Vestfold og Telemark revisjon

Informasjonssikkerhet og personvern

Forvaltningsrevisjon | Bamble kommune

22: 3813 403

Innhold

Sammendrag

I denne forvaltningsrevisjonen har vi sett på Bamble kommune sitt arbeid på informasjonssikkerhets- og personvernområdet. Rapporten omtaler ulike tiltak og rutiner innenfor personvern og behandling av personopplysninger med utgangspunkt i de kravene som stilles i personopplysningsloven. Det er utarbeidet flere revisjonskriterier som vil bli redegjort for og gjennomgått i rapportens kapitler. Overordnet sett har vi operert med to problemstillinger, hvor den ene er på et generelt nivå og handler om kommunens tiltak med tanke på personopplysningsloven, mens den andre problemstillingen handler om den praktiske oppfølgingen på dette området i kommunens enheter.

I dette sammendraget presenteres de sentrale funnene og vurderingene i rapporten, sortert under de to problemstillingene. Den første problemstillingen er:

1.1. Konklusjoner

I hvilken grad har Bamble kommune etablert tiltak for å ivareta kravene i personopplysningsloven?

Vi finner at kommunen i har etablert flere gode tiltak for å ivareta kravene i personopplysningsloven, slik dette er beskrevet i styrende dokumenter på området og andre rutinebeskrivelser. Kommunen har oppdaterte styrende dokumenter, rutinebeskrivelser og maler som hensyntar de kravene som stilles i personopplysningsloven, og kommuneledelsen orienteres jevnlig om status på området.

Bamble kommune har en utfyllende og oppdatert personvernerklæring, rutiner for håndtering av innsynsforespørsler, og rutiner for registrering og håndtering av avvik på området. Kommunen har rutiner for gjennomføring av risikoanalyser ved anskaffelser av nye systemer, og fører en behandlingsprotokoll over sine behandlingsaktiviteter.

Vi har sett at behandlingsprotokollen ikke var helt oppdatert med alle systemer som var i bruk i kommunen. Vi så også at hjemmelen for behandling av personopplysninger ikke alltid var opplyst i protokollen.

Kommunens egen systemdokumentasjon for de systemene som behandler personopplysninger er ikke alltid fullstendig. Vi har sett et eksempel på at systemdokumentasjonen indikerte at det manglet en databehandleravtale, mens nærmere undersøkelser viste at avtalen eksisterte.

Kommunens arbeid med risikovurderinger og DPIA omtales både i styrende dokumenter og egne rutinebeskrivelser. Bamble kommune har maler som er oppdatert og i tråd med Datatilsynets veileder. Vi ser at kommunen i stor grad ivaretar kravene til risikovurderinger for systemer som behandler personopplysninger. Vi har sett ett tilfelle der det manglet risikovurdering. I tillegg har vi

sett et tilfelle av en DPIA som kun var delvis gjennomført og ikke i tråd med minimumskravene for en DPIA.

Samtidig som kommunen i stor grad har gode tiltak og rutiner for å ivareta kravene i personopplysningsloven, så finner vi altså at kommunen har rom for forbedring på noen områder, samt behov for bedre rutiner når det gjelder gjennomføring og dokumentering av risikoanalyser og DPIA.

Hvordan blir sentrale krav i personopplysningsloven og kommunens egne tiltak fulgt opp i praksis i kommunens enheter?

I forbindelse med denne problemstillingen har vi undersøkt tre utvalgte enheter i kommunen gjennom intervjuer med ledelsen ved enhetene. Enhetene bestod av en skole, en barnehage og barneverntjenesten.

På et overordnet nivå fikk vi et godt inntrykk av hvordan det tenkes rundt, og jobbes med, informasjonssikkerhet og personvern i disse enhetene. Integritet, konfidensialitet og tilgjengelighet er tre sentrale personvernprinsipper. Av disse prinsippene er det særlig konfidensialitet som sikres gjennom gode systemer og rutiner, samt bevissthet rundt personvern, i den daglige driften i enhetene i kommunen.

Når det gjelder konfidensialitet er det vårt inntrykk at enhetene er bevisste på å behandle personopplysninger på en sikker måte. Behandlingen foregår i godkjente fagsystemer og utveksling/utlevering av dokumenter med personopplysninger gjøres via sikre kanaler eller ved fysiske møter. Det er gode rutiner for fullmakt ved innsynsforespørsler, og rutiner for gjennomgang av dokumentene/mappene slik at ikke opplysninger om andre personer utleveres ved en feil. Det er gode rutiner i kommunen når det gjelder tilgangsstyring for ansatte i fagsystemene, og det er en høy grad av bevissthet i enhetene når det gjelder tilgang til, og sikring av, personopplysninger. Kommunens avvikssystem kan gjøres bedre kjent ute i enhetene.

1.2. Anbefalinger

Vi anbefaler at Bamble kommune

- vurderer om det er behov for å oppdatere rutiner, roller og ansvarsfordeling når det gjelder gjennomføring av risikovurdering og DPIA for systemer som behandler personopplysninger
- vurderer om det er hensiktsmessig å fastsette en formell stillingsprosent for rollen som personvernombud, da dette i dag er en delt stilling uten en fast stillingsprosent, dersom man ser et behov for at personvernombudet i større grad gjennomfører kontrolloppgaver
- gjennomgår rutinene for oppdatering av behandlingsprotokollen slik at den til enhver tid er oppdatert med tanke på de systemene som er i bruk i kommunen
- gjennomgår rutinene for registreringer i behandlingsprotokollen, og sørger for at behandlingsgrunnlag registrerer korrekt med lovhjemmel i de tilfeller der dette kreves
- fortsetter arbeidet med å innføre et nytt kvalitetssystem, og sørger for at ansatte får nødvendig opplæring i systemet

2. Innledning

2.1. Kontrollutvalgets bestilling

Forvaltningsrevisjonen er bestilt av kontrollutvalget i Bamble kommune i sak 39/21. Informasjonssikkerhet er en del av kommunens vedtatte plan for forvaltningsrevisjon i perioden.

Reglene om forvaltningsrevisjon står i kommuneloven § 23-2 første ledd bokstav c, jf. § 23-3 og § 24-2 og i forskrift om kontrollutvalg og revisjon.

2.2. Problemstilling og revisjonskriterier

Rapporten handler om følgende problemstillinger:

1. I hvilken grad har Bamble kommune etablert tiltak for å ivareta kravene i personopplysningsloven?
2. Hvordan blir sentrale krav i personopplysningsloven og kommunens egne tiltak fulgt opp i praksis i kommunens enheter?

Revisjonskriteriene[1] i denne forvaltningsrevisjonen er hentet fra personopplysningsloven og relevante veiledere fra Datatilsynet. Kriteriene framgår under hvert kapittel i rapporten, og er nærmere omtalt i eget vedlegg.

2.3. Avgrensning

Rapporten omfatter ikke behandling av personopplysninger knyttet til folkevalgte og kommunens egne arbeidstakere.

2.4. Metode og kvalitetssikring

Denne forvaltningsrevisjonen er gjennomført av forvaltningsrevisor Lars Pedersen, med Kirsti Torbjørnson som oppdragsansvarlig.

Rapporten bygger på informasjon fra kommunens relevante dokumentasjon på området, som spenner fra styrende dokumenter og rutinebeskrivelser til systemdokumentasjon og konkrete risikovurderinger, avtaler, mv., samt informasjon hentet fra kommunens behandlingsprotokoll. Vi har også gjennomført intervjuer med kommunens personvernombud og tre enheter i kommunen. Disse tre enhetene var barneverntjenesten, en barneskole og en barnehage.

Vi har gjennomført en stikkprøvekontroll av kommunens behandlingsprotokoll. To av systemene i stikkprøven ble valgt ut fra en vurdering av risiko (omfang og type opplysninger), mens seks av systemene ble valgt tilfeldig, men innenfor en avgrenset del av behandlingsprotokollen. Denne avgrensningen var også basert på en vurdering av risiko. Hensikten med stikkprøvekontrollen var å sjekke hvilke opplysninger som var registrert i protokollen, om nødvendige opplysninger var registrert, og mer generelt undersøke hvordan kommunen bruker behandlingsprotkollen. De utvalgte behandlingsaktivitetene dannet også grunnlaget for andre undersøkelser.

Det står mer om metode og tiltak for kvalitetssikring i vedlegg 3 til rapporten.

2.5. Kommunedirektørens uttalelse

Rapporten er presentert i et møte med administrasjonen i kommunen og sendt til uttalelse 20.09.22, jf. forskrift om kontrollutvalg og revisjon § 14. Kommunedirektørens uttalelse ligger i vedlegg 1.

[1] Det skal alltid etableres revisjonskriterier i forvaltningsrevisjon, jf. forskrift om kontrollutvalg og revisjon § 15. Revisjonskriterier er de regler og normer som gjelder innenfor det området vi skal undersøke. Revisjonskriteriene er grunnlaget for revisors analyser, vurderinger og konklusjoner.

3. Om personopplysningsloven og sentrale begreper

Den gjeldende personopplysningsloven trådte i kraft juli 2018. Loven implementerer EUs personvernforordning (kjent som GDPR). Loven innledes med de norske særreglene, inndelt i paragrafer, før forordningsteksten, som er inndelt i artikler, følger. I rapporten vil derfor noen bestemmelser omtales som paragrafer, men andre vil omtales som artikler.

Personopplysningsloven inneholder en del begreper som vi kort vil gjøre rede for her:

Behandling – enhver operasjon som gjøres med personopplysninger.

Behandlingsansvarlig – den som beslutter at personopplysninger skal samles og hvordan dette skal gjøres. Er overordnet ansvarlig for å overholde personvernregelverket. I de fleste tilfeller er kommunen behandlingsansvarlig.

Behandlingsgrunnlag – rettslig grunnlag for å kunne behandle personopplysninger, hjemlene står i artikkel 6-1.

Databehandler – den som på oppdrag av en behandlingsansvarlig behandler data. Dette er gjerne IKT-leverandører som enten behandler personopplysninger direkte eller får tilgang til disse f.eks. ved vedlikehold og support av kommunens systemer. Databehandlere har ofte underleverandører og disse omtales som underdatabehandler.

Databehandleravtale – lovpålagt avtale mellom behandlingsansvarlig og databehandler som regulerer behandlingen av personopplysninger som databehandler skal gjøre på vegne av behandlingsansvarlig. Avtalen skal sikre at databehandler har egnede tekniske og organisatoriske tiltak for å oppfylle personopplysningslovens krav. Databehandleravtaler er regulert i artikkel 28-3.

Personopplysning – definert i personopplysningsloven artikkel 4-1 som: «enhver opplysning om en identifisert eller identifiserbar fysisk person».

Den registrerte – en fysisk person som kommunen behandler personopplysninger om.

Protokoll over behandlingsaktiviteter – oversikt over alle prosessene hvor kommunen behandler personopplysninger. Denne oversikten er pålagt etter personopplysingsloven artikkel 30. I denne artikkelen fremgår også hvilke krav som stilles til innholdet i protokollen.

Særlige kategorier av personopplysninger (sensitive personopplysninger) – er nærmere definert i personopplysningsloven artikkel 9-1. Det er ikke tillatt å behandle disse opplysningene med mindre man har hjemmel i artikkel 9-2.

Uttrykket «kategorier av» brukes i regelverket og kan løst oversettes til «forskjellige typer av».

4. Informasjonssikkerhet og personvern

Problemstilling 1:

I hvilken grad har Bamble kommune etablert tiltak for å ivareta kravene i personopplysningsloven?

Problemstilling 2:

Hvordan blir sentrale krav i personopplysningsloven og kommunens egne tiltak fulgt opp i praksis i kommunens enheter?

Til disse problemstillingene har vi utledet revisjonskriterier som sier at Bamble kommune skal ha:

- en organisasjon med klar plassering av ansvar og myndighet for behandlingen av personopplysninger, samt rutiner for rapportering
- personvernombud, organisert i samsvar med personopplysningsloven
- protokoll over hvilke personopplysninger kommunen behandler
- risikovurderinger og dokumenterte vurderinger av personvernkonsekvenser (DPIA)
- tiltak for å håndtere brudd på personopplysningssikkerheten
- tiltak for å ivareta innsynsretten til de registrerte
- tiltak for å ivareta de registrertes rett til informasjon om kommunens behandling av deres personopplysninger
- tiltak for å sikre at kommunen har databehandleravtale med alle databehandlere

Se vedlegg 2 for en nærmere redegjørelse av bakgrunnen for revisjonskriteriene.

4.1. Organisasjon og rutiner

Bamble kommune skal ha en organisasjon med klar plassering av ansvar og myndighet for behandlingen av personopplysninger, samt rutiner for rapportering.

4.1.1. Fakta om organisasjon og rutiner

Kommunen har et strategidokument på dette området med tittelen «Strategi for informasjonssikkerhet ved behandling av personopplysninger». Dokumentet ble oppdatert/revidert i forbindelse med implementeringen av den nye personvernforordningen i 2018, og er deretter revidert i 2020.

I strategien for informasjonssikkerhet defineres informasjonssikkerhet til å handle om sikring av konfidensialitet, integritet, tilgjengelighet og robusthet. De tre første punktene er i tråd med grunnleggende personvernprinsipper slik dette defineres av blant andre Datatilsynet. Det siste punktet, robusthet, handler om virksomhetens og systemenes evne til å gjenopprette en normaltilstand i etterkant av et sikkerhetsbrudd. Det er først og fremst de personvernrettede prinsippene som ligger til grunn i denne forvaltningsrevisjonen.

Målgruppen for strategidokumentet er alle ansatte i Bamble kommune som behandler personopplysninger, enten dette foregår digitalt/elektronisk eller manuelt (på papir). Det fremgår av strategien at alle kommunens ansatte skal ha tilstrekkelig kompetanse og gis nødvendig opplæring på dette området.

Et overordnet prinsipp i Bamble kommune er at det er IT-samarbeidet i Grenland, ITG, som er leverandør av tekniske tjenester og systemer, og som dermed har ansvaret for den tekniske sikkerheten, samt rutiner knyttet til dette. Ansvar for arbeidet med informasjonssikkerhet og personvern ligger til den enkelte kommunalsjef, som skal påse tilfredsstillende informasjonssikkerhet innen sitt myndighetsområde. Informasjonssikkerhet skal være en integrert del av de oppgavene som ligger til kommunens enheter.

Sensitive personopplysninger skal ifølge strategidokumentet kun oppbevares i definerte fagsystemer, eventuelt i sikker sone i Public 360 dersom det ikke finnes et slikt fagsystem.

Det er kommunedirektøren som er behandlingsansvarlig for kommunens behandling av personopplysninger, og som har det overordnede ansvaret for informasjonssikkerhet i kommunen. De daglige oppgavene til behandlingsansvarlig er i strategien delegert til systemeier. Systemeier er øverste leder for den virksomheten som bruker et system. Systemeier skal utnevne systemansvarlig, og kan delegere daglige oppgaver. Den systemansvarlige har da det faglige ansvaret for bruken og administrasjonen av systemet.

Strategien er tydelig på kommunens ansvar for en sikker og korrekt håndtering av personopplysninger, inkludert at det må eksistere et behandlingsgrunnlag. Strategien omtaler også de registrertes (innbyggere, brukere, mv.) rettigheter, for eksempel til innsyn, korrigering og annen behandling av egne personopplysninger.

Strategien for informasjonssikkerhet omtaler kommunens arbeid med risikovurderinger. Her fremkommer det at kommunen, som del av internkontrollen, skal ha en oversikt over hvilke personopplysninger kommunen behandler og hvordan disse behandles. Denne oversikten skal fungere som et underlag for risikovurderinger. Det er systemeier i samarbeid med sikkerhetsrådgiver som har ansvar for å gjennomføre generelle risikovurderinger. Resultatet skal meddeles rådmann/behandlingsansvarlig, sikkerhetsleder og sikkerhetsansvarlig.

Bamble kommune er en del av IT-samarbeidet i Grenland, ITG. Her avholdes det jevnlig eiermøter mellom ITG og kommunene, representert ved kommunedirektøren. I disse møtene rapporteres det status på informasjonssikkerhet og personvern. Personvernombudet deltar også i disse møtene.

4.1.2. Revisors vurdering av organisasjon og rutiner

Bamble kommune har en organisasjon med en klar plassering av ansvar og myndighet på området informasjonssikkerhet og personvern. Organisering, ansvar og delegering er fastsatt gjennom et styrende dokument som er revidert i henhold til den nye personvernlovgivningen og som oppdateres/revideres jevnlig, sist i 2020. Kommunens ledelse, representert ved kommunedirektøren, deltar jevnlig i møter med ITG (felles IT-enhet for Grenland) og personvernombud hvor status på området informasjonssikkerhet og personvern er tema.

4.2. Personvernombud

Bamble kommune skal ha et personvernombud, organisert i samsvar med personopplysningsloven.

Datatilsynet har utarbeidet en veileder hvor det er beskrevet hvilke oppgaver personvernombudet har. Her fremgår det at personvernombudet skal informere om forpliktelsene som kommunen har etter personopplysningsloven, både til behandlingsansvarlig og andre ansatte. Videre skal personvernombudet:

- kontrollere kommunens overholdelse av personvernregelverket og interne rutiner og regler,
- på forespørsel gi råd om vurdering av personvernkonsekvenser (DPIA),
- samarbeide og være kontaktpunkt for Datatilsynet og samarbeide med dem.

Videre skriver Datatilsynet at personvernombudet skal fokusere sin innsats på de områdene hvor risikoen er høyest. Datatilsynet skriver også at personvernombudet kan få andre oppgaver så lenge det ikke oppstår en interessekonflikt.

Det følger av personopplysningsloven (forordningen art. 38-3) at personvernombudet skal være uavhengig, det vil si at man ikke kan instrueres i utførelsen av oppgavene og heller ikke kan avsettes eller straffes for utførelsen av oppgavene. Videre fremgår det forordningens art. 37-5 at personvernombudet skal være faglig kvalifisert og ha kunnskap på området som er tilstrekkelig for å kunne utføre arbeidet.

4.2.1. Fakta om personvernombudet

Bamble kommune sin strategi for informasjonssikkerhet inneholder et eget kapittel om personvernombudet. Overordnet sett skal personvernombudet gi råd til kommunen om hvordan personvernet ivaretas på best mulig måte. Videre listes det opp noen konkrete oppgaver og ansvarsområder som ligger til rollen som personvernombudet. Dette handler blant annet om samarbeid med Datatilsynet, råd og veiledning på personvernområdet, opplæring av medarbeidere, kartlegging av behandlingsaktiviteter og analyser av hvorvidt behandlingsaktivitetene er i tråd med gjeldende lovverk.

Personvernombudet er en del av ITG-samarbeidet og har en delt stilling som informasjonssikkerhetskoordinator og personvernombud. Ifølge personvernombudet er det ikke noen fast fordelingsnøkkel/stillingsprosent mellom disse to rollene. Personvernombudet opplever at Bamble kommune er relativt selvstendige på flere områder, blant annet behandlingsprotokoll og aspekter relatert til det, mens kommunen er mindre selvstendig på DPIA. Dermed fungerer personvernombudet som en aktiv bidragsyter i kommunens arbeid med DPIA, mens rollen overfor Bamble kommune ellers består av rådgiver- og ombudsrollen, der rådgivning og opplæring er hovedoppgavene.

Personvernombudet opplyser at han ikke utfører kontrolloppgaver rettet mot kommunen. Han har ikke mottatt henvendelser fra Bamble kommune om kurs eller opplæringsaktiviteter, men har mottatt slike henvendelser fra andre kommuner han er personvernombud for.

Personvernombudet opplyser at Bamble kommune er i en prosess med innføring av et nytt kvalitetssystem. I første omgang vil det bestå av et nytt system for avvik via systemet Compilo. Senere er det også andre ting som skal inn i det nye kvalitetssystemet, som styrende dokumenter, rutinebeskrivelser og prosesskart. Det vurderes også om behandlingsprotokollen skal inn i Compilo. Ifølge personvernombudet vil det forenkle jobben med å registrere og oppdatere oppføringer i protokollen, gjennomføre risikoanalyser og revidere databehandleravtaler.

Bamble kommunes personvernombud har en utdanning i samfunnsvitenskapelige fag fra Universitetet i Oslo og en tilleggsutdanning innenfor informasjonssikkerhet og personvern fra Høyskolen i Innlandet. Han har jobbet innen IT siden 2007 og vært personvernombud siden 2018.

4.2.2. Revisors vurdering av personvernombudet

Personvernombudets rolle er beskrevet i kommunens styrende dokumenter på området, og personvernombudet har en faglig relevant bakgrunn for stillingen. Det er vår vurdering av kommunen har et personvernombud som er organisert i samsvar med personopplysningsloven.

Innenfor den tiden personvernombudet har til sine oppgaver går det mest tid til rådgivning, og det er dermed mindre tid til den delen av rollen som handler om å kontrollere kommunens overholdelse av personvernloven samt egne rutiner på området. Personvernombudet har en delt stilling og det er ikke fastsatt en stillingsprosent for rollen som personvernombud. Vi anbefaler at kommunen vurderer hvorvidt det er behov for en fast fordelingsnøkkel, særlig med tanke på tid og ressurser til kontrollfunksjoner, men også for generell rådgivningsvirksomhet.

4.3. Behandlingsprotokoll

Bamble kommune skal ha en protokoll over hvilke personopplysninger kommunen behandler.

Alle virksomheter som behandler personopplysninger, skal føre en protokoll over behandlingsaktivitetene de har ansvar for.

4.3.1. Fakta om kommunens behandlingsprotokoll

Datatilsynet har utarbeidet en mal for behandlingsprotokoll. Denne malen er i Excel-format. Ifølge Datatilsynet er det ingen formkrav til hvordan en behandlingsprotokoll skal føres eller hva slags verktøy som skal benyttes. Med andre ord kan det gjøres i et tekstdokument, i Excel, eller via andre løsninger.

Bamble kommune har to ulike formater for behandlingsprotokoll. Det ene formatet er et skjema i Excel basert på malen til Datatilsynet. Det andre formatet er en nettside som er tilgjengelig internt i kommunen via ansattportalen. Basert på en kryssjekk av oppføringene i protokollen som tilhører feltet oppvekst, er det slik at nettsiden i stor grad speiler informasjonen i Excel-filene, samtidig som Excel-filene inneholder noe mer informasjon om en del av systemene og behandlingsaktivitetene.

Protokollen i nettsideformat er organisert slik at administrasjon, samfunn, oppvekst, velferd og plan og økonomi har hver sine deler, som igjen består av tilhørende seksjoner. For eksempel ligger skole, barnehage, PPT og barne- og familievern under oppvekst. Strukturen på denne behandlingsprotokollen veksler når det gjelder hva slags detaljeringsnivå som er registrert. I noen tilfeller er det det enkelte systemet som danner grunnlaget for oppføringen i protokollen. Derimot er de fleste av oppføringene behandlingsprosesser, eller handlinger, som kommunen håndterer, for eksempel «arrangementstillatelse», «søknad om skolebytte», «oppmåling», «parkeringstillatelser», «byggdrift – adgangskontroll», med videre. Som en konsekvens av denne strukturen inneholder behandlingsprotokollen et stort antall oppføringer, hvorav flere av dem er nært knyttet til hverandre. En organisering av behandlingsprotokollen med utgangspunkt i enkelte behandlingsaktiviteter er i tråd med hvordan malen fra Datatilsynet er lagt opp. Protokollens struktur innebærer samtidig at det ikke er hensiktsmessig å foreta en stikkprøvekontroll med en tilfeldig utvelgelse av oppføringer fra protokollen som helhet. Vi har derfor valgt å heller ta en gjennomgang av seks tilfeldig utvalgte behandlingsprosesser under skole, samt begge behandlingsprosessene som er oppført under barne- og familievern.

For skole er følgende behandlingsprosesser valgt ut:

- skade- og sykemeldinger
- elevsamtaler
- sms, mail og meldingsfunksjon
- søknad om tilrettelagt eksamen
- karakterer, fravær og vurderinger
- søknad om skoleskyss

For barne- og familievern ble følgende behandlingsprosesser gjennomgått:

- saksbehandling knyttet til lov om barneverntjenester
- familierådgivning

I gjennomgangen undersøkte vi om følgende opplysninger var registrert for hver behandling:

- formål med behandlingen av personopplysninger (jamfør personopplysningsloven art. 30, nr. 1, bokstav b),
- kategorier av registrerte (dvs. hvem er det personopplysninger om, jamfør personopplysningsloven art. 30, nr. 1, bokstav c),
- kategoriene av personopplysninger (dvs. hvilke personopplysninger er registrert, jamfør personopplysningsloven art. 30, nr. 1, bokstav c) og
- behandlingsgrunnlag (jamfør personopplysningsloven art. 6, nr. 1)[2]

Samtlige behandlingsaktiviteter vi undersøkte inneholdt opplysningene i listen ovenfor. Av åtte behandlingsaktiviteter var det syv som brukte behandlingsgrunnlaget fra personopplysningslovens artikkel 6, nr. 1, bokstav c eller artikkel 6, nr. 1, bokstav e[3]. Det kreves hjemmel i annen lov for å bruke disse behandlingsgrunnlagene. Tre av de oppførte behandlingsaktivitetene var ikke registrert med en slik hjemmel. Dette gjelder «SMS, mail og meldingsfunksjon», «søknad om tilrettelagt eksamen», og «karakterer, fravær og vurderinger».

Vi har undersøkt om de systemene som er i bruk i de intervjuede enhetene er registrert i behandlingsprotokollen. I barnehagen er det nylig tatt i bruk et nytt system for kommunikasjon mellom barnehagen og foresatte som heter MyKid. Dette systemet er ikke oppført i behandlingsprotokollen.

4.3.2. Revisors vurdering av behandlingsprotokollen

Kommunen har en behandlingsprotokoll som viser de ulike behandlingsaktivitetene kommunen er ansvarlig for, hvilke systemer som brukes til disse behandlingsaktivitetene, og nødvendig informasjon om behandlingsaktiviteten, som kategorier av opplysninger, kategorier av registrerte, mv.

For de undersøkte behandlingsaktivitetene benyttes i hovedsak artikkel 6, nr. 1, bokstav c eller artikkel 6, nr. 1, bokstav e som behandlingsgrunnlag. Disse behandlingsgrunnlagene bygger henholdsvis på en rettslig forpliktelse eller utøvelse av offentlig myndighet. Behandlingsgrunnlagene er registrert i protokollen, men for noen av behandlingsaktivitetene med

[2] Personopplysningsloven krever ikke at dette fremgår av protokollen, men det er anbefalt i Datatilsynets mal for protokoll. Videre krever personopplysningsloven art. 6, nr. 1 at kommunen må ha et gyldig behandlingsgrunnlag for å kunne *behandle* personopplysningene.
[3] Bokstav c innebærer at behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige, mens bokstav e innebærer at behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt.

et av disse behandlingsgrunnlagene er det ikke registrert hvilken lovhjemmel behandlingsgrunnlaget er knyttet til.

Vi har identifisert et system som nylig er tatt i bruk i kommunen, hvor det behandles personopplysninger, men som ikke er registrert i behandlingsprotokollen. Kommunens behandlingsprotokoll kan dermed ikke sies til enhver tid å gi en oppdatert oversikt over systemer som behandler personopplysninger i kommunen. Vi anbefaler at kommunen går gjennom rutinene når det gjelder registreringer og oppdateringer i behandlingsprotokollen.

4.4. Risikovurderinger

Bamble kommune skal ha risikovurderinger og dokumenterte vurderinger av personvernkonsekvenser (DPIA)

4.4.1. Fakta om risikovurderinger

Kommunens strategi for informasjonssikkerhet beskriver arbeidet med risikovurderinger på et overordnet nivå. Det er systemeier som har ansvaret for at det gjennomføres en risikovurdering. Videre står det i strategien at det også skal gjennomføres en DPIA (Data Protection Impact Assessment) dersom behandlingen av personopplysninger medfører en høy risiko.

Kommunen har en «Prosedyre for anskaffelse av IT-systemer». Denne tar for seg flere deler av en anskaffelse, blant annet vurdering av behov, prosjektbeskrivelse og gevinstplan, men den inneholder også en del om risikovurderinger. Ifølge kommunens prosedyre skal alle anskaffelser innenfor IT ha en risikovurdering / risiko- og sårbarhetsanalyse (ROS).

Vi har sjekket hvorvidt det foreligger ROS-analyser, og eventuelle DPIA, for de systemene som ble plukket ut til en gjennomgang i behandlingsprotokollen. Dette gjelder følgende systemer:

- Visma Flyt Skole
- Visma Familia
- Public 360

Kommunen har dokumentert ROS-analyser for Visma Flyt Skole og Public 360. ROS-analysen for Public 360 er av noe eldre dato da den er gjennomført i 2016, men kommunen opplyser at systemet ikke har gjennomgått endringer av en slik art at en ny analyse er nødvendig. Basert på tilgjengelig dokumentasjon ser det ikke ut til å være gjennomført en ROS-analyse av Visma Familia.

Det er ikke oversendt DPIA for systemene nevnt ovenfor, men kommunen har dokumentert gjennomførte DPIA på flere andre systemer. Det er vanlig at kommunen involverer personvernombudet i dette arbeidet.

Bamble kommune har en mal for å gjennomføre DPIA. Malen innleder med en beskrivelse av formål og behandlingsgrunnlag for den planlagte behandlingen. Deretter er det en innledende vurdering av ulike sider av behandlingen. Basert på den innledende vurderingen besluttes det deretter hvorvidt det er behov for en fullstendig DPIA. Datatilsynet har en veileder for gjennomføring av DPIA inkludert en sjekkliste for de elementene som skal inngå i en slik vurdering. Kommunens mal oppfyller de vilkårene som stilles til en DPIA ifølge oversikten fra Datatilsynet, og er i stor grad lagt opp etter samme struktur/logikk som veilederen fra Datatilsynet. Vi har sjekket gjennomført DPIA for systemet Visma Flyt PPT. Ut fra den dokumentasjonen vi har fått oversendt ser det ikke ut til at de delene som omfatter risiko og tiltak er fylt ut. Ifølge veilederen fra Datatilsynet inngår disse elementene i minimumskravene som stilles til en DPIA i personopplysningsloven.

4.4.2. Revisors vurdering av risikovurderinger

Bamble kommune har rutiner for å gjennomføre risikovurderinger av systemene som benyttes til å behandle personopplysninger. Gjennomføring av ROS-analyser er et eget punkt i kommunens rutine for anskaffelse av IT-systemer.

Vi vurderer det slik at kommunens rutiner på dette området i stor grad fungerer og følges, men har sett ett eksempel på et system som behandler personopplysninger, hvor det ikke foreligger en ROS-analyse. En slik analyse skal foreligge for alle systemer som behandler personopplysninger. En manglende analyse for et operativt system innebærer dermed at dette kravet ikke er oppfylt.

Kommunen har dokumentert flere gjennomførte DPIA og har rutiner for å gjennomføre slike vurderinger når risikovurderingen tilsier at det er behov for det. Kommunens mal for DPIA er oppdatert og i tråd med Datatilsynets veiledning for slike analyser. Vi har funnet et tilfelle av en DPIA som kun er delvis gjennomført på en slik måte at gjennomføringen ikke tilfredsstiller de minimumskravene som gjelder for en DPIA.

Vi anbefaler at kommunen går gjennom sine rutiner når det gjelder både risikovurderinger og DPIA, for å sikre at det gjennomføres risikovurderinger for alle systemer som behandler personopplysninger, og slik at det gjennomføres en fullstendig DPIA i tråd med kommunens mal for de systemene der dette er relevant.

4.5. Håndtering av avvik / brudd på personopplysningssikkerheten

Bamble kommune skal ha tiltak for å håndtere brudd på personopplysningssikkerheten.

Håndtering av brudd på personopplysningssikkerheten handler om å både ha rutiner og et egnet system for registrering og oppfølging av avvik. Videre må det være kompetanse og rutiner knyttet til oppfølging av de registrerte avvikene.

4.5.1. Rutiner for avvikshåndtering

Kommunens strategi for informasjonssikkerhet omtaler håndtering av avvik på et overordnet nivå, og henviser til egne rutiner på området. Disse rutinene er beskrevet i dokumentet «Rutine for avvikshåndtering». Denne rutinen er oppdatert i henhold til den nye personvernforordningen av 2018, og beskriver hvordan avvik/brudd skal håndteres i kommunen. Det er kommunedirektøren som er ansvarlig for rutinen, mens linjeledere har ansvaret for at rutinen er kjent og blir fulgt i organisasjonen. Det slås fast at alle ansatte har plikt til å varsle nærmeste leder om avvik på personvernområdet.

Rutinen beskriver at ansatte skal varsle sin nærmeste leder straks de har mistanke om et avvik på dette området. Deretter skal nærmeste leder informere kommunalsjefen eller kommunedirektøren. Ved alvorlige avvik skal i tillegg ordfører/varaordfører, samt kommunedirektør, varsles. Ved avvik skal også personvernombudet varsles og delta i en vurdering av avvikets alvorlighetsgrad og risiko. Om avviket er av en slik art at det medfører meldeplikt skal det sendes en melding til Datatilsynet så snart som mulig og senest innen 72 timer. Nærmeste leder er ansvarlig for at avviket registreres i kommunens arkivsystem. Rutinen inneholder et flytskjema som viser rutinen/prosessen som skal følges ved oppdagelse av, eller mistanke om, et avvik.

Kommunen bruker saksbehandlingssystemet, P360, til å registrere og håndtere avvik på informasjonssikkerhetsområdet. Dette skal erstattes med en avviksmodul i Compilo når det nye kvalitetssystemet innføres.

Basert på en oversikt utarbeidet av kommunen, er det siden 2018 registrert 16 avvik i P360 på informasjonssikkerhet/personvern. Åtte avvik er meldt til Datatilsynet.

Personvernombudet har vært involvert i håndteringen av flere avvik i kommunen. Personvernombudets inntrykk av avvikshåndteringen er at avvikene følges opp og rapporteres slik de skal. Der det er relevant blir partene informert og avvikene meldes til Datatilsynet. Personvernombudet gir samtidig uttrykk for at oppfølgingen av avvik i noen tilfeller kan ta litt for lang tid etter det registreres, slik at det blir krevende å nå 72-timers fristen.

De intervjuede enhetene har ikke selv rapportert noen avvik på personvernområdet de senere årene. Ellers er enhetene kjent med rutiner for rapportering av avvik, med unntak av barnehagen, hvor disse rutinene ikke er kjent.

4.5.2. Revisors vurdering av avvikshåndtering

Kommunen har rutiner for å registrere og behandle avvik på informasjonssikkerhet og personvern, og et saksbehandlingssystem som brukes til dette arbeidet. Kommunen har dokumentert noen registrerte avvik og meldinger til Datatilsynet de senere årene. Det er vår vurdering at kommunen har tilstrekkelige rutiner på dette området. Personvernombudet opplyser at saksbehandlingen i noen tilfeller kan ta litt tid. Vi har fått opplyst at kommunen arbeider med å innføre et nytt kvalitetssystem for håndtering og saksbehandling av avvik. Vi anbefaler at kommunen fortsetter dette arbeidet. I forbindelse med innføringen av nytt system for avvikshåndtering er det viktig at kommunens ansatte får nødvendig opplæring i det nye systemet.

4.6. Ivaretagelse av innsynsrett

Bamble kommune skal ha tiltak for å ivareta innsynsretten til de registrerte.

Kommunen skal gi klar og tydelig informasjon til den registrerte. Den registrerte skal også få informasjon om hvordan vedkommende kan utøve sine rettigheter. Datatilsynet anbefaler kommunen å ha en personvernerklæring på sine nettsider, med generell informasjon om kommunens personvernpolicy.

På kommunens nettside er det utfyllende informasjon om personvern og kommunens rolle som databehandler. Her opplyses det om kommunens behandling av opplysninger og hvilke rettigheter individer har, inkludert retten til innsyn, og det er lenket direkte til et relevant kontaktskjema. Kommunen opplyser også om retten til å klage til Datatilsynet. Det er også oppgitt kontaktinformasjon til kommunens personvernombud, samt informasjon om personvernombudets rolle.

Personvernombudet opplyser å ha mottatt noen få forespørsler om innsyn fra innbyggerne. Det har da handlet om helseopplysninger. Intervjuer med utvalgte enheter i kommunen viser samtidig at forespørsler om innsyn i opplysninger først og fremst rettes direkte til den relevante enheten og ikke via personvernombudet.

Skolen har gode rutiner for å håndtere innsynsforespørsler. Ved forespørsel om innsyn i en elevmappe, har skolen en rutine på å gå gjennom elevmappen for å fjerne interne notater, eller lærernotater, fra elevmappen. Hensikten med dette er å sørge for at man ikke utleverer personopplysninger om andre personer uten deres samtykke. Ellers oppbevarer ikke skolen informasjon om tidligere elever, så i slike tilfeller må henvendelsen gå til kommunen sentralt.

Barneverntjenesten mottar flere forespørsler om innsyn. I likhet med skolen har de en rutine på å gå gjennom mappen først, for å undersøke om deler av innholdet bør tas ut eller sladdes. Hensikten med denne rutinen er å unngå at det utleveres opplysninger om andre personer, dersom det foreligger i et internt notat. Barneverntjenesten mottar også innsynsforespørsler fra andre aktører på vegne av enkeltpersoner, og har da gode rutiner for å kontrollere at samtykke foreligger. Enheten opplever at innsynsforespørsler er en økende trend.

4.6.1. Revisors vurdering av innsynsretten

Bamble kommune har tiltak for å ivareta innsynsretten til de registrerte, både interne rutiner og informasjon til publikum om rettigheter og hvordan den registrerte kan utøve rettighetene i kommunen. De undersøkte enhetene har tilstrekkelige rutiner for å håndtere forespørsler om innsyn i dokumenter/mapper fra sine brukere på en sikker måte.

4.7. Informasjon om kommunens behandling av personopplysninger

Bamble kommune skal ha tiltak for å ivareta de registrertes rett til informasjon om kommunens behandling av deres personopplysninger.

4.7.1. Fakta om informasjon om behandling av opplysninger

Rutiner for informasjon

Bamble kommunes strategi for informasjonssikkerhet inneholder et eget avsnitt om de registrertes rettigheter. Strategidokumentet beskriver at kommunen skal sørge for at de registrerte får informasjon om hvordan kommunen behandler personopplysninger, samt hvilke rettigheter de registrerte har og hvordan disse rettighetene kan tas i bruk. Denne informasjonen skal gis i en personverkerklæring som skal være tilgjengelig via kommunens nettsider.

Personvernerklæring

Kommunens personvernerklæring er tilgjengelig på kommunens nettsider via lenken «personvern og informasjonssikkerhet», som presenteres sammen med øvrig kontaktinformasjon i kommunen. Personvernerklæringen gir generell informasjon om de nye personvernreglene som ble innført i 2018 (GDPR), kommunens rolle som databehandler og hvordan opplysninger blir behandlet. Personvernerklæringen opplyser også om de registrertes rettigheter, og man får informasjon om hvordan man kan gå frem for å ta i bruk disse rettighetene. Sammen med personvernerklæringen presenteres det informasjon om personvernombudet, inkludert kontaktinformasjon.

Observasjoner

Personvernombudet har mottatt noen få henvendelser som gjelder kommunens behandling av informasjon. Dette har handlet om kommunikasjon mellom skole og hjem via ulike digitale kanaler. Ved bekymring rundt dette har man da blitt enige om alternative kommunikasjonsformer. Barneverntjenesten opplyser at de informerer klienter om hvordan tjenesten behandler personopplysninger, dersom klientene etterspør slik informasjon. Det er ikke rutiner for informasjon utover dette.

4.7.2. Revisors vurdering av informasjon om behandlings av opplysninger

Bamble kommune har tiltak for å informere sine innbyggere og brukere av kommunens tjenester om hvordan kommunen behandler personopplysninger. Det sentrale tiltaket på dette området er kommunens personvernerklæring som er tilgjengelig via kommunens nettsider. Personvernerklæringen er utfyllende og oppdatert i henhold til den nye personopplysningsloven. Brukere av kommunale tjenester får ikke alltid informasjon om hvordan opplysninger behandles i møte med kommunens ulike enheter, slik som i eksempelet fra barneverntjenesten, men man vil kunne få slik informasjon på forespørsel.

4.8. Databehandleravtaler

Bamble kommune skal ha tiltak for å sikre at kommunen har databehandleravtale med alle databehandlere.

Kravet om å inngå databehandleravtaler er omtalt i kommunens strategi for informasjonssikkerhet. Kommunen har utarbeidet en egen rutinebeskrivelse for databehandleravtaler. Rutinen gir en oversikt over sentrale begreper på området og beskriver hvilke roller og ansvar partene har. Videre beskriver rutinen når kommunen plikter å inngå en databehandleravtale og hva en slik databehandleravtale må inneholde. Her viser rutinen til den relevante delen av personvernforordningen. Ifølge rutinen kan kommunen velge å bruke sine egne maler, leverandørens mal, eller andre faglig relevante maler når det skal skrives en databehandleravtale. En gjennomgang av kommunens databehandleravtaler viser at disse er en blanding av kommunens mal og leverandørers mal/avtale.

Kommunen har utarbeidet maler for databehandleravtaler – en generell mal og en mal som er særlig tilpasset helseområdet/helseopplysninger. Datatilsynet har en veiledning som beskriver hva en databehandleravtale må inneholde, og virksomheter (herunder kommuner) står fritt til å bruke sine egne databehandleravtaler så lenge disse er i tråd med personopplysningsloven.

Vi har valgt ut systemene som brukes for de behandlingsaktivitetene som ble plukket ut til kontroll i gjennomgangen av behandlingsprotokollen, og sjekket at det foreligger databehandleravtaler for disse. Dette gjelder følgende systemer:

- Visma Flyt Skole
- Visma Familia
- Public 360

Systemdokumentasjonen for Familia, datert 01.10.2020, indikerer at det ikke foreligger en databehandleravtale for dette systemet. Kommunen har imidlertid dokumentert databehandleravtalen for Familia, i likhet med de andre systemene vi undersøkte.

4.8.1. Revisors vurdering av databehandleravtaler

Kommunen har rutiner for inngåelse av databehandleravtaler, og kravet om databehandleravtaler er beskrevet i kommunens styrende dokument på området. De nåværende databehandleravtalene er en blanding mellom leverandørenes egne maler og kommunens mal. Kommunens mal er oppdatert i henhold til personopplysningsloven og ivaretar de kravene som stilles til slike avtaler. De undersøkte databehandleravtalene ivaretar også disse kravene. De foreligger databehandleravtaler for de systemene vi undersøkte.

Systemdokumentasjonen indikerte at det manglet databehandleravtale for ett av systemene, selv om avtalen faktisk foreligger. Vi anbefaler at kommunen går gjennom rutinene som skal sikre at systemdokumentasjonen er oppdatert.

5. Konklusjoner og anbefalinger

I denne delen av rapporten vil vi oppsummere og konkludere rundt de to problemstillingene som forvaltningsrevisjonen har tatt utgangspunkt i.

5.1. Konklusjoner

I hvilken grad har Bamble kommune etablert tiltak for å ivareta kravene i personopplysningsloven?

Vi finner at kommunen i har etablert flere gode tiltak for å ivareta kravene i personopplysningsloven, slik dette er beskrevet i styrende dokumenter på området og andre rutinebeskrivelser. Kommunen har oppdaterte styrende dokumenter, rutinebeskrivelser og maler som hensyntar de kravene som stilles i personopplysningsloven, og kommuneledelsen orienteres jevnlig om status på området.

Bamble kommune har en utfyllende og oppdatert personvernerklæring, rutiner for håndtering av innsynsforespørsler, og rutiner for registrering og håndtering av avvik på området. Kommunen har rutiner for gjennomføring av risikoanalyser ved anskaffelser av nye systemer, og fører en behandlingsprotokoll over sine behandlingsaktiviteter.

Vi har sett at behandlingsprotokollen ikke var helt oppdatert med alle systemer som var i bruk i kommunen. Vi så også at hjemmelen for behandling av personopplysninger ikke alltid var opplyst i protokollen.

Kommunens egen systemdokumentasjon for de systemene som behandler personopplysninger er ikke alltid fullstendig. Vi har sett et eksempel på at systemdokumentasjonen indikerte at det manglet en databehandleravtale, mens nærmere undersøkelser viste at avtalen eksisterte.

Kommunens arbeid med risikovurderinger og DPIA omtales både i styrende dokumenter og egne rutinebeskrivelser. Bamble kommune har maler som er oppdatert og i tråd med Datatilsynets veileder. Vi ser at kommunen i stor grad ivaretar kravene til risikovurderinger for systemer som behandler personopplysninger. Vi har sett ett tilfelle der det manglet risikovurdering. I tillegg har vi sett et tilfelle av en DPIA som kun var delvis gjennomført og ikke i tråd med minimumskravene for en DPIA.

Samtidig som kommunen i stor grad har gode tiltak og rutiner for å ivareta kravene i personopplysningsloven, så finner vi altså at kommunen har rom for forbedring på noen områder, samt behov for bedre rutiner når det gjelder gjennomføring og dokumentering av risikoanalyser og DPIA.

Hvordan blir sentrale krav i personopplysningsloven og kommunens egne tiltak fulgt opp i praksis i kommunens enheter?

I forbindelse med denne problemstillingen har vi undersøkt tre utvalgte enheter i kommunen gjennom intervjuer med ledelsen ved enhetene. Enhetene bestod av en skole, en barnehage og barneverntjenesten.

På et overordnet nivå fikk vi et godt inntrykk av hvordan det tenkes rundt, og jobbes med, informasjonssikkerhet og personvern i disse enhetene. Integritet, konfidensialitet og tilgjengelighet er tre sentrale personvernprinsipper. Av disse prinsippene er det særlig konfidensialitet som sikres gjennom gode systemer og rutiner, samt bevissthet rundt personvern, i den daglige driften i enhetene i kommunen.

Når det gjelder konfidensialitet er det vårt inntrykk at enhetene er bevisste på å behandle personopplysninger på en sikker måte. Behandlingen foregår i godkjente fagsystemer og utveksling/utlevering av dokumenter med personopplysninger gjøres via sikre kanaler eller ved fysiske møter. Det er gode rutiner for fullmakt ved innsynsforespørsler, og rutiner for gjennomgang av dokumentene/mappene slik at ikke opplysninger om andre personer utleveres ved en feil. Det er gode rutiner i kommunen når det gjelder tilgangsstyring for ansatte i fagsystemene, og det er en høy grad av bevissthet i enhetene når det gjelder tilgang til, og sikring av, personopplysninger.

5.2. Anbefalinger

Vi anbefaler at Bamble kommune

- vurderer om det er behov for å oppdatere rutiner, roller og ansvarsfordeling når det gjelder gjennomføring av risikovurdering og DPIA for systemer som behandler personopplysninger
- vurderer om det er hensiktsmessig å fastsette en formell stillingsprosent for rollen som personvernombud, da dette i dag er en delt stilling uten en fast stillingsprosent, dersom man ser et behov for at personvernombudet i større grad gjennomfører kontrolloppgaver
- gjennomgår rutinene for oppdatering av behandlingsprotokollen slik at den til enhver tid er oppdatert med tanke på de systemene som er i bruk i kommunen
- gjennomgår rutinene for registreringer i behandlingsprotokollen, og sørger for at behandlingsgrunnlag registrerer korrekt med lovhjemmel i de tilfeller der dette kreves
- fortsetter arbeidet med å innføre et nytt kvalitetssystem, og sørger for at ansatte får nødvendig opplæring i systemet

Litteratur og kildereferanser

Lover og forskrifter

Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysingsloven/GDPR).
Lov 22. juni 2018 nr. 83 om kommuner og fylkeskommuner (kommuneloven).
Forskrift 17. juni 2019 nr. 904 om kontrollutvalg og revisjon.

Kommunens dokumenter

Dokument	Strategi for informasjonssikkerhet ved behandling av personopplysninger.
Dokument	Rutine for anskaffelser av IKT-systemer.
Dokument	Rutine for håndtering av avvik.
Dokument	Kommunens systemdokumentasjon for de undersøkte systemene.
Dokument	Kommunens oversendte risikovurderinger og DPIA og tilhørende maler.
Dokument	Kommunens mal for databehandleravtale.
Dokument/system	Kommunens databehandlingsprotokoll.

Elektroniske kilder

Datatilsynet: https://www.datatilsynet.no/, nettsides beskrivelser og veiledere knyttet sentrale deler av etterlevelse av personvernloven:

- «Behandlingsansvarlig og databehandler», sist endret 17.07.19. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/databehandleravtale/behandlingsansvarlig-og-databehandler
- «Behandlingsgrunnlag», sist endret 08.08.19. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsgrunnlag/veileder-om-behandlingsgrunnlag/
- «Hvordan lage en databehandleravtale?», sist endret 20.12.19. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/databehandleravtale/hvordan-lage-en-databehandleravtale/
- «Veiledning om de grunnleggende personvernprinsippene», sist endret 16.07.19. https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/
- «Vurdering av personvernkonsekvenser (DPIA)», sist endret 17.07.19. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/

Bøker

Jarbekk, Eva og Simen Sommerfeldt, Personvern og GDPR i praksis. Oslo: Cappelen Damm Akademisk, 2019.

Vedlegg

Vedlegg 1: Kommunedirektørens uttalelse

Bamble kommune
Service- og dokumentsenter

Vestfold og Telemark revisjon IKS
Postboks 2805
3702 SKIEN

Unntatt offentlighet ihht § Offl § 5

Deres ref.	Vår ref.	Dato
	22/06520-12	28.09.2022

Svar - foreløpig rapport til høring: Forvaltningsrevisjon personvern

Viser til foreløpig rapport om informasjonssikkerhet og personvern i Bamble kommune.

Rapporten har vært sendt på intern høring og følgende tilbakemeldinger er mottatt innen oppgitt frist:

Pkt. 4.1.2 Siste ledd:
Foreslår at sist setning endres til:
Kommunens ledelse, representert ved kommunedirektøren, deltar jevnlig i møter med ITG – felles IT-enheten i Grenland, driftssamarbeidet og personvernombud hvor status på området informasjonssikkerhet og personvern er tema.

Viktig å erstatte IT-leverandør til ITG samarbeidet, da IT-leverandører omfavner alle våre leverandører og det blir ikke riktig at Kommunedirektøren deltar på disse møtene, da det er delegert ut i linjen.

Det er ikke kommet andre merknader til høringsrapporten.

Bamble kommune vil utarbeidet en plan for å iverksette nødvendige tiltak for å få på plass anbefalinger som kommer fram av rapporten.

Nytt system for internkontroll og avvik, Compilo er under implementering og opplæring er en vesentlig del av implementeringen og er helt avgjørende for å lykkes med prosjektet.

I tillegg har systemet en egen GDPR modul som vi kommer til å ta i bruk i løpet av implementeringsfasen. Vi håper at det vil bidra til bedre kvalitetssikring og oppdatering av lovpålagte krav, da vi ser for oss å utarbeide årshjul som sikrer oppfølging i organisasjonen knyttet til informasjonssikkerhet og personvern.

Postadresse
Bamble kommune
Postboks 80
3993 LANGESUND

Besøksadresse
Kirkeveien 12
3970 LANGESUND

www.bamble.kommune.no

Telefon: +47 35965000

Epost: postmottak@bamble.kommune.no

Bankgiro: 2601.35.89681
Org.nr.: 940 244 145 MVA

Med hilsen

Geir Håvard Bjelkemyr-Østvang
Kommunedirektør
Mobil 97058570

Brevet er godkjent elektronisk.

Kopi til: Lars Pedersen
Administrasjon og organisasjonsutvikling /v Grim Eide
Plan og økonomi /v Gunn Ellen Berg
Service- og dokumentsenter /v Sissel Jensen
Service- og dokumentsenter /v Anne Marie Eliassen
Service- og dokumentsenter /v Ole Kristian F Olsen

Vedlegg 2: Revisjonskriterier

Kommunens ansvar for forsvarlig håndtering av personopplysninger er regulert av personopplysningsloven. Personopplysningsloven gjennomfører EUs personvernforordning (GDPR) i norsk rett, jf. personopplysningsloven § 1. Formålet er å fastsette regler om vern av fysiske personer i forbindelse med behandling av personopplysninger, og regler om fri utveksling av personopplysninger.

Personopplysningsloven og forordningen gjelder for helt eller delvis automatisert behandling av personopplysninger og for ikke-automatisert behandling av personopplysninger dersom opplysningene inngår i eller skal inngå i et register, jf. personopplysningsloven § 2.

Kommunen behandler personopplysninger om innbyggere, ansatte og politikere. For å ivareta en forsvarlig behandling av personopplysningene, plikter kommunen å sette i verk egnede tiltak for å sikre og påvise at personopplysninger behandles i samsvar med regelverket, jf. personvernforordningen art. 24. Tiltakene skal være både tekniske og organisatoriske, og kommunen skal ha en systematisk tilnærming til dette (internkontroll). Internkontrollen skal ivareta den registrertes rettigheter og friheter, og ivareta virksomhetens mål med behandlingen av personopplysningene. Tiltakene skal dokumenteres og oppdateres ved behov.

Personopplysningene skal beskyttes mot uberettiget innsyn og endringer, men skal være tilgjengelige for de som trenger opplysningene, når de trenger dem. Dette blir ofte benevnt med at kommunens informasjonssikkerhetsarbeidet skal ivareta personopplysningenes:

- konfidensialitet
- integritet (riktighet)

- tilgjengelighet

Behandlingsansvarlig

Behandlingsansvarlig er en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes, jf. personvernforordningen art. 4. Det betyr at Bamble kommune er behandlingsansvarlig for personopplysninger som kommunen samler inn og benytter.

Den som behandler personopplysninger på vegne av andre, er databehandler. Personvernforordningen setter strenge krav til databehandlere. Vi undersøker ikke situasjoner der Bamble kommune eventuelt er databehandler på vegne av andre oppdragsgivere.

Det er Bamble kommune som juridisk person som er behandlingsansvarlig. Ledelsen kan delegere oppgaver knyttet til behandling av personopplysninger, men selve behandlingsansvaret kan ikke delegeres.

Personvernombud

Offentlige myndigheter og organer som behandler personopplysninger, skal utpeke personvernombud. Personvernombudet skal utpekes på grunnlag av faglige kvalifikasjoner, og særlig på grunnlag av dybdekunnskap om personopplysningsloven og praksis på området samt evne til å utføre oppgavene. Personvernombudet kan være en ansatt hos kommunen, eller kommunen kan kjøpe tjenesten. Personvernombudet skal ikke ha andre oppgaver som kommer i konflikt med rollen, og kan ikke avsettes eller straffes for å utføre sine oppgaver som personvernombud. Personvernombudet skal gi råd til ledelsen i kommunen, kontrollere at kommunen følger personvernreglene og være kontaktpunkt for Datatilsynet (personvernforordningen art. 37, 38 og 39).

Personvernprinsippene

Når virksomheter behandler personopplysninger, skal behandlingen baseres personvernprinsippene i art. 5 i personvernforordningen. Prinsippene er:

- lovlighet, rettferdighet og åpenhet
- formålsbegrensning
- dataminimering
- riktighet
- lagringsbegrensning
- integritet og fortrolighet
- ansvarlighet

Personopplysningsloven bygger på disse prinsippene. Datatilsynet har utdypet prinsippene i en veileder. Bamble kommune som behandlingsansvarlig har ansvar for å følge opp disse prinsippene.

Lovlig, rettferdig og gjennomsiktig

Personvernforordningen art. 6 regulerer i hvilke tilfeller det er lovlig å behandle personopplysninger. Det rettslige grunnlaget kan blant annet være samtykke fra den registrerte, at behandlingen er nødvendig for å oppfylle en rettslig forpliktelse, eller for å utøve offentlig myndighet.

Dersom kommunen behandler sensitive personopplysninger, må i tillegg minst ett av vilkårene i personvernforordningen art. 9 være oppfylt. Disse kravene er blant annet at det foreligger uttrykkelig samtykke fra den registrerte, at behandlingen er nødvendige for at kommunen skal oppfylle sine forpliktelser innenfor arbeidsrett, trygderett og sosialrett, eller at behandlingen er nødvendig for å yte helse og sosialtjenester.

At behandlingen skal være rettferdig, innebærer at kommunen skal ha respekt for den registrertes interesser og rimelige forventinger.

At en behandling er åpen, innebærer at det er oversiktlig og forutsigbart for den registrerte. Personvernforordningen kapittel III omhandler den registrertes rettigheter. Art. 12 krever at kommunen skal gi klar og tydelig informasjon til den registrerte. Den registrerte skal også få informasjon om hvordan vedkommende kan utøve sine rettigheter. Datatilsynet anbefaler kommunen å ha en personvernerklæring på sine nettsider, med generell informasjon om kommunens personvernpolicy. Den registrerte skal få informasjon fra kommunen ved innsamling av opplysningene (art. 13), og har rett til innsyn i de personopplysningene kommunen har om vedkommende (art. 15). Den registrerte skal ha rett til å få uriktige personopplysninger om seg selv rettet (artikkel 16), og kan også i spesielle tilfeller ha rett til å få slettet personopplysninger om seg selv (art. 17).

Formålsbegrensning
Personopplysninger skal bare brukes til det formålet de er innhentet for. Hvis personopplysninger skal gjenbrukes, må behandlingen enten være lovfestet eller det må innhentes nytt samtykke.

Dataminimering
Prinsippet om dataminimering innebærer å begrense mengden innsamlede personopplysninger til det som er nødvendig for å realisere innsamlingsformålet.

Riktighet
Personopplysninger som behandles skal være korrekte. Opplysningene skal også oppdateres hvis det er nødvendig.

Lagringsbegrensning

Prinsippet om lagringsbegrensning innebærer at personopplysninger skal lagres slik at de slettes eller anonymiseres når de ikke lengre er nødvendige for formålet de ble innhentet for. Kommunen bør innføre tidsfrister for sletting eller periodisk gjennomgang for å sikre at personopplysninger ikke oppbevares lengre enn nødvendig.

Integritet og fortrolighet
Kommunen skal sørge for:

- beskyttelse mot uautorisert utlevering og tilgang til personopplysninger
- beskyttelse mot utilsiktet og ulovlig ødeleggelse, tap og endringer av personopplysninger
- at personopplysninger er tilgjengelige for autoriserte personer når det er nødvendig
- at personopplysninger ikke gjøres tilgjengelig for et ubegrenset antall mennesker uten den berørte personens medvirkning
- å spore endringer som gjøres i systemet og for å kunne håndtere sikkerhetsbrudd
- at systemene som behandler personopplysninger er robuste mot for eksempel sårbarheter, angrep og uhell

Ansvarlighet
Kommunen har ansvar for å opptre i samsvar med reglene for behandling av personopplysninger. Kommunen må også kunne vise at den faktisk opptrer i samsvar med reglene. Dette betyr at kommunen må ha internkontroll.

Internkontroll

Ifølge kommuneloven § 25-1 skal kommunen ha internkontroll med administrasjonens virksomhet for å sikre at lover og forskrifter følges. Kommunedirektøren er ansvarlig for internkontrollen.

Kravene til internkontroll for personvern står i kapittel IV i personvernforordningen.

Datatilsynets veileder for internkontroll og informasjonssikkerhet legger til grunn at internkontroll skal bestå av:

- styrende elementer, som i hovedsak retter seg mot ledelsen, herunder hvilke beslutninger og føringer de legger for internkontroll.
- gjennomførende elementer, som i hovedsak retter seg mot ansatte. Her finner man beskrivelse av rutiner som er tilpasset den enkeltes arbeidssituasjon.
- kontrollerende elementer, som bidrar til å fange opp avvik fra systemet og til at det gjennomføres periodiske gjennomganger.

Typiske styrende og kontrollerende elementer i internkontrollen er blant annet at ansvar og myndighet må være tydelig plassert, og det må etableres rutiner for rapportering og kontroll.

Ved innføring av internkontroll må virksomheten først identifisere hvilke personopplysninger som behandles. Deretter må det utarbeides en risikovurdering. Så må kommunen lage rutiner og retningslinjer som reduserer risikoen til et akseptabelt nivå.

Art. 30 krever at kommune fører protokoller over behandlingsaktiviteter. En protokoll skal vise formålet med behandlingene, hvilke kategorier personopplysninger kommunen behandler, tidsfrister for sletting og beskrivelse av tekniske og organisatoriske sikkerhetstiltak. Hvis det er aktuelt, skal også eventuelle databehandlere stå oppført i protokollen.

Art. 35 krever at ved behandlinger som vil medføre høy risiko for fysiske personers rettigheter og friheter, skal kommunen gjennomføre en vurdering av personvernkonsekvenser, også kalt DPIA[4]. DPIA er nødvendig siden kommunen behandler sensitive opplysninger i stor skala. Vurderingen skal minst inneholde:

a) en systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålene med behandlingen,
b) en vurdering av om behandlingsaktivitetene er nødvendige og står i et rimelig forhold til formålene,
c) en vurdering av risikoene for de registrertes rettigheter og friheter, og
d) de planlagte tiltakene for å håndtere risikoene og for å påvise at personvernreglene overholdes.

Personvernforordningen artikkel 5 nr. 1 bokstav e) krever at kommunen har rutiner som sikrer tilstrekkelig sikkerhet for integriteten og konfidensialiteten til personopplysningene. Kommunen skal sikre personopplysningene mot uautorisert eller ulovlig behandling, og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak. Ifølge artikkel 24 skal kommunen gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med personvernforordningen. Ifølge artikkel 32 skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som passer til risikoen.

Kommunen skal ha et system for å fange opp brudd på personopplysningssikkerheten. Hvis det oppstår brudd på sikkerheten rundt personopplysninger, skal kommunen melde fra til Datatilsynet. Dersom det er sannsynlig at bruddet vil føre til risiko for personene det gjelder, skal kommunen underrette den registrerte. Alle brudd på personopplysningssikkerheten skal dokumenteres (art. 33 og 34).

Internkontroll og arbeidet med informasjonssikkerhet er et dynamisk arbeid som alltid vil være under utvikling. Datatilsynet anbefaler derfor å ha rutiner for å forbedre internkontrollen, herunder

[4] DPIA står for Data Protection Impact Assessment

rutiner for rapportering fra sikkerhetshendelser, avvikshåndtering og egenkontroll. Rapporteringen skal beskrive hvilke erfaringer som er gjort og inneholde forslag til forbedringer.

Ledelsen i kommunen skal også ha en årlig gjennomgang av sikkerhetsmål, sikkerhetsstrategi og organisering av informasjonssystemene. Målet for gjennomgangen er å sikre at internkontrollen oppfyller kommunens behov og gjøre nødvendige oppdateringer.

Registrertes rettigheter

Den registrerte er den personen personopplysningene omhandler. Den registrerte har rett til å få informasjon ved innsamling av opplysningene, blant annet om formålet og det rettslige grunnlaget for behandlingen, og eventuelle mottakere av personopplysningene (personvernforordningen art 13).

Den registrerte har rett til innsyn i hvilke personopplysninger om vedkommende kommunen behandler (personopplysningsloven art.15). Den registrerte har rett til å be om at uriktige personopplysninger om seg selv rettes (personopplysingsloven art 16). Videre kan den registrerte be om å få personopplysninger om seg selv slettet (personopplysningsloven art 17). Det er imidlertid flere begrensninger på retten til å få personopplysninger slettet. Blant annet kan ikke kommunen slette personopplysninger som skal bevares for arkivformål, eller som må bevares for å oppfylle en rettslig forpliktelse.

Databehandlere

En databehandler behandler personopplysninger på vegne av en behandlingsansvarlig (kommunen). Et eksempel på en databehandler er en leverandør av programvare som kommunen bruker til å behandle personopplysninger, hvis leverandøren har tilgang til programmet for å gjøre oppdateringer og support.

Forholdet mellom en behandlingsansvarlig virksomhet og databehandleren skal være regulert i en databehandleravtale. Avtalen skal sikre at personopplysningene blir behandlet i samsvar med regelverket, også av databehandleren, og skal sette en klar ramme for hvordan databehandleren kan behandle personopplysningene. En databehandleravtale kan være en frittstående avtale mellom partene, eller en integrert del av annet avtaleverk.

Den behandlingsansvarlige kan bare benytte databehandlere og underleverandører som kan dokumentere tilstrekkelige garantier for

- at kravene i personopplysningloven blir ivaretatt
- at personopplysningene som behandles er tilstrekkelig sikret (personopplysningsloven artikkel 28 nr. 1).

Kommunen skal vurdere om databehandleren gir tilfredsstillende garantier for de personopplysningene som skal behandles.

En databehandleravtale skal inneholde:

- behandlingens art, formål og varighet
- kategorier av registrerte og typer av personopplysninger
- pliktene og rettighetene til den behandlingsansvarlige
- forpliktelsene til databehandleren

Revisjonskriterier

På denne bakgrunn har vi utledet følgende revisjonskriterier:

Bamble kommune skal ha

- en organisasjon med klar plassering av ansvar og myndighet for behandlingen av personopplysninger, samt rutiner for rapportering
- personvernombud, organisert i samsvar med personopplysningsloven
- protokoll over hvilke personopplysninger kommunen behandler
- risikovurderinger og dokumenterte vurderinger av personvernkonsekvenser (DPIA)
- tiltak for å håndtere brudd på personopplysningssikkerheten
- tiltak for å ivareta innsynsretten til de registrerte
- tiltak for å ivareta de registrertes rett til informasjon om kommunens behandling av deres personopplysninger
- tiltak for å sikre at kommunen har databehandleravtale med alle databehandlere

Vedlegg 3: Metode og kvalitetssikring

Forvaltningsrevisjonen startet opp ved oppstartsbrev 10.05.22. Oppstartsmøte ble gjennomført 25.05.22 med virksomhetsleder service- og dokumentsenter, kommunens personvernombud og øvrige representanter for kommunens IT-arbeid.

Forvaltningsrevisjoner skal gjennomføres på en måte som sikrer at informasjonen i rapporten er relevant og pålitelig. At dataene er relevante (gyldige/valide) innebærer at de beskriver de forholdene som problemstillingene omhandler. Pålitelighet (reliabilitet) handler om at innsamling av data skal skje så nøyaktig som mulig og at det ikke har skjedd systematiske feil underveis.

Innsamling av data, relevans og pålitelighet

Datainnsamlingen startet i mai 2022 og pågikk ved behov gjennom arbeidet med forvaltningsrevisjonen, da vi ble gitt tilgang til kommunens intranett hvor store mengder relevant dokumentasjon foreligger. For å kartlegge kommunens tiltak for å ivareta kravene i personopplysningsloven har vi innhentet og gjennomgått dokumentasjon fra kommunen. Denne dokumentasjonen har vært styringsdokumenter, rutinebeskrivelser, maler for ulike dokumenter/prosesser, systemdokumentasjon og registreringer i kommunens systemer. Gjennomgangen av kommunens dokumentasjon gir et bredt bilde av kommunens arbeid på området informasjonssikkerhet og personvern. I tillegg til en generell gjennomgang av dokumentasjonen har vi også brukt deler av dokumentasjonen som utgangspunkt for stikkprøver, hvor vi har sett nærmere på enkelte systemers risikovurderinger, databehandleravtaler og

registreringer i behandlingsprotokollen. Vi har også gjennomført intervjuer med utvalgte enheter i kommunen, samt med kommunens personvernombud.

Intervjuer
Vi har gjennomført intervjuer med kommunens personvernombud, leder for barneverntjenesten, og ledelsen ved Stathelle skole og Falkåsen barnehage. Intervjuene var semi-strukturerte, hvilket betyr at det ble brukt en intervjuguide, men at intervjuene ellers var åpne med rom for oppfølgingsspørsmål, avklaringer og temaer utenfor intervjuguiden. Intervjudeltakerne ble orientert om tema/agenda på forhånd, og i etterkant av intervjuene ble det sendt ut et referat til godkjenning. Her kunne deltakerne også korrigere eventuelle feil i referatet.

Stikkprøver
Vi gjennomførte en stikkprøvekontroll av kommunens behandlingsprotokoll. Det ble gjort en tilfeldig utvelgelse av seks ulike behandlingsaktiviteter knyttet til skole. I tillegg inngikk alle registreringene under barne- og familievern. Avgrensningen til disse områdene ble gjort ut fra en vurdering av risiko (omfang og type personopplysninger). På grunn av protokollens struktur ville en tilfeldig utvelgelse med hele protokollen som utgangspunkt kunne resultere i at de undersøkte behandlingsaktivitetene var mindre relevante. Hensikten med stikkprøvekontrollen var å sjekke hvilke opplysninger som var registrert i protokollen, hvorvidt nødvendige opplysninger var registrert, og mer generelt undersøke hvordan kommunen bruker behandlingsprotkollen. De systemene som inngikk i de undersøkte behandlingsaktivitetene, ble også undersøkt nærmere når det gjelder risikovurderinger og databehandleravtaler.

Vi har sjekket ut med administrasjonen at fakta i rapporten er korrekt framstilt. Rapporten er sendt kommunedirektøren til uttalelse, jf. forskrift om kontrollutvalg og revisjon § 14. Uttalelsen ligger i vedlegg 1.

Personopplysninger

I forbindelse med denne forvaltningsrevisjonen har vi behandlet personopplysninger som navn og epostadresse til ansatte i kommunen.

Vårt rettslige grunnlag for å behandle personopplysninger er kommuneloven § 24-2 fjerde ledd.

Vi behandler personopplysninger slik det er beskrevet i vår personvernerklæring. Personvernerklæringen er tilgjengelig på vår nettside vtrevisjon.no.

God kommunal revisjonsskikk - kvalitetssikring

Forvaltningsrevisjon skal gjennomføres, dokumenteres, kvalitetssikres og rapporteres i samsvar med kommuneloven og god kommunal revisjonsskikk.[5]

Kvalitetssikringen skal sikre at undersøkelsen og rapporten har nødvendig faglig og metodisk kvalitet. Videre skal det sikres at det er konsistens mellom bestilling, problemstillinger, revisjonskriterier, data, vurderinger og konklusjoner.

Vestfold og Telemark revisjon IKS har et system for kvalitetskontroll som er i samsvar med den internasjonale standarden for kvalitetskontroll.[6] Denne forvaltningsrevisjonen er kvalitetssikret i samsvar med vårt kvalitetskontrollsystem og i samsvar med kravene i RSK 001.

[5] God kommunal revisjonsskikk i forvaltningsrevisjon og eierskapskontroll kommer til uttrykk først og fremst i RSK 001 Standard for forvaltningsrevisjon og RSK 002 Standard for eierskapskontroll. Gjeldende standarder er fastsatt av Norges Kommunerevisorforbunds styre høsten 2020. Standarden bygger på norsk regelverk og internasjonale prinsipper og standarder, fastsett av International Organization of Supreme Audit Institutions (INTOSAI) og Institute of Internal Auditors (IIA).

[6] ISQC 1 Kvalitetskontroll for revisjonsfirmaer som utfører revisjon og begrenset revisjon av regnskaper samt andre attestasjonsoppdrag og beslektede tjenester

På vakt for fellesskapets verdier

Rapporten er utarbeidet av
Vestfold og Telemark revisjon IKS

Har du spørsmål til rapporten?
Ta kontakt med oss:
Telefon: 33 07 13 00
E-post: post@vtrevisjon.no

www.vtrevisjon.no

22: 3813 403