Rapport

SARPSBORG KOMMUNE

04.04.2023

Forvaltningsrevisjon

Personvern

Innhold

1 SAMMENDRAG

Bakgrunn

Østre Viken kommunerevisjon IKS utfører forvaltningsrevisjon på oppdrag fra Sarpsborg kontrollutvalg. I plan for forvaltningsrevisjon 2022-2024, som bystyret vedtok 27.01.2022 i sak 2/22, ble det vedtatt at det skulle gjennomføres en undersøkelse av Sarpsborg kommunes ivaretakelse av personvern, i planperioden. Under møtet til Sarpsborg kontrollutvalg den 28.09.2022, sak 22/39, vedtok kontrollutvalget et innspill om at forvaltningsrevisjonen på personvern burde se nærmere på bruk av nettbrett/programmer i skolen.

Revisjonens fremgangsmåte

Temaet som kontrollutvalget ønsket undersøkt, er løst gjennom en forvaltningsrevisjon i tråd med «Standard for forvaltningsrevisjon» (RSK 001/god revisjonsskikk) og ved å følge Østre Viken kommunerevisjons (ØVKR) mal for forvaltningsrevisjoner. Revisjonen er utført med bistand fra rådgivningsselskapet BDO AS. Som et ledd i etterlevelse av RSK 001 har det vært en dedikert ressurs med ansvar for å kvalitetssikre at revisjonen har fulgt standarden. Revisjonen har også hatt dialog med både ØVKR og Sarpsborg kommune under gjennomføringen av revisjonen.

Fremdriftsplanen besto av følgende elementer:

- Planlegging
  - Oppstartsmøter
  - Forankring av revisjonskriterier hos ØVKR.
  - Oppstartsbrev, informasjonsinnhenting og oversendelse av revisjonskriterier.
- Gjennomføring
  - Analyse av dokumenter og forespørsel om ytterlige dokumentasjon.
  - Gjennomføring av intervju og spørreundersøkelse.
  - Beskrivelse av datagrunnlag.
  - Analyse, vurdering og konklusjon.
- Sluttføring
  - Utarbeidelse av rapport.
  - Verifisering av faktagrunnlag fra Sarpsborg kommune.
  - Gjennomgang av rapport med Sarpsborg kommune.

Revisjonskriterier

Revisjonskriteriene er basert på sentrale krav i personopplysningsloven[1] og EUs personvernforordning 2016/679 (heretter GDPR), samt Datatilsynets veiledere som utdyper hvordan kravene skal tolkes.

Revisjonens funn

Revisjonen har jobbet ut fra problemstillingen:
Har Sarpsborg kommune sikret at kommunen etterlever kravene i personopplysningsloven, herunder personvernforordningen (GDPR)?
Revisjonen har hatt et særlig fokus på bruk av nettbrett og programmer i skolen.

Revisjonen vurderer at Sarpsborg kommune har iverksatt en rekke tiltak som kan bidra til å sikre at kommunen etterlever kravene i personopplysningsloven og GDPR. Kommunen ivaretar flere krav på en tilfredsstillende måte, men enkelte krav er likevel ikke ivaretatt tilfredsstillende.

[1] Lov av 15. juni 2018 nr. 38 om Lov om behandling av personopplysninger

Kommunen har lykkes godt i å utarbeide et helhetlig styringssystem for personvern, men dette inneholder enkelte elementer som ikke er tilfredsstillende. Disse elementene er beskrevet under. Kommunen har sikret at styringssystemet er implementert, og kommunen har i stor grad har lykkes med å etablere en personvernkultur. Revisjonen vil trekke frem at de styrende dokumentene og de større kontrollaktivitetene som kommunen har etablert, er hensiktsmessige. Kommunen viser en modenhet når det gjelder gjennomføring av risikovurderinger innen personvern og personvernkonsekvensvurderinger, selv om arbeidet med flere av vurderingene ikke er ferdigstilt.

Revisjonen mener at de kravene som kommunen ikke ivaretar tilfredsstillende, i hovedsak er

- utforming av dokumenterte rutiner og retningslinjer. Dette påvirker også kommunens etterlevelse av andre sentrale krav som sletting, oppfyllelse av de registrertes rettigheter og lovlighetsvurderinger.
- dokumentasjon av lovlighetsvurderinger og vurderinger av overføringer av personopplysninger til land utenfor EØS (tredjeland).
- utfylling og vedlikehold av protokoll over behandlingsaktiviteter. Dette påvirker også kommunens evne til å dokumentere etterlevelse av andre sentrale krav, som for eksempel kravene til å definere slettefrister og dokumentere overføringer av personopplysninger til land utenfor EØS (tredjeland).
- kontroll av databehandlere og revisjon av databehandleravtaler.

Revisjonens konklusjon og anbefalinger

Revisjonen konkluderer med at Sarpsborg kommune har etablert en rekke tiltak som vil bidra til at kommunen etterlever personopplysningsloven og GDPR, men at det er noen krav i GDPR som ikke er ivaretatt på en tilfredsstillende måte.

Basert på våre vurderinger og konklusjon har vi følgende anbefalinger:

a) Risikovurderinger av kommunens behandling av personopplysninger bør ferdigstilles og deretter oppdateres jevnlig. Kommunen bør også vurdere å sikre at alle risikovurderinger inneholder beskrivelser av hvilke momenter som er vektlagt, og hvilke konkrete konsekvenser knyttet til personvern som risikoscenariene kan lede til.

   Videre kan kommunen utdype kriteriene for fastsetting av score for konsekvenser innen personvern slik at disse for eksempel dekker flere grader av økonomisk tap og grader av helseskade, samt flere ofte brukte personvernkonsekvenser som integritetstap i forskjellig grad, tap av tilgang på tjenester og nedkjølingseffekt.

b) Kommunen bør utarbeide flere rutiner og retningslinjer som beskriver hvordan (altså fremgangsmåten når) kommunen skal ivareta sentrale krav som
   - lovlighet[2]
   - DPIA
   - samtlige av de registrertes rettigheter, herunder frister og formkrav som gjelder ved oppfølging av forespørsler om håndheving av rettighetene
   - sletting av personopplysninger
   - kartlegging og vurdering av overføringer av personopplysninger til tredjeland

   I den grad det er naturlig, kan kommunen legge dette inn i eksisterende rutiner og retningslinjer.

   Videre bør følgende temaer oppdateres i eksisterende rutiner:

[2] Etter GDPR artikkel 6, artikkel 9 og artikkel 10, samt personopplysningsloven § 12.

- Beskrivelsen av personvernprinsippene i retningslinjen for behandling av personopplysninger, slik at denne i større grad gjenspeiler definisjonene i GDPR artikkel 5.
- Beskrivelsen av hva den registrerte skal motta ved innsynsforespørsel etter GDPR, slik at denne samsvarer med kravene i GDPR artikkel 15.

c) Egenkontrollen for informasjonssikkerhet bør utvides eller suppleres med flere spørsmål knyttet til personvern. Dette kan for eksempel være spørsmål som:
   - Har enheten påbegynt ny behandling av personopplysninger, eller endret eksisterende behandling av personopplysninger?
   - Har enheten utført kontroll av at sine aktiviteter i protokollen over behandlingsaktiviteter og personvernerklæringen det siste året?
   - Har enheten vurdert behovet for å oppdatere DPIA-er det siste året?
   - Har enheten vurdert behovet for å revidere databehandleravtaler og utføre kontroll med databehandlere det siste året?
   - Har enheten utført kontroller knyttet til sletting av personopplysninger?
   - Har enheten utført kontroller knyttet til lagring av personopplysninger i korrekt fagsystem?
   - Har enheten utført stikkprøver eller andre kontroller på at enhetens personvernrutiner følges?

d) Kommunen bør sikre at den har vurdert og dokumentert lovlighet etter alle relevante bestemmelser i GDPR for alle behandlingsaktiviteter som kommunen utfører.

e) Det bør utarbeides slettefrister for alle behandlingsaktiviteter, der det er aktuelt, bør plikten til å bevare personopplysningene dokumenteres i stedet. Kommunen kan gjøre dette i forbindelse med oppdatering av protokollen over behandlingsaktiviteter.

f) Kommunen bør vurdere å fullt ut implementere Datatilsynets krav om når det alltid skal gjennomføres en DPIA, i kommunens rutiner som beskriver når DPIA skal gjennomføres.

g) Det bør sikres at kommunen har en fullstendig oversikt over alle databehandlere og at det er inngått databehandleravtale med disse. Det bør også sikres at det utføres periodisk kontroll med databehandlere og periodisk revisjon av databehandleravtaler, slik at det sikres at databehandleravtalene er oppdaterte. Omfang og hyppighet bør baseres på en risikobasert tilnærming. Kommunen kan hente inspirasjon fra det danske datatilsynets veileder for tilsyn (kontroll) med databehandlere. Videre kan kommunen vurdere å klargjøre i sine rutiner at det ikke bare er IKT-leverandører som kan være databehandlere.

h) Kartleggingen av og dokumentasjon av alle overføringer av personopplysninger til tredjeland bør ferdigstilles. Kommunen bør også sikre at alle overføringer er vurdert og fulgt opp i tråd med Datatilsynets veiledning for området og at innholdet i vurderingene dokumenteres.

i) Pågående og planlagte aktiviteter som oppdatering av protokoll over behandlingsaktiviteter og oppfriskningskurs i personvern bør gjennomføres.

2 MANDAT FOR FORVALTNINGSREVISJONEN

Revisjonen skal i henhold til kommuneloven § 24-2 (1) utføre forvaltningsrevisjon. Etter loven innebærer forvaltningsrevisjon å gjennomføre systematiske vurderinger av økonomi, produktivitet, regeletterlevelse, måloppnåelse og virkninger ut fra kommunestyrets vedtak og forutsetninger. Østre Viken kommunerevisjon IKS gjennomfører forvaltningsrevisjon i tråd med god kommunal revisjonsskikk. God kommunal revisjonsskikk er å følge RSK 001; Standard for forvaltningsrevisjon, utarbeidet av Norges kommunerevisorforbund (NKRF). Dette innebærer blant annet at rapporten skal skille klart mellom hva som er innsamlet data og hva som er revisjonens vurderinger. Det skal være en tydelig sammenheng mellom problemstillinger, faktaopplysninger, vurderinger, konklusjoner og eventuelle anbefalinger. Etter kommuneloven skal revisor rapportere resultatene av sin revisjon til kontrollutvalget.

Forvaltningsrevisjonen er gjennomført på bakgrunn av plan for forvaltningsrevisjon vedtatt i bystyret 27.01.2022 sak 2/22. Plan for gjennomføring av forvaltningsrevisjonen ble vedtatt i kontrollutvalget 29.november 2022 i sak PS 22/20. Planen ble vedtatt i tråd med revisjonens forslag.

Forvaltningsrevisjonen er gjennomført etter vedtatt prosjektplan i tidsrommet desember 2022 til februar 2023. Vi har gjennomført oppstartsmøte med kommuneadministrasjonen slik at også administrasjonens innspill er tatt hensyn til.

Vi har kvalitetssikret faktagrunnlaget underveis, både gjennom verifisering av intervjuer og intern kvalitetssikring. I tillegg er rapportens faktaopplysninger i sin helhet verifisert av kommunen, slik at eventuelle feil eller misforståelser er rettet opp. Revisjonen avholdt avsluttende møte med administrasjonen 20.02.2023 hvor revisjonens vurderinger, konklusjoner og anbefalinger ble gjennomgått. I etterkant av møtet er rapporten sendt på høring til kommunedirektøren. Kommunedirektørens uttalelse fremgår av vedlegg (kap. 5.3).

Forvaltningsrevisjonen er gjennomført av Arnt Olav Aardal, Astrid Eikenes Skorpen, Linda Madeleine Olszewski, Øyvind Sunde, Elisabeth Aspaas Runsjø og Nichlas Ødegaard Gundelach. Revisorenes habilitet og uavhengighet er vurdert opp mot kommunen og den undersøkte virksomheten, og revisjonen finner de habile til å utføre forvaltningsrevisjonen.

Revisor vil takke kontaktpersoner og andre som har deltatt i forvaltningsrevisjonen, for godt samarbeid i forbindelse med arbeidet.

Østre Viken kommunerevisjon IKS
Rolvsøy, 4. april 2023

Casper Støten (sign.)
oppdragsansvarlig revisor

Arnt Olav Laueng Aardal (sign.)
utførende forvaltningsrevisor

Astrid Eikenes Skorpen (sign.)
utførende forvaltningsrevisor

Øyvind Sunde (sign.)
utførende forvaltningsrevisor

3 FREMGANGSMÅTE

3.1 Problemstilling og avgrensninger

Rapporten besvarer følgende problemstilling:
Har Sarpsborg kommune sikret at kommunen etterlever kravene i personopplysningsloven, herunder personvernforordningen (GDPR)?

I tråd med Sarpsborg kontrollutvalg vedtak i sak 22/39 28.09.2022, har forvaltningsrevisjonen hatt et særlig fokus på bruk av nettbrett og programmer i skolen.

Revisjonen har i hovedsak utgjort en overordnet gjennomgang av kommunens etterlevelse av sentrale krav i GDPR. Revisjonen har ikke omfattet krav til informasjonssikkerhet og behandling av personopplysninger i særlovgivning som helse- og omsorgslovgivningen, arbeidsmiljøloven, e-forvaltningsforskriften, sikkerhetsloven mv.

Revisjonen har fokusert på om Sarpsborg kommune har etablert rutiner og andre tiltak for å sikre at kravene i GDPR etterleves, og hvorvidt kommunen har gjennomført og dokumentert nødvendige vurderinger. Revisjonen har ikke innhentet alle arbeidsrutiner for linjen som inneholder elementer knyttet til personvern. Revisjonen har prioritert sentrale personvernrutiner og rutiner relatert til personvern i skolene. Revisjonen har i begrenset grad gjennomført stikkprøvekontroller og tester av om kommunen faktisk etterlever rutinene på området. Revisjonen har for eksempel ikke gjennomgått alle databehandleravtaler og personvernkonsekvensvurderinger kommunen har utført. Revisjonen har heller ikke utført en fullstendig kvalitetssikring av vurderingene som revisjonen har mottatt fra kommunen.

I undersøkelsene knyttet til bruk av nettbrett og programmer i skole, har revisjonen fokusert på kravene i GDPR om personopplysningssikkerhet, personvernkonsekvensvurdering, databehandleravtale og overføring av personopplysninger til land utenfor EØS. I den grad revisjonen har vurdert personopplysningssikkerhet eller informasjonssikkerhet i kommunen, så har dette vært begrenset til overordnede tiltak og ikke den operasjonelle sikkerheten.

Det finnes ingen legaldefinisjon eller fast standard på personvernområdet, for begrepsbruk for det som vanligvis kalles styringssystem, internkontroll eller ledelsessystem. Revisjonen benytter begrepet styringssystem.

Revisjonen er basert på fremlagt dokumentasjon, og revisjonen forutsetter at denne informasjonen er fullstendig og korrekt. Vi gjør oppmerksom på at forvaltningsrevisjonen ikke kan erstatte kommunens egne kontrollaktiviteter som internrevisjon, stikkprøvekontroller og tester av at tiltak har ønsket effekt.

3.2 Om revisjonskriterier

I henhold til forskrift om kontrollutvalg og revisjon § 15 skal revisor fastsette revisjonskriterier for den enkelte forvaltningsrevisjon. Revisjonskriteriene er den objektive målestokk som setter revisor i stand til å gjøre vurderinger på de fleste områder uten å ha formell fagspesifikk kompetanse. Revisjonskriteriene og revisors kunnskap og erfaring innen forvaltningsrevisjonsmetodikk, gjør at revisor kan gjøre objektive og holdbare vurderinger.

Revisjonskriteriene etablerer den norm som de innsamlede dataene skal vurderes opp mot. I tillegg til dette skal revisjonskriteriene også gjøre det tydelig for den reviderte enhet hva de måles opp mot. Revisjonskriteriene klargjør også overfor folkevalgte, media og andre lesere av forvaltningsrevisjonen, hva revisors vurderinger bygger på. Dette vil gjøre det enklere å etterprøve revisors vurderinger. Revisjonskriteriene skal være relevante, konkrete og i samsvar med de kravene som gjelder for revidert enhet.

Revisjonskriterier fastsettes vanligvis med basis i en eller flere følgende kilder: lovverk, politiske vedtak og føringer, kommunens egne retningslinjer, anerkjent teori på området, eller andre sammenlignbare virksomheters løsninger og resultater.

3.3 Revisjonsmetoder

I samsvar med god revisjonsskikk, skal praksis og/eller tilstand innen området som er revidert beskrives i et omfang som i tilstrekkelig grad underbygger revisors vurderinger og konklusjoner. Revisjonen har benyttet data fra ulike kilder og ulike metoder for innsamling av data, for å sikre et faktagrunnlag med høyest mulig grad av gyldighet og pålitelighet i denne forvaltningsrevisjonen.

Utfordringer og begrensninger i rapportens faktagrunnlag beskrives i teksten under, hvor metodene revisjonen har benyttet beskrives nærmere.

I denne forvaltningsrevisjonen er informasjonen hentet inn gjennom bruk av følgende metoder:

- Dokumentanalyse
- Intervjuer
- Spørreundersøkelse

Dokumentanalyse

Revisjonen har gjennomgått sentrale dokumenter fra Sarpsborg kommunes styringssystem for informasjonssikkerhet og personvern, som revisjonen har mottatt fra kommunen. Styrende dokumenter og prosedyrer fra styringssystemet har vært sentrale for revisjonens undersøkelser.

Revisjonen har også innhentet dokumentasjon på enkelte vurderinger som er sentrale på personvernområdet, som for eksempel risikovurderinger, personvernkonsekvensvurderinger (DPIA) og rapporter fra internrevisjoner. En fullstendig oversikt over dokumentene fremgår av kapittel 5.2.

Intervjuer

Det er totalt gjennomført 17 intervjuer for å sikre involvering av nøkkelpersoner innen personvern og informasjonssikkerhet. Intervjuene er verifisert ved at det enkelte intervjuobjektet har fått mulighet til å gå gjennom referatet fra sitt intervju og bekrefte at innholdet i intervjuet er korrekt gjengitt. Det var også mulig å be om endringer eller rette opp i eventuelle misforståelser.

Revisjonen har gjennomført intervjuer med:

- Kommunedirektør, Turid Stubø Johnsen
- Direktør oppvekst, Erik Bråthen
- Direktør teknisk, Hasse Ekman
- Direktør helse og velferd, Kirsti Skaug
- Direktør samfunn, Sigmund Vister
- Direktør organisasjon, Elin Cathrine Hagen
- Direktør teknologi og endring (inkludert arkiv), Tone Hankø Sandvei
- Assisterende direktør oppvekst, Elisabeth Grønberg Langvik

- Assisterende direktør oppvekst, Hanne Lothe
- Personvernombud, Bjørg Gustavsen
- Virksomhetsleder oppvekstjenester, Ingrid Fodstad Larsen
- IT-sjef, Knut Eggen
- Avdelingsleder innovasjon og utvikling, Leif Tore Martinsen
- Fagansvarlig informasjonssikkerhet, Bjørn Lande
- Beredskapskoordinator i kommunen, Lise-Lotte Torp Berglind
- Kvalitetsansvarlig, Linn Gjerlaugsen
- Ansvarlig for juridisk rådgivning, Andre Odsbu

Spørreundersøkelse

Det er gjennomført en spørreundersøkelse blant alle ansatte i Sarpsborg kommune. Undersøkelsen er gjennomført ved hjelp av det nettbaserte spørreundersøkelsesverktøyet Feedback. Revisjonen mottok 463 svar på undersøkelsen.

Spørreundersøkelsen besto av ni ordinære spørsmål, og et tilleggsspørsmål til ansatte som arbeider i eller med skole. Formålet med spørreundersøkelsen var å kartlegge personvernkulturen i kommunen. Undersøkelsen tok for seg temaer som opplæring, kjennskap til rutiner, kjennskap til avvikssystem og egen oppfatning av risikoområder innen personvern. Tilleggsspørsmålet knyttet til skole dreide seg om kjennskap til kravene som stilles til personvern ved bruk av digitale verktøy i skolen.

Det ble identifisert noen mindre utfordringer knyttet til:

- Forsinkelser fra revisjonens side gjorde at spørreundersøkelsen var tilgjengelig i et noe kortere tidsrom enn ønsket.
- Kommunen hadde ikke mulighet til å sende spørreundersøkelsen direkte til alle ansatte i kommunen. Spørreundersøkelsen ble publisert på kommunens intranett og ledere ble oppfordret til å ta kontakt med sin avdeling/enhet og oppfordre ansatte til å svare på spørreundersøkelsen.
- Det ble gjennomført andre spørreundersøkelser i kommunen, som ble publisert henholdsvis uken før og uken etter at revisjonens spørreundersøkelse ble publisert.

4 ETTERLEVELSE AV KRAVENE I PERSONOPPLYSNINGSLOVEN

Problemstilling: Har Sarpsborg kommune sikret at kommunen etterlever kravene i personopplysningsloven, herunder personvernforordningen (GDPR)?

4.1 Revisjonskriterier

4.1.1 Oppsummering av revisjonskriterier

1. Kommunen har etablert et tilfredsstillende styringssystem for personvern.
    a. Kommunen har beskrevet overordnede rammer for personvernarbeidet i styrende dokumenter.
    b. Kommunen har gjennomført risikovurderinger for å identifisere behov for tekniske og organisatoriske tiltak.
    c. Kommunen har etablert tilfredsstillende rutiner og retningslinjer for håndtering av personopplysninger basert på en risikovurdering og sørget for å kommunisere disse ut i organisasjonen.
    d. Kommunen har sørget for at ansvar og roller innen personvern er kommunisert og forstått.
    e. Kommunen sørger for regelmessig og rollebasert opplæring innen personvern.
    f. Kommunen sørger for regelmessig evaluering og forbedring av styringssystemet.
2. Kommunen har en oppdatert protokoll over behandlingsaktiviteter som tilfredsstiller kravene i GDPR artikkel 30.
3. Kommunen sørger for at rettslig grunnlag for behandling av personopplysninger blir vurdert og dokumentert.
4. Kommunen har etablert sletterutiner for sin behandling av personopplysninger.
5. Kommunen har sørget for å informere registrerte om behandlingen av deres personopplysninger.
6. Kommunen har etablert rutiner for håndtering av forespørsler fra de registrerte om å utøve sine rettigheter.
7. Kommunen har etablert egnede tiltak for å ivareta personopplysningssikkerheten.
8. Kommunen sørger for å gjennomføre personvernkonsekvensvurderinger når det er nødvendig.
9. Kommunen sørger for at databehandlere ivaretar krav til personvern og sikrer at det inngås databehandleravtaler.
10. Kommunen har kartlagt overføringer av personopplysninger til land utenfor EU/EØS og har gjennomført nødvendige vurderinger og tiltak ved overføringer.
11. Kommunen har utpekt et personvernombud med ansvar og oppgaver som tilfredsstiller GDPR artikkel 37-39.
12. Kommunen sørger for at avvik knyttet til personvern blir meldt, registrert og håndtert.

Utledningen av revisjonskriterier fremkommer av kapittel 5.1.

4.2 Datagrunnlag

4.2.1 Internkontroll for personvern

4.2.1.1 Overordnede rammer og styrende dokumenter

Sarpsborg kommune har utarbeidet et ledelsessystem for informasjonssikkerhet og personvern (heretter internkontroll/internkontrollen). I dokumentet «Om ledelsessystem for informasjonssikkerhet» har kommunen vist til at internkontrollen er inndelt i en styrende del, en gjennomførende del og en kontrollerende del. Det fremgår at internkontrollen er basert på en ISO-standard: NS-EN ISO/IEC 27001:2017. Det vises til at veiledere og faktaark for Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) skal benyttes i så stor grad som mulig. Videre fremgår det at kommunens prinsipper for IKT sikkerhet er forankret i NSMs grunnprinsipper for IKT-sikkerhet versjon 2.0, og at grunnprinsippene utgjør rammen for sikkerhetsprinsipper og krav til IKT sikkerhet i kommunen. Dokumentasjonen på internkontrollen oppbevares i kommunens kvalitetssystem, Netpower, som bl.a. sikrer at godkjennelser, versjoner og hvem som er ansvarlig for dokumenter dokumenteres.

Sarpsborg kommune har utarbeidet flere styrende dokumenter som inngår i internkontrollen. Kommunen har definert roller og ansvar for personvern og informasjonssikkerhet i dokumentet «Roller i sikkerhetsorganiseringen». I dokumentet fremgår også deres oppgaver. Rollene som benyttes er

- behandlingsansvarlig
- leder
- fagansvarlig informasjonssikkerhet
- personvernombud
- IKT-driftsleder
- IKT-leverandør/databehandler
- medarbeider
- systemeier
- systemforvalter (-ansvarlig)
- tjenesteansvarlig
- fagansvarlig arkiv

Det er også utarbeidet egne funksjonsbeskrivelser for fagansvarlig informasjonssikkerhet og personvernombudet i egne dokumenter.

Det overordnede ansvaret for ivaretakelse av personvern og informasjonssikkerhet er tildelt kommunedirektøren, som har rollen som behandlingsansvarlig. Behandlingsansvarlig kan delegere sin myndighet for enkelte tjenester til direktørene, og slik myndighet kan delegeres videre til virksomhetsledere. Delegering skal fremgå av den enkeltes lederavtale. Virksomhetsleder, avdelingsleder og teamleder har ansvar for den daglige og praktiske oppfølgingen av informasjonssikkerhet og personvern i sin enhet. [3]

Øvrige styrende dokumenter utgjør

- sikkerhetsmål og -strategi
- IKT sikkerhetsinstruks
- IKT-reglement for Sarpsborg kommune
- rutine for håndtering av risiko, personopplysninger

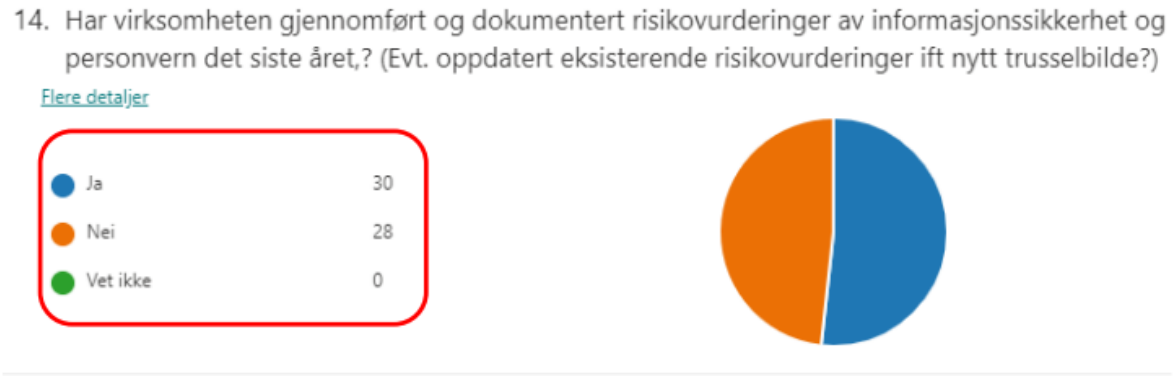
I sistnevnte rutine defineres risikomatrisen kommunen benytter og kriteriene for risikoaksept.

[3] Roller i sikkerhetsorganiseringen side 1 og 2

4.2.1.1 Risikovurdering for å identifisere behov for tekniske og organisatoriske tiltak

Det følger av Sarpsborg kommunes retningslinje for personvern at det skal gjennomføres risikovurdering og vurdering av personvernkonsekvenser av ny behandling av personopplysninger. Dette suppleres av kommunens rutine for gjennomføring av risikovurdering hvor det fremgår at den som har fått delegert behandlingsansvar, skal sikre at risikovurdering gjennomføres og dokumenteres årlig, samt oppdateres ved behov.[4] I samtaler har kommunen opplyst at den benytter både Excel-skjemaer og modul i Netpower til å dokumentere risiko- og sårbarhetsanalyser (heretter ROS-analyse/ROS-analyser). Kommunen har fremlagt et utkast til veileder for gjennomføring av risiko- og sårbarhetsanalyse, som beskriver kommunens metodikk for slike analyser. Det beskrives blant annet at konsekvenser for registrerte som skal hensyntas, er den registrertes sikkerhet og tap av liv og helse.

Ifølge dokumentasjonen fra ledelsens gjennomgang i februar 2022, så var det flere virksomheter som ikke hadde utarbeidet eller oppdatert dokumentert ROS-analyse for personvern i 2021:



Figur 1 – Statistikk fra ledelsens gjennomgang i februar 2022, som viser andel virksomheter som hadde opprettet eller oppdatert dokumentert ROS-analyse i 2021

Revisjonen har mottatt en oversikt over ROS-analyser innen personvern og informasjonssikkerhet som er gjennomført i perioden 15. oktober 2021 til 13. desember 2022. Denne viser at kommunen opprettet 55 analyser i perioden, hvorav åtte er registrert med status «fullført», og øvrige med «under arbeid». I samtaler med revisjonen opplyste de fleste som hadde fått delegert behandlingsansvar, at de hadde gjennomført ROS-analyse for personvern og informasjonssikkerhet på et tidspunkt, men ikke alle kunne bekrefte at disse hadde blitt oppdatert det siste året.

Kommunen har fremlagt flere eksempler på ROS-analyser, for eksempel ROS-analyse knyttet til at personopplysninger i helsetjenesten kommer på avveie, personvern og informasjonssikkerhet i hjemmetjenesten, bruk av Teams-chat i skole, samt flere analyser av IKT-løsninger som brukes i skolen. I analysene fremgår det hvem som har bidratt i analysen, dato for oppretting, kriterier for å fastsette score for sannsynlighet og konsekvens, tiltak, restrisiko og om restrisikoen er akseptert. ROS-analysene inneholder et stort antall risikoscenarier. For enkelte scenarier er det få tekstbeskrivelser utover beskrivelser av scenarier og årsaker, mens for andre er også konsekvensvurderingen dokumentert. Enkelte scenarier mangler score og/eller risikoaksept eller oppfølgingsplan. Risikoanalysen av verdikjeden i bekymringsmelding (barnevern) er utarbeidet i samarbeid med Kommunesektorens organisasjon (KS). I denne analysen redegjøres det i større grad for trusler og sårbarheter, enn i øvrige eksempler som er fremlagt.

[4] Rutine for gjennomføring av risikovurderinger, informasjonssikkerhet og personvern side 1

Kommunen har belyst flere konsekvenstyper, og for personvern gjelder følgende:

3.5. Konsekvens - Personvern

Tittel	Beskrivelse
Svært liten konsekvens	Liten konsekvens, krever ingen spesielle tiltak. Opprettelig skade.
Liten konsekvens	Middels konsekvens, krever at det iverksettes enkle tiltak. Opprettelig skade.
Middels konsekvens	Stor konsekvens, krever at det iverksettes tiltak og har negative konsekvenser. Opprettelig skade.
Stor konsekvens	Svært stor konsekvens, krever at det iverksettes omfattende tiltak og har store økonomiske konsekvenser. Uopprettelig skade.
Svært stor konsekvens	Dødsfall og/eller svært alvorlig skade

Figur 2 – Kriterier for fastsetting av score for konsekvens i kategorien personvern, hentet fra dokumentet håndtering av person-sensitiv og annen sensitiv informasjon

4.2.1.2 Rutiner og retningslinjer for personvern og implementering av disse

Sarpsborg kommune har en prosjektveiviser som utgjør kommunens system for prosjektadministrasjon. Av den fremgår det at man må vurdere om behandling av personopplysninger vil forekomme i forbindelse med nye løsninger og ved nye tjenester. Hvis behandling av personopplysninger forekommer, kreves det at man setter seg inn i kommunens retningslinjer for behandling av personopplysninger. Det fremgår også at fagansvarlig innen informasjonssikkerhet og personvernombudet skal involveres.

I retningslinjen for behandling av personopplysninger har kommunen definert en rekke krav til behandling av personopplysninger. I avsnittet fremgangsmåte er det bestemt at før personopplysninger behandles på en ny måte, skal den som er behandlingsansvarlig sette seg inn i kravene i retningslinjen. Videre skal alle nye behandlingsaktiviteter registreres i kommunens protokoll over behandlingsaktiviteter.

Det fremgår blant annet at kommunen skal oppfylle følgende prinsipper:

> *«1. Enhver behandling av personopplysninger skal være lovlig, rimelig og gjennomsiktig. Den skal ha lovhjemmel eller være basert på samtykke.*
> *2. Opplysninger skal ikke brukes til annet formål enn de er samlet inn for, uten samtykke fra brukeren.*
> *3. Kommunen skal ikke registrere mer opplysninger enn det som er nødvendig for formålet.*
> *4. Opplysningene skal være korrekte og om nødvendig ajourførte. Ukorrekte eller utdaterte personopplysninger skal rettes eller slettes, dersom ikke annet kreves av særlov.*
> *5. Personopplysninger skal ikke lagres lenger enn det som er nødvendig for formålet, dersom ikke annet følger av særlov.*
> *6. Personopplysninger skal gjennom egnede organisatoriske og tekniske tiltak beskyttes mot uautorisert eller ulovlig tilgang, utilsiktet tap, ødeleggelse eller skade.*
> *7. Den behandlingsansvarlige har ansvar for, og må kunne dokumentere at regelverket blir etterlevd.»*[5]

[5] Retningslinje for behandling av personopplysninger side 2

Videre stilles det krav til risikoanalyse, vurdering av personvernkonsekvenser, innebygd personvern, avviksregistrering og -håndtering, og håndtering av innsynsforespørsler. Avslutningsvis vises det til at alle virksomheter skal utføre en årlig egenkontroll som inngår i kommunens kvalitetssystem, og at utførelsen av kontrollen skal dokumenteres.

Sarpsborg kommune har fremlagt flere eksempler på rutiner for behandling av personopplysninger på spesifikke områder, herunder:

- Prosedyre for videomøter i MS Teams med sensitivt innhold
- Rutine for etablering og drift av kameraovervåking
- Rutine for klassetrivsel
- Rutine for anskaffelse av digitalt læremiddel ved enkeltskoler
- Rutine for bruk av klassetrivsel
- Rutiner for årlig gjennomgang av digitalt personvern i skole (inkl. presentasjon med opplæringsmateriell)
- Rutine for passordhåndtering for elever i grunnskolen

Kommunen har også fremlagt rutiner for håndtering av personvernavvik og rutiner for håndtering av innsynsforespørsler.

I spørreundersøkelsen revisjonen har gjennomført, har 82,9 % svart at de vet hvor de finner kommunens rutiner og retningslinjer for personvern. 56,4 % har bekreftet at de i stor grad er kjent med hvilke retningslinjer for personvern som gjelder dem, mens 16,8 % har svart at de i svært stor grad er kjent med retningslinjene. På spørsmål om de etterlever retningslinjene, har 44,5 % svart «i stor grad», mens 41,6 % har svart «i svært stor grad».

I samtaler med revisjonen har enkelte medarbeidere opplyst at de mener det er utfordrende å implementere styringssystemet for informasjonssikkerhet og personvern, ytterst i linjen. Enkelte ansatte sitter lite på kontor, mens andre kjenner seg lite igjen i kravene og scenariene som benyttes i retningslinjene.

4.2.1.1 Opplæring og implementering av roller og ansvar

Sarpsborg kommune har opplyst at de benytter et e-læringskurs i personvern og informasjonssikkerhet, som er tilpasset kommunesektoren. Alle ansatte må fullføre fem moduler i kurset. For medarbeidere som håndterer større mengder sensitive personopplysninger, er det en tilleggsmodul, mens det for ledere er tre tilleggsmoduler. For ansatte som sjeldent arbeider ved et kontor, benyttes felles klasseromsundervisning eller gjennomgang av e-læringskurset i fellesskap (f.eks. på personalmøte) til opplæring.

Kurset skal i utgangspunktet gjennomføres av alle ansatte, og det er opp til virksomhetsleder å sikre at dette skjer for både eksisterende ansatte og nyansatte. Innrulling av nyansatte er ikke automatisert. Fagansvarlig for informasjonssikkerhet følger opp gjennomføringsprosenten og rapporterer på denne til virksomhetslederne. På tidspunktet for revisjonen lå den totale gjennomføringsprosenten på 75 %. For ansatte som i det daglige arbeider på et kontor, lå gjennomføringsprosenten på 96 %. Kommunen har opplyst at det som følge av jevnlige nyansettelser, ikke er realistisk at gjennomføringsprosenten ligger på 100 %. I spørreundersøkelsen revisjonen gjennomførte, har 12,4 % svart at de ikke har deltatt på organisert opplæring innen personvern.

Kommunen har opplyst at det skal gjennomføres et oppfriskningskurs i form av e-læring i 2023.

I samtaler fikk revisjonen forklart at det gjennomføres egne lederopplæringer over fire dager, hvor de blant annet går gjennom leders ansvar for personvern og informasjonssikkerhet. Det ble også vist til at dette tydeliggjøres i rollebeskrivelser i kommunens internkontroll og i egenkontrollskjemaet.

Spørreundersøkelsen revisjonen har gjennomført, viser at 31,5 % av deltakerne har opplevd at personvern jevnlig har vært et tema på fellesmøter og samlinger. 51,4 % svarte at de hadde opplevd dette noen få ganger. 10% av deltakerne hadde ikke opplevd dette, mens 7,2 % var usikre.

33 % av deltakerne i spørreundersøkelsen arbeidet i eller med skole. Blant disse svarte 64,9 % at de i stor grad var kjent med personvernkravene som stilles til digitale verktøy i skole. 11 % oppga at de i svært stor grad kjente til dette. I samtaler har revisjonen fått opplyst at kommuneområdet oppvekst bruker virksomhetsmøter til å kommunisere om rutiner og tiltak til de ansatte. Dette er tatt inn i områdets årshjul for HMS.

I flere samtaler har det blitt trukket frem at det tidligere og det nåværende personvernombudet har brukt mye tid på å møte organisasjonen i avdelingsmøter, samlinger og dialog, for å skape bevissthet og forståelse for personvern. Det er trukket frem at dette har hatt god effekt.

4.2.1.2 Evaluering og forbedring av internkontroll

Sarpsborg kommune benytter en årlig egenkontroll der virksomhetslederne rapporterer på personvern og informasjonssikkerhet via et egenkontrollskjema. Skjemaet tar for seg temaer som:

- Enhetsleders kjennskap til sikkerhetsmål, sikkerhetsstrategi, sikkerhetsorganisering, eget ansvar og kriterier for risikoaksept.
- Informasjon og opplæring gitt til medarbeidere
- Tilgangsstyring i IKT-systemer
- Registrering av avvik
- Gjennomføring/oppdatering av risikovurdering

Personvernombudet og fagleder for informasjonssikkerhet legger i fellesskap frem resultatet av egenkontrollen, under ledelsens årlige gjennomgang.

Etter kommunens retningslinje for ledelsens gjennomgang innen informasjonssikkerhet, er det følgende faste agendapunkter i gjennomgangen:

1. Trusselbildet og hendelser siste året
2. Resultat fra sikkerhetsrevisjoner og egenmeldinger fra virksomhetene
3. Risikovurderinger og avviksbehandling
4. Ansvarsforhold og organisering med hensyn til sikkerhet
5. Oversikt over behandlinger av personopplysninger
6. Sikkerhetsmål, nivå for akseptabel risiko og strategier for informasjonssikkerhet
7. Kontroll og oppfølging av inngåtte avtaler
8. Tiltak fremover

Kommunen har fremlagt referat og presentasjoner fra ledelsens gjennomgang i februar 2022 som viser at samtlige agendapunkter ble gjennomgått. Det ble blant annet redegjort for personvernutfordringer som oppsto under pandemien, utfordringer knyttet til bruk av store teknologiaktører som Google og Facebook og kjente personvernsaker fra nyhetsbildet.

I samtaler er det vist til at kommunen årlig utfører tre til fire internrevisjoner innen personvern og informasjonssikkerhet. Disse gjennomføres på virksomhetsnivå, og de utføres av personvernombudet, fagansvarlig for informasjonssikkerhet og controller. Valg av virksomheter som skal revideres, er risikobasert og utføres av kommuneledelsen i samråd med direktøren for det aktuelle kommuneområdet.
Flere har vist til at revisjonene er nyttige og oppdragende for både virksomheten som revideres og andre tilsvarende virksomheter. Virksomhetene er gode på å utveksle funn og erfaringer.

Kommunen har ikke fremlagt dokumentasjon på, eller beskrevet kontroller som utføres lenger ute i linjen.

4.2.2 Protokoll over behandlingsaktiviteter

Kommunen har etablert en protokoll over behandlingsaktiviteter (heretter protokoll/protokollen).[6] Protokollen gir oversikt over:

- behandlingens formål og rettslig grunnlag,
- hvem de registrerte er og hvilke personopplysninger som behandles,
- hvilket kommuneområde behandlingsaktiviteten hører til og behandlingsansvarlig (internt i kommunen),
- hvor opplysningene er innhentet fra,
- om det er gjennomført risikovurdering,
- når personopplysninger registreres og ev. hvem de utleveres til,
- hvem som har tilgang til personopplysningene,
- når enkelte personopplysninger slettes og henvisning til spesifikke sletterutiner,
- oversikt over hvem som skal ha tilgang til de gjeldende opplysningene og administratorer av tilganger,
- om personopplysninger overføres til en tredjepart utenfor EU/EØ og ev. hva slags hva slags garantier som stilles for utlevering, og
- hvilke systemer de ulike behandlingsaktivitetene håndteres i.

Protokollen er etablert i Excel og tar utgangspunkt i formålene med behandlingene. Den er delt opp i faner etter de ulike kommuneområdene. For enkelte av områdene er deler av protokollen ikke fylt ut. Dette gjelder særlig for samfunn, organisasjon, teknisk og teknologi og endring. Det er ikke ført inn oversikt over felles behandlingsansvar eller oversikt over behandlinger hvor kommunen er databehandler.

Kommunen har ikke fremlagt rutiner for regelmessig oppdatering og/eller kvalitetssikring av protokollen. I samtaler har det kommet frem at det er et fokusområde for kommunen å oppdatere protokollen, og at det er bevissthet knyttet til at enkelte deler av protokollen har mangler. Det ble også opplyst at kommunen har satt i gang et arbeid med oppdatering av protokollen.

4.2.3 Behandlingens lovlighet

I retningslinjen for behandling av personopplysninger har kommunen definert at
«Enhver behandling av personopplysninger skal være lovlig, rimelig og gjennomsiktig. Den skal ha lovhjemmel eller være basert på samtykke.»

Sarpsborg kommune benytter protokollen til å dokumentere rettslig grunnlag for behandling av personopplysninger. Av protokollen skal også eventuelt supplerende rettsgrunnlag og eventuelt grunnlag for behandling av særlige kategorier av personopplysninger, fremgå. Denne informasjonen er oppgitt for

[6] Behandlingsprotokoll Sarpsborg kommune

de fleste behandlingsaktivitetene som er ført inn i protokollen, men behandlingsgrunnlag og/eller supplerende rettsgrunnlag mangler for enkelte behandlingsaktiviteter.

Kommunen har ikke redegjort for hvordan den dokumenterer interesseavveininger etter GDPR artikkel 6 (1) (f). Det er heller ikke fremlagt eksempler på slike vurderinger.

4.2.4 Kravet til lagringsbegrensning

I retningslinjen for behandling av personopplysninger har Sarpsborg kommune bestemt at personopplysninger ikke skal lagres lengre en nødvendig for å oppnå formålet ved behandlingen, og at personopplysninger skal rettes og slettes dersom de ikke er korrekte eller at den registrerte ber om dette. Revisjonen har ikke utover dette mottatt noen konkrete sletterutiner.

I protokollen over behandlingsaktiviteter er det utfylt lagringsperioder for de fleste behandlingsaktiviteter og på noen steder henvist til konkrete sletterutiner. Det er forskjeller på de ulike kommuneområdene hvor mye som er utfylt under oversikten over lagringsperiode. Helse og velferd og oppvekst har fylt ut for nesten alle sine behandlingsaktiviteter. Under fanene for flere områder er lagringsperiodene gjennomgående beskrevet som å være «til evig tid» eller «Følger arkivlovens regler om arkivplikt».

I intervjuer er det nevnt gjentatte ganger at det er lite kjennskap til konkrete sletterutiner og hvordan sletting håndteres innenfor det aktuelle virksomhetsområdet. Det ble trukket frem at sletting av noen av de ansattes personopplysninger utføres ved arbeidsforholdets opphør, men at dette er en manuell prosess. Flere har nevnt at kommunen er underlagt arkivlovgivningen og dermed er forpliktet til å lagre mye informasjon.

4.2.5 Oppfyllelse av informasjonsplikten

Kommunen har utarbeidet en personvernerklæring som er tilgjengelig på kommunens nettside. I retningslinjen for behandling av personopplysninger fremgår det at de registrerte skal få informasjon om behandling av personopplysninger gjennom denne. Erklæringen er bygget opp av en rekke overskrifter som man kan trykke på for å få mer informasjon.

Personvernerklæringen inneholder generell informasjon om:

- hjelpetekster om personvern og GDPR, samt informasjon om behandlingsansvarlig,
- informasjon om formål, rettslige grunnlag kommunen benytter og lagringstid,
- hvor personopplysninger innhentes fra og utleveres til,
- hvilke personopplysninger kommunen behandler,
- sikkerhetstiltak,
- den registrertes rettigheter og forholdet til innsynsrettigheter i andre lovverk,
- klagemuligheter, og
- kommunens bruk av informasjonskapsler, herunder Google analytics.

I tillegg er kontaktinformasjon til personvernombudet og postmottak oppgitt.

4.2.6 De registrertes rettigheter

I «Retningslinje for behandling av personopplysninger» er det beskrevet følgende i punkt 10:

> *«Alle innbyggere har rett til innsyn i egne personopplysninger. Rutine for svar på innsynsforespørsler beskriver prosessen med å besvare denne type forespørsler. Innbygger har også krav på å kunne reservere seg mot automatisk saksbehandling ut fra personprofiler. Feilaktige opplysninger skal slettes eller rettes. Kommunen skal ikke lagre opplysninger det ikke lenger er behov for, dersom disse ikke kreves lagret gjennom særlov».*

Håndtering av innsynsforespørsler er beskrevet i «Rutine for svar på innsynsforespørsler». Rutinen beskriver overordnet fremgangsmåte når innsynsforespørsler mottas, samt at forespørselen må besvares innen 30 dager. Det er bestemt at den registrerte som et minimum skal motta følgende informasjon:

Kommuneområde	System	Hva slags opplysninger	Hvem har tilgang	Hva er formålet	Hva er behandlingsgrunnlaget
Velferd	Gerica	Personalia Et aktivt vedtak To avsluttede vedtak IPLOS-registreringer Journalposter Saksbehandlingsnotat	Saksbehandlere og helsearbeidere i team xx	Helsehjelp, pleie- og omsorgsformål	Helsepersonelloven §45 Pasientjournalloven §2 Helsepersonelloven §3

Figur 3 – Skjermbilde fra rutinen for svar på innsynsforespørsler, som viser hva slags informasjon den registrerte kan kreve å motta

Revisjonen har ikke fått oversendt flere skriftlige rutiner for håndtering av registrertes rettigheter enn disse to som er nevnt.

I intervjuer er det kommet frem at det mottas få henvendelser fra registrerte som ønsker å få håndhevet sine rettigheter. Når det kommer henvendelser, gjelder dette oftest innsynsforespørsler som blir håndtert etter retningslinjene. Forespørsler kommer ofte i forbindelse med at de registrerte får beskjed om at det behandles personopplysninger, for eksempel når foreldre får forespørsel om overføring av personopplysninger om deres barn mellom barneskolen og ungdomsskolen ved trinnskifte.

4.2.7 Personopplysningssikkerhet

Sarpsborg kommune har utnevnt en fagansvarlig for informasjonssikkerhet som har det overordnede operative ansvaret for informasjonssikkerhet i kommunen. Kommunen har utarbeidet et felles styringssystem for informasjonssikkerhet og personvern. Se beskrivelsene i avsnitt 4.2.1 for mer informasjon om dette, herunder implementering og opplæring.

Fremlagt dokumentasjon viser at status på IKT-sikkerhet, herunder trusselbildet og oppfølging av sårbarheter og planlagte tiltak, utgjorde en stor del av ledelsens gjennomgang i februar 2022. Gjennomgangen tok utgangspunkt i trusselvurderinger og risikorapporter fra anerkjente aktører som e-tjenesten, PST, NSM, NorSIS og ENISA.

I samtaler ble det beskrevet at det er utpekt systemeiere og systemforvaltere for de fleste IKT-systemene kommunen benytter. De fleste forvalterne har teknisk bakgrunn, og det er en sammenheng mellom hvor kritiske systemene er, og hvem de har satt som forvalter. Det ble opplyst at IT-avdelingen utfører systematisk oppfølging av IKT-løsninger, og at de har et eget system for dette (System manager). For noen særområder som e-helse og oppvekst, er det bygget opp egne forvaltningsteam hos kommuneområdet som ivaretar forvaltningen av systemer. Der benyttes også fagpersonell som helsepersonell og pedagoger.

I spørreundersøkelsen ble de ansatte spurt om å oppgi hva de mente at var den største risikoen knyttet til personvern i Sarpsborg kommune. Temaer som gikk igjen, var:

- Korrekt lagring av personopplysninger
- Bruk av Teams til lagring av elevmapper
- Ivaretakelse av taushetsplikt
- Bruk av e-post, herunder i skole

- Deling av personopplysninger
- Kunnskap om personvernregelverket

Sarpsborg kommune har opprettet virksomheten oppveksttjenester som har et overordnet ansvar for personvern og informasjonssikkerhet på skolene. Virksomheten ble opprettet fordi det var et behov for større samhandling mellom skolene og et behov for å stramme inn praksis. Oppveksttjenester har utarbeidet en sentral læremiddelpakke. Pakken er utarbeidet i arbeidsgrupper med blant annet lærere og rådgivere, og de har hatt en lang prosess for å forankre hos skoleledelsen på den enkelte skole betydningen av godt personvern. Oppveksttjenester utfører aktiviteter som innkjøp og oppsett av utstyr, inngåelse av databehandleravtale, vedlikehold av protokoll over behandlingsaktiviteter, ROS-analyse og DPIA[7]. Det er virksomhetsleder for oppveksttjenester som aksepterer restrisiko.

Skolene kan anskaffe egne digitale løsninger, og det er virksomhetsleder som er ansvarlig for oppfølgingen av disse. Det er utarbeidet en rutine for slike anskaffelser, med tilhørende sjekkliste. I samtaler fikk revisjonen opplyst at det er utfordrende å nå ut med bevissthet og rutiner til ytterste ledd i linjen. De bruker leselister i kvalitetssystemet, men det er tidvis utfordrende å få «oversatt» hva den praktiske konsekvensen av rutinene er. Det er også utfordrende å sikre tilstrekkelig bevissthet og kompetanse hos lærere og elever, slik at det for eksempel gjøres nødvendige vurderinger av gratis programvare.

Kommunen har opplyst at informasjonssikkerhetshendelser er tatt inn i beredskapsplanen, og at det i nyere tid er gjennomført en beredskapsøvelse med et slikt scenario. I samtaler har revisjonen fått opplyst at kommunen ikke utfører sikkerhetsrevisjoner av leverandører per i dag, og at det heller ikke utføres penetrasjonstester av systemer. Kommunen utfører imidlertid sårbarhetsscan av systemer jevnlig. Det ble også opplyst at kommunen har noen mindre utfordringer knyttet til eldre maskinvare og servere på enkelte områder. Det ble beskrevet at de har gjort mange oppgraderinger de siste årene, og de har for eksempel få gamle servere igjen. Det har imidlertid vært utfordrende å sikre kapasitet til å forbedre og fornye store fagsystemer.

4.2.8 Personvernkonsekvensvurderinger (DPIA)

I rutinen for gjennomføring av risikovurdering har kommunen definert at DPIA skal gjennomføres når det er sannsynlig at en behandling av personopplysninger vil medføre høy risiko for personvernet. Det henvises til ti kriterier, og at dersom minst to av disse er til stede, skal det gjennomføres DPIA. Kravet er også nevnt i retningslinjen for behandling av personopplysninger. Der fremgår det også at personvernombudets evaluering av DPIA-en skal innhentes, og at forhåndsdrøfting med Datatilsynet skal benyttes dersom kommunen ikke lykkes i å dempe risikoen til et akseptabelt nivå.
Kommunen benytter malen for DPIA som er utarbeidet av Bærum kommune og Foreningen Kommunal Informasjonssikkerhet (KiNS). Sarpsborg kommune har fremlagt flere eksempler på gjennomførte DPIA-er, blant annet for digitale løsninger som benyttes av skolene. I samtaler fikk revisjonen opplyst at de i skole er opptatt av å innhente de registrertes synspunkter gjennom dialog med foresatte.

4.2.9 Bruk av databehandlere

I retningslinjen for behandling av personopplysninger har Sarpsborg kommune bestemt at det skal inngås databehandleravtale med IKT-leverandører. Det stilles også krav til vurdering av kommunen og leverandørers rolle i forbindelse med anskaffelser i kommunens standard kravspesifikasjon for konkurransegrunnlag. I denne kreves det også at tilbyder beskriver personvern- og informasjonssikkerhetstiltak, herunder blant annet:

[7] *«en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet»* jf. GDPR artikkel 35 (1)

- Styringssystem for informasjonssikkerhet
- Lagring av personopplysninger i EØS eller et tredjeland som EU kommisjonen har vedtatt at har et tilstrekkelig beskyttelsesnivå
- Redegjørelse for tilbyders rutiner
- Redegjørelse for oppdragsgivers (kommunens) adgang til å revidere tilbyder
- Redegjørelse for hvordan tilbyder sikrer tilstrekkelige garantier jf. kravet i GDPR artikkel 28 (1)
- Redegjørelse for ivaretakelse av kravet til innebygd personvern, personvernprinsippene og sentrale sikkerhetstiltak (f.eks. tilgangsstyring, autorisasjon, logging og gjenoppretting)
- Beskrivelse av integrasjon om sentrale IT-løsninger som kommunen bruker

Kommunen har fremlagt sin egen mal for databehandleravtale, men det er ikke fremlagt retningslinjer for inngåelse av databehandleravtale.

Oversikter over applikasjoner og inngåtte databehandleravtaler finnes i kommunens protokoll over behandlingsaktiviteter med vedlegg. I samtaler har revisjonen fått opplyst at dokumentene dekker de aller fleste systemene kommunen benytter, men at den ikke er helt komplett. Revisjonen har fått fremlagt et eksempel på et slikt vedlegg, som gir oversikt over systemer som benyttes av kommuneområdet oppvekst. I denne fremgår det at kommunen har inngått databehandleravtale med de fleste av leverandørene, og at det er gjennomført ROS-analyse for de fleste systemene. Saksnummer som er oppgitt i oversikten, tilsier at de fleste databehandleravtalene er inngått i 2017.

Revisjonen har fått opplyst at kommunen arbeider med å ta i bruk Kommunesektorens Organisasjon (KS) sin løsning for leverandøroppfølging (Digiorden). Det ble også opplyst at kommunen ikke utfører kontroller eller revisjoner av leverandører, herunder revisjon av eksisterende med leverandører.

4.2.10 Oppfølging av overføringer av personopplysninger til land utenfor EU/EØS

Sarpsborg kommune har ikke fremlagt rutiner for vurderinger av overføringer av personopplysninger til land utenfor EU/EØS (tredjeland). Kommunen har heller ikke fremlagt eksempler på vurderinger. Eventuelle overføringer skal fremgå av kommunens protokoll over behandlingsaktiviteter, men dette feltet er ikke fylt ut for de fleste behandlingsaktivitetene som er oppført i protokollen.

I kommunens standardtekst for kravspesifikasjon er det definert at for nye anskaffelser, skal lagring av personopplysninger skje i EØS eller et tredjeland som EU kommisjonen har vedtatt at har et tilstrekkelig beskyttelsesnivå.

Kommunen har opplyst at det tidligere personvernombudet sendte ut en forespørsel til alle leverandører 17. september 2020 (rett etter EU-domstolens Schrems II-avgjørelse).[8] Leverandørene ble bedt om å redegjøre for eventuelle overføringer til tredjeland som de eller deres underleverandører utførte. De ble også bedt om å beskrive hvordan de ivaretok kravene til gyldig overføringsgrunnlag dersom de utførte slike overføringer. I samme brev presiserte kommunen at dens oppfatning var at:
«Bruk av EU-kommisjonens standardbestemmelser er i prinsippet fortsatt tillatt, men det må gjennomføres en vurdering av om beskyttelsesnivået som oppnås, reelt sett er tilsvarende som i EU/EØS, samt hvilke sikkerhetstiltak som eventuelt må settes inn.»

[8] I EU-domstolen avgjørelse C-311/18 (Schrems II), erklærte EU-domstolen at overføringsgrunnlaget Privacy Shield var ugyldig. EU-domstolen utledet også et «nytt» krav, om at man må sikre at ikke tredjelandet har lovgivning eller praksis som undergraver beskyttelsesnivået som overføringsgrunnlaget skal sikre.

Kommunen har fremlagt en oversikt over leverandørenes svar på forespørselen. Oversikten inneholder 63 leverandører, og kommunen har ført inn det følgende:

- Status på fire leverandører som har svart er markert som rød.
- Status på syv leverandører som har svart er markert med gul.
- Status på 28 leverandører som har svart er markert med grønn.
- Status på 20 leverandører er at de ikke har svart på forespørselen.
- Fire leverandører mangler status.

I samtaler ble det også opplyst at virksomheten for oppvekstsjenester har gjennomført flere vurderinger av overføringer i forbindelse med inngåelse av nye databehandleravtaler.

4.2.11 Kravene til å utpeke et personvernombud

I den styrende dokumentasjonen er det etablert en funksjonsbeskrivelse for rollen som personvernombud.[9] Videre er personvernombudet tilskrevet ansvar i andre rutiner som for eksempel rutinen for ledelsens gjennomgang og prosedyren for håndtering av alvorlige sikkerhetsbrudd.[10][11]

Sarpsborg kommune har etablert stillingen personvernombud, og det er satt av rundt et halvt årsverk til denne. I samtaler fremkom det at dette er fleksibelt, og at personvernombudet selv sikrer at ikke ombudet er ansvarlig for å utføre eller utfører oppgaver som kan true personvernombudets uavhengighet. Tidligere personvernombud var i rollen i 11 år. Nåværende personvernombud har vært i stillingen siden 22. august 2022, og har siden 2018 jobbet tett med det tidligere personvernombudet.

Personvernombudet gjennomfører for tiden en personvernutdannelse ved Høgskolen i Lillehammer. Hun har tidligere vært engasjert i personvernprosjekter i kommunen, blant annet som leder for et implementeringsprosjekt rundt 2018, som gikk ut på å etablere protokollen over behandlingsaktiviteter, å lage retningslinjer og utarbeidet strategi.

I intervjuer fremkom det at personvernombudet i Sarpsborg kommune er delaktig i kommunens arbeid med å etterleve GDPR. Hun engasjeres når det skal gjøres personvernvurderinger av både større og mindre omfang, og samarbeider med controller og fagansvarlig for informasjonssikkerhet når det gjennomføres årlige internrevisjoner i kommunen. Arbeidet til personvernombudet er derfor både proaktivt (oppsøkende) og reaktivt.

I intervjuer fremkom det at det er bevissthet knyttet til at personvernombudet skal ha en uavhengig rolle. Det er akseptert av kommunen at personvernombudet skal ha en rådgivende funksjon og ivareta de registrertes rettigheter. Flere av de oversendte rutinene er godkjent av tidligere personvernombud. I intervjuer er det kommet frem at tidligere personvernombud også har vært med på å utarbeide disse.

Personvernombudet deltar i kommunens sikkerhetsråd sammen med kommuneledelsen og fagansvarlig for informasjonssikkerhet. Rapporteringen foregår i den årlige gjennomgangen med kommuneledelsen som kalles «ledelsens gjennomgang». Her rapporterer og oppdaterer personvernombudet og fagansvarlig for informasjonssikkerhet til kommuneledelsen om hva som er status på deres fagområder. Revisjonen har også fått opplyst at personvernombudet rapporterer fortløpende til kommunedirektøren ved behov.

[9] Funksjonsbeskrivelse for personvernombud
[10] Ledelsens gjennomgang – informasjonssikkerhet
[11] Prosedyre for håndtering av alvorlige sikkerhetsbrudd

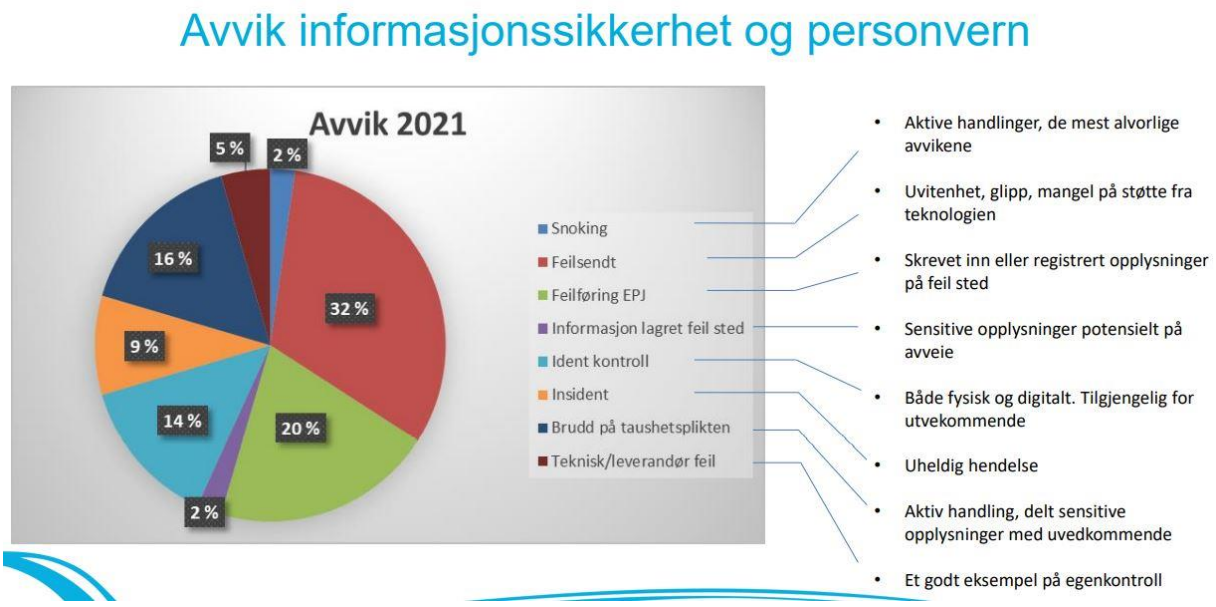
4.2.12 Kravene til å melde, registrere og håndtere personvernavvik

I kommunen defineres personvernavvik som sikkerhetsbrudd. Kommunen har i «Prosedyre for håndtering av alvorlige sikkerhetsbrudd»[12] en detaljert rutine for hvordan et personvernavvik skal håndteres. Rutinen skal sikre at meldepliktige avvik meldes til Datatilsynet innen tidsfristen på 72 timer. Det er også gitt mer overordnede instrukser om avvikshåndtering i IKT- sikkerhetsinstruks og retningslinjen for behandling av personopplysninger.

Når det oppstår avvik, skal det gis beskjed til nærmeste leder og meldes i kvalitetssystemet (Netpower). Personvernombudet mottar varsel om alle personvernavvik, og ved behov involveres hun eller andre fagpersoner for å bistå med evaluering og håndtering av avviket. Avvikssystemet er opplyst å være lett å bruke. Det er også opplyst at avvik håndteres av virksomhetsleder, og at dersom det ikke er lukket innen 14 dager, varsles direktøren for kommuneområdet.

I samtaler er det kommet frem at det har skjedd avvik innenfor de fleste kommuneområdene av varierende alvorlighetsgrad. Når avvikene har oppstått, har de blitt håndtert etter gjeldende rutiner. Jevnt over opplever de revisjonen har hatt samtaler med, at det er en god avvikskultur og at rapportering av avvik er ønskelig. Det rapporteres på personvern og informasjonsavvik årlig i det som kalles ledelsens gjennomgang. Når det oppstår avvik i en virksomhet som kan tenkes å være relevant for andre virksomheter, utveksles det kunnskap mellom virksomhetene slik at læringsutbytte blir størst mulig. Kommunen bruker avvikene som oppstår aktivt for å forbedre seg.

Av statistikk fra ledelsens gjennomgang i 2022, ser man at det har vært meldt avvik i noe varierende grad innenfor personvern og informasjonssikkerhet. Hovedandelen av avvikene er knyttet til feilsending, feilføring og brudd på taushetsplikt.



Figur 4 – Statistikk over typer personvern- og informasjonssikkerhetsavvik i 2021

[12] Prosedyre for håndtering av alvorlige sikkerhetsbrudd

Videre viser statistikken at det var en nedgang i rapporterte personvernavvik i 2021:

Avvik informasjonssikkerhet og personvern

	2016	2017	2018	2019	2020	2021
Antall avvik totalt	1825	2306	2726	2731	2863	2544
Personvern og informasjonssikkerhet	30	40	80	75	65	44

Figur 5 – Avviksstatistikk i perioden 2016 til 2021

4.3 Vurderinger

4.3.1 Kommunen har i stor grad etablert et tilfredsstillende styringssystem for personvern

Revisjonen vurderer at Sarpsborg kommune har etablert og implementert et styringssystem for personvern. Styringssystemet er bygd opp med elementer som samsvarer med Datatilsynets veiledning. Revisjonen ser positivt på at styringssystemet for personvern også dekker informasjonssikkerhet. Dette kan bidra til synergier og effektivitet, og blant annet sikre at lignende aktiviteter fra de to fagområdene slås sammen til én aktivitet. Revisjonen ser også positivt på at styringssystemet er basert på ISO-standarden: NS-EN ISO/IEC 27001:2017.[13]

Revisjonen har avdekket noen forbedringsbehov som er beskrevet i avsnittene nedenfor.

4.3.1.1 Kommunen har beskrevet overordnede rammer for personvernarbeidet i styrende dokumenter

Revisjonen vurderer at Sarpsborg kommunes styrende dokumenter for informasjonssikkerhet og personvern dekker de områdene som er anbefalt i Datatilsynets veiledning.

Gjengivelsen av personvernprinsippene i retningslinjen for behandling av personopplysninger er noe upresis, og dette kan lede til misforståelser av kravene i personvernprinsippene. Kommunen har definert kravene til henholdsvis lovlighet og viderebehandling snevrere enn det som fremgår i GDPR. Beskrivelsen av kravet til lagringsbegrensning mangler også noen nyanser. Det vil derfor være hensiktsmessig å justere beskrivelsen av prinsippene, slik at kravene i større grad samsvarer med definisjonene i GDPR.

4.3.1.2 Kommunen har i noen grad gjennomført risikovurderinger for å identifisere behov for tekniske og organisatoriske tiltak

Revisjonen vurderer at kommunen har utarbeidet tilfredsstillende rutiner, veiledning og maler for risikovurdering for å identifisere behov for tekniske og organisatoriske tiltak. Det er positivt at kommunen har etablert virksomheten oppvekstjenester, som har dybdekunnskap om personvern og utfører risikovurderinger av felles digitale læremidler som skolene bruker.

Kommunen har kommet godt i gang med arbeidet med risikovurderinger av både prosesser og systemer, men det har også kommet frem at flere risikovurderinger ikke er ferdigstilt. Under egenkontrollen for 2021 som ble fremlagt for kommuneledelsen i februar 2022, rapporterte 28 ledere at de ikke hadde gjennomført eller oppdatert dokumentert dokumentasjon av risikovurderinger innen personvern i 2021. Dette utgjør nesten halvparten av lederne i egenkontrollen. Revisjonen mener at det er av stor betydning at kommunen utarbeider og ferdigstiller risikovurderinger av personopplysningssikkerheten på alle områder der det behandles personopplysninger. Risikovurderingen skal ikke bare sikre at krav i GDPR er ivaretatt, men også gi kommunen grunnlag for å vurdere hvilke tiltak som er egnet for å sikre at styringssystemet er av et tilstrekkelig og hensiktsmessig omfang.

Det er en svakhet at enkelte av risikovurderingene som er fremlagt ikke dokumenterer hvilke momenter som er vektlagt og hvilke konkrete konsekvenser som risikoscenariene kan lede til. Dette gjør det utfordrende å kontrollere vurderingen som er foretatt, og det kan gjøre det utfordrende for kommunen å bruke vurderingene videre ved oppdatering av analysen og ved nye vurderinger ved implementering av tiltak.

[13] Standarden er blant annet utpekt av Digitaliseringsdirektoratet som anbefalt rammeverk for styringssystem for informasjonssikkerhet i offentlig forvaltning.

Revisjonen oppfatter at beskrivelsene i kriteriene for fastsetting av score for konsekvens er lite konkrete på enkelte områder, særlig når det kommer til de laveste scorene. Det vil komme tydeligere frem at kommunen har vurdert konsekvenser for de registrertes rettigheter og friheter, om kommunen bruker parametere som grad av økonomisk tap og grad av helseskade, og legger til ofte brukte personvern-konsekvenser som for eksempel integritetstap i forskjellig grad, tap av tilgang på tjenester og nedkjølingseffekt.

4.3.1.3 Kommunen har noen grad etablert rutiner og retningslinjer for håndtering av personopplysninger basert på en risikovurdering og sørget for å kommunisere disse ut i organisasjonen

I lys av kommuners kompleksitet og risikoen den innebærer, er revisjonens vurdering at kommunen har et mindre omfang av rutiner og retningslinjer for personvern, enn forventet. Dette gjelder både antallet rutiner og retningslinjer, og deres omfang. Revisjonen mener at rutiner og retningslinjer er det området der Sarpsborg kommunes styringssystem har størst potensial for forbedring.

Kommunen har i stor grad definert aktuelle krav fra GDPR i rutiner, men at det i liten grad beskrevet hvordan kommunen skal gå frem for å ivareta kravene. For eksempel er det i begrenset grad uttrykt hvilke momenter forskjellige vurderinger kan eller skal inneholde, der dette ikke er ivaretatt i maler. Det er i liten grad definert hvilke maler som kan eller skal benyttes i forskjellige sammenhenger, samt hvor vurderinger skal dokumenteres. Når disse elementene mangler, kan det være utfordrende å

- sikre enhetlig praksis og tilstrekkelig kvalitet,
- kontrollere at rutinene ivaretas, og
- dokumentere at kommunen har ivaretatt kravene, både for å oppfylle ansvarlighetsprinsippet og for et eventuelt tilsyn fra Datatilsynet.

Det kan være et særlig behov for dette på områder med høy risiko for brudd på personvernet og på områder der vurderinger utføres av medarbeidere som i liten grad arbeider med personvern til vanlig. Revisjonen opplever at dette er bedre håndtert innenfor skole, som har flere hensiktsmessige personvernrutiner.

Basert på svarene i spørreundersøkelsen, hvor 82,9 prosent svarte at de kjente til hvor personvernrutiner finnes og til sammen 73,2 prosent svarte at de i stor grad eller svært stor grad er kjent med rutinenes innhold, vurderer revisjonen at kommunens personvernrutiner i stor grad er implementert. Revisjonen mener at det likevel bør være et mål at de fleste ansatte er godt kjent med kommunens personvernrutiner.

4.3.1.4 Kommunen har sørget for at ansvar og roller innen personvern er kommunisert og forstått

Revisjonen vurderer at kommunen har etablert tilfredsstillende kommunikasjon om roller og ansvar gjennom e-læringskurs som er tilpasset den enkeltes rolle, og at informasjonssikkerhetsansvarlig rapporterer på antallet som har gjennomført kursene til de respektives ledere. Dette støttes av at lederne i den årlige egenkontrollen må gi bekreftelser knyttet til enhetens kjennskap til ansvar for personvern, og at de ansatte har fått informasjon om taushetsplikt og krav til håndtering av sensitive personopplysninger.

4.3.1.5 Kommunen sørger for rollebasert opplæring innen personvern

Etter revisjonens vurdering har kommunen etablert innledende opplæring innen personvern som er tilfredsstillende. Mange ansatte har allerede gjennomført det aktuelle e-læringskurset, og det følges opp at nye ansatte tar kurset. Revisjonen mener at kommunen også burde ha oppfriskningskurs eller lignende for ansatte som ikke er nye, og kommunen har opplyst at den planlegger dette i 2023.

Personvern har vært et tema på fellesmøter og samlinger for flere enheter i kommunen, men til sammen 17,2 prosent svarte at de ikke hadde registrert dette, eller at de var usikre på om de hadde registrert dette. Slik opplæring er ofte bedre tilpasset hverdagen til de ansatte, og kan derfor bidra til økt forståelse for GDPR og interne rutiner. Kommunen kan derfor vurdere om dette skal følges opp mer systematisk fremover.

Det er positivt at oppveksttjenester har etablert en fast aktivitet for bevisstgjøring innen personvern for ansatte på skolene.

4.3.1.6 Kommunen sørger i stor grad for regelmessig evaluering og forbedring av styringssystemet

Kommunen har i stor grad etablert rutiner og aktiviteter som sikrer regelmessig forbedring av styringssystemet. Det er særlig egenkontrollen, internrevisjoner og ledelsens gjennomgang som sørger for at dette er ivaretatt. Revisjonen vurderer at kommunen i stor grad har etablert rutiner og aktiviteter som sikrer regelmessig forbedring av internkontrollen. Det er særlig egenkontrollen, internrevisjoner og ledelsens gjennomgang som sørger for at dette er ivaretatt. Revisjonen mener likevel at egenkontrollen burde suppleres med, eller utvides med, flere spørsmål knyttet til personvern. Kommunen bør ha en risikobasert tilnærming ved utvelgelsen av spørsmål/kontroller.

Revisjonen mener også at det vil styrke kommunens arbeid med personvern dersom den etablerer enkle kontroller og stikkprøver som utføres av linjen. Dette vil bidra til å avdekke forbedringspotensial og områder der styringssystemet ikke fungerer tilstrekkelig. Dersom kommunen utarbeider mer utfyllende rutiner, som beskrevet over, vil det også bli lettere å utarbeide slike kontrollaktiviteter.

4.3.2 Kommunen har en protokoll over behandlingsaktiviteter som i noen grad tilfredsstiller kravene i GDPR artikkel 30

Malen for protokollen over behandlingsaktiviteter, som kommunen benytter, er etter revisjonens syn utformet slik at kravene i GDPR artikkel 30 er ivaretatt. Ettersom kommunen er en stor virksomhet, oppfatter revisjonen at det er hensiktsmessig at protokollen er inndelt i faner for de forskjellige kommuneområdene.

Etter revisjonens vurdering har protokollen mangler når det gjelder utfyllingen av malen. Det mangler blant annet slettefrister, informasjon om eventuelle utleveringer og beskrivelse av eventuelle overføringsgrunnlag for flere behandlingsaktiviteter.

Det er en svakhet at kommunen ikke har rutiner for periodisk kontroll eller kvalitetssikring av protokollen, og at slike aktiviteter ikke er gjennomført etter at protokollen ble utarbeidet. Kommunen har opplyst at den har påbegynt en slik gjennomgang, som er positivt.

4.3.3 Kommunen sørger i noen grad for at rettslig grunnlag for behandling av personopplysninger blir vurdert og dokumentert

Kommunen har fremlagt rutiner som beskriver at behandlingens lovlighet skal ivaretas. Etter vår vurdering er rutinene mangelfulle. Rutinene gir inntrykk av at behandlingsgrunnlagene som finnes, er lovhjemmel og samtykke fra den registrerte. Øvrige behandlingsgrunnlag og kravene til lovlighet i GDPR artikkel 9 og 10, samt personopplysningsloven § 12, er ikke beskrevet. Rutinene omhandler heller ikke fremgangsmåte ved vurdering av behandlingsgrunnlag, eller hvordan vurderingene skal dokumenteres.

Revisjonen ser positivt på at kommunen dokumenterer resultatet av lovlighetsvurderinger, herunder hvilke supplerende rettsgrunnlag kommunen bruker, i protokollen over behandlingsaktiviteter. Siden

protokollen ikke er fullstendig fylt ut, mangler imidlertid kommunen dokumentasjon på at lovligheten er vurdert for enkelte behandlingsaktiviteter.

4.3.4 Kommunen har i begrenset grad etablert sletterutiner for sin behandling av personopplysninger

Sletterutinene kommunen har fremlagt, er ikke tilfredsstillende. Kommunen har definert lagringsbegrensning som et krav i sine styrende dokumenter og i enkelte rutiner. Kommunen har også satt slettefrister i protokollen over behandlingsaktiviteter, men dette er ikke gjort for alle behandlingsaktiviteter.

Rutinene beskriver ikke hvordan sletting skal utføres, og informasjon fra samtaler viser at slike rutiner er lite kjent for flere ansatte. Revisjonen har forståelse for at kommunen plikter bl.a. å føre offentlig journal, arkivere og føre pasientjournal, og at dette medfører at kommunen skal bevare mange dokumenter i lang tid. Revisjonen mener at det likevel er viktig at kommunen har vurdert og dokumentert når disse pliktene inntreffer, samt at det foreligger rutiner for hvordan kommunen sikrer sletting av personopplysninger som ikke omfattes.

4.3.5 Kommunen har sørget for å informere registrerte om behandlingen av deres personopplysninger

Revisjonen vurderer at kommunens personvernerklæring dekker de emnene som kreves etter informasjonsplikten på en tilfredsstillende måte. Det bemerkes at revisjonen ikke har kontrollert at all behandling av personopplysninger som kommunen utfører er omtalt i personvernerklæringen. Revisjonen har likevel merket seg at beskrivelsen av overføringer til tredjeland er lite detaljert og trolig ikke oppdatert etter kartleggingen kommunen har gjennomført.

4.3.6 Kommunen har ikke etablert tilfredsstillende rutiner for håndtering av forespørsler fra de registrerte om å utøve sine rettigheter

Kommunens rutiner for håndtering av forespørsler fra registrerte om å utøve deres rettigheter er ikke tilfredsstillende. Rutinen beskriver kun hvordan innsynsforespørsler skal ivaretas og ikke hvordan forespørsler om retting, sletting, begrensning og protester skal håndteres. Påkrevd fremgangsmåte ved innsynsforespørsler er, etter revisjonens syn, i begrenset grad beskrevet. Oversikten over hva den registrerte skal motta av opplysninger samsvarer heller ikke med kravene i GDPR artikkel 15. Dette medfører en risiko for at kommunen ikke håndterer innsynsforespørsler etter GDPR på tilstrekkelig måte.

4.3.7 Kommunen har etablert egnede tiltak for å ivareta personopplysningssikkerheten

Basert på revisjonens overordnede gjennomgang, vurderer revisjonen at de delene av styringssystemet som gjelder personopplysningssikkerhet i hovedsak er tilfredsstillende. Det er en svakhet at ikke alle IT-systemer er kartlagt og at kommunen ikke har fått gjenopprettet nettverket for systemforvaltere. Det er også en svakhet at kommunen ikke fører kontrollen med databehandlere, og dette er nærmere beskrevet under avsnitt 4.3.9 om databehandlere. Kommunen kan vurdere å ta i bruk penetrasjonstesting for å øke sannsynligheten for at kommunen avdekker sårbarheter i IT-systemene.

4.3.8 Kommunen sørger for å gjennomføre personvernkonsekvensvurderinger når det er nødvendig

Kommunens rutiner for personvernkonsekvensvurdering (DPIA) og forhåndsdrøfting med Datatilsynet samsvarer med kravene i GDPR. Revisjonen mener likevel at det er en svakhet at kommunens rutiner ikke fullt ut gjenspeiler Datatilsynets liste over behandlingsaktiviteter som alltid medfører en plikt til å gjennomføre DPIA.

Revisjonen har funnet at malen som kommunen benytter til DPIA, et stykke på vei hjelper brukeren av malen med å sikre at vurderingen inneholder påkrevde momenter. Utover det, og kravet til involvering av personvernombudet, er ikke kommunens krav til fremgangsmåte i en DPIA dokumentert. Selv om det ikke er et uttrykkelig krav i GDPR, mener revisjonen at kommunen vil kunne dra fordeler av å ha en rutine som beskriver fremgangsmåte i DPIA for å sikre en enhetlig praksis og kvalitet i vurderingene som utføres. Revisjonen ser positivt på at oppvekstsjenester med sin særlige kompetanse innen personvern, utfører DPIA av felles digitale tjenester for skole.

Videre inneholder personvernkonsekvensvurderingene kommunen har fremlagt, de momentene som kreves etter GDPR. Det understrekes at revisjonen ikke har gjort en kvalitetssikring av DPIA-ene som er fremlagt.

4.3.9 Kommunen sørger for at databehandlere ivaretar krav til personvern og sikrer i noen grad at det inngås databehandleravtaler

Kommunen har fremlagt tilfredsstillende tiltak og rutiner som skal sikre at kommunen inngår databehandleravtale når det engasjeres nye databehandlere. Etter revisjonens syn er malen for databehandleravtale, som kommunen benytter, godt egnet til å sikre at databehandlere forplikter seg til å ivareta krav til personvern i samsvar med kravene i GDPR artikkel 28 nr. 3..

Det er positivt at kommunen i stor grad har kartlagt sine IT-systemer og leverandører, og dokumentert at det er inngått databehandleravtale med de fleste av leverandørene. Det er en likevel en svakhet at kommunens leverandøroversikter ikke er helt komplette, og at det mangler databehandleravtale med enkelte leverandører. Revisjonen mener også at det er en svakhet at de fleste databehandleravtalene er inngått i 2017, og at det ikke er foretatt revisjon eller kontroll av databehandlerne i etterkant. Dette medfører en risiko for at databehandleravtaler ikke er oppdatert i samsvar med slik databehandleroppdragene utføres i dag. Videre er det en risiko for at kommunen ikke avdekker at leverandører opptrer i strid med avtalen. Ytterligere er det en risiko for at databehandleravtaler ikke er oppdatert med gyldig overføringsgrunnlag der hvor EUs standard personvernbestemmelser for overføring av personopplysninger til tredjeland (SCC) benyttes som overføringsgrunnlag. SCC-ene som ble benyttet i 2017, er ikke lenger gyldige, og disse ble erstattet med nye SCC-er i 2021.

Revisjonen oppfatter at kommunens definisjon av at det skal inngås databehandleravtale med IKT-leverandører kan være noe misvisende. Revisjonen erfarer at det i noen (men begrenset grad) finnes IKT-leverandører som ikke er databehandlere. Revisjonen mener også at definisjonen kan misforstås og oppfattes slik at det kun er IKT-leverandører som kan være databehandlere og ikke andre leverandører.

Revisjonen ser positivt på at kommunen planlegger å ta i bruk KS sin løsning for leverandøroppfølging, som vil gjøre det lettere å få oversikt over og planlegge og dokumentere oppfølging av leverandører og leverandøravtaler.

4.3.10 Kommunen har i stor grad kartlagt overføringer av personopplysninger til land utenfor EU/EØS og i noen grad gjennomført nødvendige vurderinger og tiltak ved overføringer

Revisjonen vurderer at Sarpsborg kommune har kommet godt i gang med kartlegging av overføringer til tredjeland, men at denne ikke er ferdigstilt. Det er dokumentert at kommunen har sendt ut spørreskjemaer til leverandører, og at en større andel har besvart spørreskjemaene. Oversikten fra denne aktiviteten og protokollen over behandlingsaktiviteter viser imidlertid at ikke alle overføringer er kartlagt og dokumentert.

Revisjonen mener at Sarpsborg kommune må dokumentere sine vurderinger av overføringer til tredjeland grundigere, det bør blant annet komme tydeligere frem

- hvilke personopplysninger som overføres til hvilke tredjeland
- hvilket overføringsgrunnlag som brukes i hvert tilfelle
- eventuelle andre faktiske forhold kommunen har vektlagt
- datering og innhold i kommunens vurdering av om beskyttelsen av personvernet i tredjelandet er vesentlig likt beskyttelsesnivået i EU/EØS, herunder konklusjon, og
- beskrivelse av eventuelle supplerende tiltak kommunen har iverksatt.

Revisjonen har forståelse for at dette er utfordrende og at arbeidet preges av at de rettslige kravene er uklare, samtidig som praktiske løsninger for å ivareta kravene, ikke eksisterer eller er lite tilgjengelige. Revisjonen mener likevel at kommunen bør sikre at den ivaretar de kravene som er tydelig beskrevet i Datatilsynets veileder for overføring av personopplysninger til tredjeland, som for eksempel kravene knyttet til kartlegging, vurderingenes innhold og dokumentasjon. Revisjonen ser positivt på at oppvekst-tjenester bistår skolene med vurderinger av overføringer av personopplysninger til tredjeland.

4.3.11 Kommunen har utpekt et personvernombud med ansvar og oppgaver som tilfredsstiller GDPR artikkel 37-39

Kommune har utpekt et personvernombud i tråd med kravene i GDPR. Vedkommende har erfaring med personvernarbeid i kommunen, og kommunen har sikret at personvernombudet får utviklet sin kompetanse gjennom et deltidsstudium innen personvern og med deltakelse i eksterne nettverk. Den skriftlige rollebeskrivelsen til personvernombudet er i tråd med definisjonene og kravene til personvernombudet i GDPR artikkel 37 til 39.

Etter samtaler er revisjonens oppfatning at personvernombudet involveres i sentrale aktiviteter knyttet til personvern i kommunen. Revisjonen mener også at personvernombudets adgang til å rapportere til øverste leder i kommunen er ivaretatt gjennom fast årlig rapportering under ledelsens gjennomgang og ved løpende rapportering etter behov.

Revisjonen har merket seg at det tidligere personvernombudet er oppført som eier og/eller godkjenner av flere dokumenter i styringssystemet for informasjonssikkerhet og personvern. Kommunen har opplyst at dette ikke gir uttrykk for hvem som i realiteten har besluttet rutinenes innhold. Revisjonen mener at det er uheldig at det kan oppfattes som at personvernombudet har utarbeidet og/eller godkjent dokumenter i styringssystemet, ettersom dette kan true personvernombudets uavhengighet. Det er uheldig om personvernombudet tilsynelatende kontrollerer sitt eget arbeid, også dersom dette ikke er realiteten. Revisjonen mener at kravet til personvernombudets uavhengighet ikke er til hinder for at personvernombudet kvalitetssikrer og kommer med anbefalinger og forslag til innhold i dokumentasjonen. Det bør imidlertid synliggjøres hvem som i realiteten utarbeidet dokumentet og hvem som har godkjent det.

4.3.12 Kommunen sørger for at avvik knyttet til personvern blir meldt, registrert og håndtert

Kommunens system for registrering og håndtering av brudd på personopplysningssikkerheten vurderes som tilfredsstillende. Kvalitetssystemet kommunen har tatt i bruk sikrer at personvernavvik dokumenteres og rapporteres til riktig ledelsesnivå for håndtering. Videre sikrer systemet at personvernombudet involveres omgående for å gi råd om eventuell meldeplikt til Datatilsynet og berørte registrerte. Ledelsens gjennomgang sikrer at kommunen ser avvikene i sammenheng, og at kommunedirektøren informeres årlig.

Basert på opplysninger fra intervjuer, fremlagt avviksstatistikk og spørreundersøkelsen revisjonen gjennomførte, er det vår vurdering at kommunen sikrer at et stort antall personvernavvik blir registrert. Revisjonen mener likevel at kommunen kan forbedre sin praksis og sikre at enda flere avvik meldes. Spørreundersøkelsen viser at 24 prosent av deltakerne ikke var kjent med hvordan personvernavvik skulle meldes. Dette forsterkes av opplysninger revisjonen mottok i samtaler, hvor flere uttrykte en oppfatning om at det trolig er en underrapportering av mindre alvorlige personvernavvik, på tross av at en rekke avvik blir registrert i henhold til rutinen.

Kommunens rutine for håndtering av personvernavvik retter seg mot personvernavvik som er alvorlige sikkerhetsbrudd. Selv om det ikke er et uttrykkelig krav i GDPR, er revisjonens oppfatning at kommunen kunne hatt en rutine som også dekker personvernavvik som ikke utgjør brudd på personopplysningssikkerheten. Dette vil bidra til at kommunen avdekker utfordringer og forbedringsområder. Personvernavvik som ikke er sikkerhetsbrudd, vil blant annet være brudd på interne rutiner og retningslinjer og uønskede hendelser. Sistnevnte kan for eksempel være hendelser som leder til en økt sikkerhetsrisiko uten at det foreligger et brudd på personopplysningssikkerheten.

4.4 Konklusjon og anbefalinger

Revisjonen konkluderer med at Sarpsborg kommune har etablert en rekke hensiktsmessige tiltak for å sikre at kommunen etterlever kravene i personopplysningsloven og GDPR. Kommunen har kommet langt i arbeidet med etablering og implementering av styringssystem og kulturbygging innen personvern. Det er særlig de styrende dokumentene og kontrollaktiviteter som kommunen har kommet langt med. Selv om kommunen ikke fullt ut ivaretar kravet til å gjennomføre risikovurderinger og personvernkonsekvensvurderinger på en tilfredsstillende måte, så utviser kommunen en modenhet på området.

Revisjonen har likevel identifisert flere krav som ikke er ivaretatt på en tilfredsstillende måte. Dette gjelder i hovedsak omfang og innhold i rutiner og retningslinjer, dokumentasjon av enkelte vurderinger som lovlighetsvurderinger og vurderinger av overføringer av personopplysninger til tredjeland. Videre gjelder dette utfylling og vedlikehold av protokoll og oppfølging av databehandlere.

Basert på våre vurderinger og konklusjon har vi følgende anbefalinger:

a) Risikovurderinger av kommunens behandling av personopplysninger bør ferdigstilles og deretter oppdateres jevnlig. Kommunen bør også vurdere å sikre at alle risikovurderinger inneholder beskrivelser av hvilke momenter som er vektlagt, og hvilke konkrete konsekvenser knyttet til personvern som risikoscenariene kan lede til.

   Videre kan kommunen utdype kriteriene for fastsetting av score for konsekvenser innen personvern slik at disse for eksempel dekker flere grader av økonomisk tap og grader av helseskade, samt flere ofte brukte personvernkonsekvenser som integritetstap i forskjellig grad, tap av tilgang på tjenester og nedkjølingseffekt.

b) Kommunen bør utarbeide flere rutiner og retningslinjer som beskriver hvordan (altså fremgangsmåten når) kommunen skal ivareta sentrale krav som
   - lovlighet[14]
   - DPIA
   - samtlige av de registrertes rettigheter, herunder frister og formkrav som gjelder ved oppfølging av forespørsler om håndheving av rettighetene
   - sletting av personopplysninger
   - kartlegging og vurdering av overføringer av personopplysninger til tredjeland

[14] Etter GDPR artikkel 6, artikkel 9 og artikkel 10, samt personopplysningsloven § 12.

I den grad det er naturlig, kan kommunen legge dette inn i eksisterende rutiner og retningslinjer.

Videre bør følgende temaer oppdateres i eksisterende rutiner:

- Beskrivelsen av personvernprinsippene i retningslinjen for behandling av personopplysninger, slik at denne i større grad gjenspeiler definisjonene i GDPR artikkel 5.
- Beskrivelsen av hva den registrerte skal motta ved innsynsforespørsel etter GDPR, slik at denne samsvarer med kravene i GDPR artikkel 15.

c) Egenkontrollen for informasjonssikkerhet bør utvides eller suppleres med flere spørsmål knyttet til personvern. Dette kan for eksempel være spørsmål som:
   - Har enheten påbegynt ny behandling av personopplysninger, eller endret eksisterende behandling av personopplysninger?
   - Har enheten utført kontroll av at sine aktiviteter i protokollen over behandlingsaktiviteter og personvernerklæringen det siste året?
   - Har enheten vurdert behovet for å oppdatere DPIA-er det siste året?
   - Har enheten vurdert behovet for å revidere databehandleravtaler og utføre kontroll med databehandlere det siste året?
   - Har enheten utført kontroller knyttet til sletting av personopplysninger?
   - Har enheten utført kontroller knyttet til lagring av personopplysninger i korrekt fagsystem?
   - Har enheten utført stikkprøver eller andre kontroller på at enhetens personvernrutiner følges?

d) Kommunen bør sikre at den har vurdert og dokumentert lovlighet etter alle relevante bestemmelser i GDPR for alle behandlingsaktiviteter som kommunen utfører.

e) Det bør utarbeides slettefrister for alle behandlingsaktiviteter, der det er aktuelt, bør plikten til å bevare personopplysningene dokumenteres i stedet. Kommunen kan gjøre dette i forbindelse med oppdatering av protokollen over behandlingsaktiviteter.

f) Kommunen bør vurdere å fullt ut implementere Datatilsynets krav om når det alltid skal gjennomføres en DPIA, i kommunens rutiner som beskriver når DPIA skal gjennomføres.

g) Det bør sikres at kommunen har en fullstendig oversikt over alle databehandlere og at det er inngått databehandleravtale med disse. Det bør også sikres at det utføres periodisk kontroll med databehandlere og periodisk revisjon av databehandleravtaler, slik at det sikres at databehandleravtalene er oppdaterte. Omfang og hyppighet bør baseres på en risikobasert tilnærming. Kommunen kan hente inspirasjon fra det danske datatilsynets veileder for tilsyn (kontroll) med databehandlere. Videre kan kommunen vurdere å klargjøre i sine rutiner at det ikke bare er IKT-leverandører som kan være databehandlere.

h) Kartleggingen av og dokumentasjon av alle overføringer av personopplysninger til tredjeland bør ferdigstilles. Kommunen bør også sikre at alle overføringer er vurdert og fulgt opp i tråd med Datatilsynets veiledning for området og at innholdet i vurderingene dokumenteres.

i) Pågående og planlagte aktiviteter som oppdatering av protokoll over behandlingsaktiviteter og oppfriskningskurs i personvern bør gjennomføres.

5 KILDER OG VEDLEGG

5.1 Utledning av revisjonskriterier

Revisjonskriteriene er basert på sentrale krav i personopplysningsloven[15] og EUs personvernforordning 2016/679 (heretter GDPR), med hovedvekt på sistnevntes kapittel II til V. Kravene i GDPR er i stor grad generelt utformet. Revisjonen har derfor sett hen til Datatilsynets veiledere som utdyper hvordan kravene skal tolkes. Krav til behandling av personopplysninger i spesiallovgivning, herunder for områder som arbeidsmiljø, helse, arkiv, samt plan og bygg, faller utenfor revisjonens område.

Plikten til å etablere styringssystem for personvern

Kravet om å utarbeide et styringssystem for personvern følger av GDPR artikkel 24 nr. 1, hvor det fremgår at behandlingsansvarlig skal sikre at alle aktuelle plikter etter GDPR etterleves gjennom tekniske og organisatoriske tiltak, og at etterlevelsen kan dokumenteres. GDPR stiller ikke eksplisitte krav til hvordan styringssystemet skal utformes, utover at den skal være tilpasset behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene som virksomheten står overfor.

Datatilsynet har utformet en veileder for å etablere internkontroll (styringssystem) hvor det er presisert at styringssystem:
«[…] skal være ledelsens verktøy for å ivareta sitt ansvar og demonstrere etterlevelse etter personvernregelverket, og de ansattes verktøy for å utføre oppgaver på en forsvarlig og sikker måte»[16].

Ledelsen er ansvarlig for å sikre etterlevelse av GDPR. Ledelsen må derfor implementere personvern i virksomhetsstyringen, og sikre at det er tilstrekkelig med ressurser, verktøy og kompetanse for å sikre etterlevelse.

Datatilsynet definerer at styringssystemet bør bestå av styrende elementer, gjennomførende elementer og kontrollerende elementer som er proporsjonale med behandlingen virksomheten utfører.[17] Virksomheten må ta utgangspunkt i behandlingsaktivitetene den er behandlingsansvarlig for. Videre må virksomheten identifisere hvilke plikter den er underlagt, og hvilke risikoer som foreligger for de registrerte, og tilpasse styringssystemet deretter. Det bør være en sammenheng mellom omfanget av gjennomførende og kontrollerende elementer, og risikoen for de registrertes rettigheter og friheter ved behandlingen. Risiko for virksomhetens verdier skal ikke vektlegges.[18]

Ledelsen må sikre at styringssystemet gir et korrekt bilde av de faktiske aktivitetene og organiseringen av personvernarbeidet i virksomheten. Dette innebærer at styringssystemet må gjennomgås og oppdateres jevnlig. De styrende elementene skal gi en overordnet og systematisk beskrivelse av hvilke krav og plikter virksomheten må oppfylle, virksomhetens strategi og målsetninger, samt fordeling av roller og ansvar. Dette er vanligvis beskrevet i dokumenter som danner grunnlag for- og gir en oversikt over gjennomførende tiltak, samt dokumentasjon av disse. De gjennomførende elementene består vanligvis av rutiner og instrukser for systemer og prosesser som innebærer behandling av personopplysninger. Tonen fra ledelsen vil ha stor betydning i den gjennomførende prosessen. Det er en forutsetning for å lykkes med etterlevelsen at ledelsen er proaktive når det gjelder å bygge en personvernkultur i virksomheten. De kontrollerende elementene består normalt av kontrollrutiner som dokumenterer at rutiner og

[15] Lov av 15. juni 2018 nr. 38 om Lov om behandling av personopplysninger
[16] Datatilsynet veileder "Etablere internkontroll" punkt 1
[17] Datatilsynet veileder "Etablere internkontroll" punkt 1
[18] Datatilsynet veileder "Etablere internkontroll" punkt 2

arbeidsinstrukser følges, og som fanger opp eventuelle avvik. De kontrollerende elementene må også sikre ledelsens systematiske gjennomgang og forbedring av styringssystemet.

Kravet til kartlegging av behandlingsaktiviteter

Behandlingens art, omfang, formål og sammenhengen den utføres i får betydning for hvilke tekniske og organisatoriske tiltak den behandlingsansvarlige skal iverksette etter GDPR artikkel 24 nr. 1 og artikkel 32 nr.1. Det er derfor nødvendig å kartlegge virksomhetens behandlingsaktiviteter. Kartleggingen dokumenteres normalt i protokollen over behandlingsaktiviteter, som virksomheten er pliktig å utarbeide etter GDPR artikkel 30. Krav til protokollens innhold fremgår av GDPR artikkel 30 nr.1. Etter bestemmelsen skal det fremgå hvem den behandlingsansvarlige er og hvordan vedkommende kan kontaktes, hvilke behandlingsaktiviteter den behandlingsansvarlige er ansvarlig for, behandlingenes formål, hvilke kategorier av personopplysninger og registrerte som omfattes av behandlingen, eventuelle mottakere av personopplysningene og hvorvidt personopplysningene overføres til tredjestater eller internasjonale organisasjoner. Dersom det er mulig skal det også fremgå slettefrister eller slettekriterier for de forskjellige kategoriene av personopplysninger, og overordnede tekniske og organisatoriske tiltak som den behandlingsansvarlige har iverksatt for behandlingen.

Protokollen er et sentralt verktøy i arbeidet med etterlevelse av personvernlovgivningen, innholdet danner grunnlaget for en rekke nødvendige vurderinger, herunder risikovurderinger.

Krav til rettslig grunnlag for behandling av personopplysninger

Lovlighet ved behandling av personopplysninger reguleres i flere bestemmelser i GDPR. For at behandling av personopplysninger skal være lovlig følger det for eksempel av GDPR artikkel 6 at behandlingen må ha et rettslig grunnlag.

Det er i utgangspunktet ulovlig å behandle særlige kategorier av personopplysninger. Dette er personopplysninger om «*rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering*». For å behandle denne typen personopplysninger må tilleggskravene i GDPR artikkel 9 være oppfylt. Det følger av personopplysningsloven §§ 6,7 og 9 at slik behandling er lovlig i spesifikke tilfeller.

Etter GDPR artikkel 10 følger det at opplysninger om straffedommer eller lovovertredelser kun kan behandles under kontroll av offentlige myndigheter eller der det er fastsatt i lov. Når denne typen personopplysninger behandles uten offentlig myndighets kontroll, følger det av personopplysningsloven § 11 at det gjelder samme krav som nevnt i artikkel 9 (2) (a) og (c) til (f) samt §§ 6, 7 og 9. Det stilles også særskilte krav til når fødselsnummer kan behandles, i personopplysningsloven § 12.

Det følger av ansvarlighetsprinsippet i artikkel 5 (2) at behandlingsgrunnlag må dokumenteres.

Krav til sletting av personopplysninger

Det er ulovlig å oppbevare personopplysninger når de ikke lenger tjener til å oppfylle formålet de ble samlet inn for. Dette innebærer at virksomheten må slette opplysninger når formålet er oppfylt, uavhengig av om den registrerte har bedt om det eller ikke. Når den registrerte ber om å få sine personopplysninger slettet, må den behandlingsansvarlige slette disse «uten ugrunnet opphold», med mindre det foreligger forhold som angitt i GDPR artikkel 17 (1) (a) til (f). Sletting må også gjennomføres når det ikke lenger foreligger gyldig behandlingsgrunnlag, som for eksempel samtykke.

For at sletting skal bli gjennomført, må virksomheten ha systemer og rutiner som sikrer dette.

Krav til å informere de registrerte om behandling av deres personopplysninger og krav til behandling av innsynsforespørsler

Det er krav om at de registrerte skal få informasjon om hvordan deres personopplysninger behandles. Det er ingen spesifikke krav knyttet til hvordan virksomheten skal gi informasjon til de registrerte, men den bør gis skriftlig med et enkelt og forståelig språk.

Det følger av GDPR artikkel 13 og 14 at det er ulike krav til hva slags informasjon som skal gis avhengig av om opplysningene hentes inn fra den registrerte selv eller en tredjepart. I alle tilfeller må det gis informasjon om virksomhetens og personvernombudets kontaktinformasjon, formålet med behandlingen, behandlingsgrunnlag, lagringsperiode og kriterier for denne, navn på mottakere av opplysningene og om de skal overføres til et land utenfor EU/EØS, vurderingene som ligger til grunn for overføringer til land utenfor EU/EØS, den registrertes rettigheter, retten til å trekke tilbake samtykke, retten til å klage til Datatilsynet, om det er frivillig eller påkrevet å oppgi personopplysninger og eventuelle konsekvenser av å ikke oppgi dem, forekomstens av automatiserte individuelle avgjørelser, eventuelle nye formål, og konsekvensene av behandlingen .[19]

Dersom den registrerte ber om å få innsyn i behandlingen av sine personopplysninger, så er behandlingsansvarlig forpliktet til å gi innsyn i personopplysningene. Det skal også gis informasjon om visse aspekter ved behandlingen av personopplysninger.

Når den registrerte ber om å få håndhevet sine rettigheter, har den behandlingsansvarlige plikt til å legge til rette for å vurdere, uføre og gi tilbakemeldinger uten ugrunnet opphold og senest innen en måned. I GDPR artikkel 12 stilles det formkrav til eventuelle avslag.

Kravet til informasjonssikkerhet ved behandling av personopplysninger

Styringssystemet skal dekke alle aktuelle plikter etter GDPR, herunder kravet til informasjonssikkerhet i GDPR artikkel 32. Det følger av GDPR artikkel 32 nr. 1 at: «Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen» Kravene til etablering av tekniske og organisatoriske tiltak i artikkel 32 nr. 1 må ses i sammenheng med kravene i GDPR artikkel 24. Begge bestemmelsene tar utgangspunkt i hva slags behandlinger som utføres og risikoen den medfører, og tiltakene som er påkrevd etter hver av bestemmelsene er overlappende. Et styringssystem for informasjonssikkerhet omfatter også informasjonssikkerhet knyttet til personvern, og vil kunne bidra til etterlevelse av både artikkel 24 og artikkel 32.

Kravet til inngåelse av databehandleravtaler

Dersom en tredjepart behandler personopplysninger på vegne av den behandlingsansvarlige, stiller GDPR artikkel 28 krav om inngåelse av databehandleravtale. Formålet med avtalen er å sørge for at databehandleren behandler opplysninger etter instruks fra den behandlingsansvarlige. Avtalen må derfor konkret beskrive hvordan behandlingen skal skje, behandlingens art, hva som er formålet med behandlingen, hvor lenge avtalen skal vare, hva slags personopplysninger som er registrert og hvilke kategorier av personer personopplysningene gjelder.[20]

---

[19] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/gi-informasjon/informasjon-og-apenhet/hva-skal-virksomheten-gi-informasjon-om/

[20] Datatilsynets veileder " Hvordan lage en databehandleravtale?"

Databehandleravtalen fungerer som et instrument som avklarer roller og ansvar, og er en viktig forutsetning for at GDPR etterleves og at de registrertes rettigheter ivaretas.[21] Personvern er et dynamisk rettsområde og GDPR er et regelverk som stadig presiseres og utvikles, for eksempel via praksis fra EU-domstolen, Datatilsynet og Personvernnemda. Den behandlingsansvarlige virksomheten bør derfor jevnlig gjennomføre kontroller av databehandleravtalene sine for å forsikre seg om at de ivaretar kravene etter GDPR, og eventuelt reviderer avtalene dersom dette ikke er tilfellet. Det er også slik at behandlingsansvarlig kun skal engasjere databehandlere som stiller tilstrekkelige garantier. Behandlingsansvarlig bør derfor kontrollere at databehandleravtalene etterleves.

Krav ved overføring av personopplysninger til land utenfor EU/EØS

Ved overføring av personopplysninger ut av EØS, må det foreligge et gyldig overføringsgrunnlag etter GDPR kapittel V for at overføringen skal være lovlig. Virksomheten må i henhold til EU-domstolens Schrems II-avgjørelse (Case C-311/18) og tilhørende veiledning fra Datatilsynet også selv vurdere om beskyttelsesnivået i landet personopplysningene overføres til er tilsvarende som i EØS, ved bruk av de vanligste overføringsgrunnlagene. Dersom virksomheten mener at beskyttelsesnivået er utilstrekkelig, så må den implementere kompenserende tiltak i disse tilfellene. Lykkes ikke virksomheten i å identifisere og implementere slike tiltak, så vil overføringen regnes som ulovlig.[22]

Kravet til gjennomføring av risikovurderinger

Den behandlingsansvarlige er indirekte pålagt å gjennomføre risikovurderinger av egne behandlingsaktiviteter. Dette følger ikke direkte av ordlyden i GDPR artikkel 24 eller 32, men i veileder for etablering av internkontroll uttrykker Datatilsynet at det er nødvendig for å oppfylle kravene i bestemmelsene. De tekniske og organisatoriske tiltakene som bestemmelsene pålegger virksomhetene å etablere, skal baseres på resultatet av risikovurderingene.

Krav til personvernombud med ansvar og oppgaver som tilfredsstiller GDPR artikkel 37-39

GDPR artikkel 37 krever at enhver offentlig myndighet og ethvert offentlig organ skal utnevne et personvernombud. Forarbeidene til personopplysningsloven angir at dette gjelder for samme organer som er omfattet av forvaltningsloven § 1.

Personvernombudet skal utpekes på grunnlag av faglige kvalifikasjoner og kunnskap om personvernregelverket, i tillegg til evnen til å kunne utføre oppgavene som tilligger personvernombudet etter GDPR i artikkel 39.

Det stilles krav om at personvernombudet skal involveres i «alle spørsmål som gjelder vern av personopplysninger». Det bør etableres klare rutiner for når og hvordan ombudet skal involveres[23], og det skal settes av nok ressurser til at ombudet får utført sine oppgaver.

Det følger av artikkel 38 (3) at personvernombudet skal være uavhengig og ikke kan instrueres, avsettes eller straffes for utførelsen av sine oppgaver. Videre skal personvernombudet rapportere direkte til øverste administrative ledelse i virksomheten. Dette skal sikre at ansvaret for etterlevelsen av forordningen er plassert riktig.

---

[21] Åste Marie Bergseng Skullerud mfl., *Personvernforordningen. Lovkommentar*, Artikkel 28. Databehandler, Juridika (kopiert 24. januar 2023)

[22] Datatilsynets veileder "Overføring av personopplysninger ut av EØS"

[23] Åste Marie Bergseng Skullerud mfl., *Personvernforordningen. Lovkommentar*, Artikkel 38. Personvernombudets stilling, Juridika (kopiert 25. januar 2023)

Personvernombudet skal også gi råd og informasjon til virksomhetens ledelse og de ansatte om forpliktelsene de har etter GDPR og annen relevant lovgivning om behandling av personopplysninger. I utførelsen av oppgavene skal personvernombudet ha en risikobasert tilnærming.

Personvernombudet skal være virksomhetens kontaktpunkt for tilsynsmyndighetene.

Kravene til avvikshåndtering i GDPR artikkel 33 og 34

GDPR artikkel 33 og 34 beskriver hvordan den behandlingsansvarlige skal håndtere personvernavvik.

Etter artikkel 33 nr. 5 skal den behandlingsansvarlige
«*dokumentere ethvert brudd på personopplysningssikkerheten, herunder de faktiske forhold rundt nevnte brudd, virkningene av det og hvilke tiltak som er truffet for å utbedre det*».

Videre må den behandlingsansvarlige etter artikkel 33 nr. 1 «*senest 72 timer etter å ha fått kjennskap til det, melde bruddet til vedkommende tilsynsmyndighet … med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter*».

Det følger også av artikkel 34 nr. 1 at «*Dersom det er sannsynlig at bruddet på personopplysningssikkerheten vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige uten ugrunnet opphold underrette den registrerte om bruddet*».

Dette innebærer at den behandlingsansvarlige må sikre at personvernavvik avdekkes, dokumenteres og håndteres i samsvar med kravene og tidsfristene i bestemmelsene.

5.2 Mottatte dokumenter

Dokumentasjon fra styringssystem:

1. Retningslinje for bruk av kvalitetssystem i Sarpsborg kommune (utkast)
2. Om ledelsessystem for informasjonssikkerhet
3. Sikkerhetsorganisering i Sarpsborg kommune
4. Roller i sikkerhetsorganiseringen
5. Funksjonsbeskrivelse for fagansvarlig informasjonssikkerhet
6. Funksjonsbeskrivelse for personvernombud
7. Sikkerhetsmål og -strategi
8. Behandlingsprotokoll Sarpsborg kommune
9. Retningslinje for behandling av personopplysninger
10. Rutine for håndtering av risiko, personopplysninger
11. Rutine for gjennomføring av risikovurderinger, informasjonssikkerhet og personvern
12. Forberedelse til risikovurdering
13. Veileder for risikovurderinger av IT-systemer
14. IKT-sikkerhetsinstruks
15. IKT-reglement for Sarpsborg kommune
16. Min elektroniske arbeidsplass informasjonssikkerhet
17. Prosedyre for håndtering av alvorlige sikkerhetsbrudd
18. Prosedyre for videomøter i MS Teams med sensitivt innhold
19. Rutine for etablering og drift av kameraovervåkning
20. Rutine for svar på innsynsforespørsler
21. ROS mal 2020- IT-systemer
22. Sjekkliste for egenkontroll informasjonssikkerhet
23. DPIA-mal
24. Ledelsens gjennomgang – informasjonssikkerhet
25. Rutine for egenkontroll, informasjonssikkerhet og personvern
26. Bilag 1 - Oppdragsgivers Kravspesifikasjon-1
27. Krav i prosjektveilederen
28. Databehandleravtale Sarpsborg kommune 2022
29. Databehandleravtale Sarpsborg bilag 2022
30. brosjyre-kins-kurs-personvern-og-informasjonssikkerhet
31. Sikker passordhåndtering for elever i grunnskolen
32. Anskaffelse av digitalt læremiddel ved enkeltskoler (m/vedlegg)
33. Årlig gjennomgang knyttet til digitalt personvern
34. Rutine for bruk av klassetrivsel
35. Anskaffelse av digitalt læremiddel ved enkeltskoler
36. Årlig gjennomgang av temaer knyttet til digitalt personvern i skolen (m/vedlegg)
37. Bruk av chat i Microsoft Teams i oppvekst

Vurderinger og referater, rapporter og andre oversiktsdokumenter:

1. DPIA Individuell plan
2. Risikovurdering – Bekymringsmelding Q3 2020
3. Håndtering av personsensitiv og annen konfidensiell informasjon
4. Informasjonssikkerhet hjemmetjenesten
5. Informasjonssikkerhet og personvern – Virksomhet boveiledning sentrum
6. KS FIKS Bekymringsmelding barnevern
7. Risikovurderinger siste år
8. Internrevisjon Forebyggende virksomhet (m/vedlegg)
9. Internrevisjon Virksomhet KORPH (m/vedlegg)
10. Internrevisjon Sarpsfossen (m/vedlegg)
11. Digitale læremidler_ Feidepålogging bruker har enkel_ min side_
12. Digitale læremidler_ Feidepålogging_ kartlegging ikke blir generert
13. DPIA for Vigilo 2019
14. DPIA klassetrivsel
15. Kikora
16. Showbie
17. Vedlegg til BP_ arbeidsdokument apper og sikkerhetsvurderinger
18. Vedlegg til BP_ arbeidsdokument oversikt feidetjenester og databehandleravtaler
19. 22-02-15 Ledelsens gjennomgang

20. 22-02-15 Ledelsens gjennomgang – egenmeldinger
21. 2021 - Sjekkliste egenkontroll informasjonssikkerhet og personvern (1-55) (2)
22. 2022-02-15 - MØT_KL. – Referat
23. Gjennomført kurs
24. Opplæringsprogram i informasjonssikkerhet - v2
25. Forvaltningsrevisjon IT-sikkerhet 2020 (m/vedlegg og oppfølgingsrapport)
26. Schrems II_20_16822-1 Brev til Sarpsborg kommunes leverandører vedr 3002273_2_1.
27. Schrems II

Sarpsborg kommune

~~Unntatt offentlighet~~
~~OFL §5~~

BDO AS
Postboks 1704 Vika
0121 OSLO

Deres ref.:	Vår ref.:	Dato:
	23/06271-3	28.02.2023

Høringsutkast rapport forvaltningsrevisjon personvern - kommunedirektørens tilsvar

Vedlagt oversendes kommunedirektørens tilsvar til høringsutkast revisjonsrapport for personvern.

Med hilsen

Bjørg Gustavsen

Dette brevet er signert elektronisk

Vedlegg: Kommunedirektørens tilsvar til høringsutkast revisjonsrapport

Saksbehandler: Bjørg Gustavsen, Virksomhet stabstjenester

Org.nr: 938 801 363
Postadr: Postboks 237, 1702 Sarpsborg
Fakturaadr: Postboks 505, 1703 Sarpsborg
Sarpsborg rådhus: Glengsgt. 38, 1707 Sarpsborg
tlf: 69 10 80 00 / faks: 69 15 00 13 / e-post: postmottak@sarpsborg.com

Sarpsborg kommune

Dato: 28.02.2023
Saksnr.: 23/06271-2

~~**Unntatt offentlighet OFL §5**~~

Kommunedirektørens tilsvar til høringsutkast revisjonsrapport

BDO har på oppdrag fra Østre Viken kommunerevisjon foretatt en forvaltningsrevisjon på personvern i Sarpsborg kommune.
Det er positivt at kontrollutvalget vedtok en slik revisjon, og arbeidet som er gjort gir Sarpsborg kommune en mulighet til å få konkrete tilbakemeldinger på vår etterlevelse av personopplysningsloven og GDPR.
Kommunedirektøren legger merke til at revisjonen peker på at Sarpsborg kommune har iverksatt en rekke tiltak for å sikre etterlevelse av personopplysningsloven og GDPR, at kommunen har kommet langt i etableringen og implementeringen av styringssystem og at det er jobbet godt med å bygge en god kultur innen personvern.

Kommunedirektøren merker seg revisjonens liste på ni anbefalinger for oppfølging, og har følgende kommentarer:

a) Risikovurderinger av kommunens behandling av personopplysninger bør ferdigstilles og deretter oppdateres jevnlig. Kommunen bør også vurdere å sikre at alle risikovurderinger inneholder beskrivelser av hvilke momenter som er vektlagt, og hvilke konkrete konsekvenser knyttet til personvern som risikoscenariene kan lede til.

   Videre kan kommunen utdype kriteriene for fastsetting av score for konsekvenser innen personvern slik at disse for eksempel dekker flere grader av økonomisk tap og grader av helseskade, samt flere ofte brukte personvernkonsekvenser som integritetstap i forskjellig grad, tap av tilgang på tjenester og nedkjølingseffekt.

   Svar: Det jobbes kontinuerlig med bevisstgjøring av verdien av risikovurderinger og dette vil følges opp i det videre arbeidet

b) Kommunen bør utarbeide flere rutiner og retningslinjer som beskriver hvordan (altså fremgangsmåten når) kommunen skal ivareta sentrale krav som
   - lovlighet[1]
   - DPIA

[1] Etter GDPR artikkel 6, artikkel 9 og artikkel 10, samt personopplysningsloven § 12.

- samtlige av de registrertes rettigheter og frister og formkrav som gjelder ved oppfølging av forespørsler om håndheving av dem
- sletting av personopplysninger
- kartlegging og vurdering av overføringer av personopplysninger til tredjeland

I den grad det er naturlig, kan kommunen legge dette inn i eksisterende rutiner og retningslinjer.
Videre bør følgende temaer oppdateres i eksisterende rutiner:

- Beskrivelsen av personvernprinsippene i retningslinjen for behandling av personopplysninger, slik at denne i større grad gjenspeiler definisjonene i GDPR artikkel 5.
- Beskrivelsen av hva den registrerte skal motta ved innsynsforespørsel etter GDPR, slik at denne samsvarer med kravene i GDPR artikkel 15.

Svar: Kommunen tar anbefalingen til etterretning, og vil gjennomgå eksisterende rutiner og retningslinjer for å oppdatere disse, samt etablere nye der det er nødvendig.

c) Egenkontrollen for informasjonssikkerhet kan utvides eller suppleres med flere spørsmål knyttet til personvern. Dette kan for eksempel være spørsmål som:
   - Har enheten påbegynt ny behandling av personopplysninger, eller endret eksisterende behandling av personopplysninger?
   - Har enheten utført kontroll av at sine aktiviteter i protokollen over behandlingsaktiviteter og personvernerklæringen det siste året?
   - Har enheten vurdert behovet for å oppdatere DPIA-er det siste året?
   - Har enheten vurdert behovet for å revidere databehandleravtaler og utføre kontroll med databehandlere det siste året?
   - Har enheten utført kontroller knyttet til sletting av personopplysninger?
   - Har enheten utført kontroller knyttet til lagring av personopplysninger i korrekt fagsystem?
   - Har enheten utført stikkprøver eller andre kontroller på at enhetens personvernrutiner følges?

   Svar: Egenkontrollen for informasjonssikkerhet sendes til alle virksomhetsledere og avdelingsledere årlig (ved årsskiftet), i forbindelse med forberedelse til ledelsens gjennomgang. Anbefalingen om å utvide eller supplere den vil bli fulgt opp før neste års egenkontroll.

d) Kommunen bør sikre at den har vurdert og dokumentert lovlighet etter alle relevante bestemmelser i GDPR for alle behandlingsaktiviteter som kommunen utfører.

   Svar: Dette vil bli fulgt opp gjennom arbeidet med oppdateringen av behandlingsprotokollen.

e) Det bør utarbeides slettefrister for alle behandlingsaktiviteter, der det er aktuelt, bør plikten til å bevare personopplysningene dokumenteres i stedet. Kommunen

kan gjøre dette i forbindelse med oppdatering av protokollen over behandlingsaktiviteter.

Svar: Dette vil bli fulgt opp gjennom arbeidet med oppdateringen av behandlingsprotokollen.

f) Kommunen bør vurdere å fullt ut implementere Datatilsynets krav om når det alltid skal gjennomføres en DPIA i kommunens, rutiner som beskriver når DPIA skal gjennomføres.

Svar: Retningslinje for gjennomføring av DPIA vil bli oppdatert med Datatilsynets krav om hva som skal legges til grunn for at det skal gjennomføres en full DPIA.
.

g) Det bør sikres at kommunen har en fullstendig oversikt over alle databehandlere og at det er inngått databehandleravtale med disse. Det bør også sikres at det utføres periodisk kontroll med databehandlere og periodisk revisjon av databehandleravtaler, slik at det sikres at databehandleravtalene er oppdaterte. Omfang og hyppighet bør baseres på en risikobasert tilnærming. Kommunen kan hente inspirasjon fra det danske datatilsynets veileder for tilsyn (kontroll) med databehandlere. Videre kan kommunen vurdere å klargjøre i sine rutiner at det ikke bare er IKT-leverandører som kan være databehandlere.

Svar: Dette vil bli fulgt opp i det videre arbeidet.

h) Kartleggingen av og dokumentasjon av alle overføringer av personopplysninger til tredjeland bør ferdigstilles. Kommunen bør også sikre at alle overføringer er vurdert og fulgt opp i tråd med Datatilsynets veiledning for området og at innholdet i vurderingene dokumenteres.

Svar: Å sikre at kommunen håndterer overføring av personopplysninger til tredjeland ihht regelverket er en ressurs- og kompetansekrevende oppgave. Det vil derfor kreve noe tid og ressurser før vi har fått etablert en full oversikt og vurdert alle overføringer. Kommunedirektøren anbefaler at arbeidet følger en risikobasert tilnærming.

i) Pågående og planlagte aktiviteter som oppdatering av protokoll over behandlingsaktiviteter og oppfriskningskurs i personvern bør gjennomføres.

Svar: Arbeidet med oppdatering av behandlingsprotokollen er startet, og rutine for jevnlig ajourhold skal etableres. Planlagt aktivitet om oppfriskningskurs gjennomføres i løpet av 2023, samt gjennom aktiviteter ifbm sikkerhetsmåneden i oktober.

Turid S. Johnsen
Kommunedirektør