



Håndtering av meldeplikt om avvik til Datatilsynet og informasjonsplikt til berørte

Versjon/dato: 1.0, 22.01.2021	Godkjent/vedtatt av: Leder for Avdeling for jus og informasjonsforvaltning
Dokumentnummer: 20/23250-6	Beskrivelse: Håndtering av meldeplikt om avvik til Datatilsynet og informasjonsplikt til berørte
Neste versjon: 2.0	Ansvar for revisjon: Leder for Avdeling for jus og informasjonsforvaltning
Første gang vedtatt: 22.01.2021	Gjelder for: Ledere som behandler interne avviksmeldinger for personvern og informasjonssikkerhet, system- og tjenesteeiere og -forvaltere, Avdeling for jus og informasjonsforvaltning og personvernombudet.

Formål med rutinen

Noen personvern- og informasjonssikkerhetsavvik plikter vi etter regelverket å melde til Datatilsynet. Hensikten med denne rutinen er å tydeliggjøre internt ansvar og oppgaver i denne forbindelse.

Om meldeplikten til Datatilsynet

Melding til Datatilsynet skal gjøres så raskt som mulig og senest innen 72 timer fra avviket ble kjent for oss. Meldeplikten til Datatilsynet er kun aktuelt for informasjonssikkerhetsavvik. Avvik knyttet til andre sider ved personvernet er det altså ikke meldeplikt for, eksempelvis brudd på slettefrist, formålspriippet eller dataminimering.

Datatilsynet har også informasjon på sine hjemmesider om avviksmelding. Det kan du lese mer om [her](#).

Terskelen for meldeplikten til Datatilsynet er knyttet til avvikets konsekvenser for den/de personopplysningene handler om. Bestemmelsen sier at Datatilsynet skal informeres «med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske

personers rettigheter og friheter». Grensedragningen for det meldepliktige kan oppleves som vanskelig.

I meldingen til Datatilsynet skal vi gjøre rede for avviket og beskrive hva vi har gjort så langt i behandlingen. Tidlig overblikk og vurderingen av avvikets karakter og alvorlighet er avgjørende for å identifisere om et avvik er meldepliktig, og for å kunne agere innen tidsfristen. Rask vurdering av avviket er også avgjørende for å komme hurtig i gang med tiltak i de saker hvor det ut fra avvikets art er påkrevd.

Meldeplikt til Datatilsynet er dels en løpende vurdering. Vurderingen må baseres på hva vi til enhver tid kjenner til om omfang, alvorlighet og hvordan hendelsen kan få konsekvenser for berørte. Hva som først fortone seg som et mindre avvik uten meldeplikt kan senere se ut som et alvorlig avvik med meldeplikt.

Plikten til å informere berørte har høyere terskel enn meldeplikten til Datatilsynet. I praksis kan vi derfor isolere vurderingen av informasjonsplikt til saker hvor vi mener det er meldeplikt.

Hvem gjør hva?

- Det interne ansvaret for å sende melding om avvik til Datatilsynet, jf GDPR artikkel 33, er tillagt **Avdeling for jus og informasjonsforvaltning**. Avdelingen treffer også beslutningen om at avviket skal meldes Datatilsynet eller ikke. Hvis et avvik er vurdert som meldepliktig skal avdelingen også ta stilling til informasjonsplikt til berørte, jf GDPR artikkel 34. Informasjon til berørte kan håndteres av avdelingen selv eller andre etter nærmere dialog, for eksempel den aktuelle tjenesten hvor avviket har skjedd. Avdelingen skal ha lav terskel for å rådføre seg med personvernombudet om melde- og informasjonsplikt i konkrete saker.
- **Behandlere av relevante avvikssaker, samt system- og tjenesteeiere og systemforvaltere**, skal raskt og på eget initiativ informere Jus og informasjonsforvaltning om avvikssaker, som definert ovenfor. Terskelen for å ta kontakt skal være lav.
- **Personvernombudet** kan gi råd til alle som inngår i avvikshåndteringen. På forespørsel eller på eget initiativ kan ombudet gi skriftlige råd om meldeplikten eller informasjon til berørte. Slike råd skal lagres sammen med øvrig dokumentasjon på avviksbehandlingen.
- **Leder for avdeling for jus og informasjonsforvaltning, informasjonssikkerhetsrådgiver og personvernombud** skal ha tilgang til relevante avvikssaker i kvalitets- og avvikshåndteringssystemet QM+. Gjennom denne tilgangen skal disse også kunne fange opp avvikssaker som skal meldes til Datatilsynet.

Nødvendig kompetanse og tilgjengelig veiledning

- Relevante bestemmelser er personvernforordningen (GDPR) [artikkel 33 og 34](#).
- **Alle roller/medarbeidere som denne rutinen retter seg mot** skal være kjent med hvem de kan rådføre seg med internt, samt være kjent med Datatilsynets veiledning om meldeplikt [her](#), som også har eksempler. Det viktigste for avviksbehandlerne er å si ifra internt om relevante avvikssaker hvor melding til Datatilsynet bør vurderes. Det er tjenlig, men ikke forventet at avviksbehandlere har god kunnskap om denne meldeplikten. Faglig kompetanse og dybdekunnskap om temaet skal ivaretas av Avdeling for jus og informasjonsforvaltning, og personvernombudet.

Øvrige føringer

- Å unnlate å sende melding til Datatilsynet vil lett forstås som «å feie ting under teppet», og vil representerer det motsatte av den åpenhet som fylkeskommunen skal kjennetegnes ved. Prinsippet om «heller en for mye enn en for lite» skal gjelde i tvilssaker.
- I en tidlig fase vil enkelte avvikssaker være beheftet med stor usikkerhet om omfang, alvorlighet og konsekvenser. Dette kan igjen gi tvil om et avvik skal meldes eller ikke, eller om vi skal se saken an til vi vet mer. Som hovedprinsipp skal vi i slike saker, når 72-timersfristen nærmer seg, ta utgangspunkt i hva vi tror er mest sannsynlig. Dersom vi tror at saken mest sannsynlig er så alvorlig at den bør meldes, skal vi melde saken til Datatilsynet innen fristen, med den informasjon og den usikkerhet som eksisterer der og da. I slike saker skal vi normalt på et senere tidspunkt supplere meldingen til Datatilsynet med mer sikker informasjon.
- Vi har erfaring med at det i enkelte saker har vært opplevd som både tillitsvekkende og rimelig å informere berørte selv om saken ikke har vært vurdert som stor nok for melding til Datatilsynet. Denne rutinen skal ikke stå til hinder for at fylkeskommunen informerer berørte når det oppleves som rimelig, selv om regelverket strengt tatt ikke krever det.