



PERSONVERNOMBUDET I FOLLDAL-ALVDAL-RENDALEN-TOLGA-TYNSET

**Personvernombudet (PVO)
i kommunene
Folldal-Alvdal-Rendalen-Tolga-Tynset**

**Årsmelding
2022**



Innholdsfortegnelse

1. Om personvernombudet og rapporteringen	3
2. Generelt om behandling av personopplysninger og ansvar	3
3. Generelle momenter og tiltak.....	3
Sikkerhetsforståelse blant de ansatte.....	3
Tilgjengelighet til systemer uten å på være på arbeidsplassen	4
Økt bruk av skytjenester	4
Noen generelle tiltak.....	4
4. Avvik meldes til Datatilsynet (DT)	4
5. Fokusområder på personvernområdet som må videreføres i 2023	5
Personvernombudets tilgang til å melde avvik på vegne av kommunene.....	5
Behandlingsoversikt må holdes oppdatert	5
Informasjon og registrertes rettigheter- personvernerklæringer	5
Databehandleravtaler	6
Gjennomføring av risikovurderinger og personvernkonsekvensvurderinger (DPIA)	6
Melding om nye behandlinger	6
Avvikshåndtering.....	6
Opplæring av alle ansatte i IKT-sikkerhet og personvern	6
Avslutning.....	6



1. Om personvernombudet og rapporteringen

Personvernombudets hovedoppgave er å informere og gi råd om de forpliktelsene virksomheten har etter personvernlovgivningen til den behandlingsansvarlige (øverste leder, kommunedirektøren) eller databehandleren (drifter av datasystemet), samt til de ansatte som utfører behandlingen av personopplysninger. Personvernombudet (PVO) fungerer også som kontaktperson og rådgiver for spørsmål om behandling av personopplysninger og de rettigheter den enkelte registrerte har etter personopplysningsregelverket.

Personombudets rolle kan kort oppsummeres slik:

- Skal bidra til å utvikle en «ryggmargsrefleks for personvern» hos ledere og ansatte
- Kommer vi dit at **alle tenker: «her tror jeg det er noe personverngreier - best vi undersøker litt!»**, da har vi kommet langt!

Personvernombudet skal gi skriftlig rapport til kommunedirektørene i kommunene om arbeidet foregående kalenderår innen 1. mars hvert år. Det utarbeides en felles rapport til alle FARTT-kommunene. Rapporten legges også fram for styret i IKT Fjellregionen IKS til orientering.

Personvernombudet er medlem i IKT-sikkerhetsutvalget i FARTT og samarbeider tett med dette utvalget om problemstillinger omkring til personvern.

2. Generelt om behandling av personopplysninger og ansvar

God informasjonssikkerhet og søkelys på personvern blir stadig viktigere i dagens samfunn. Alle muligheter og fleksibilitet som elektronisk samhandling gir, skaper også utfordringer for både brukere, driftsteknikere og systemleverandører.

Personopplysningsloven inkludert personvernforordningen (GDPR) stiller detaljerte og omfattende krav til fokus på og sikring av informasjon generelt og personopplysninger spesielt.

Systemleverandører skal sørge for at datasystemene har innebygget personvern i sin oppbygging og ha standardinnstillinger som sikrer personvernet på en best mulig måte. Dette skal sørge for at informasjonssystemene oppfyller personvernprinsippene, og at de ivaretar de registrertes rettigheter.

I kommunen skal kommunedirektøren som den overordnede behandlingsansvarlige for personopplysninger i kommuneorganisasjonen sørge for at regelverket i forhold til personvern overholdes i alle ledd i sin organisasjon. Virksomheten skal ha full oversikt over sin behandling av personopplysninger og skal iverksette de nødvendige tekniske og organisatoriske tiltak som gjør at loven følges. Virksomhetene har ansvar for å dokumentere at de følger loven.

3. Generelle momenter og tiltak

Sikkerhetsforståelse blant de ansatte

Parallelt med at mulighetene for forenklet elektronisk samhandling og informasjonshåndtering øker blir også behovet for at de ansatte tar ansvar for egne handlinger stadig mer gjeldende.

Her kan det virke som at teknologien løper litt i forveien, og at ikke alle ansatte helt ser de store sikkerhetsrisikoer dette medfører. Dette kan gjelde ukritisk dokumentlagring, sending av personsensitive data og fødselsnummer i epost, publiseringer, håndtering av elektroniske enheter m.v.



PERSONVERNOMBUDET I FOLLDAL-ALVDAL-RENDALEN-TOLGA-TYNSET

En kommuneorganisasjon består av mange ulike faggrupper av medarbeidere og mange ulike arbeidsoppgaver skal løses. I de forskjellige sektorene og enhetene og blant de ansatte vil det være forskjellig hvilke holdninger og normer som er fremtredende i forhold til sikkerhet. Dette må ledelsen være bevisst på og ta hensyn til ved opplæring og oppfølging av den enkelte ansatte og grupper av ansatte i IKT-sikkerhet og personvern. Mer om dette kan lese på [Digdir.no](https://digdir.no). Her finnes også en [interessant \(og morsom\) plakat som beskriver de forskjellige personlighetstypene](#) man kan finne i kommuneorganisasjonen og deres holdninger i forhold til IKT-sikkerhet m.v..

Tilgjengelighet til systemer uten å på være på arbeidsplassen

Mange av de ansatte har tjenstlig behov for at systemtilgang skal bli mer tilgjengelig, da med tanke på tilgang fra egne enheter og bruk av systemene når de ikke er på arbeidsplassen. Utvalgte ansatte (ledere og nøkkelpersonell) med spesielle behov for tilgang til systemer kan gis tilgang til intern sone og sikker sone på kommunalt eid bærbar PC utenfor arbeidsstedet (hjemme, på reiser mv). Dette forutsetter bruk godkjente løsninger for sterk autentisering for å høyne sikkerheten.

Økt bruk av skytjenester

Det er en gjennomgående trend at flere og flere IKT-systemer som også vi i kommunene bruker blir skybasert. Da vil ikke dataoverføring, dataprosessering og datalagring skje i IKT Fjellregionens serverpark, men fra eksterne serverparker tilknyttet internett et annet sted i Norge eller i Europa. Noen store aktører behandler data også i andre land, som USA. Dette medfører spesielle utfordringer personvernmessig da de har et annet lovverk på området enn EU/EØS.

Noen generelle tiltak

Ved bruk av skytjenester må det sørges for gode databehandleravtaler med skytjenesteleverandørene som sikrer at all data og personopplysninger behandles trygt og sikkert i samsvar med norsk lovgivning.

Grundig opplæring av system-brukerne vil være en nøkkelfaktor for å heve sikkerhetsnivået betydelig. Opplæringen bør i tillegg til dedikert system-opplæring også baseres på generell utøvelse av god sikkerhetskultur samt forståelse av risikobildet og forståelse av risiko ved egne handlinger.

Behovet vil til enhver tid endres og opplæring vil til tider kanskje måtte utføres som intensive opplæringsbolker som kommer parallelt med endringer i sikkerhets- og trusselbildet. Tett dialog mellom IT-drift, ledere, faggrupper og personvernombudet vil også være essensielt for godt sikkerhetsarbeid.

På arbeidsplassen å sørge for at plassering av pc-skjermer er slik at ingen andre enn brukeren selv kan se skjermen, låsing av skjermen og døra når kontoret forlates, ikke la utskrifter bli liggende på skriveren, og å forhindre at uvedkommende får tilgang til fysiske posthyller er enkle og selvfølgelig tiltak for å forbedre sikkerheten.

4. Avvik meldes til Datatilsynet (DT)

Brudd på personopplysningssikkerheten skal varsles som avvik til Datatilsynet (DT). PVO er gitt tilgang til å varsle slike avvik til DT på vegne av alle FARTT-kommunene (via Altinn).

Brudd på personopplysningssikkerheten kategoriseres i:



PERSONVERNOMBUDET I FOLLDAL-ALVDAL-RENDALEN-TOLGA-TYNSET

1. **Brudd på konfidensialitet**, det vil si at det har vært en utilsiktet eller ulovlig utlevering av eller tilgang til personopplysninger.
2. **Brudd på integritet**, det vil si at det har vært en utilsiktet eller ulovlig endring av personopplysninger.
3. **Brudd på tilgjengelighet**, det vil si der det har vært et utilsiktet eller ulovlig tap av tilgang til eller tilintetgjøring av personopplysninger.

I 2021 ble det meldt 3 avvik til datatilsynet fra FARTT-kommunene.

Ingen avvik er meldt til DT i 2022.

5. Fokusområder på personvernområdet som må videreføres i 2023

Arbeidet med å ivareta personvernet på en best mulig i henhold til lovverket er en prosess som må pågå kontinuerlig og det er viktig å ha et konstant søkelys på dette temaet.

Arbeidet videre vil måtte foregå skrittvis for å få innfridd alle pålagte krav som kommunene skal oppfylle.

Personvernombudets tilgang til å melde avvik på vegne av kommunene

Kommunedirektørene i alle FARTT-kommunene har gitt personvernombudet nødvendig tilgang til å melde avvik på personvernområdet på vegne av den enkelte kommune.

Avvik meldes til Datatilsynet via Altinn. Kommunedirektøren skal holdes orientert.

Behandlingsoversikt må holdes oppdatert

Den enkelte kommune er pliktig til å føre protokoll over behandlinger av personopplysninger som utføres under dens ansvar. Det vil si at vi skal ha en skriftlig oversikt over alle datasystemer og papirarkiver som har personopplysninger lagret, jf. [artikkel 30](#) i personopplysningsloven/ personvernforordningen. Denne oversikten skal være «grunnmuren» i kommunens dokumenterte internkontrollsystem på området. Oversikten må kontinuerlig oppdateres ved endringer.

FARTT-kommunene er i samarbeid godt i gang med å lage oversikten, men det kreves nok mer fokus på dette arbeidet for å få oversiktene opp på et tilfredsstillende nivå. I denne forbindelse og i sikkerhetsarbeidet generelt er det behov for å få på plass et styringssystem for IKT-sikkerhet og Personvern til bruk i kommunene.

Informasjon og registrertes rettigheter- personvernerklæringer

Kommunene har plikt til å behandle innbyggernes og andre registrertes personopplysninger på en åpen måte. Med åpen måte menes at kommunen må legge ut kort og forståelig informasjon om hvordan de behandler personopplysninger.

Den enkleste og beste måten å gjøre dette på er via personvernerklæring som legges ut på kommunens hjemmeside. Informasjonen skal rette seg **mot innbyggerne og øvrige personer** som har data om seg som blir lagret og behandlet hos kommunen. I eller ved siden av den erklæringen må det også ligge en egen erklæring som gjelder personvernet ved bruk av kommunens hjemmeside (informasjonskapsler mv).

I tillegg til dette må kommunene ha på plass en personvernerklæring mot **sine ansatte** som inneholder informasjon om hvilke personopplysninger vi lagrer om dem, hvor lenge m.v. Videre må



PERSONVERNOMBUDET I FOLLDAL-ALVDAL-RENDALEN-TOLGA-TYNSET

de ansatte informeres om den loggingen av aktiviteten som skjer når de bruker de forskjellige IT-systemene til kommunen.

Den enkelte kommune sjekker opp sin status.

Databehandleravtaler

Den enkelte kommune må sørge for å ha signerte databehandleravtaler med alle driftere av IKT-systemene sine på plass, og ha avtalene lagret på en sikker og oversiktlig måte.

Gjennomføring av risikovurderinger og personvernkonsekvensvurderinger (DPIA)

Hver gang kommunen planlegger å ta i bruk et nytt IKT-system har kommunedirektøren ansvaret for at det foretas en vurdering av konsekvensene for personvernet til de personene som får opplysninger om seg lagret og behandlet i det nye systemet.

I 2022 ble gjort en DPIA (personvernkonsekvens-vurdering) på Google G-Suite tilleggstjenester som brukes mye i skolene i FARTT-kommunene. Risikoen for personvernet til brukerne av disse tjenestene vurderes som liten/akseptabel når nødvendige organisatoriske og tekniske tiltak legges inn i systemet, og god informasjon gis til elever, foresatte og lærere.

Melding om nye behandlinger

Før nye systemer og apper tas i bruk skal dette meldes til personvernombudet. IKT-sikkerhetsgruppa i FARTT har laget prosedyrer for melding av behandlinger.

Rutinene er opprettet for å sikre at behandlinger registreres korrekt i behandlingsoversikten, samt at personvernombudet kontrollerer behandlingsinformasjon som er registrert og vurderer i samråd med IKT Fjellregion IKS om det må kjøres en personvernkonsekvensvurdering (DPIA) før systemet/appen kan tas i bruk.

Avvikshåndtering

Det er utarbeidet en rutine for avviksmelding og håndtering av avvik som skjer på personvernområdet. «Prosedyre for avviksbehandling personvernsaker» skal ligge tilgjengelig i Compilo i alle 5 kommunene..

Den enkelte kommune sjekker opp sin status.

Opplæring av alle ansatte i IKT-sikkerhet og personvern

Kommunedirektøren skal kunne dokumentere at alle ansatte som behandler personopplysninger i sitt arbeid har fått nødvendig opplæring i IKT-sikkerhet og personvern.

KS-læring har et godt e-læringsprogram, «KINS-kurs- Informasjonssikkerhet og personvern», som lagrer dokumentasjon om hvem som har gjennomført programmet. Bruk av dette krever at kommunen abonnerer på bruk av KS læring.

De fleste FARTT-kommunene er nå i gang med å gjennomføre dette opplæringsprogrammet for sine ledere og ansatte. Det bør tas sikte på at alle nåværende ansatte har fullført kurset i løpet av første halvdel av 2023 og det må etableres rutiner for at alle nyansatte tar kurset i løpet av den første måneden på jobb i kommunen.

Avslutning

IKT Fjellregionen IKS og personvernombudet har i løpet av 2022 vært rundt og snakket om IKT-sikkerhet og personvern i ledergruppene i alle de fem FARTT-kommunene.



PERSONVERNOMBUDET I FOLLDAL-ALVDAL-RENDALEN-TOLGA-TYNSET

Personvernombudet kontaktes jevnlig av ansatte, ledere og innbyggere med spørsmål omkring vern av personopplysninger.

Problemstillinger det har vært mye søkelys på for Personvernombudet og IKT-sikkerhetsutvalget i 2022, og som det skal jobbes videre med i 2023 er:

- Personvern omkring bruk av Chromebook og Googles tjenester i skolen
- Sending av fødselsnummer og sensitive opplysning via vanlig ukryptert epost
- Lagring av dokumenter fødselsnummer og sensitive opplysning i OneDrive mv
- Opplæring og dokumentasjon av opplæring i IKT-sikkerhet og Personvern for alle ansatte
- Få på plass et godt styringssystem for IKT-sikkerhet og Personvern til bruk i kommunene.

Tolga 18.01.2023

Kjetil Brodal

PVO i FARTT-kommunene

epost pvo@fartt.no

tlf 416 00 264