens kontrollspørsmål

- Er ansvaret for etablering av behandlingsprotokoll tydelig plassert i kommunen?
- Har kommunen tilfredsstillende behandlingsprotokoller på plass for alle tjenesteområder?
- Kan behandlingsprotokollen gjøres tilgjengelig for tilsynsmyndigheten?
- Har kommunen rutiner for gjennomgang og vedlikehold av behandlingsprotokollene?

2. Organisering av ansvarsforhold

Organisering av ansvarsforhold (Del 2 punkt 9 i Datatilsynets rapport)

Ansvarlighetsprinsippet i personvernforordningens art. 5 nr.2 stiller omfattende krav til blant annet oversiktlige rammer og ansvar for etterlevelse av personvernregelverket, og fortalepunkt 79 presiserer dette kravet. Flere bestemmelser i personvernforordningen, som f. eks art. 24 og art. 32, pålegger behandlingsansvarlige plikter som forutsetter en nødvendig oversikt over ansvarsforholdene for personvern.

Utfordringer/funn i brevtilsynet

I rapporten beskrives det at et flertall av kommunene har sendt oversiktlige beskrivelser av ansvars- og oppgavefordeling for etterlevelse personvernregelverket. 16 kommuner har ikke besvart spørsmålet eller sendt utilstrekkelig informasjon, og flertallet av disse har ikke et tilfredsstillende styringssystem. Videre har 21 kommuner sendt mangelfulle beskrivelser av sin organisering av ansvarsforholdene på området, blant annet mangler konkrete rutiner for organisering og delegering. Enkelte beskrivelser er fragmenterte og gir liten oversikt.

Veiledning og forslag til tiltak

Kommunene bør blant annet ha:

- klare rammer og beskrivelser for ansvar og roller, samt plassering av ansvar og roller
- en oversikt over kommunens samlede behandlingsansvar og en oversikt over ansvar som er delegert, og
- rutiner som sikrer at de har reell styring og kontroll av etterlevelse av personvernregelverket i hele organisasjonen, og ansvarslinjer bør være forankret i styringssystemet

Eksempler/ressurser

- Datatilsynets forslag til innholdet i en ansvarsbeskrivelse
- KS veiledning «Orden i eget hus»
- Digdirs veiledning Ledelsens styring og oppfølging

Kommunedirektørens kontrollspørsmål

- Har kommunen etablert klare rammer og beskrivelser for plassering av ansvar og roller på personvernområdet?
- Har kommunen en overordnet oversikt med tydelige ansvars- og rollebeskrivelser som gir et klart bilde av kommunens *samlede* behandlingsansvar?
- Har kommunen etablert rutiner som gir behandlingsansvarlig reell styring og kontroll av etterlevelse av personvernforpliktelsene i hele kommunen?
- Er ansvarslinjene forankret i et styringssystem og relevante rutiner som sikrer sammenhengende ansvarslinjer fra behandlingsansvarlig og ut til alle som utfører oppgaver på vegne av behandlingsansvarlig?
- Har kommunen delegeringsrutiner og er det delegerte ansvaret tydelig beskrevet?
- Har delegerte oppgaver en klar forankring i ledelsen med tydelige krav til rapportering?

3. Overordnet styringssystem

Overordnet styringssystem (del 2 punkt 10 i Datatilsynets rapport)

Ved tilsyn ber Datatilsynet om at kommunene gir en kort beskrivelse av overordnet styringssystem (internkontroll) for etterlevelse av personvernregelverket. Hvilke verktøy som eventuelt brukes etterspørres også.

Kommunen har en plikt til å ha et styringssystem for å sikre og påvise at behandling av personopplysninger utføres i samsvar med personvernforordningen, jf. art. 24.

Styringssystemet (internkontrollen) er ledelsens verktøy for å ivareta sitt ansvar, og for å kunne demonstrere etterlevelse etter personvernregelverket i sin organisasjon. Tiltakene skal også være de ansattes verktøy for å utføre oppgaver på en forsvarlig og sikker måte.

Utfordringer/funn i brevtilsynet

Mange kommuner har etablert et styringssystem, og flere viser til at de har fulgt veiledningen KS har utarbeidet for internkontroll; *Orden i eget hus.* Undersøkelsen gir imildertid ikke grunnlag for å si noe om hvorvidt kommunene har fylt systematikken med innhold. Mange av kommunene beskriver dessuten at de er i pågående prosesser hvor de utbedrer eller endrer sitt styringssystem.

Veiledning og forslag til tiltak

Styringssystemet skal:

- ha **styrende** del med dokumenter som definerer retning for arbeidet med informasjonssikkerhet og personvern
- ha en **gjennomførende** del som beskriver hvordan kommunen implementerer og opprettholder styringen
- ha en **kontrollerende** del for evaluering og måling av effekt

Styringssystemet bør:

- være egnet ut fra definert behov og risiko
- være forankret i ledelse
- ha en klar ansvarsfordeling, delegering og beskrivelse av roller
- være systematisk og oversiktlig
- fremstå praktisk anvendelig og lett tilgjengelig
- ha oppdatert dokumentasjon
- inneholde rutiner for revisjon og gjennomgang

Eksempler/ressurser

- Digitaliseringsdirektoratet (Digdir): Internkontroll i praksis
- KS – Orden i eget hus
- KiNS - styringssystem
- Norm for informasjonssikkerhet i helse- og omsorgssektoren (Normen)

Kommunedirektørens kontrollspørsmål

- Hvem har besluttet retning for arbeidet med informasjonssikkerhet og personvern?
- Hvordan rapporteres det på implementering og opprettholdelse av styring?
- Hvor ofte har vi revisjon og gjennomgang av at aktivitetene våre fungerer?
- Etterspør ledelsen rapporter fra arbeidet med personvern og informasjonssikkerhet

4. Risiko- og sårbarhetsanalyser

Risiko- og sårbarhetsanalyser (del 2 punkt 11 i Datatilsynets rapport)

Krav til gjennomføring av risiko og sårbarhetsanalyser er forankret i personvernforordningens artikkel 24 og artikkel 32. Forordningen krever at den behandlingsansvarlige skal beskytte personopplysninger med egnet sikkerhetsnivå. Dette innebærer at det må gjøres konkrete vurderinger av risiko. Dette må/bør sees i sammenheng med kommunens beredskapsplikt og gjennomføring av helhetlig risiko- og sårbarhetsanalyse (ROS) for kommunen.
Generelt skal retningslinjen/rutinen inneholde overordnet beskrivelse av arbeidet med ROS-analyser, for eksempel hvem om har ansvaret, frekvens/hyppighet på revisjon og kontrollaktiviteter, som rapportering og oppfølging.

Utfordringer/funn i brevtilsynet

Rapporten fra tilsynet beskriver retningslinjer som er svært fragmentert og beskrevet i ulike dokumenter. En tredjedel har mangelfulle retningslinjer og en tredjedel har helt manglende eller svært utilstrekkelige retningslinjer. Det betyr at majoriteten av kommunene mangler en tilstrekkelig overordnet retningslinje med vurdering av risiko. Selv om mange kommuner har rutiner og skjemaer for hvordan en ROS-analyse skal gjennomføres, så mangler det en helhetlig systematikk i arbeidet med vurdering av risiko.

Veiledning og forslag til tiltak

På det strategiske nivået må/bør retningslinjene sees i lys av kommunens beredskapsplikt og kommunens styringssystem og internkontroll. Det bør utarbeides en overordnet retningslinje som beskrevet i første punkt. Det vil danne grunnlaget for å identifisere risiko, og vurdert opp mot etablerte akseptkriterier, synliggjøre behov for risikoreduserende tiltak slik at et tilfredsstillende nivå kan oppnås. Det vil også danne grunnlag for at risikovurderinger gjøres systematisk og konsistent, gjeldende for alle tjenesteområder.

Før behandling av personopplysninger, skal det gjennomføres en risikovurdering. Ved endrede forhold som påvirker informasjonssikkerheten, f.eks. endringer i trussel- og sårbarhetsbildet, eller behovet for behandlingen skal det gjennomføres nye risikovurderinger.

Eksempler/ressurser

- Datatilsynets generelle veiledninger: Risikovurdering
- Malverk på Kins.no: Mal for risikovurdering
- Videre finnes ressurser hos Digdir, NSM med flere.

Kommunedirektørens kontrollspørsmål

- Har vi overordnede retningslinjer for ROS analyser, og er disse iverksatt til de som er risikoeiere?
- Er våre retningslinjer tydelige på ansvar/roller/myndighet, beskriver de frekvens/hyppighet på revisjon og kontrollaktiviteter, som rapportering og oppfølging?
- Er nivå for akseptabel risiko definert?
- Har vi oversikt over våre behandlingsaktiviteter?
    - Hvor og hvilke persondata, som behandles i de ulike informasjonssystemene?
    - Er det gjennomført ROS-analyser for disse?
    - Er restrisikoer vurdert og er de innenfor akseptable nivåer (evnt tiltak)?
- Er det beskrevet hendelser ift personvern som i alvorlig grad kan påvirke våre tjenester i lys av beredskapsplikten?

5. Sikkerhetsstrategi

Sikkerhetsstrategi (Del 2 punkt 12 i Datatilsynets rapport)

Beskrivelse av sikkerhetsmål og strategi er virksomhetenes overordnede styrende dokument for ivaretakelse av informasjonssikkerhet. Strategien skal bidra til at virksomhetenes styringssystem for informasjonssikkerhet er i samsvar med lovkravene iblant annet personvernforordningen. Typisk vil strategien inneholde beskrivelse av roller og ansvar, rutiner for kvalitetssikring og revisjon, samt ledelsens gjennomgang.

Selv om personvernforordningen ikke har klare krav til å etablere en sikkerhetsstrategi, settes det krav til beskrivelse av mål og strategi for *informasjonssikkerhet* for virksomheten (sikkerhetsmål og sikkerhetsstrategi) i eForvaltningsforskriften.

Utfordringer/funn i brevtilsynet

Det er en stor andel av kommunene som har svært mangelfulle eller mangler en overordnet sikkerhetsstrategi. Det er gjennomgående at strategiene mangler beskrivelser av ansvarsfordeling og rutiner for gjennomføring av revisjoner og ledelsens gjennomgang.

Veiledning og forslag til tiltak

Brevtilsynet *anbefaler* at det utarbeides en overordnet sikkerhetsstrategi (i lys av personvernet), men dette må sees i lys av eForvaltningsforskriften. Forskriften setter som krav, at virksomheten skal beskrive mål og strategi for styring av *informasjonssikkerheten* (sikkerhetsmål og sikkerhetsstrategi). Dette skal danne grunnlaget for kommunenes internkontroll for informasjonssikkerhet.

- Skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks
- Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem
- Omfang og innretning på internkontrollen skal være tilpasset risiko
- Samt i den utstrekning relevant; adressere/stille krav slik som gitt i forskriften

Eksempler/ressurser

eForvaltningsforskriften med veileder. Både Digdir og NSM gir veiledning på overordnet og operasjonelt plan.

Kommunedirektørens kontrollspørsmål

- Har kommunen en sikkerhetsstrategi?
- Dekker den krav gitt i forskriften?
- Er internkontrollen tilpasset risiko?
- Er internkontrollen en del av kommunenes helhetlige styringssystem?

6. IKT-samarbeid

IKT-samarbeid (Del 2 punkt 13 i Datatilsynets rapport)

Med bakgrunn i et ønske om en generell oversikt over IKT-samarbeid mellom kommuner, ba tilsynet kommunene om å rapportere hvilke samarbeid som er etablert. I tillegg var det et ønske om å se nærmere på om dette kunne ha påvirkning på kommunenes evne til å etterleve personvernregelverket. Personvernordningen krever at fordelingen av ansvar og oppgaver er tydelig regulert (ansvar og relasjoner i behandlingen). Dette kan (og bør) ses i lys av fordeler (og ulemper) med sentralisering av tjenester, der utnyttelse av knappe ressurser, spesialisering (kompetanse) og standardisering kan være noen nøkkelord. Videre kan dette relateres til grad av modenhet innenfor det digitale domenet. Gjelder dette «tradisjonelle» driftsmiljøer, eller er det et samarbeide hvor man i større grad ser organisasjon-, forretningsmodeller, arbeidsprosesser og informasjonssystemer, i et helhetlig perspektiv?

Utfordringer/funn i brevtilsynet

Et flertall av kommunene deltar i et formelt IKT-samarbeid, dette er formalisert gjennom samarbeidsavtale/vertskommune, interkommunale selskap og i kommunale fellesskap. Et mindretall av kommunene oppgir å ikke ha et formalisert arbeid, men kan ha samarbeid ift andre tjenester. Digitaliseringsnettverk oppgis også som samarbeidsform, der disse kan bidra til å sette felles strategisk retning på digitaliseringsarbeidet.

Ift grunnlaget er det vanskelig å trekke valide slutninger, men en tendens er at de som har samarbeid, har sendt inn dokumentasjon som i større grad vurderes som tilstrekkelig, enn kommuner uten formalisert samarbeid. Men det kan ikke konkluderes med at det er en klar tendens. I negativ retning er det en svak tendens til at deltakende kommuner i for stor grad hviler seg på vertskommunen.

Veiledning og forslag til tiltak

Å etablere IKT-samarbeid kan ha store fordeler, men den enkelte kommune må være sitt ansvar bevist. Selv om oppgaver settes ut, så forblir behandlingsansvaret hos den enkelte kommune, relatert til personvernet.

Et samarbeid kan også sess i et bredere perspektiv, knyttet til stordriftsfordeler, der utnyttelse av kompetanse, profesjonalisering, øket redundans, standardisering og tilgjengelighet kan gi positive effekter. Videre kan samarbeid bidra i positiv retning for å øke den digitale modenheten.

Eksempler/ressurser

NSMs anbefaling/oppfordring til konsolidering av driftsmiljøer i rapporten "Ti sårbarheter i norske IKT-systemer"

Kommunedirektørens kontrollspørsmål

- Kan vi forbedre våre tjenester ved å inngå samarbeid med andre kommuner?
- Har vi kontroll på og utøves eget ansvar ved samarbeid med andre kommuner?
- Hvilken samarbeidsform tjener partene best på?
- Hvordan kan et samarbeid øke den digitale modenheten?

7. Autentiseringsløsninger

Autentiseringsløsninger (Del 2 punkt 14 i Datatilsynets rapport)

Datatilsynet ba i brevkontrollen kommunene om å oversende styrende retningslinje for autentiseringsløsninger. De ønsket å se kommunens strategi for å sikre konfidensialitet gjennom sikker bekreftelse av brukers identitet, jfr. personvernforordningen Art. 32.1.b.

For kommunen betyr dette å etablere en strategi for løsninger med tilstrekkelig autentisering av brukeren som skal ha tilgang. Sikkerhetsnivået i løsningene må gjenspeile systemenes kritikalitet, datas verdi, og sørge for at systemene er motstandsdyktige mot angrep fra ondsinnede aktører. Autentiseringsløsningen må også sørge for tilgang når brukere har behov for det (tilgjengelighet).

(Autentisering: Bekrefte brukerens identitet
Autorisering: Brukerens tilgang til data og ressurser)

Utfordringer/funn i brevtilsynet

Datatilsynet har ikke gjengitt funn eller vurderinger i samlerapporten.

Veiledning og forslag til tiltak

Datatilsynet viser i samlerapporten til en trend hvor brudd på personopplysningssikkerhet oppstår ved at ondsinnede aktører utnytter svake autentiseringsløsninger. En klar retningslinje for sterk autentisering ved bruk av multifaktor-autentisering vil forhindre at sikkerhetsnivået avhenger av sluttbrukerens evne til å lage, og forvalte, gode passord.

Kommunen bør ha en styrende retningslinje for autentiseringsløsninger som

- Er basert på risikovurdering av system og verdivurdering av data
- Gjelder for alle enheter med tilgang til kommunens infrastruktur (Pc, mobil, nettbrett)
- Gjelder for kamera, sensorteknologi, SD-anlegg, mm.
- Gjelder for interne brukere, administratorer og eksterne brukere
- Beskriver krav til overvåkning og driftsrutiner
- Er basert på HR-system og legger til rette for automatiserte prosesser for administrasjon av brukerkontoer (hvis mulig).

Eksempler/ressurser

- NSM - grunnprinsipper for IKT-sikkerhet Kap. 2.6
- Normen – autentisering
- KINS – Mal for styringssystem

Kommunedirektørens kontrollspørsmål

- Har kommunen en overordnet retningslinje for autentiseringsløsninger?
- Er autentiseringsløsningene motstandsdyktige mot angrep fra ondsinnede aktører?
- Er retningslinjen gjeldende for alle brukergrupper, også administratorer og eksterne leverandører?
- Har kommunen driftsrutiner for å administrere brukerkontoer?
- Har kommunen overvåkningsrutiner for å avdekke eventuelt misbruk/kompromittering av brukerkontoer?
- Ivaretar kommunen krav til autentiseringsløsninger i anskaffelser av IT-løsninger?

8. Sikkerhetskopiering og gjenoppretting

Sikkerhetskopiering og gjenoppretting (Del 2 punkt 15 i Datatilsynets rapport)

Datatilsynet ba i brevkontrollen kommunene om å oversende styrende retningslinje for sikkerhetskopiering og gjenoppretting. Begrunnelsen var å få en oversikt over kommunenes evne til å gjenopprette tjenester og tilgang til personopplysninger dersom det oppstår en hendelse, jfr. personvernforordningen art. 32.1.b og c.

For kommunen betyr dette å ha en strategi og plan for sikkerhetskopiering og prosedyre for gjenoppretting. Strategien må gjelde både for egen drift og eksterne leverandører. Det betyr også at kommunen jevnlig må teste evnen til å gjenopprette tjenester og data.

Utfordringer/funn i brevtilsynet

Datatilsynet har ikke gjengitt funn eller vurderinger i samlerapporten.

Veiledning og forslag til tiltak

En alvorlig sikkerhetshendelse kan medføre datatap, data på avveie og nedetid i kommunale tjenester. Sikkerhetskopiering og gjenoppretting er avgjørende for kommunens robusthet og evne til å gjenopprette daglig tjenesteproduksjon.

Kommunen bør velge frekvens og omfang for sikkerhetskopiering basert på risiko, nivå for akseptabelt datatap og krav til gjenopprettingstid.

Prosedyre for gjenoppretting bør inngå i kommunens beredskapsplan og testes jevnlig som en del av kommunens beredskapsøvelser.

I arbeidet med å etablere styrende retningslinje for sikkerhetskopiering og gjenoppretting bør kommunen

- Kartlegge kommunens systemer
- Gjøre verdivurdering av data for å finne systemenes kritikalitet
- Etablere plan for sikkerhetskopiering og revidere denne jevnlig
- Etablere prosedyre for gjenoppretting som møter forventning om gjenopprettingstid
- Etablere krav og strategi for beskyttelse av sikkerhetskopier (kryptering, tilgangsstyring, separasjon fra driftsmiljø)
- Lage plan for test av sikkerhetskopiering og gjenoppretting som del av beredskapsplan og sikkerhetsrevisjon.

Eksempler/ressurser

- NSM - grunnprinsipper for IKT-sikkerhet Kap. 2.9
- Normen – sikkerhetskopiering
- KINS – Mal for styringssystem

Kommunedirektørens kontrollspørsmål

- Har kommunen en strategi og plan for sikkerhetskopiering som jevnlig revideres?
- Har kommunen kartlagt systemer og gjort verdivurderinger av data som grunnlag for sikkerhetskopiering?
- Oppbevares kritiske sikkerhetskopier adskilt fra driftsmiljø?
- Har kommunen er prosedyre for gjenoppretting som testes jevnlig?
- Ivaretar kommunen krav til sikkerhetskopiering og gjenoppretting i anskaffelser av IT-løsninger?

9. Sikkerhetsrevisjon

Sikkerhetsrevisjoner (Del 2 punkt 16 i Datatilsynets rapport)

Datatilsynet ba i brevkontrollen om redegjørelse for hvordan kommunen tester, analyserer og vurderer effekten av tekniske og organisatoriske sikkerhetstiltak for å beskytte personopplysninger, jfr. personvernforordningen art. 32.1.d.

For kommunen som behandlingsansvarlig betyr dette å etablere rutiner for å jevnlig vurdere effekten av tekniske og organisatoriske sikkerhetstiltak, dokumentere resultatene og følge opp disse for å justere eller iverksette nye risikoreduserende tiltak. Det innebærer også å utføre sikkerhetsrevisjon av databehandlere og leverandører med betydning for personopplysningssikkerheten.

Utfordringer/funn i brevtilsynet

Datatilsynet funn viser at kommunene samlet sett i liten grad har tilfredsstillende dokumentasjon tilknyttet sikkerhetsrevisjoner og at dokumentasjonen er fragmentert og lite helhetlig. Det mangler også tidfesting for gjennomføring og oppfølging av revisjoner. Redegjørelser viser også at mange kommuner har startet arbeidet i forbindelse med brevkontrollen, noe Datatilsynet mener er positivt.

Veiledning og forslag til tiltak

Ved etableringen av sikkerhetstiltak skal det tas hensyn til risikoene forbundet med behandling av personopplysninger. Sikkerhetsrevisjoner henger derfor tett sammen med kommunens risikostyring, hvor kontroll og evaluering av tiltak er en del av det løpende arbeidet. Resultat fra sikkerhetsrevisjoner skal være en del av ledelsens årlige gjennomgang.

Kommunen bør som en del av styringssystemet utarbeide rutiner og prosedyrer for

- hvordan utarbeide og gjennomføre en revisjonsplan (for interne og/eller eksterne revisjoner)
- hvordan sikkerhetsrevisjonen skal gjennomføres
- hvem som har ansvaret for gjennomføring
- hvem som har ansvaret for oppfølging
- tidsfrist for oppfølging av resultat

Eksempler/ressurser

- Digdir – måling, evaluering og revisjon
- NSM - grunnprinsipper for IKT-sikkerhet Kap. 3
- KS - Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet Kap. 6.3
- Normen – sikkerhetsrevisjon faktaark 06
- KINS – Mal for styringssystem

Kommunedirektørens kontrollspørsmål

- Har kommunen dokumenterte rutiner for gjennomføring og oppfølging av sikkerhetsrevisjon?
- Gjennomføres disse i henhold til planen?
- Er ansvaret for sikkerhetsrevisjoner tydelig beskrevet og er det tilstrekkelige ressurser til arbeidet?
- Er gjennomgang av resultater og oppfølging av revisjoner en del av ledelsens gjennomgang?

10.Personvernerklæring

Personvernerklæring (del 2 punkt 17 i Datatilsynets rapport)

Ved tilsyn ber Datatilsynet om at kommunene sender ved lenke til kommunens personvernerklæring. Kommuner behandler mye personopplysninger om både innbyggere og ansatte, og kommunen har i følge personvernregelverket en plikt til å gjøre dette på en åpen måte. Det er flere bestemmelser i personvernforordningen som spesifiserer kravet til åpenhet gjennom plikter til å gi konkret informasjon. Eksempler er artiklene 12, 13 og 14.

En måte å oppfylle deler av informasjonsplikten er å utarbeide en personvernerklæring som er tilgjengelig fra kommunens nettsider. Kommunen skal gi informasjon på en klar og tydelig måte om hvilke personopplysninger som behandles og hvordan. Informasjonen skal legge til rette for at innbyggere og ansatte kan bruke sin rett til innsyn.

Utfordringer/funn i brevtilsynet

Flere kommuner har mangelfulle personvernerklæringer. En særskilt utfordring er at mange personvernerklæringer er for overordnet, og ikke gir utfyllende informasjon knyttet til spesifikke tjenester. F.eks vil en innbygger som lurer på hvordan personopplysninger behandles i helsetjenesten sjelden finne informasjon om dette i personvernerklæringen.

Tilsynene har tydeliggjort sammenhengen mellom behandlingsprotokollen (artikkel 30) og informasjonsplikten (artiklene 12-14). Kommuner som har fått til en løsning med automatikk mellom disse to pliktene har større grad av etterlevelse.

Veiledning og forslag til tiltak

- Sett av ressurser til å ta en gjennomgang av kommunens personvernerklæring for å sjekke at den gir enten tilstrekkeleg informasjonen eller informasjon om hvor du kan få mer informasjon.
- Vurdere å utarbeide spesifikke personvernerklæringer per tjenesteområde.
- Vurdere verktøy som kan automatisere generering av personvernerklæring(er) basert på behandlingsprotokoll.

Eksempler/ressurser

- Datatilsynet har utarbeidet veiledning om hvordan informasjon skal gis til de registrerte
- Eksempel på personvernerklæring generert fra behandlingsprotokoll
- Eksempel på generell personvernerklæring supplert med tjenestespesifikk informasjon
- Eksempel på løsning med personvernerklæring med lagvis informasjon

Kommunedirektørens kontrollspørsmål

Gir kommunens personvernerklæring svar på følgende:

- innsikt i hvilke kategorier av personopplysninger kommunen behandler?
- innsikt i hvorfor de enkelte personopplysningene er nødvendige, hvor de lagres og hvem som har tilgang?
- innsikt i om kommunen bruker opplysninger til å profilere innbyggere og/eller ansatte?
- innsikt i hvordan innbygger eller ansatt kan bruke sine rettigheter, som f.eks innsyn, retting og sletting?

11. Personvernombud

Personvernombud (del 2 punkt 18 i Datatilsynets rapport)

Ved tilsyn ber Datatilsynet om at kommunene gir informasjon om kommunens personvernombud. Informasjon som forventes er kontaktopplysninger, lenke til kommunens nettside med mer informasjon om personvernombudet, samt informasjon om hvordan funksjonen er organisert i kommunen.

Kommunene er pålagt å utpeke personvernombud, jf. artikkel 37 nr. 1 bokstav a)[1].

Personvernforordningen (artikkel 38, pkt 4) slår videre fast at de registrerte (alle nåværende og tidligere ansatte og innbyggere i kommunen) kan kontakte personvernombudet dersom de har spørsmål om behandlingen av personopplysninger og utøvelsen av sine rettigheter og friheter på dette området.

Utfordringer/funn i brevtilsynet

- Det er store forskjeller i kommunenes organisering av personvernombudsordningen
- Stillingsprosenten som personvernombud varierer fra 3% til 100%
- Flere kommuner deler på en ekstern ressurs
- Mange kommuner mangler mandat eller rollebeskrivelse

Veiledning og forslag til tiltak

- Sørg for at personvernombudet har en stillingsprosent som gjør det mulig å ivareta oppgavene som fremgår av forordningen
- Sørg for at personvernombudet har en uavhengig stilling, og er plassert i organisasjonen på en måte som sikrer uavhengigheten
- Sørg for tydelig (klart språk-prinsippene) og lett tilgjengelig informasjon om ombudet, med rolle, oppgaver og mandat

Eksempler/ressurser

- Datatilsynets veiledning om personvernombudsordningen;
- Personvernombud | Datatilsynet
- Rollebeskrivelse og mandat
- Rapporter til politisk og administrativ ledelse

Kommunedirektørens kontrollspørsmål

- Vet innbyggerne og de ansatte at kommunen har et personvernombud?
- Vet innbyggerne og de ansatte hva personvernombudet kan bistå dem med?
- Er personvernombudets særlige oppgaver synliggjort i relevante rutiner?
- Har personvernombudet nok tid til å ivareta oppgavene som er lagt til rollen?
- Har personvernombudet kompetansen som skal til for å ivareta rollen sin?
- Har personvernombudet tilgang på de riktige ressursene internt i kommunen? (juridisk, HR, arkiv, digitalisering, sikkerhetsmiljø osv.)
- Har personvernombudet de nødvendige tilgangene for å utføre oppgavene sine?

[1] Forordningen åpner for at flere kommuner kan utpeke ett felles personvernombud, og også for at man kan anskaffe tjenesten eksternt gjennom en tjenesteavtale.