Vestfold og Telemark revisjon

# Er innbyggernes opplysninger sikre?

## Informasjonssikkerhet i Porsgrunn kommune

Forvaltningsrevisjon | Porsgrunn kommune

2021:3806 404

# Innhold

# Sammendrag

Porsgrunn kommune har på enkelte områder kommet langt i arbeidet med å oppfylle personopplysingslovens krav, mens det på andre områder fortsatt gjenstår arbeid.

I 2015 utarbeidet kommunen Strategi for informasjonssikkerhet i Porsgrunn kommune. Strategien ble sist revidert i 2018. Strategien har i utgangspunktet en oversiktlig struktur over rolle- og ansvarsfordeling innenfor informasjonssikkerhet og personvern, men likevel er innholdet til dels utydelig. Det er omtrent fire år siden strategien ble revidert, og vi mener at tiden er moden for en revidering.

Strategi for informasjonssikkerhet beskriver kun i begrenset grad hvordan det skal rapporteres innenfor organisasjonen på informasjonssikkerhet og personvern. Når det gjelder rapportering til rådmannens ledergruppe er det i praksis kun rapportert i den årlige gjennomgangen av informasjonssikkerheten. I tidsrommet vi har undersøkt ble ikke årlig rapportering gjennomført i 2019 eller 2021.

Vi vurderer at kommunens organisering av personvernombudet ikke er i samsvar med personopplysningsloven. I skrivende stund vurderer vi at organiseringen av personvernombudet ikke sikrer tilstrekkelig tid og ressurser til arbeidet. Vi vurderer videre at personvernombudet ikke har den uavhengighet som er påkrevd i lovverket. Personvernombudets rolle kan med fordel gis en mer utfyllende beskrivelse i kommunens strategi. Vi er kjent med at kommunen har utnevnt et nytt personvernombud som skal ta over oppgaven fra 01.03.22.

Kommunens protokoll over behandlingsaktiviteter er i hovedsak godt utfylt. Våre undersøkelser viser likevel at opplysninger som skal fremgå i protokollen i noen tilfeller manglet. Det fremgår ikke noen datering for behandlingsaktiviteter av protokollen, noe vi mener kan medføre risiko for at det vil være vanskelig å sikre at protokollen er oppdatert.

Av strategi for informasjonssikkerhet går det frem at kommunen skal gjennomføre risikovurderinger, men de fleste systemer vi har sett på hadde verken vurdert behovet for risikovurdering eller gjennomført risikovurdering. Kommunalområdet Helse og omsorg har gjennomført både risikovurderinger og vurdering av personvernkonsekvenser (DPIA) i samarbeid med andre kommuner, noe vi vurderer som positivt. Kommunen bør sikre at det gjøres risikovurderinger og DPIA, sistnevnte når det er relevant, i alle deler av kommunen.

Kommunen synes å ha et hensiktsmessig system for å håndtere brudd på personopplysningsloven (avvik). Våre undersøkelser viser at flertallet av de registrerte avvikene på dette området knytter seg til Helse og omsorg. Kommunen bør vurdere om den i tilstrekkelig grad sikrer at avvik innenfor informasjonssikkerhet og personvern fanges opp i hele organisasjonen.

Vi mener at kommunen i hovedsak har tiltak for å ivareta de registrertes rett til informasjon om kommunens behandling av deres personopplysninger, og at kommunen har tiltak for å ivareta innsynsretten til de registrerte.

Av strategi for informasjonssikkerhet går det frem at det skal inngås databehandleravtale med alle kommunens databehandlere. Kommunen har en ryddig oversikt over inngåtte databehandleravtaler, men våre undersøkelser viser at det manglet informasjon om databehandler og databehandleravtale i enkelte systemer.

## Anbefalinger

Vi anbefaler kommunen å:

- vurdere en evaluering og revisjon av strategi for informasjonssikkerhet
- sikre at ledelsens gjennomgang av informasjonssikkerhet blir gjennomført i samsvar med retningslinjer i strategi for informasjonssikkerhet
- organisere personvernombudsordningen i samsvar med kravene i personopplysingsloven art. 37-39
- sørge for at protokollen oppfyller lovkravene for alle registrerte IKT-systemer og vurdere tiltak for å sikre at informasjonen i protokollen er oppdatert
- sikre at alle IKT-systemer som behandler personopplysninger har et gyldig behandlingsgrunnlag
- sikre at ansvaret for å gjennomføre risikovurderinger er tydelig og sørge for at risikovurderinger blir gjennomført
- sørge for at kommunen har databehandleravtale med alle som behandler personopplysninger på vegne av kommunen

Horten, 03.03.22

# 1. Innledning

## 1.1. Kontrollutvalgets bestilling

Forvaltningsrevisjonen[1] er bestilt av kontrollutvalget i Porsgrunn kommune i sak 18/21.

## 1.2. Problemstilling og revisjonskriterier

Rapporten handler om følgende problemstillinger:

1. I hvilken grad har Porsgrunn kommune etablert tiltak for å ivareta kravene i personopplysningsloven?
2. Har de undersøkte områdene ivaretatt sentrale krav i personopplysningsloven?

I rapporten er de to problemstillingene behandlet sammen i kapittel 3, slik at tiltak og etterlevelse vurderes sammen under hvert revisjonskriterium.

Revisjonskriteriene[2] i denne forvaltningsrevisjonen er hentet fra personopplysningsloven og veiledere fra Datatilsynet. Kriteriene blir presentert fortløpende i kapittel 3, og er nærmere omtalt i vedlegg 2 til rapporten.

## 1.3. Avgrensning

Vi vil ikke undersøke hvordan kommunen håndterer personopplysninger knyttet til politikere og egne arbeidstakere.

Vi har avgrenset våre undersøkelser til perioden 2018-2021, med mindre annet er oppgitt.

## 1.4. Metode og kvalitetssikring

Denne forvaltningsrevisjonen er gjennomført av forvaltningsrevisor Trygve Børsting, med Bente Hegg Ljøsterød som oppdragsansvarlig.

Vi har benyttet flere forskjellige metoder i prosjektet. Dette har gjort at vi kan triangulere data, det vil si at vi bruker data fra flere kilder for å underbygge våre funn.

Vi har gjennomgått dokumentasjon fra administrasjonen og hatt en løpende e-postkorrespondanse med vår kontaktperson i administrasjonen. Vi har også intervjuet personvernombudet.

---

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

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

Som en del av undersøkelsene våre har valgt ut fire casestudier, to virksomheter (en skole og et sykehjem) og to IKT-systemer (SafeMate GPS-sporing og Teams). Utvalget ble gjort blant annet på grunnlag av bestillingen fra kontrollutvalget. Skolen og sykehjemmet ble valgt ut tilfeldig blant skolene og sykehjemmene i kommunen.

Vi har også gjennomført en stikkprøvekontroll av IKT-systemer i kommunens protokoll over behandlingsaktiviteter. IKT-systemene ble valgt ut tilfeldig.

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

## 1.5. Rådmannens uttalelse

Rapporten er presentert i et møte med administrasjonen i kommunen og sendt til uttalelse 16.02.22, jf. forskrift om kontrollutvalg og revisjon § 14. Rådmannens uttalelse ligger i vedlegg 1.

# 2. Om personopplysningsloven og sentrale begreper

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

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

**Behandling** – enhver operasjon som gjøres med personopplysninger.

**Behandlingsansvarlig** – den som beslutter at personopplysninger skal samles og/eller hvordan personopplysningene skal behandles. Er overordnet ansvarlig for å overholde personvernregelverket. I de fleste tilfeller er kommunen behandlingsansvarlig.

**Behandlingsgrunnlag** – rettslig grunnlag for å kunne behandle personopplysninger, de nærmere hjemlene står i art. 6, nr. 1.

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

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

**Personopplysning** – definert i personopplysningsloven art. 4, nr. 1 som: «enhver opplysning om en identifisert eller identifiserbar fysisk person».

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

**Protokoll over behandlingsaktiviteter** – oversikt over alle prosessene hvor kommunen behandler personopplysninger. Denne oversikten er pålagt etter personopplysingsloven art. 30, hvor det også fremgår hvilke krav som stilles til innholdet i protokollen.

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

Uttrykket «kategorier av» skal forstås som «forskjellige typer av».

# 3. Informasjonssikkerhet og personvern – tiltak og etterlevelse

## 3.1. Organisering – ansvar, myndighet og rapportering

**Porsgrunn kommune skal ha en organisasjon med klar plassering av ansvar og myndighet, samt rutiner for rapportering.**

### 3.1.1. Ansvars- og myndighetsfordeling

Kommunens sentrale styringsdokument for informasjonssikkerhet og personvern er *Strategi for informasjonssikkerhet i Porsgrunn kommune*. Dokumentet ble først utarbeidet i 2015, men er revidert i 2018. Dokumentet består av to hoveddeler: første del inneholder mål og krav til informasjonssikkerhetsarbeidet, mens andre del inneholder rolle- og ansvarsbeskrivelser.

Strategiens del to beskriver ledernes ansvar, stillinger med spesielt ansvar og det ansvaret som alle i ansatte i kommunen har for informasjonssikkerhet. Vi vil i det følgende redegjøre for hvordan de ulike gruppenes ansvar beskrives.

**Ordfører og rådmann**

Det fremgår av strategien at ordfører er «juridisk behandlingsansvarlig for kommunen, men har delegert den administrative del av kommunen til rådmannen som har det faglige ansvar.» Videre fremgår det at rådmann «er behandlingsansvarlig for all behandling av personopplysninger», og at rådmannen har det overordnede ansvaret for informasjonssikkerhet i kommunen. Det presiseres at rådmannen har ansvar for blant annet:

- å bestemme formålet for behandlinger
- å sørge for at databehandleravtaler inngås
- internkontroll for informasjonssikkerhet
- å sikre at det er tilstrekkelige ressurser for at tilfredsstillende informasjonssikkerhet opprettholdes

**Kommunalsjefer (rådmannens ledergruppe)**

Kommunen har fire kommunalsjefer[3] som representerer rådmannen innenfor sin fagsektor. Det vil si at de har et tilsvarende ansvar som rådmannen for informasjonssikkerhet innenfor sin fagsektor. Det er likevel kun rådmannen som signerer på databehandleravtaler.

Rådmannens ledergruppe er tillagt følgende oppgaver i arbeidet med personvern og informasjonssikkerhet:

- godkjenne endringer i strategi for informasjonssikkerhet og sørge for at den er kjent blant ansatte

[3] Kommunalsjef for administrasjon og støtte er per tiden ubesatt.

- sørge for at det gjøres risikovurderinger av kommunens informasjonsverdier
- fastsette nivå for akseptabel risiko
- gjennomgå kritiske sikkerhetshendelser og resultater av sikkerhetsrevisjoner
- godkjenne og stå bak gjennomføring av viktige sikkerhetstiltak

**Virksomhetsledere**
Det følger av strategien at informasjonssikkerhet er en viktig lederoppgave for virksomhetslederne, som har det overordnede ansvaret innenfor sitt område. Virksomhetslederne skal:

- ha oversikt over behandlinger i egen virksomhet
- delegere og følge opp internkontroll og informasjonssikkerhetsarbeid
- sikre finansiering
- kommunisere viktigheten av arbeidet med informasjonssikkerhet
- vurdere status for arbeidet minst en gang årlig
- sikre nødvendig og lovpålagt dokumentasjon, herunder risikovurderinger av informasjonssikkerhet og personvern i avdelingen og avdelingens aktiviteter.

**Ledere med personalansvar**
Ledere med personalansvar har ansvar for å sikre at medarbeiderne får informasjon om krav til konfidensialitet, og at taushetserklæring blir underskrevet som en del av arbeidsavtalen. De skal også varsle de ansvarlige for tilgangskontroll i aktuelle IKT-systemer når noen slutter. Videre har de ansvar for:

- å ha oversikt over eget ansvarsområde, informasjonsbehandling, IKT-system og informasjonssikkerhet
- å planlegge og gjennomføre nødvendige risikovurderinger, foreslå håndtering av risiko og gjennomføre godkjente tiltak
- å vurdere personvernkonkonsekvenser før ny behandling starter
- å ha kjennskap til relevante lover, regler og avtaler
- at medarbeidere som har ansvar for informasjonssystemer har nødvendig kompetanse
- å informere og sikre fokus på informasjonssikkerhet og personvern i egen enhet
- å iverksette tiltak eller reaksjoner overfor medarbeidere som har brutt kommunens regler eller prosedyrer, HR-avdelingen skal involveres hvis personalmessige reaksjoner blir vurdert

**Systemeier og systemansvarlig**
For hvert IKT-system som kommunen benytter skal det oppnevnes en systemeier og en systemansvarlig. Systemeier er en leder med ansvar for å utvikle, forvalte og drifte IKT-systemet. Systemansvarlig, som blir utpekt av systemeier, har det daglige hovedansvaret for IKT-systemet og er hovedkontakten til leverandøren.

Systemeiers ansvar for sine IKT-systemer innebærer blant annet å:

- stille krav til tilgjengelighet, konfidensialitet og kvalitet, slik at lovkrav og andre krav blir overholdt
- sikre at informasjonen i systemet er relevant og nødvendig for formålet
- definere roller og hvilken tilgang de skal ha
- påse at risikovurderinger og sikkerhetsrevisjoner blir gjennomført
- påse at det utarbeides sikkerhetsrutiner og at disse følges
- sørge for opplæring
- følge opp brudd på informasjonssikkerhet og retningslinjer
- for systemer som behandler personopplysninger:
    - dokumentere behandlingsgrunnlag
    - fastsette formål for systemet, i tråd med rådmannens vurdering
    - sørge for at personvernombudet blir varslet om ny behandling av personopplysninger
    - påse at det er oppdaterte sletterutiner som følges

Vi har undersøkt hvor mange IKT-systemer et utvalg kommunalsjefer og virksomhetsledere er systemeier for (vi har sett etter ledere som er systemeiere for et høyt antall systemer):

*Tabell 1 Et utvalg kommunalsjefer og virksomhetsledere med antall systemer hvor hen er systemeier*

| Rolle: | Antall IKT-systemer hvor hen er systemeier: |
|---|---|
| **Kommunalsjef helse og omsorg** | 13 |
| **Kommunalsjef oppvekst** | 22 |
| **Virksomhetsleder service** | 13 |
| **Virksomhetsleder IKT** | 18 |
| **Virksomhetsleder kommunalteknikk** | 14 |

*Kilde: protokoll over behandlingsaktiviteter per 11.11.21. Stikkprøven i avsnitt 3.3.2 viste at noen av systemene opplistet i protokollen ikke var i bruk, disse har vi trukket fra i tabellen over.*

Systemansvarliges oppgaver er også spesifisert i strategien. Oppgavene inkluderer blant annet å:

- godkjenne brukere og bestemme tilgangsnivå
- ha inngående kunnskap om systemet og oppgavene det skal løse
- assistere og gi opplæring til superbrukere
- rette systemfeil i samarbeid med IKT-avdelingen og leverandør
- oppdatere og vedlikeholde rutiner
- beskrive og følge opp sikkerhetsrutiner
- følge gjeldende lover, regler og lisensbetingelser

Basert på en rask gjennomgang av protokoll over behandlingsaktiviteter synes det som at systemansvarlig i praksis gjerne har ansvar for mellom ett og fire IKT-systemer. To systemansvarlige har ansvar for henholdsvis 18 og 10 systemer.[4]

**IKT-sjef**
IKT-sjefen har ansvar for å sikre sine IKT-systemer i samsvar med avtalt sikkerhetsnivå, retningslinjer og rutiner. Videre skal IKT-sjefen blant annet:

- etablere og vedlikeholde retningslinjer for drift av IKT-infrastruktur, blant annet:
  - sikkerhetskopiering
  - logging av utførte oppgaver og feil
- etablere og opprettholde driftsmessig endringskontroll
- etablere og vedlikeholde driftsinstrukser og prosedyrer for håndtering av feil
- sikre tilstrekkelig kapasitet og ressurser
- etablere beredskapsløsning

**Rådgiver for informasjonssikkerhet**
Strategien for informasjonssikkerhet sier at rådgiver for informasjonssikkerhet skal være en pådriver og ressursperson i arbeidet med informasjonssikkerhet. Rådgiver har blant annet følgende oppgaver:

- støtte kommunen i spørsmål om internkontroll og informasjonssikkerhet, rapportere til kommunens ledelse innenfor fagområdet, og forberede ledelsens årlige gjennomgang
- delta på ledelsens årlige gjennomgang
- øke sikkerhetsbevisstheten i kommunen
- utarbeide retningslinjer for informasjonssikkerhet
- sikre at det foreligger oversikt over behandlinger av personopplysninger, bruk av databehandlere og databehandleravtaler
- koordinere håndheving av krav om innsyn, retting og sletting etter personvernreglement
- bidra ved gjennomføring av risikovurderinger
- følge opp brudd på informasjonssikkerheten og retningslinjer

Da kommunen ansatte personvernombud i 2017, var oppgaven kombinert med rollen som rådgiver for informasjonssikkerhet. Organisasjonsmessig var vedkommende tilsatt i IKT-avdelingen. Da personvernombudet, i november 2019, gikk over i en ny stilling i kommunen, ble oppgavene til rådgiver for informasjonssikkerhet tatt over av IKT-leder.

[4] Stikkprøven i avsnitt 3.3.2 viste at noen av systemene opplistet i protokollen ikke var i bruk, disse har vi trukket ifra.

**Personvernombud**
Personvernombudet er kun kort omtalt i strategi for informasjonssikkerhet. Her går det frem at hen skal ivareta lovkravene til personvernombudet, ta imot meldinger om nye behandlinger og være uavhengig. Vi kommer nærmere inn på rollen som personvernombud i avsnitt 3.2.

**Alle ansatte**
Avslutningsvis i strategien beskrives ansvaret hver enkelt medarbeider har for informasjonssikkerhet. Her går det frem at alle medarbeidere skal være bevisst på hvilken informasjon de behandler og på krav til informasjonsbehandling i lov og retningslinjer. De skal også rapportere om sikkerhetshendelser og mulige sikkerhetssvakheter eller sikkerhetstrusler. Slike varsler kan gis til nærmeste leder eller til personvernombudet. Det presiseres at ansatte har taushetsplikt for informasjon hvor konfidensialitet er nødvendig, og for all informasjon som har betydning for informasjonssikkerheten.

**DigiForum**
DigiForum er ikke omtalt i strategi for informasjonssikkerhet, men har en betydelig rolle i kommunens arbeid med informasjonssikkerhet. Forumet ble opprettet i november 2018, hadde sitt første møte i januar 2019 og er et samarbeidsforum med representanter for de forskjellige kommunalområdene. Vi har mottatt mandatet for DigiForum,[5] hvor forumets rolle beskrives nærmere. Forumets hovedoppgave er å vurdere forslag til digitaliseringsprosjekter. Representantene i DigiForum fungerer som kontaktledd til sine kommunalområder.

Ved anskaffelse av digitale løsninger eller IKT-systemer skal DigiForum informeres, jf. *Reglement for delegasjon i Porsgrunn kommune*. Dette bør gjøres så tidlig som mulig i prosessen, og det bør følge med beskrivelse av behov og utkast til gevinstrealisering. Anskaffelsen vil bli vurdert av DigiForum. DigiForum skal dessuten koordinere og prioritere innføringen av nye systemer, og forhindre at det ikke blir gjort innkjøp av systemer som kommunen allerede har.

Personvernombudet samarbeider med DigiForum i forbindelse med utfylling av protokoll over behandlingsaktiviteter.

**Observasjoner fra casestudier**
Som en del av vår datainnhenting valgte vi ut to virksomheter og to IKT-systemer, som vi har sett nærmere på. Dette omtales i det videre som casestudier. Alle som vi snakket med i forbindelse med casestudiene, mente at ansvarsfordelingen i forbindelse med behandling av personopplysninger i utgangspunktet er tydelig i kommunen, men at det gjøres visse lokale tilpasninger i oppgavefordelingen. For et av IKT-systemene vi så på i casestudiet, var det en rådgiver som utførte noen av oppgavene som i utgangspunktet ligger til systemeier. Dette hang sammen med at rådgiveren var kommunalområdets representant i Digiforum. For det andre IKT-systemet vi så på, fortalte intervjudeltakerne at arbeidsdelingen mellom systemeier og

[5] Denne har tittelen «DigiForum – Utdyping av mandat 2022».

systemansvarlig var litt flytende. De vurderte at det generelt i kommunen nok var litt varierende arbeidsfordeling mellom systemeier og systemansvarlig.

En systemeier opplevde at oppgavene som lå til vedkommende kunne være noe utfordrende, både fordi de krever inngående IKT-kompetanse og fordi det er utfordrende å vite hvor langt man skal gå for å utføre oppgavene.

### 3.1.2. Rapportering og årlig gjennomgang av informasjonssikkerheten i kommunen

Strategi for informasjonssikkerhet beskriver i begrenset grad hvordan det skal rapporters på området.

I strategi for informasjonssikkerhet står det at virksomhetsleder har ansvar for å vurdere status på arbeidet årlig, og skal sikre dokumentasjon av behandlingen mm. Det fremgår imidlertid ikke noe om rapportering til rådmann. For ledere med personalansvar, IKT-sjef, systemeier og systemansvarlig fremgår det ikke noe rapporteringskrav. Rådgiver for informasjonssikkerhet skal rapportere til kommunens ledelse, herunder forberede og delta på ledelsens årlige gjennomgang.

Det fremgår ikke noe rapporteringskrav for personvernombudet i strategi for informasjonssikkerhet. Personvernombudet fortalte at han ikke rapporterer til kommuneledelsen utover årlig gjennomgang.

Ledergruppen skal ha en årlig gjennomgang av informasjonssikkerheten i kommunen, som skal forberedes av rådgiver for informasjonssikkerhet. I forbindelse med gjennomgangen forberedes det en overordnet risikoanalyse som vurderes i møtet. Denne risikoanalysen er basert på kriteriene konfidensialitet, integritet og tilgjengelighet.

Vi har fått fremlagt dokumentasjon på at ledergruppens gjennomgang er utført i april 2018, desember 2018 og juni 2020. For hver gjennomgang består dokumentasjonen av en presentasjon og en risikovurdering. [6]

Presentasjonen fra april 2018 inneholder først en generell gjennomgang av informasjonssikkerhet, inkludert strategi for informasjonssikkerhet og kommunens delegasjonsreglement. Videre inneholder presentasjonen status og videre fremdrift på arbeidet innenfor informasjonssikkerhet og risikovurdering for informasjonssikkerhet og personvern.

Presentasjonene fra desember 2018 inneholder fokus siden sist (gjennomførte tiltak), vurdering av risikobilde og akseptabel risiko, samt en oppsummering av viktigste tiltak (fremover). Presentasjonen fra juni 2020 inneholder tiltak og fokus siden sist, hva som gjenstår av tiltak og risikomatrisen for gjenværende risiko (fra risikovurderingen for 2020). Det fremgår av presentasjonene at man har arbeidet med anskaffelser av IKT-systemer, og at det i den forbindelse ble gjort endringer i delegasjonsreglementet for å sikre bedre kontroll med

[6] Risikovurderingene kommer vi nærmere inn på i avsnitt 3.4.1.

anskaffelsesprosessen. Vi har mottatt referatet fra møtet i rådmannens ledergruppe juni 2020 hvor den årlige gjennomgangen ble gjennomført.

Personvernombudet er ikke kjent med at det er gjennomført en gjennomgang av informasjonssikkerheten i 2021. Han opplyser at han ved to anledninger har bedt om å få det satt på agendaen.

### 3.1.3. Revisors vurdering av ansvars- og rollefordeling og rapportering

Strategi for informasjonssikkerhet har i utgangspunktet en oversiktlig struktur når det gjelder rolle- og ansvarsfordeling, men innholdet er til tider utydelig. For eksempel har ordføreren «delegert den administrative del av kommunen til rådmannen som har det faglige ansvar.» Dette samsvarer ikke med påfølgende avsnitt hvor det står at rådmann har ansvar for *all* behandling i kommunen. Kommunen bør vurdere om strategien kan tydeliggjøres.

At ordfører i utgangspunktet er juridisk behandlingsansvarlig for kommunen vurderer vi at er i strid med personopplysingsloven art. 4 nr. 7, som sier at behandlingsansvaret ligger hos kommunen som juridisk subjekt.[7] Kommunestyret er kommunens øverste organ,[8] og behandlingsansvaret vil derfor i utgangpunktet ligge der. Følgelig er det kommunestyret som har myndighet til å eventuelt delegere behandleransvaret til ordfører eller rådmann.

Noen systemeiere har ansvar for mange systemer. Her må fordelen med å ha oversikt over IKT-systemene innenfor sitt område og risikoen for at man ikke får fulgt opp hvert enkelt system i tilstrekkelig grad veies opp mot hverandre.

Vi vil også påpeke at personvernombudet rollebeskrivelse er svært kortfattet, vi kommer nærmere inn på personvernombudets rolle i avsnitt 3.2.

DigiForum har en sentral rolle i arbeidet informasjonssikkerhet og personvern, blant annet ved anskaffelse av nye IKT-systemer. Vi mener at DigiForum er et nyttig tiltak, som kan bidra til bedre samordning i kommunens digitaliseringsarbeid. Forumet har et eget mandat, men er ikke omtalt i Strategi for informasjonssikkerhet. Vi vurderer at det vil være en fordel at DigiForum er omtalt i strategi for informasjonssikkerhet, og at dette bør vurderes ved neste revisjon av strategien.

Strategi for informasjonssikkerhet ble sist revidert i 2018, antakelig i forbindelse med ny personopplysningslov. Det er hensiktsmessig å prøve ut hvordan ny organiseringen fungerer før strategien evalueres. På bakgrunn at det nå har gått snart fire år siden siste revidering vurderer vi at strategien, herunder oppgave- og ansvarsfordelingen, er moden for revidering.

Rapportering er i begrenset grad beskrevet i strategi for informasjonssikkerhet. Det er imidlertid noe omtale av rapportering til rådmannens ledergruppe. Ledergruppa skal ha en årlig

[7] Se også Datatilsynet, «Behandlingsansvarlig og databehandler»
[8] Jamfør kommuneloven § 5-3.

gjennomgang av informasjonssikkerheten. I praksis er det kun den årlige gjennomgangen som er gjennomført, og den er ikke gjort i 2019[9] og 2021. De tre gjennomgangene som er gjort, har etter vår vurdering et hensiktsmessig format.

Vi mener at det i strategien tydelig bør fremgå hvordan personvernombudet skal rapportere. Det følger av personopplysingsloven art. 38, nr. 3 at personvernombudet skal rapportere direkte til det høyeste ledernivået i kommunen.

[9] Gjennomgangen ble imidlertid gjennomført både i april og desember 2018.

## 3.2. Personvernombudsordningen i Porsgrunn kommune

**Porsgrunn kommune skal ha personvernombud, organisert i samsvar med personopplysningsloven.**

### 3.2.1. Bakgrunn

Fra omtrent 2011 til 2014 hadde Porsgrunn kommune en frivillig ordning med personvernombud. Da vedkommende sluttet ble ikke rollen videreført.

Kommunen tilsatte igjen personvernombud i november 2017.[10] Stillingen ble lagt til IKT-avdelingen, og var i utgangspunktet kombinert med rollen som rådgiver for informasjonssikkerhet. Det daværende personvernombudet har opplyst at rådgiverrollen ble utøvd i tett samarbeid med IKT-leder. I november 2018 gikk personvernombudet over til en ny stilling i kommunen, men beholdt rollen som personvernombud i tillegg til sine nye oppgaver. Det ble startet et arbeid for å finne et nytt personvernombud, uten at dette lyktes før høsten 2019. Da sa leder for service seg villig til å være personvernombud, og har fungert som det fra desember 2019 til dags dato.

I sluttmøtet fikk vi opplyst at kommunen har oppnevnt et nytt personvernombud, han vil ta over rollen fra 1. mars.[11] Siden dette skjer etter vi har avsluttet våre undersøkelser, og vi ikke har hatt noen kontakt med han, har vi ikke vurdert det nye personvernombudet, men forholdt oss til personvernombudet som har hatt rollen fra høsten 2019.

### 3.2.2. Stillingsbeskrivelse og arbeidsoppgaver

I strategi for informasjonssikkerhet er rollen som personvernombud kun kort beskrevet, ved at personvernombudet:

> *Ivaretar kravene til et personvernombud i henhold til personvernregelverket. Ombudet er ansvarlig for å motta meldinger om ny behandling av personopplysninger i kommunen.*
>
> *Rollen skal være uavhengig.*

Da vi ba om å få oversendt personvernombudets stillingsinstruks e.l., sendte administrasjonen en stillingsutlysning fra høsten 2017. Stillingsutlysningen var for en rådgiver som skulle arbeide med informasjonssikkerhet og personvern. Vi legger til grunn at dette er stillingsutlysningen fra da det forrige personvernombudet ble tilsatt.

I intervjuet med oss fortalte personvernombudet at han har fokusert på å ta unna de forefallende oppgavene, og ikke på utvikling av personvernarbeidet. Denne prioriteringen er gjort i forståelse

[10] Ble registrert som personvernombud hos Datatilsynet den 10.01.18.
[11] Det nye personvernombudet vil ha avsatt en 40 prosent stilling til arbeidet. Han har utdanning innenfor økonomi, administrasjon og informatikk. Han har også erfaring fra disse områdene samt prosjektledelse.

med kommunalsjef og rådmann, og skyldes at personvernombudet har begrenset kapasitet å bruke på dette arbeidet.[12]

Det daglige personvernarbeidet består i stor grad i å besvare mottatte henvendelser fra ansatte og innbyggere, samt gjennomlesing av databehandleravtaler før de signeres av rådmannen. Videre samarbeider personvernombudet med DigiForum. Han forteller at dette samarbeidet er nyttig med tanke på kvalitetssikring av anskaffelsesprosesser som gjøres i DigiForum, og i arbeidet med å fylle ut protokollen for behandlingsaktiviteter. Utfylling av protokoll skjer i samarbeid med de systemansvarlige.

### 3.2.3. Personvernombudets uavhengighet

Personvernombudet skal være uavhengig. Kravet om uavhengighet innebærer blant annet at personvernombudet ikke skal instrueres i arbeidet og at hen ikke skal ha oppgaver som kan komme i konflikt med oppgavene som personvernombud.

Det nevnes i strategi for informasjonssikkerhet at personvernombudet skal være uavhengig, men det utdypes ikke nærmere hva dette innebærer og hvordan det skal ivaretas.

I intervju med personvernombudet har han selv fremhevet at oppgaven som personvernombud i noen tilfeller kommer i konflikt med de andre arbeidsoppgavene han har. Eksempler på dette er at han er ansvarlig for kommunens arkiv, og at han er systemansvarlig for flere IKT-systemer. Han presiserer at dagens løsning ble gjort for å løse en situasjon hvor kommunen sto uten personvernombud.

IKT-leder har gitt utrykk for at han mener personvernombudet verken bør arbeide i avdelingen som har ansvar for arkivet eller i IKT avdelingen.

### 3.2.4. Kompetanse

I strategi for informasjonssikkerhet fremgår det ikke noe krav til kompetanse for personvernombudet. I stillingsutlysningen fra 2017, som administrasjonen har fremlagt som stillingsbeskrivelsen for personvernombudet, er det listet opp følgende kvalifikasjonskrav:

- relevant høyere utdanning. Lang og relevant erfaring kan kompensere for utdanningskravet
- erfaring fra arbeid med informasjonssikkerhet
- god kjennskap til problemstillinger knyttet til personvern og informasjonssikkerhet
- kjennskap til standarder og rammeverk som er relevant for informasjonssikkerhet
- erfaring fra arbeid med sikkerhetsledelse er en fordel
- erfaring fra arbeid i eller nært knyttet til et IKT-miljø er en fordel

[12] Personvernombudet har blant annet følgende roller: virksomhetsleder for service, virksomhetsleder for politikk og revisjon, ansvar for økonomi for rådmannens stab, medlem i krisestab og medlem av Akan. Han er også personvernombud for Grenland brann og redning IKS.

- inngående kjennskap til relevante lover og reguleringer er en fordel

Personvernombudet fortalte i intervju at han har utdanning fra forsvaret med videreutdanning i bla. personal og ledelse. Han har arbeidserfaring som yrkesmilitær, politiet og helsevesenet. I disse stillingene arbeidet han med personalledelse. Hans hovedstilling i kommunen er som leder av virksomheten service, som han har hatt siden 2010. Her er han blant annet ansvarlig for arkivet. Gjennom dette arbeidet har han opparbeidet seg erfaring med behandling av personopplysninger, bla. i arbeid med innsynsbegjæringer, offentlighetsloven og forvaltningsloven. Da han fikk rollen som personvernombud, tok han flere juridiske kurs (dette ble gjort på starten av 2020) med gjennomgang av lovverket innenfor informasjonssikkerhet og personvernombudsrollen.

### 3.2.5. Revisors vurdering av personvernombudsordningen i Porsgrunn kommune

Kommunen som behandlingsansvarlig, har ansvaret for å sikre at den som oppnevnes til personvernombud kan oppfylle kravene som stilles i personopplysningsloven.

Vi vurderer at personvernombudet i skrivende stund ikke tilstrekkelig uavhengig da han, i tillegg til å være personvernombud, også har ansvar for kommunens arkiv og er systemansvarlig for flere IKT-systemer. I rollene som ansvarlig for arkiv og systemansvarlig skal han bestemme formålet for behandling, oppbevaring mm. av personopplysninger, og vil da i neste omgang ikke være uavhengig til å vurdere disse beslutningene som personvernombud. Vi vil påpeke at det finnes tilfeller hvor virksomheter i Europa har blitt bøtelagt for personvernombudets manglede uavhengighet.[13]

Han som er personvernombud i skrivende stund har kompetanse og erfaring som leder av service, og har skaffet seg relevant kompetanse etter at han ble personvernombud. Dette synes å ha gitt personvernombudet nødvendige kvalifikasjoner.

Videre fremstår det for oss som personvernombudet ikke har tilstrekkelig tid til å ivareta alle sine oppgaver.

Personvernombudet er svært kortfattet omtalt i strategi for informasjonssikkerhet. Strategien sier lite om personvernombudets oppgaver eller hva det innebærer at personvernombudet skal være uavhengig. Det står heller ikke noe om rapportering eller krav til kompetanse. Vi vurderer at dette bør tydeliggjøres ved neste revisjon av strategien.

[13] Næss og Østmoe, «Hvordan skape et supert personvernombud?», *Lov & Data*, 2/2021, s. 9

## 3.3. Protokoll over behandlingsaktiviteter

**Porsgrunn kommune skal ha protokoll over hvilke personopplysninger kommunen behandler.**

### 3.3.1. Rutiner for protokoll

Administrasjonen har organisert kommunens protokoll i et excelark, sortert etter IKT-program. Protokollen er nærmest identisk med malen som Datatilsynet har publisert på sine nettsider, det viktigste unntaket er at administrasjonen registrerer opplysningene *per IKT-program,* og ikke *per behandlingsprosess,* som Datatilsynets mal legger opp til. Vi har fått opplyst dette gjort for å gjøre utfyllingen av protokollen håndterbar. Fremgangsmåten kommunen har valgt er etter vår kjennskap benyttet i flere andre kommuner. I tillegg er Datatilsynet kolonne «internt ansvarlig» delt i to kolonner i kommunens protokoll: en for systemeier og en for systemansvarlig. Det er ikke angitt datoer i protokollen for når informasjonen om de enkelte systemene er lagt til, og det fremgår heller ikke når protokollen som helhet sist er revidert. Dette er ikke påkrevd i personopplysingsloven, og malen fra Datatilsynet inneholder kun en revideringslogg for hele dokumentet. Kommunen protokoll har også en slik revideringslogg, men denne er ikke utfylt..

Administrasjonen har opplyst at innholdet i protokollen er resultatet av et omfattende kartleggingsarbeid i 2018, i form av et idéverksted med de systemansvarlige, initiert av det daværende personvernombudet. Det viktigste var da å kartlegge behandlingsgrunnlag og formål, fordi dette var opplysninger kommunen ikke kunne få fra andre kilder.

Kommunen har ikke noen skriftlig rutine vedrørende utfylling og oppfølging av protokollen. Personvernombudet forteller at utfylling av protokoll gjøres i samarbeid med kommunens DigiForum og systemansvarlig. Oppdatering av protokollen er et av områdene personvernombudet har prioritert å følge opp. Det tidligere personvernombudet, som i dag er medlem av DigiForum, opplyser at det kommer en årlig påminnelse i forumet om å oppdatere protokollen med eventuell ny informasjon. Hun opplyser også at det ble gjort en gjennomgang av protokollen for å sjekke eventuell overføring til tredjeland etter Schems II-dommen kom i 2020.[14]

### 3.3.2. Stikkprøvekontroll av protokoll

Vi har gjennomført en stikkprøvekontroll av opplysningene som er registrert i protokollen for et utvalg IKT-systemer. Utvalget skulle bestå av ti tilfeldig utvalgte IKT-systemer fra kommunens protokoll.[15] Etter at vi hadde gjort utvalget fikk vi tilbakemelding om at tre av de utvalgte systemene ikke var i bruk. For et av disse fikk vi tilbakemelding så raskt at vi hadde anledning til å trekke et nytt system, med det rakk vi ikke for de to andre. Dette medfører at stikkprøvekontrollen er gjort i åtte systemer.[16]

[14] Schrems II-dommen er en dom fra EU-domstolen som omhandler overføring av personopplysninger til land utenfor EU/EØS (kilde: Digdir, *Hva er Schrems II-dommen*).
[15] Utvalg og undersøkelsen ble gjort protokoll mottatt 11.11.21.
[16] For mer detaljer om utvalg se vedlegg 3.

IKT-systemene i utvalget er som følger:

- Lekdommer
- Trio
- ISY Eiendom
- Easypark
- When I work
- Gerica LMP
- ReMin
- Telenor Min Bedrift

I stikkprøven undersøkte vi om følgende opplysninger var registrert for hvert IKT-system:

- formål med behandlingen av personopplysninger (jamfør personopplysningsloven art. 30, nr. 1, bokstav b),
- kategorier av registrerte (dvs. hvem er det personopplysninger om, jamfør personopplysningsloven art. 30, nr. 1, bokstav c),
- kategoriene av personopplysninger (dvs. hvilke personopplysninger er registrert, jamfør personopplysningsloven art. 30, nr. 1, bokstav c) og
- behandlingsgrunnlag (jamfør personopplysningsloven art. 6, nr. 1)[17]

**IKT-systemer i ordinær drift**

De 8 undersøkte systemene hadde alle oppgitt formålet med behandlingen av personopplysninger. Hvilke kategorier av registrerte som var i systemet, var oppgitt i 7 av de 8 programmene. Det samme gjaldt for kategorier av personopplysninger. Hvorvidt behandlingsgrunnlag var oppgitt har vi oppsummert i tabell 2.

*Tabell 2 Behandlingshjemmel for et utvalg av systemer*

| System | Hjemmel | Beskrivelse hjemmel og tilleggshjemmel |
|---|---|---|
| **Lekdommer** | Art. 6, nr. 1, bokstav b | Oppfylle avtale med den registrerte |
| **Trio** | Ikke oppgitt | |
| **ISY Eiendom** | Art. 6, nr. 1, bokstav b | Oppfylle avtale |

[17] Personopplysningsloven krever ikke at dette fremgår av protokollen, men det er anbefalt i Datatilsynets mal for protokoll. Videre krever personopplysningsloven art. 6, nr. 1 at kommunen må ha et gyldig behandlingsgrunnlag for å kunne *behandle* personopplysningene. Merk at bruk av hjemmelsgrunnlagene i artikkel 6, nr. 1, bokstav c eller 6, nr. 1, bokstav e også krever hjemmel i en annen lov for å brukes.

| System | Hjemmel | Beskrivelse hjemmel og tilleggshjemmel |
|---|---|---|
| **Easypark** | Art. 6, nr. 1, bokstav b | Oppfylle avtale |
| **When I work** | Art. 6, nr. 1, bokstav b | Oppfylle avtale |
| **Gerica LMP** | Art. 6, nr. 1, bokstav e | Allmenhetens interesse/ utøve offentlig myndighet, jamfør helsepersonelloven §§ 26, 39 og 40; helse- og omsorgstjenesteloven; pasientjournalloven § 8, jamfør helsepersonelloven § 39 |
| **ReMin** | Art. 6, nr. 1, bokstav e | Allmenhetens interesse/ utøve offentlig myndighet, jamfør smittevernloven § 3-6 |
| **Telenor Min Bedrift** | Ikke oppgitt | |

Som tabellen viser, er hjemmel for behandling oppgitt for 6 av 8 systemer. Fire av disse bruker hjemmelen at behandlingen gjøres for at kommunen skal oppfylle en avtale. To systemer bruker hjemmelen at behandlingen er i allmenhetens interesse eller at kommunen skal utøve offentlig myndighet som den er pålagt ved lov. For disse to systemene skal det vises til hjemmel i annen lov, noe som er gjort.

### 3.3.3. Hjemmel for behandling av særskilte kategorier av personopplysninger

For å behandle særskilte kategorier av personopplysninger kreves en egen hjemmel, i tillegg til det generelle grunnlaget i personopplysingsloven art. 6, nr. 1. Hjemlene for å behandle særskilte kategorier av personopplysninger er listet opp i personopplysingslovens art. 9, nr. 2 og 10. For noen av disse grunnlagene kreves det også hjemmel i annen lov.

Totalt er det 18 systemer i kommunens protokoll hvor hjemmel for å behandle særskilte kategorier av personopplysninger er oppgitt. Disse er fordelt på: art. 9, nr. 2, bokstav a (uttrykkelig samtykke), art. 9, nr. 2, bokstav b (behandlingen er nødvendig for å oppfylle plikter og rettigheter innenfor arbeidsrett, trygderett og sosialrett)[18] og art. 9 nr. 2, bokstav h (behandlingen er nødvendig for å yte blant annet helse- og sosialhjelp).[19] Behandling av særskilte personopplysninger etter art. 9, nr. 2, bokstav b og 9, nr. 2 bokstav h krever hjemmel i annen lov. Administrasjonen har ikke oppgitt

[18] Personopplysingsloven art. 9, nr. 2, bokstav b: «Behandlingen er nødvendig for at den behandlingsansvarlige eller den registrerte skal kunne oppfylle sine forpliktelser og utøve sine særlige rettigheter på området arbeidsrett, trygderett og sosialrett i den grad dette er tillatt i henhold til unionsretten eller medlemsstatenes nasjonale rett, eller en tariffavtale i henhold til medlemsstatenes nasjonale rett som gir nødvendige garantier for den registrertes grunnleggende rettigheter og interesser».

[19] Personopplysingsloven art. 9, nr. 2, bokstav h: «Behandlingen er nødvendig i forbindelse med forebyggende medisin eller arbeidsmedisin for å vurdere en arbeidstakers arbeidskapasitet, i forbindelse med medisinsk diagnostikk, yting av helse- eller sosialtjenester, behandling eller forvaltning av helse- eller sosialtjenester og -systemer på grunnlag av unionsretten eller medlemsstatenes nasjonale rett eller i henhold til en avtale med helsepersonell og med forbehold for vilkårene og garantiene nevnt i nr. 3».

slik hjemmel i protokollen. For 15 av disse 18 IKT-systemene er det oppgitt en tilleggshjemmel i forbindelse med det ordinære behandlingsgrunnlaget, jamfør art. 6, det er imidlertid ikke tydeliggjort om denne tilleggshjemmelen også gjelder for behandlingsgrunnlaget for særskilte personopplysninger.

### 3.3.4. Observasjoner fra casestudie

Vi undersøkte også om de to IKT-systemene i casestudien vår var registrert i protokollen og stilte også spørsmål om dette i intervjuene.

**SafeMate**

SafeMate er registrert i protokollen med blant annet informasjon om formål, kategorier av registrerte og kategorier av personopplysninger. Behandlingsgrunnlaget som er oppgitt er personopplysingsloven art. 6, nr. 1, bokstav e (allmenhetens interesse/ utøve offentlig myndighet) jamfør helse- og omsorgstjenesteloven § 3-2, første ledd, nr. 6a. Det er også oppgitt hjemmel for behandling av særlige kategorier av personopplysninger (personopplysningsloven art. 9, nr. 2, bokstav h). Her kreves hjemmel også i annen lov, men vi kan ikke se at det er oppgitt. Helse- og omsorgstjenesteloven er imidlertid angitt i forbindelse med det generelle behandlingsgrunnlaget (jamfør personopplysingsloven art. 6).

De ansvarlige for SafeMate opplyser at systemet ble registrert i protokollen som en del av kartleggingsarbeidet i 2018. De mener at det ikke har vært noe oppdatering av informasjonen for SafeMate siden den gang.

På spørsmål om hjemmel for behandlingen viser de ansvarlige for SafeMate til hjemmelen for å behandle særlige kategorier av personopplysninger (personopplysingsloven art. 9) og helse- og omsorgstjenesteloven § 3-2. Videre fortalte de at siden mange av brukerne ikke er samtykkekompetente, fattes det vedtak om tjenesten med hjemmel i pasient- og brukerrettighetsloven § 4, nr. 6, bokstav a. Denne paragrafen gir kommunen mulighet til å fatte vedtak på visse vilkår når brukeren ikke er samtykkekompetent.

**Teams**

Teams er ikke registrert i kommunens protokoll. Administrasjonen opplyser at årsaken til dette er at de vurderte at Teams ikke skulle behandle personsensitive opplysninger, og at registering derfor ikke var nødvendig. Administrasjonen har i ettertid sett at dette var en feilvurdering, siden systemet behandler personopplysninger.

Hjemmel for å behandle personopplysninger i Teams[20] vurderer intervjudeltakerne enten til å være allmenhetens interesse eller lovpålagt oppgave (det vil si personopplysingsloven art. 6, nr. 1, bokstav e, eventuelt art. 6, nr. 1, bokstav c).

[20] I intervjuet fant vi det mest relevant å fokusere på de personopplysninger som brukes for å administrere systemet.

### 3.3.6. Revisors vurdering av protokoll over behandlingsaktiviteter

Administrasjonens arbeid med protokollen har resultert i en ryddig og i hovedsak godt utfylt protokoll.

Kommunen bruker et excelark for sin protokoll. Vi ser noen begrensninger som følger av dette valget; det begrenser hvor detaljert tekstinformasjon man kan legge inn, og det er begrensede muligheter til å gjøre uttrekk eller generere statistikk av tekstinformasjonen i Excel.

Manglende datering av opplysningene i protokollen medfører at det kan være vanskelig å vite om opplysningene i protokollen er oppdaterte. At det mangler gode systemer for oppdatering viste seg i vår stikkprøvekontroll, der to av de utvalgte programmene ikke lenger var i bruk.[21]

Stikkprøvekontrollen viste at de opplysningene vi kontrollerte i hovedsak var registrert. Informasjonen fremstår kortfattet og informativ. Det var imidlertid noen systemer hvor det manglet lovpålagte opplysninger i protokollen, og et av de to systemene i casestudien vår var ikke registrert i protokollen. Kommunen må sikre at protokollen oppfyller kravene i personopplysingsloven for alle sine IKT-systemer som behandler personopplysninger.

For to av systemene i stikkprøven var det ikke oppgitt hjemmel for behandlingen av personopplysninger. For systemet Lekdommer har administrasjonen brukt personopplysningslovens art. 6, nr. 1, bokstav b (oppfylle en avtale) som hjemmel for behandlingen av personopplysninger. Vi er usikre om dette er rett hjemmel, da vi ikke kan se hva slags avtale som skal oppfylles. Vi mener at mer relevante hjemler er personopplysingsloven art. 6, nr. 1, bokstav c eller 6, nr. 1, bokstav e, jamfør domstolloven §§ 66-69. Kommunen bør forsikre seg om at de har hjemmel for alle systemer som behandler personopplysninger og at denne er riktig.

For de systemene som behandler særlige kategorier av personopplysninger har kommunen i hovedsak benyttet art. 9, nr. 2, bokstav b eller h. Disse behandlingsgrunnlagene krever at kommunen også hjemler dette i en annen lov. Dette har kommunen ikke angitt i protokollen. Kommunen bør forsikre seg om at de har et tilstrekkelig hjemmelsgrunnlag for å behandle særlige kategorier av personopplysninger.

[21] Et av disse var markert i rødt, men det var ikke forklart hva som var årsaken til dette. I tillegg er det et program som ble registrert i forbindelse med et forarbeid i 2018, men har aldri vært tatt i bruk. Dette IKT-systemet var markert med «NB ikke i bruk enda».

## 3.4. Risikovurderinger og vurdering av personvernkonsekvenser

**Porsgrunn kommune skal ha risikovurderinger og dokumenterte vurderinger av personvernkonsekvenser (DPIA).**

### 3.4.1. Overordnede risikovurderinger

I Strategi for informasjonssikkerhet fremgår det at rådmannens ledergruppe er ansvarlig for å sørge for at det gjøres risikovurderinger av kommunens informasjonsverdier. For hele kommunen lages det en risikovurdering av informasjonssikkerheten i forbindelse med ledergruppens årlige gjennomgang. Vi har fått fremlagt risikovurderinger fra april 2018, desember 2018 og juni 2020. Risikovurderingene er relativt kortfattede, med varierende detaljeringsgrad i beskrivelsene. I april 2018 er det identifisert seks uønskede hendelser/risikoer, mens i desember 2018 og juni 2020 er det identifisert ti uønskede hendelser/risikoer. Risikovurderingen fra juni 2020 bygger på vurderingen fra 2018, dette vises blant annet ved at beskrivelsen av risikoene og vurderingen av sannsynlighet i hovedsak er like. Den viktigste forskjellen fra 2018 til 2020 er at rutinene for anskaffelser av IKT-system er endret, slik at sannsynligheten for uønskede hendelser på dette området anses redusert. Dette har videre ført til endringer i vurderingen av risiko og behovet for nye tiltak. Dette blir også bekreftet av den andre dokumentasjonen vi har fått og intervju med personvernombudet.

Risikovurderingene fra desember 2018 og juni 2020 er tydelige på hvilke risikoer som skal aksepteres (altså det gjøres ikke nye tiltak) og hvor det foreslås tiltak. I noen tilfeller er det både et alternativ å akseptere risikoen og å gjøre tiltak, eller at det er satt opp alternative tiltak. Dette er i samsvar med strategi for informasjonssikkerhet, hvor rådmannens ledergrupper er ansvarlig for å beslutte hvilket risikonivå som skal aksepteres. Vi har imidlertid ikke sett dokumentasjon som viser noen beslutning om hva som aksepteres av risiko og ikke.

### 3.4.2. Risikovurderinger i organisasjonen

Strategi for informasjonssikkerhet fastsetter at virksomhetsledere skal dokumentere risikovurderinger. Ledere med personalansvar skal planlegge og gjennomføre nødvendige risikovurderinger. Administrasjonen har avklart at dette skal være risikovurderinger av informasjonssikkerhet og personvern innenfor leders eget ansvarsområde. Det fremgår her også at ledere med personalansvar skal «vurdere personvernkonsekvenser før ny behandling av personopplysninger». Administrasjonen opplyser det er meningen at leder med personalansvar skal gjennomføre en risikovurdering og vurdere behovet for å gjennomføre en utvidet risikovurdering (vurdering av personvernkonsekvenser/DPIA).[22]

I casestudiene våre spurte vi virksomhetslederne[23] i de to enhetene som vi intervjuet om de har gjennomført egne risikovurderinger. De fortalte at det ikke var gjennomført skriftlige lokale

[22] «Vurdering av personvernkonsekvenser» (også kjent som DPIA) er en utvidet risikovurdering som kommunen skal gjennomføre på visse vilkår, jamfør personopplysningsloven art. 35-1, se også avsnitt 3.4.5.
[23] Det deltok også en avdelingsleder i en et av intervjuene. Alle disse tre hadde også (i forskjellig grad) personalansvar.

risikovurderinger av informasjonssikkerhet og personvern. De vektla at de brukte systemer som var felles for kommunen og baserer seg på at kommunen har vurdert disse systemene.

### 3.4.3. Risikovurderinger av IKT-systemer

Systemeier har ansvaret for at det gjennomføres risikovurdering av sine IKT-systemer. I strategi for informasjonssikkerhet fremgår det at: «Kommunen skal systematisk vurdere behov for, og gjennomføre risikovurderinger». På spørsmål om hvordan dette følges opp, svarer administrasjonen at dette vurderes fortløpende av virksomhetsledere og systemeiere som et ledd i kommunens kvalitetsarbeid, og gjennom verktøy i kommunens kvalitetssystem TQM. Videre svarer kommunen at IKT-avdelingen benytter en mal for kravspesifikasjoner som utarbeides. Dette for å sikre at alle nye anskaffelser stiller krav til informasjonssikkerhet.

Administrasjonen har ikke noen samlet oversikt over risikovurderinger som er utført av det enkelte IKT-system, og viser videre til systemeierne.

**Stikkprøver av risikovurderinger for IKT-system**

Vi har undersøkt om administrasjonen har vurdert behovet for risikovurdering av informasjonssikkerhet og personvern, og om slike risikovurderinger er gjennomført. Vi har brukt det samme utvalget som for stikkprøvene av protokollen, se detaljer om utvalget i avsnitt 3.3.2. For hvert system sendte vi en henvendelse til systemeier. Vi spurte om de hadde gjort en vurdering av behovet for å gjennomføre en risikovurdering for det aktuelle systemet, og vi bad om å få oversendt de to siste risikovurderingene som de hadde gjennomført for systemet. Tilbakemeldingene er oppsummert i tabell 3.

*Tabell 3 Vurdering av behov for og gjennomføring av risikovurdering for utvalgte IKT-system*

| IKT-system | Vurdering av behov for risikovurdering | Gjennomført risikovurdering |
|---|---|---|
| **Lekdommer** | Nei | Nei |
| **Trio** | Nei | Nei |
| **ISY Eiendom** | Nei | Nei |
| **Easypark** | Ja, men vektlegger primært tilgjengelighet. Udatert, e-post mottatt 05.01.22. | Nei |
| **When I work** | Ja,12.01.22 | Ja, 10.01.22 |

| IKT-system | Vurdering av behov for risikovurdering | Gjennomført risikovurdering |
|---|---|---|
| **Gerica LMP** | Ja, udatert, antakelig i 2018. Utført i et felles arbeid med velferdsteknologi mellom flere kommuner | Ja, 12.12.18 (generell risikovurdering for elektronisk pasient journal på mobil, men ikke for Erica LMP). 2016 – ved innføring ble det laget en oversikt over tiltak ved forskjellige hendelser, utgjør ikke ROS i seg selv, men kunne ha utgjort en del av en ROS. |
| **ReMin** | Nei | Ja, 15.09.20 |
| **Telenor Min Bedrift** | Nei | Nei |

**Vurdering av behov for risikovurdering**
Vi ser av tabellen at tre av åtte IKT-systemer kan vise til en vurdering av behovet for en risikovurdering. Vurderingen for Easypark konkluderer med at det ikke er behov for risikovurdering. Dette begrunnes med høy tilgjengelighet av tjenesten (den er en tilleggstjeneste til kommunens egen parkeringsapp og derfor er ikke nedetid kritisk) og personvern/informasjonssikkerhet er ikke vurdert.

For When I Work opplyser kultur- og idrettssjefen at de generelt gjennomfører ROS ved anskaffelse, utvikling og utskifting. Hun viser også til gjennomgang i 2018 i forbindelse med GDPR. Kulturhussjefen viser til at risiko og den lave mengden med behandling gjør at det ikke har vært behov for å gjennomføre en risikovurdering av When I Work tidligere. Som et resultat av vår henvendelse har de valgt å gjennomføre en risikovurdering allikevel.

For Gerica LMP har vi blitt fortalt at behovet for risikovurdering ble vurdert i et samarbeid om velferdsteknologi mellom Bamble, Siljan, Porsgrunn og Skien, trolig i 2018.[24] Denne vurderingen ble gjort for forskjellige typer velferdsteknologi og ikke for Gerica LMP konkret. Resultatet av den felles vurderingen var at det ble gjennomført en risikovurdering og vurdering av personvernkonsekvenser (DPIA) for elektronisk pasientjournal på mobil.

For ReMin har vi fått opplyst at dette systemet ble anskaffet i 2020, i forbindelse med smittesporing under koronapandemien, og at det har vært et stort arbeidspress på tjenesten i denne perioden.

[24] Selve risikovurderingen er datert til desember 2018.

**Gjennomførte risikovurderinger**
Det er gjennomført risikovurderinger tre av systemene. Et av disse (When I Work) ble risikovurdert i forbindelse med forvaltningsrevisjonen, og vurderingen er kortfattet. De to andre systemene som er risikovurdert er begge innenfor Helse og omsorg.

For Gerica LMP viser administrasjonen til risikovurderingen som ble gjort i samarbeidet mellom Grenlandskommunene om velferdsteknologi (nevnt over) i desember 2018. Denne vurderingen gjelder generelt for elektroniske pasientjournaler på mobil, og ikke for Gerica LMP spesifikt. Videre viser administrasjonen til et dokument som ble utarbeidet i 2016 ved innføring av systemet hvor forskjellige hendelser og hvilke tiltak som skulle settes inn er listet opp. Administrasjonen opplyser at dette ikke utgjør en fullstendig risikovurdering alene, men kunne ha vært en del av en risikovurdering. Her er det en ganske omfattende liste av uønskede hendelser, men begrunnelsen for vurdert konsekvens og sannsynlighet er ikke like godt utfylt.

For ReMin har vi mottatt en risikovurdering, denne skal være loggført til 15.09.20. Administrasjonen opplyser at grunnet det høye arbeidspresset under koronapandemien tok de utgangspunkt i maler fra leverandør, og har benyttet seg av hva leverandør og andre kommuner har vurdert, i den grad dette sammenfaller med kommunens egne forhold. Risikovurderingen er ganske detaljert og omfattende. Den beskriver årsak/trussel, uønsket hendelse og mulige konsekvenser. Det er fastsatt nivå på sannsynlighet, konsekvens og risiko. I tillegg er eksiterende tiltak og aktuelle forslag til nye tiltak beskrevet.

### 3.4.4. Observasjoner fra casestudier – risikovurdering av IKT-system
I casestudien hadde vi med to IKT-systemer. I intervjuene stilte vi spørsmål om hvilke risikovurderinger som var gjennomført for IKT-systemene.

**Teams**
Intervjudeltakerne opplyste at det var gjennomført en risikoanalyse for hele Office 365, som Teams er en del av. Det var ikke gjennomført en egen risikoanalyse for Teams, men det var planer om å gjennomføre risikoanalyser for hver enkeltkomponent i Teams. IKT-leder fortalte at det generelt har vært lite risikovurdering av personvern og informasjonssikkerhet i IKT-systemer i Porsgrunn kommune. Praksis har i hovedsak vært å gjennomføre risikoanalyse i forbindelse med anskaffelse av systemer. Videre kunne de fortelle at det nå var igangsatt en prosess med samsvaranalyse. Samsvaranalysen skal utføres at et eksternt konsulentselskap. Denne analysen omfatter alle kommunens IKT-systemer, og vil blant annet inneholde risikovurderinger.

**SafeMate**
Når det gjelder SafeMate opplyste intervjudeltakerne at det ble gjennomført en risikoanalyse i 2018, og at denne ble revidert i februar 2021. De tok utgangspunkt i uønskede hendelser, og tjenesten hadde gjort et godt forarbeid med å utarbeide en liste over hva som kunne skje. Det blir vektlagt at man må sikre at systemet funger slik som det skal når det er behov, da det motsatte kan føre til tapt tillit og utrygghet hos bruker/pasient.

### 3.4.5. Vurdering av personvernkonsekvenser (DPIA)

**Rutiner for DPIA**

Vurdering av personvernkonsekvenser (DPIA[25]) er en utvidet risikovurdering som skal utføres når en behandling av personopplysninger i kommunen oppfyller visse kriterier. I henhold til personopplysingslovens art. 35, nr. 1 skal DPIA utføres når behandlingen «vil medføre en høy risiko for fysiske personers rettigheter og friheter». Videre har Datatilsynet utarbeidet en liste over behandlinger hvor det skal gjennomføres en DPIA, jf. personopplysingsloven art. 35, nr. 4.

Administrasjonen viser til Strategi for informasjonssikkerhet avsnitt 1.3 for rutiner knyttet til gjennomføringen av DPIA. Her fremgår det at kommunen systematisk skal vurdere behov for, og gjennomføre risikovurderinger. Rådmannens ledergruppe har ansvaret for å se til at det gjennomføres risikovurderinger, og vi antar at dette også gjelder DPIA. Videre har vi fått opplyst at leder med personalansvar skal gjennomføre en risikovurdering og vurdere behovet for en DPIA. Kommunen har en mal for gjennomføring av DPIA, denne vil vi beskrive i det følgende. Vi er ikke kjent med at kommunen har andre rutiner for gjennomføringen av DPIAer.

Kommunens mal for DPIA har innledningsvis felter for å oppgi grunnleggende informasjon om IKT-systemet og gjennomføringen av DPIAen. Deretter er det et avkrysningsskjema hvor man kan vurdere behovet for å gjennomføre en DPIA. Etter dette består skjemaet av to hoveddeler. Den første delen er en beskrivelse av behandlingen av personopplysninger, blant annet:

- hva behandling består i
- omfanget av behandlingen
- formålet med behandlingen
- i hvilken sammenheng behandlingen gjøres
- kilder, mottakere, informasjonssikkerhet og ansvarsforhold

For hvert av disse punktene er det detaljerte spørsmål for å hjelpe den som skal fylle ut skjemaet til å gi en grundig beskrivelse.

Den andre hoveddelen er tabell hvor det er listet opp forskjellige personvernsutfordringer, hvor man for hver av disse skal vurdere i de påfølgende kolonnene: nødvendighet og proporsjonalitet, vurdering av risiko, risikobegrensende tiltak og konklusjon.[26] De forskjellige personvernsutfordringene er:

- lovgrunnlag for databehandling/ overføring
- formålsbegrensning (at data ikke brukes utover sitt originale formål)
- dataminering (at man ikke innhenter mer personopplysninger enn nødvendig)
- korrekte og oppdaterte opplysninger

[25] Data Protection Impact Assessment.
[26] Det er ikke spesifisert hva man skal konkludere på, men vi antar at man skal vurdere om de risikobegrensende tiltakene reduserer risikoen tilstrekkelig.

- lagringsbegrensing (at personopplysninger ikke lagres lengre enn det som er nødvendig)
- konfidensialitet og integritet
- ansvarlighet/ tilsynsmekanisme
- den registrertes rettigheter
- den registrertes friheter

For hvert punkt er det i malen spørsmål for å bistå i utfyllingen av kolonnen nødvendighet og proporsjonalitet. Etter tabellen kommer det veiledninger for utfylling av kolonnen vurdering av risiko og risikobegrensende tiltak. I veiledningen for risiko vektlegges det at risikovurderingen skal gjøres fra perspektivet til de registrerte.

Av andre elementer vil vi fremheve at malen minner om at de registrerte skal representeres når DPIAen utarbeides. Det er også et felt hvor man skal lage en sammenstilling for et beslutnings-grunnlag når ledelsen skal validere DPIAen (med validering mens evaluering og evt. godkjenning). I malen er det også en veiledning til hvordan dette skal gjøres. Det fremgår også at hvis man etter behandling i ledelsen finner at risikoen fortsatt er høy og man fortsatt ønsker å gjennomføre behandlingen skal kontakte Datatilsynet for forhåndsdrøftelse.

**Gjennomførte DPIAer**
Vi har fått informasjon om fire DPIAer som kommunen har gjennomført, disse er beskrevet i tabell 4.

*Tabell 4 Gjennomførte DPIAer i Porsgrunn kommune*

| System | Formål | Kommunalområde | Datering |
|---|---|---|---|
| **SafeMate (GPS)** | Lokalisering av hjemmeboende tjenestemottakere med former for kognitiv svikt | Helse og omsorg | Udatert |
| **Gerica Mobil elektronisk pasient journal (EPJ)** | Tilgang til journalopplysninger om tjenestemottakere | Helse og omsorg | Udatert, 12.12.18* |
| **RoomMate** | Digitale tilsyn og varsling om fall, forlatt rom/stol osv. | Helse og omsorg | 10.02.21 |
| **ReMin** | Smittesporing | Helse og omsorg | Udatert, 17.09.20* |

* DPIA er udatert, dato hentet fra informasjon mottatt i forbindelse med stikkprøve av risikovurderinger.

ReMin bruker ikke kommunens egen mal for DPIA. Systemet ble anskaffet for å håndtere smittesporing under koronapandemien, og på grunn av stor arbeidsbelastningen pandemien valgte

administrasjonen å ta utgangspunkt i leverandørens maler, samt vurderinger fra leverandør og andre kommuner når dette falt sammen med kommunens faktiske forhold. Fra hva vi kan se er DPIAen utarbeidet av leverandøren og det er ikke markert hvor endringer er gjort av kommunen.

Vi har videre fått opplyst at både DPIAen for SafeMate og Gerica Mobil EPJ har vært utført i samarbeid med andre kommuner.

Ingen av DPIAene har opplysninger om hvordan de registrerte eller deres representanter har blitt involvert i arbeidet, jamfør personopplysingsloven art. 35, nr. 9. Vi kan heller ikke se at det er beskrevet hvordan kommunens ledelse er involvert i verifisering av DPIAene, slik som kommunens mal legger opp til.[27]

DPIAene for SafeMate og Gerica Mobil EPJ er ikke utfylt med grunnleggende informasjon som datering og deltakere. I DPIAen for SafeMate er ikke alle personvernsutfordringer fylt ut. Vurdering av risiko, risikobegrensende tiltak og konklusjon er heller ikke utfylt. I DPIAen for Gerica Mobil EPJ er første hoveddel kortfattet utfylt, og det er steder hvor det virker som det er meningen at kommunen skal skrive inn utfyllende informasjon. Andre hoveddel av DPIAen mangler konklusjon (reduserer tiltakene risikoen tilstrekkelig).

De ansvarlige for SafeMate mener at det er en utfordring å involvere pasienter som bruker systemet, da man får denne tjenesten når man har kognitiv svikt. Man har imidlertid informert om arbeidet med velferdsteknologi til eldrerådet og andre folkevalgte. De vektlegger også at bruken av denne type velferdsteknologi er nasjonale innsatsområder, hvor man har involvering av brukere. De opplyser at kommunen bruker kun velferdsteknologi som er anbefalt nasjonalt.

### 3.4.6. Revisors vurdering av risikovurdering og DPIA

**Risikovurderinger**

Kommunen har rutiner for å gjennomføre risikovurderinger, men våre undersøkelser tyder på at disse ikke blir fulgt opp tilstrekkelig i hele kommunen. Kommunen har en mal for gjennomføring av DPIA, men mangler rutiner utover denne. De registrerte er ikke involvert i arbeidet med DPIA, og kommunens ledelse har ikke fått presentert resultatene av DPIAene. Alle gjennomførte DPIAer er gjort i helse og omsorg. Kommunen bør sikre at systemer i andre kommunalområder, hvor DPIA er aktuelt, blir fanget opp.

I forbindelse med rådmannens ledergruppes årlige gjennomgang av informasjonssikkerheten skal det også gjøres en risikovurdering. I den grad dette er gjennomført, er risikovurderingen hovedsakelig fokusert inn mot organisasjonsforhold. Vi vil understeke at kommunen er pålagt å gjøre både organisatoriske og tekniske tiltak, basert på bla. risiko (jf. personopplysningslovens art. 24, nr. 1), og risikovurderingen bør derfor omfatte både organisatoriske og tekniske risikoer.

[27] Dette samsvarer med Datatilsynets veiledning, se Datatilsynet, «Vurdering av personvernkonsekvenser (DPIA)».

Vi ser at det er sammenheng mellom risikovurderingene og presentasjonene til ledergruppa og at det har blitt fulgt opp med tiltak (primært endinger i hvordan IKT-anskaffelser gjøres). Vi ser imidlertid lite dokumentasjon på at rådmannens ledergruppe har tatt konkret stilling til om risikoer skal aksepteres eller om det skal gjøres gjøre tiltak. Et mulig unntak er igjen risikoen ved IKT-anskaffelser.

Virksomhetsledere og ledere med personalansvar har også et ansvar for å gjennomføre risikovurderinger innenfor sitt ansvarsområde. Det er begrenset omtale av dette i strategien, og på virksomhetsnivå vil mange løsninger være felles med andre deler av kommunen. Kommunen bør tydeliggjøre ansvaret for og innholdet i risikovurderinger på dette nivået, også for å forebygge pulverisering av ansvaret.

For de fleste systemene vi har undersøkt, er det ikke tatt stilling til behovet for risikovurdering, og det er heller ikke gjennomført risikovurdering. Helse og omsorg synes imidlertid å ha fulgt opp dette i større grad. Dette mønsteret ser vi også i casestudien vår. Administrasjonen har ikke noe samlet oversikt over eller kunnskap om gjennomførte risikovurderinger for IKT-system. Den sprikende praksisen og manglende gjennomføring av risikovurderinger tyder på at oppgaven ikke er tilstrekkelig fulgt opp. Administrasjonen bør etter vår vurdering treffe tiltak for å sikre at risikovurderinger av IKT-systemene blir gjennomført i hele kommunen.

**DPIA**

Strategi for informasjonssikkerhet angir hvem som har ansvar for å gjennomføre risikovurderinger av informasjonssikkerhet, men omtaler ikke DPIAer spesielt. Vi mener at plassering av ansvaret for å gjennomføre DPIA med fordel kan tydeliggjøres.

Kommunen har gjennomført flere DPIAer, og alle disse er gjennomført for systemer i helse og omsorg. Kommunen bør sikre at også systemer i andre deler av kommunen som er aktuelle for DPIA blir fanget opp.

I de gjennomførte DPIAene er malen i varierende grad utfylt. Derfor er det vanskelig å vurdere om prosessen er fullstendig gjennomført. Dette gjelder særlig involvering av de registrerte og av kommunens ledelse.

Det er positivt at kommunen samarbeider med andre i arbeidet med DPIAer - det er ikke nødvendig å «finne opp hjulet» på nytt hver gang. Men kommunen må også gjøre sine egne vurderinger av det felles grunnlaget for å sikre at det tas høyde for lokale forhold. For DPIAene som er utført i felleskap eller basert på andre grunnlag er det vanskelig for oss å se om og hvor kommunen har gjort egne vurderinger.

## 3.5. Avvikshåndtering

**Porsgrunn kommune skal ha tiltak for å håndtere brudd på personopplysnings-sikkerheten.**

### 3.5.1. Kommunens rutiner for å håndtere avvik

Kommunen har en generell rutine for registering og behandling av uønskede hendelser, avvik og forbedringsforslag. Alle hendelser skal registreres i kvalitetssystemet TQM.

Avvik skal behandles og lukkes av nærmeste leder. Når nærmeste leder mottar avviket, er hen ansvarlig for å kategorisere hendelsen, velge tiltakstype og hvem som skal være saksbehandler for utformingen av tiltaket. Deretter skal avviket lukkes og godkjennes når tiltaket er gjennomført.

I strategi for informasjonssikkerhet står det at alle ansatte har ansvar for å rapportere sikkerhetshendelser og sikkerhetssvakheter eller trusler. Dette skal rapporteres til nærmeste leder eller til personvernombudet**.** I TQM er det en egen kategori for «Personvern (GDPR) og taushetsplikt».

Det fremgår også av strategi for informasjonssikkerhet at rådmannens ledergruppe skal gjennomgå og følge opp kritiske sikkerhetshendelser. Som nevnt over, har vi fått opplyst at det er personvernombudet som ivaretar dette. Dette er løst med at personvernombudet får automatiske varslinger om personvernavvik. Personvernombudet opplyste imidlertid at det i forbindelse med forvaltningsrevisjonen ble oppdaget at den automatiske varslingen var slått av, og derfor hadde ikke personvernombudet fått varsel om alle personvernavvik. Automatiske varslinger er nå slått på igjen.

### 3.5.2. Statistikk på avvik om personvern/informasjonssikkerhet

Kommunen har sendt oss kopi av avvikene som er registrert i kategorien «personvern (GPDR) og taushetsplikt» i perioden 2019 - 2021. Noen av tilfellene er regirestert som uønskede hendelser og et er registret som forbedringsforslag. Disse er inkludert oversikten under.[28] Vi har oppsummert avvikene per kommunalområde i tabell 5.

*Tabell 5 Avvik på personvern/GDPR og taushetsplikt per kommunalområde*

| Kommunalområde | 2019 | 2020 | 2021 |
|---|---|---|---|
| **Administrasjon og støtte** | 0 | 3 | 0 |
| **Oppvekst** | 0 | 0 | 4 |
| **Helse og omsorg** | 6 | 11 | 7 |

[28] Kommunen definerer uønsket hendelse som «Hendelser som oppstår til tross for at alle forskrifter og prosedyrer er fulgt.» Forbedringsforslag defineres som «Ofte knyttet til kvalitetsforbedrende forslag til tiltak for virksomheten.» Det forbedringsforslaget gjelder utskrift på feil printer. Et tilsvarende tilfelle ble registrert som avvik. Vi har derfor inkludert forbedringsforslaget i statistikken.

| Kommunalområde | 2019 | 2020 | 2021 |
|---|---|---|---|
| Miljø og byutvikling | 0 | 0 | 1 |
| Sum | 6 | 14 | 12 |

Som tabellen viser, har det vært en viss økning i antall rapporterte avvik i perioden 2019-2021. Tabellen viser at helse og omsorg er det tjenesteområdet med høyest antall avvik. Generelt er det ikke uvanlig at helse og omsorg rapporterer flest avvik. Innholdet i avvikene fra helse og omsorg knytter seg ofte til forlagte dokumenter med personopplysninger, og det synes å være etablert praksis at slike avvik tas det opp med den det gjelder eller på avdelingsmøter e.l. Det er også avvik knyttet til bruk av IKT-systemer, typisk at utskrifter har kommet på feil sted. Dette er da fulgt opp med IKT-avdelingen. Avvik fra de øvrige avdelingene gjelder også i stor grad dokumenter som er enten feilsendt eller digitalt tilgjengelig for uvedkommende. Som oftest synes avviket å knytte seg til menneskelige feil, men i noen tilfeller er det også tekniske feil. I sakene med menneskelig feil er det beskrevne tiltaket som oftest å gjennomgå egne rutiner eller å ta opp saken med den det gjelder.

### 3.5.3. Rapportering av avvik til Datatilsynet

Vi har ikke mottatt noen rutiner for varsling av avvik til Datatilsynet. Personvernombudet har imidlertid opplyst at han vurderer avvik sammen med kommunalsjefen. Her inngår en vurdering av om avviket skal sendes til Datatilsynet. Når det sendes avvik til Datatilsynet, blir alltid kvitteringen fra Datatilsynet lagt på postlista. Dette mener personvernombudet bidrar til åpenhet rundt disse varslingene. Personvernombudet forteller også at når det varsles sak til Datatilsynet, skal også de behandlede som er berørt av avviket få varsel om dette.

Vi har fått opplyst at det ikke føres noe statistikk på avviksmeldinger til Datatilsynet. I de avvikene vi har mottatt fra perioden 2019-2021 er det sendt to meldinger til Datatilsynet, en gang i 2020 og en gang i 2021.

Avviket i 2020 knytter seg til at innstillinger i ansettelsessaker fra kommunens rekrutteringsprogram hadde blitt publisert i fulltekst på kommunens hjemmeside. Dokumentene var unntatt offentlighet, men inneholdt ikke personnummer eller personsensitive data. Som følge av dette er metadataene på stillingsinnstillingene endret, slik at de ikke skulle komme ut på postlisten i fremtiden. Saken ble meldt til Datatilsynet, og er lukket fra Datatilsynets side. De berørte registrerte ble varslet om saken.

Avviket fra 2021 skjedde hos en ekstern tjenesteleverandør, hvor dokumenter ble sendt til feil kunde. Den eksterne tjenesteleverandøren varslet da kommunen. Tjenesteleverandøren opplyste at dette var en menneskelig feil og vil gjennomgå sine rutiner. Kommunen meldte saken til Datatilsynet.

### 3.5.4. Observasjoner fra casestudier

I casestudiene stilte vi spørsmål om avvik og avvikshåndtering, og ba om eksempler på hva som utgjorde et avvik.

Et tenkt eksempel på et avvik fra sykehjemmet er at journalnotat blir skrevet på feil pasient. Avdelingslederen som deltok på intervjuet, ga også et eksempel fra virkeligheten. Dette gjaldt et kartleggingsnotat hvor informasjonen kunne settes sammen slik at andre pasienter ble identifisert. Dette ble håndtert ved at dokumentet ble bearbeidet slik at andre pasienter ble anonymisert. Det ble også skrevet et avvik på saken.

Intervjudeltakeren fra skole ga som eksempel på avvik at personopplysninger blir sendt på e-post, og at man gir ut opplysninger til foreldre om andres barn. Intervjudeltakeren har ikke mottatt avvik med brudd på informasjonssikkerheten. Hvis han skulle motta avvik, må dette håndteres med den aktuelle ansatte, og skoleeier skal også varsles ved grove brudd. Videre viser han til at lærerne kan legge inn avvik i TQM, og at han vil være ansvarlig for å behandle dem.

De ansvarlige for Teams ga som eksempler på avvik at noen får tilgang til et team som de ikke skulle ha hatt tilgang til, eller at noen bruker Teams til personsensitiv informasjon. De har ikke mottatt avvik på Teams. Hvis det skulle ha oppstått avvik, ville de koble på personvernombudet. De mener at det er personvernombudet som skal vurdere om det er reelt brudd og hva som skal gjøres videre. Personvernombudet er også ansvarlig for eventuell videre rapportering til Datatilsynet.

De ansvarlige for SafeMate ga følgende eksempler på hva som kan utgjøre avvik: Vakttelefon på avveie og at SafeMate-appen var åpen. Det kan tenkes at en ansatt kan spore en pasient mer enn det som det er tjenstlig behov for, men de ansvarlige for SafeMate mener at det er vanskelig å se hvilken motivasjon en ansatt skal ha for å gjøre dette. Da er angrep utenfra mer relevant, eks. hacking. Den mest sannsynlige avvikssituasjonen er at ingen av de ansatte på jobb har tilgang til SafeMate. Et annet mulig avvik er at en ansatt fortsatt har tilgang til systemet etter at arbeidsforholdet er avsluttet. Slike avvik vil bli meldt i TQM, som andre avvik i tjenesten. I praksis vil man prøve å finne løsning, drøfte med leverandører og diskutere med personvernombud. Hvis det er aktuelt, vil man varsle Datatilsynet.

### 3.5.5. Revisors vurdering av avvik

Kommunen synes å ha et hensiktsmessig system for å registrere avvik. Det synes å være god kvalitet på informasjonen som blir registret om avviket og oppfølgningen. Vi ser positivt på at det er økende trend i perioden 2019-2021 på antall registrerte avvik. Vi merker oss allikevel at flertallet av de registrerte avvikene knytter seg til kommunalområde helse og omsorg. Kommunen bør vurdere om de i tilstrekkelig grad fanger opp avvik på informasjonssikkerhet og personvern i alle kommunalområder og vurdere relevante tiltak.

Ved en feil hadde varslene om relevante avvik til personvernombudet blitt skrudd av, selv om dette har blitt rettet, ble feilen oppdaget som et resultat av oppstarten av denne forvaltningsrevisjonen.

Vi vil i denne forbindelse minne på at tidsaspektet kan være viktig i saker som berører personvern informasjonssikkerhet både når det gjelder å gjøre korrigerende tiltak, men også å varsle Datatilsynet innen fristen hvor dette er relevant. Administrasjonen må derfor sikre at varsling av avvik fungerer slik de skal.

## 3.6. Retten til informasjon

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

### 3.6.1. Rutiner for informasjon

Ifølge kommunens strategi for informasjonssikkerhet skal alle som ber om det, få generell informasjon om kommunens behandling av personopplysninger. Kommunens internkontroll skal sikre at de registrertes rettigheter blir ivaretatt, og retten til informasjon er en slik rettighet. Utover dette er det ikke beskrevet hvem som har ansvar for å sikre at de behandlede får informasjon.

### 3.6.2. Personvernerklæring

Kommunen har en personvernerklæring på sine nettsider. Denne gir informasjon om blant annet hvem som er ansvarlig for behandlingen, på hvilket grunnlag kommunen behandler opplysninger, når kommunen kan utlevere opplysninger, hvilke rettigheter den behandlede har og hvordan man kan håndheve rettighetene. Til slutt er det informasjon om personvernombudet og hvordan man kan kontakte ham.

### 3.6.3. Observasjoner fra casestudie – informasjon

Intervjudeltakerne fra sykehjemmet fortalte at de ikke informerer pasienter om hvordan de behandler personopplysninger, men sier at det finnes noe informasjon på kommunes hjemmesider.

Intervjudeltakeren fra skole fortalte at skolen informerer foresatte om hvordan skolen bruker saksbehandlingssystemet og det skoleadministrative systemet. Dette blir det informert om på foreldremøter. Skolen har også sendt ut skriv til foresatte om temaet. I praksis viser det seg at ikke alle foreldre fanger opp denne informasjonen. Det har for eksempel kommet spørsmål om hvor lenge skolen oppbevarer informasjon om elever, eks. 9A-saker.[29] Intervjudeltakeren mener at elever ikke er godt informert, og kjenner nok ikke til at personopplysninger om dem blir oppbevart i kommunens IKT-systemer. Unntaket er noen få elever der det er sensitive opplysninger. De kan etter samtaler med rektor være kjent med at personopplysninger om dem blir oppbevart.

De ansvarlige for SafeMate forteller at det er enten systemadministrator eller demenssykepleier som informerer om systemet. De snakker både med pasienten og pårørende, og gir informasjon om hvordan systemet virker. Da dette er et tilbud til personer med reduserte kognitive evner, er det nok ikke alltid at vedkommende husker det etter en viss tid. Det er deres opplevelse at de fleste forstår at det er et hjelpemiddel ment for å gi trygghet. Siden GPS-sporeren er et fysisk objekt som man tar på seg hver dag (da den lades om natta) er tiltaket synlig for pasienten. Av denne grunnen har man valgt å ikke bruke løsninger som er skjulte for pasienten, eks. sporingsenheter som sitter i skosålen.

[29] 9A-saker er saker i skolen hvor skolen har fått beskjed om at en elev ikke har et trygt og godt skolemiljø. I slike saker plikter skolen å lage en plan med tiltak for å sikre at eleven har et trygt og godt skolemiljø.

De ansvarlige for Teams fortalte at det ikke gis informasjon om hvordan personopplysninger spesifikt behandles i Teams. De arbeider imidlertid med å sikre at elevene skal oppleve integritet rundt egne data. De mener at det er viktig at elever blir bevist på hvordan de håndterer det de har produsert og at de er bevisste på hva som skjer når man lagrer eller deler et dokument, og at dette er viktig kompetanse for at elevene skal klare seg i den digitale skolehverdagen.

### 3.6.4. Revisors vurdering av retten til informasjon

Vi mener at kommunen i hovedsak har tiltak for å ivareta de registrertes rett til informasjon om kommunens behandling av deres personopplysninger. Personvernerklæringen på kommunens nettsider gir informasjon på en overordnet, kortfattet og lett forståelig måte. Vi vurderer dette som hensiktsmessig for informasjon på dette nivået, men vi vil allikevel påpeke at dette medfører at kommunen må gi mer detaljert informasjon når kommunen starter behandling av personopplysninger. Våre observasjoner fra casestudiene viser at det noe variasjon i hvor mye informasjon de behandlede får når behandlingen starter.

## 3.7. Retten til innsyn

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

### 3.7.1. Rutiner for innsyn

I strategi for informasjonssikkerhet er det et sikkerhetsmål at alle som ber om det skal få innsyn i de personopplysninger som er registret om seg selv, og at dette skal sikres i internkontrollen. Det fremgår også i strategien at rådgiver for informasjonssikkerhet skal koordinere håndtering av krav om innsyn, retting og sletting. Det er ikke beskrevet hvem som konkret skal håndtere forespørslene.

I kommunens personvernerklæring er det informasjon om de behandles rettigheter. Her er blir det informert om at man har rett til innsyn i hvilke opplysninger kommunen behandler om en, hvordan det gjøres og hvor data hentes fra. Hvis man ønsker å be om innsyn blir man bedt om å ta kontakt med kommunens servicesenter. Det oppgitt e-post og telefonnummer til servicesenteret. Det står også at hvis man har spørsmål om sine rettigheter kan man ta kontakt med kommunens personvernombud. Navn og e-post til personvernombudet står i personvernerklæringen.

### 3.7.2. Observasjoner fra casestudie - innsyn

De ansvarlige for Teams og for SafeMate forteller at det ikke hadde kommet forespørsler om innsyn i personopplysninger i deres system.

Intervjudeltakerne på sykehjemmet fortalte at de får innsynsforespørsler, og at det er en økende mengde. Det er hovedsakelig pasientjournal og tilsynssaker det bes om innsyn i. Når de mottar innsynsforespørsler, vurderer de pasientens samtykkekompetanse, og om pasienten i så fall er samtykker til at evt. pårørende kan få informasjon. For pasienter som ikke har samtykkekompetanse, er det hovedpårørende som skal henvende seg ved ønske om innsyn. De får da tilbud om å gå igjennom journalen med en ansatt. I noen tilfeller har den pårørende ikke ønsket slik gjennomgang, og da gir man ut journalen på papir.

Intervjudeltakeren på skolen forteller at skolen har mottatt innsynsforespørsler. De foresatte har rett til å se det meste, men ikke alt. De må også være beviste på at det er noen få tilfeller hvor foreldre ikke har innsynsrett.

### 3.7.3. Revisors vurdering – innsyn

Kommunen har tiltak for å sikre innsynsretten til de registrerte. På kommunens nettsider gis det god og konkret informasjon om retten til innsyn og hvordan man kan be om innsyn. Det er positivt at ivaretakelse av de behandledes rettigheter er beskrevet som et mål i kommunens strategi. Kommunes strategi sier ikke hvem som har ansvaret for å behandle forespørsler om innsyn, utover at rådgiver for informasjonssikkerhet har overordnet koordineringsansvar.

## 3.8. Databehandleravtaler

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

### 3.8.1. Rutiner for databehandleravtaler

For alle IKT-systemer som behandler personopplysninger på vegne av kommunen skal det inngås en databehandleravtale. I strategi for informasjonssikkerhet fremgår det at det er rådmannens ansvar å sørge for at det inngås databehandleravtaler med kommunens databehandlere. I strategi for informasjonssikkerhet fremgår det at kommunen fortrinnsvis benytte skal sin egen mal for databehandleravtale.

Personvernombudet forteller at han får databehandleravtaler til gjennomlesning før de blir signert av kommunen. Han forteller videre at avtalene har blitt ganske like, og at han derfor fokuserer mest på hvor dataene blir lagret (innenfor/utenfor EU/EØS).

Det fremgår nå av kommunens delegasjonsreglement, at rådmannen skal godkjenne inngåelsen av alle databehandleravtaler og signere dem. Vi har fått opplyst at det er kun rådmannen eller hennes stedfortreder som kan signere. Kommunalsjefene har ikke myndighet til dette. Etter signering blir avtalene arkivert.

Systemansvarlige har ansvar for å følge opp leverandører og databehandlere (disse to sammenfaller ofte), mens systemansvarlig er hovedkontakt for leverandøren.

Strategi for informasjonssikkerhet fastsetter at rådgiver for informasjonssikkerhet skal ha oversikt over kommunens databehandlere og databehandleravtaler. Det blir ført oversikt over databehandlere og databehandleravtaler i kommunens protokoll.

De ansvarlige for Teams opplyser at de har inngått databehandleravtale med Microsoft, som også omfatter Teams. De fortalte at i møte med de store internasjonale aktørene har ikke kommunen annet valg enn å bruke selskapenes standardavtaler. Dette gjelder også for Teams og Microsoft. De fortalte at avtalen ble gjennomgått med personvernombudet før den ble signert.

Vi har fått vite fra det tidligere personvernombudet at programmer i protokollen ble gjennomgått etter at Schems II dommen kom i 2020. Det ble da sjekket for utlevering til tredjeland (det vil si land utenfor EØS/EU). Eventuell utlevering til tredjeland krever at personopplysningene er like trygge som der som i EØS/EU, og at det gjøres eventuelle tiltak for å sikre dette. Dette reguleres eventuelt i databehandleravtalen mellom kommunen og databehandleren.

### 3.8.2. Stikkprøve av registering av databehandleravtale i protokollen

Vi har gjort en stikkprøve for å undersøke om administrasjonen har registrert opplysninger om databehandler og databehandleravtale i kommunens protokoll over behandlingsaktiviteter. Det er ikke lovpålagt å ha denne informasjonen i protokollen, men det er anbefalt i Datatilsynets mal for

protokoll. Utvalget er det samme som for stikkprøvene av opplysninger i protokollen, se avsnitt 3.3.2. Vi har oppsummert funnene våre i tabell 6.

*Tabell 6 Registering i protokollen av databehandler og databehandleravtale for et utvalg selskaper*

| System | Databehandler (avtalepart) | Databehandleravtale og dato for signering |
|---|---|---|
| **Lekdommer** | Ja | Ja, 25.09.18 |
| **Trio** | Ja | Ja, 21.08.18 |
| **ISY Eiendom** | Ja | Ja, 24.09.18 |
| **Easypark** | Ja | Ja, 21.06.18 |
| **When I work** | Nei | Nei |
| **Gerica LMP** | Ja | Ja, 04.09.18. |
| **ReMin** | Ja | Ja, 18.09.20, oppdatert 10.09.21 |
| **Telenor Min Bedrift** | Nei | Nei |

Som tabellen viser, mangler to av de åtte IKT-systemene informasjon om databehandler og databehandleravtale. Det er uklart for oss om dette er fordi det ikke er databehandler, fordi avtale mangler eller om det er fordi informasjon om databehandler og avtale ikke er lagt inn. Der det foreligger databehandleravtaler er disse datert.

### 3.8.3. Revisors vurdering av databehandleravtaler

Kommunen har gjennom delegeringsreglement og strategi for informasjonssikkerhet retningslinjer for hvem som har ansvar for og myndighet til å inngå databehandleravtaler, og ansvar for den videre oppfølgningen av avtalene. Kommunen synes å ha en ryddig oversikt over inngåtte databehandleravtaler i protokollen, men kommunen må sikre at det er databehandleravtaler for alle IKT-systemer hvor dette er relevant. Terskel for at det skal være databehandleravtale er lav. eks. selv om all data blir lagret lokalt skal man fortsatt ha databehandleravtale hvis leverandøren får tilgang til systemet og personopplysninger ved support eller vedlikehold. Vi mener det er positivt at administrasjonen har registrert dato for når avtalene er inngått i protokollen. Vi merker oss at i stikkprøven var alle databehandleravtalene fra 2018, med et unntak som vi er kjent med er en nyere anskaffelse. Kommunen bør være bevisst på at endret bruk av IKT-systemene kan medføre behov for å revidere databehandleravtalene.

# 4. Konklusjoner og anbefalinger

## 4.1. Konklusjoner

Porsgrunn kommunes strategi for informasjonssikkerhet har en oversiktlig struktur over rolle- og ansvarsfordeling innenfor informasjonssikkerhet og personvern, men innholdet i strategien er til dels utydelig. Det er omtrent fire år siden strategien ble revidert, og vi mener at tiden er moden for en revidering.

Strategien for informasjonssikkerhet beskriver rapportering kun i begrenset grad. I praksis blir det kun rapportert til rådmannens ledergruppe om informasjonssikkerhet i den årlige gjennomgangen. Gjennomgangen ikke blitt gjennomført i 2019 eller 2021.

Vi vurderer at kommunens organisering av personvernombudet i skrivende stund ikke er i samsvar med personopplysningsloven. Denne organiseringen av personvernombudet vurderer vi at ikke sikrer tilstrekkelig tid og ressurser til oppgaven. Vi vurderer videre at personvernombudet ikke har den uavhengighet som er påkrevd i lovverket. Kommunen har oppnevnt et nytt personvernombud fra 1. mars 2022, da dette er etter at vi har avsluttet våre undersøkelser har vi ikke hatt kontakt med eller gjort vurderinger av vedkommende.

Kommunens protokoll over behandlingsaktiviteter er i hovedsak godt utfylt. Våre undersøkelser viser likevel at det opplysninger som skal fremgå i protokollen manglet i noen tilfeller. Det fremgår ikke noen datering av opplysninger eller endringer i protokollen. Dette mener vi kan medføre risiko for at protokollen ikke er oppdatert.

Av strategien for informasjonssikkerhet går det frem at kommunen skal gjennomføre risikovurderinger, men de fleste IKT-systemene vi har sett på hadde verken vurdert behovet for risikovurdering eller gjennomført risikovurdering. Kommunalområdet Helse og omsorg har gjennomført både risikovurderinger og vurdering av personvernkonsekvenser (DPIA) i samarbeid med andre kommuner, noe vi vurderer som positivt. Kommunen bør likevel tilpasse disse vurderingene til lokale forhold.

Kommunen synes å ha et hensiktsmessig system for å håndtere brudd på personopplysningsloven (avvik). Våre undersøkelser viser at flertallet av de registrerte avvikene knytter seg til helse og omsorg. Kommunen bør vurdere om den i tilstrekkelig grad sikrer at avvik innenfor informasjonssikkerhet og personvern fanges opp i hele organisasjonen.

Vi mener at kommunen i hovedsak har tiltak for å ivareta de registrertes rett til informasjon om kommunens behandling av deres personopplysninger. Det at kommunens personvernerklæring er relativt kortfattet medfører behov for at utfyllende informasjon må gis når kommunen faktisk behandler personopplysninger. Vi vurderer at kommunen har tiltak for å ivareta innsynsretten til de registrerte.

Av strategi for informasjonssikkerhet går det frem at det skal inngås databehandleravtale med alle databehandlere. Kommunen har en ryddig oversikt over inngåtte databehandleravtaler, men våre undersøkelser viser at det manglet informasjon om databehandler og databehandler i enkelte av systemene vi så på.

## 4.2. Anbefalinger

Vi anbefaler kommunen å:

- vurdere en evaluering og revisjon av strategi for informasjonssikkerhet
- sikre at ledelsens gjennomgang av informasjonssikkerhet blir gjennomført i samsvar med retningslinjer i strategi for informasjonssikkerhet
- organisere personvernombudsordningen i samsvar med kravene i personopplysingsloven art. 37-39
- sørge for at protokollen oppfyller lovkravene for alle registrerte IKT-systemer og vurdere tiltak for å sikre at informasjonen i protokollen er oppdatert
- sikre at alle IKT-systemer som behandler personopplysninger har et gyldig behandlingsgrunnlag
- sikre at ansvaret for å gjennomføre risikovurderinger er tydelig og sørge for at risikovurderinger blir gjennomført
- sørge for at kommunen har databehandleravtale med alle som behandler personopplysninger på vegne av kommunen

# Litteratur og kildereferanser

## Lover og forskrifter

Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysingsloven/GDPR)

Lov 22. juni 2018 nr. 83 om kommuner og fylkeskommuner (kommuneloven).

Forskrift 17. juni 2019 nr. 904 om kontrollutvalg og revisjon

## Offentlige dokument

Prop.56 LS (2017–2018) Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen)

## Kommunens dokumenter

Dokument Informasjonssikkerhet og personvern; overordnet styringsdokument (vedtatt kommunestyret den 18.09.18)

## Elektroniske kilder

Datatilsynet: https://www.datatilsynet.no/, nettside herunder følgende veiledere:

- «Behandlingsansvarlig og databehandler», sist endret 17.07.19, hentet 23.06.21, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/databehandleravtale/behandlingsansvarlig-og-databehandler
- «Behandlingsgrunnlag», sist endret 30.05.18, hentet 23.06.21, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsgrunnlag/veileder-om-behandlingsgrunnlag/
- «Etablere internkontroll», sist endret 30.10.18, hentet 23.06.21, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/
- «Grunnleggende personvernprinsippener», sist endret 16.07.19, hentet 23.06.21, https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/
- «Hvordan lage en databehandleravtale?», sist endret 20.12.19, hentet 23.06.21, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/databehandleravtale/hvordan-lage-en-databehandleravtale/
- «Informasjon og åpenhet», sist endret 08.06.18, hentet 23.06.21, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/gi-informasjon/informasjon-og-apenhet/

- «Mal for behandlingsansvarliges protokoll», datert april 2018, https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/forordningen/artikkel-30_protokoll-behandlingsansvarlig.xlsx
- «Melde avvik til Datatilsynet», sist endret 07.08.18, hentet 24.08.21, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvikshandtering/melde-avvik-til-datatilsynet/
- «Når og hvordan melde avvik?», sist endret 07.08.18, hentet 25.06.21, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvikshandtering/nar-skal-jeg-melde-avvik/
- «Protokoll over behandlingsaktiviteter», sist endret 19.06.18, hentet 02.07.21, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/protokoll-over-behandlingsaktiviteter/
- «Risikovurdering», sist endret 16.07.19, hentet 25.06.21, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/risikovurdering/
- «Sjekkliste for vurdering av personvernkonsekvenser (DPIA)», https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/veiledere/dpia-veileder/sjekkliste-for-dpiafaser.pdf
- «Vurdering av personvernkonsekvenser (DPIA)», sist endret 17.07.19, hentet 23.06.21, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/

DFØ, Miniveileder om oppfølgning av informasjonssikkerhet i styringsdialogen, sist endret 10.02.20, hentet 23.11.21, https://dfo.no/fagomrader/etats-og-virksomhetsstyring/etatsstyring/miniveileder-om-oppfolging-av-informasjonssikkerhet-i-styringsdialogen/om-veilederen

DigDir, *Hva er Schrems II-dommen,* udatert, hentet 20.01.21, https://www.digdir.no/handlingsplanen/hva-er-schrems-ii-dommen/2581

Porsgrunn kommune, *Personvernerklæring,* sist revidert 28.01.20, hentet 29.11.21.


## Bøker


ISO/ICE 2701:2013 Informasjonsteknologi – sikringsteknikker – styringssystemer for informasjonssikkerhet

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


## Artikler


Næss, Kristine og Steinar Østmoe, «Hvordan skape et supert personvernombud?», *Lov & Data*, 2/2021, s. 9

# Vedlegg

## Vedlegg 1: Rådmanenns uttalelse

Vi mottok følgende høringssvar fra rådmannen den 02.03.22 per e-post:

Hei igjen,

Vi har følgende kommentarer til den foreløpige rapporten:

Konklusjonen i rapporten er svært samsvarende med det som har kommet frem i et parallelt løp igangsatt av IT-avdelingen hos oss, der det er gjennomført en samsvarsanalyse. Vi er derfor ikke overrasket over det som kommer frem i rapporten.

For øvrig vil jeg legge til at vi har fått et personvernombud på plass. Formalitetene i forholdet til Datatilsynet er nå på plass. Informasjon om dette er tidligere sendt deg.

Utover dette har vi ingen ytterligere kommentarer.

**Med vennlig hilsen**
**Rose-Marie Christiansen**
Rådmann
Porsgrunn kommune
Tlf: 901 08 693
rose.marie.christiansen@porsgrunn.kommune.no
Besøksadresse: Rådhuset, 1. etg.

# Vedlegg 2: Revisjonskriterier

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

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

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

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

- konfidensialitet
- integritet (riktighet)
- tilgjengelighet

## Behandlingsansvarlig

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

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

Vi undersøker ikke situasjoner der Porsgrunn kommune eventuelt er databehandler på vegne av andre oppdragsgivere.

## Personvernombud

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

## Personvernprinsippene

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

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

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

### Lovlig, rettferdig og gjennomsiktig

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

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

At behandlingen skal være «rettferdig», innebærer at kommunen skal ha respekt for den registrertes interesser og rimelige forventinger.[30]

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

**Formålsbegrensning**
Personopplysninger skal bare brukes til det formålet de er innhentet for, personopplysningsloven art. 6, nr. 1. Hvis personopplysninger skal gjenbrukes, må behandlingen enten være lovfestet eller det må innhentes nytt samtykke, jf. personopplysningsloven art. 5, nr. 1, bokstav b.

**Dataminimering**
Prinsippet om dataminimering innebærer å begrense mengden innsamlede personopplysninger til det som er nødvendig for å realisere innsamlingsformålet, jf. personopplysningsloven art. 5, nr. 1, bokstav c.

**Riktighet**
Personopplysninger som behandles skal være korrekte. Opplysningene skal også oppdateres hvis det er nødvendig, jf. personopplysningsloven art. 5, nr. 1 bokstav d.

**Lagringsbegrensning**
Prinsippet om lagringsbegrensning innebærer at personopplysninger skal lagres slik at de slettes eller anonymiseres når de ikke lengre er nødvendige for formålet de ble innhentet for. Kommunen bør innføre tidsfrister for sletting eller periodisk gjennomgang for å sikre at personopplysninger ikke oppbevares lengre enn nødvendig, jf. personopplysningsloven art. 5, nr. 1, bokstav e.

**Integritet og fortrolighet**
Kommunen skal sørge for personopplysningenes integritet og fortrolighet, jf. personopplysningsloven art. 5, nr. 1 bokstav f, dette kan inkludere:

- beskyttelse mot uautorisert utlevering og tilgang til personopplysninger
- beskyttelse mot utilsiktet og ulovlig ødeleggelse, tap og endringer av personopplysninger
- at personopplysninger er tilgjengelige for autoriserte personer når det er nødvendig

[30] Datatilsynet, «Grunnleggende personvernprinsipper», sist endret 16.07.19, hentet 23.06.21.

- at personopplysninger ikke gjøres tilgjengelig for et ubegrenset antall mennesker uten den berørte personens medvirkning
- å spore endringer som gjøres i systemet og for å kunne håndtere sikkerhetsbrudd
- at systemene som behandler personopplysninger er robuste mot for eksempel sårbarheter, angrep og uhell

**Ansvarlighet**
Kommunen har ansvar for å opptre i samsvar med reglene for behandling av personopplysninger. Kommunen må også kunne vise at den faktisk opptrer i samsvar med reglene, jf. personopplysningsloven art. 5, nr. 2. Dette betyr at kommunen må ha internkontroll.[31]

## Internkontroll

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

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

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

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

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

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

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

[31] Datatilsynet, «Grunnleggende personvernprinsipper»

Art. 35 krever at ved behandlinger som vil medføre høy risiko for fysiske personers rettigheter og friheter, skal kommunen gjennomføre en vurdering av personvernkonsekvenser, også kalt DPIA[32]. DPIA er nødvendig i kommuner, siden de behandler sensitive opplysninger i stor skala. Vurderingen skal minst inneholde

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

Personopplysningsloven art. 5.1 bokstav e krever at kommunen har rutiner som sikrer tilstrekkelig sikkerhet for integriteten og konfidensialiteten til personopplysningene. Kommunen skal sikre personopplysningene mot uautorisert eller ulovlig behandling, og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak. Ifølge artikkel 24 skal kommunen gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med personopplysningsloven. Ifølge artikkel 32 skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som passer til risikoen.

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

Internkontroll og arbeidet med informasjonssikkerhet er et dynamisk arbeid som alltid vil være under utvikling. Datatilsynet anbefaler derfor å ha rutiner for å forbedre internkontrollen, herunder rutiner for rapportering fra sikkerhetshendelser, avvikshåndtering og egenkontroll. Rapporteringen skal beskrive hvilke erfaringer som er gjort og inneholde forslag til forbedringer.

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

## Registrertes rettigheter

[32] DPIA står for Data Protection Impact Assessment.
[33] «Etablere internkontroll», sist endret 30.10.18, hentet 23.06.21

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

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

### Databehandlere

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

Forholdet mellom en behandlingsansvarlig virksomhet og databehandleren skal være regulert i en databehandleravtale, jamfør personopplysningsloven artikkel 28 nr. 3. Avtalen skal sikre at personopplysningene blir behandlet i samsvar med regelverket, også av databehandleren, og skal sette en klar ramme for hvordan databehandleren kan behandle personopplysningene. En databehandleravtale kan være en frittstående avtale mellom partene, eller en integrert del av annet avtaleverk.

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

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

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

En databehandleravtale skal inneholde:

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

## Revisjonskriterier

På denne bakgrunn har vi utledet følgende revisjonskriterier:

**Porsgrunn kommune skal ha:**

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

# Vedlegg 3: Metode og kvalitetssikring

Forvaltningsrevisjonen startet opp ved oppstartsbrev 21.09.21. Oppstartsmøte ble holdt 20.10.21 med rådmann, rådmannens ledergruppe, personvernombud, tidligere personvernombud og IKT-leder til stede.

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

Vi vil nedenfor redegjøre for datagrunnlaget vårt og hvilke metoder vi har brukt for å svare på problemstillingene. Vi vil også beskrive hvilke tiltak som er brukt for å sikre dataenes relevans og pålitelighet.

## Innsamling av data, relevans og pålitelighet

Datainnsamling og rapportskriving har foregått i perioden oktober 2021 til februar 2022.

For å få oversikt over administrasjonens rutiner og planer for arbeidet med informasjonssikkerhet og personvern har vi gjort en dokumentgjennomgang. Slik har vi kartlagt administrasjonens rutiner og systemer. Vi har sett på dokumenter for å vurdere administrasjonens etterlevelse. Dokumenter kan imidlertid gi et begrenset grunnlag til å vurdere hvordan administrasjonen arbeider i praksis. Vi har derfor også intervjuet personvernombudet og vi har sendt skriftlige spørsmål til blant annet vår kontaktperson i administrasjon.

For å ytterligere kartlegge hvordan informasjonssikkerhetsarbeidet blir gjort valgte vi ut fire casestudier; to virksomheter og to IKT-systemer. I bestillingen fra kontrollutvalget var det bestemt at disse skulle velges fra kommunalområdene helse og omsorg og skole og oppvekst. Vi har gjort en vurdering av hvor det er risiko knyttet til behandlingen av personopplysninger da vi bestemte oss for hvilke typer virksomheter og IKT-systemer vi skulle ta med i casestudien. De to virksomhetene, en skole og et sykehjem, ble tilfeldig valgt ut blant kommunens skoler og virksomheter. De to IKT-systemene, SafeMate GPS-sporing og Teams, ble valgt ut etter en konkret vurdering av oss. Vi gjennomførte intervju med alle fire casestudiene samt at vi fikk oversendt dokumentasjon for de to IKT-systemene. Fra alle intervju ble det skrevet referat som ble godkjent av de som deltok i intervjuet. Intervjuer har en svakhet i at data fra disse vil til en viss grad være basert på subjektive erfaringer og hva intervjudeltakerne husker i intervjuet, men vi mener at dette avhjelpes ved kildene nevnt ovenfor.

For å ytterligere kartlegge praksis i kommunen gjennomførte vi en stikkprøvekontroll med utvalg IKT-systemer fra kommunens protokoll. IKT-programmene ble valgt ut tilfeldig. I utgangspunktet valgte vi ut 10 IKT-programmer. Vi fikk tilbakemelding om at to av disse ikke lengre var i bruk, et tredje system var aldri tatt i bruk. For et av disse tre fikk vi tilbakemeldingen raskt, og vi valgte derfor ut et nytt IKT-program. De to andre fikk vi tilbakemeldingen rett før fristen, slik at vi ikke

hadde tid til å velge et nytt IKT-program. Derfor ble det totalt 8 IKT-programmer i utvalget. Dette utvalget ble brukt til å vurdere utfylling av protokoll, risikovurderinger og databehandleravtaler.

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

## Personopplysninger

I forbindelse med denne forvaltningsrevisjonen har vi behandlet personopplysninger som navn, stilling og epostadresse til ansatte i kommunen (evt. foretaket). I intervjuene har vi fått personopplysninger i form av intervjudeltakernes personlige vurderinger.

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

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

## God kommunal revisjonsskikk - kvalitetssikring

Forvaltningsrevisjon skal gjennomføres, dokumenteres, kvalitetssikres og rapporteres i samsvar med kommuneloven og god kommunal revisjonsskikk.[34]

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

Vestfold og Telemark revisjon IKS har et system for kvalitetskontroll som er i samsvar med den internasjonale standarden for kvalitetskontroll.[35] Denne forvaltningsrevisjonen er kvalitetssikret i samsvar med vårt kvalitetskontrollsystem og i samsvar med kravene i RSK 001.

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

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

# På vakt for fellesskapets verdier

**Rapporten er utarbeidet av**
**Vestfold og Telemark revisjon IKS**

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

**www.vtrevisjon.no**