Oslo

Byrådsavdeling for finans

Veileder om brudd på personopplysnings-sikkerheten

En veileder om krav til avvikshåndtering og prosess for melding til Datatilsynet og informasjon til de registrerte.

Foto: Arvid Malde

Om veilederen

Om veilederen

Gjennom personopplysningsloven er EUs personvernforordning (GDPR) gjort til en del av norsk rett. I henhold til GDPR artikkel 4 nr.12, art 33 og 34 reguleres når det foreligger et brudd på personopplysningssikkerheten, når Datatilsynet skal motta avviksmelding fra virksomheten og når den berørte registrerte skal informeres om bruddet.

Veilederen vil ta leseren gjennom definisjonen på et brudd på personopplysningssikkerheten, ansvarsplassering og selve avvikshåndteringen. Til slutt vil veilederen beskrive prosessen med melding til Datatilsynet og informasjon til de(n) berørte registrerte.

Formål

Formålet med veilederen er å bidra til å sikre etterlevelse av lover, regelverk og kommunens styrende dokumenter ved å gi ansatte og ledere i Oslo kommune konkret veiledning for avvikshåndtering, melding til Datatilsynet og informasjon til de registrerte. Dette dokumentet gir informasjon om hvilke problemstillinger som må vurderes i saksbehandlingsprosessen.

Veilederen skal bidra til at alle ansatte vet hva et brudd på personopplysningssikkerheten er og hvilket ansvar som ligger til ulike roller. Veilederen sikrer også at dedikerte ressurser vet hva som kreves i den videre håndtering av avviket, samt når Datatilsynet og de(n) registrerte skal varsles.

Virksomheter i Oslo kommune vil ha ulike behov og ulikt utgangspunkt for å vurdere avvik og videre håndtering av denne. Veilederen er utformet på et generelt grunnlag for å kunne omfavne så mange ansatte som mulig, og vil derfor ikke besvare konkrete problemstillinger i hver enkelt sak siden omstendighetene vil variere.

Målgruppe

Veilederen gjelder for alle ansatte og ledere i Oslo Kommune som er involvert i et avvik, og kan være særlig relevant også for ansatte med definerte oppgaver innen personvern. Dette omfatter f.eks. personvernkoordinatorer, systemeiere, systemforvaltere, andre ressurser med konkrete oppgaver innen personvern mv.

Anvendelsesområdet

Veilederen kan brukes ved avvikshåndtering i den enkelte virksomhet.

Innhold

Hva er et avvik?

Etter personopplysningsloven defineres et brudd på personopplysningssikkerheten som «*et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet*[1]».

Brudd på personopplysningssikkerheten er ofte omtalt som brudd på

- Konfidensialitet,
- Integritet
- Tilgjengelighet

Disse begrepene innebærer at personopplysningene kan være tilfeldig (uhell) eller ulovlig tilgjengeliggjort for ansatte eller uvedkommende (konfidensialitet). Brudd på personopplysningssikkerheten kan også være at opplysningene har blitt ulovlig eller tilfeldig endret på av ansatte eller andre uvedkommende, men også systemer kan gjøre dette ved en feil (integritet). Videre kan også et brudd på personopplysningssikkerheten oppstå når man ved en tilfeldighet mister tilgang til personopplysningene eller det kan foreligge en ulovlig hindrer av tilgang til opplysningene (tilgjengelighet).

Det er viktig å merke seg at her er det tale om **brudd på sikkerheten** ved behandling av personopplysninger, og ikke nødvendigvis brudd på ulike bestemmelser etter personvernregelverket, for eksempel hvor det mangler databehandleravtaler med leverandør etter artikkel 28.

I denne veilederen kaller vi brudd på personopplysningssikkerheten for et avvik.

Det er viktig å huske at avvik alltid vil være et brudd på sikkerheten, men et brudd på sikkerheten vil ikke alltid være et avvik som omfatter personopplysninger. Det kan dermed ha oppstått et brudd på sikkerheten uten at dette har konsekvenser for behandling av personopplysninger i virksomheten.

Hvem har ansvar og hvilke roller er tilknyttet avviksprosessen?

Alle ansatte i Oslo kommune har et ansvar for å rapportere avvik som de avdekker. Denne rapporteringen skal skje i henhold til virksomhetens rutiner.

Personvernkoordinator i virksomheten skal bidra til å håndtere personvernhendelser og brudd på personopplysningssikkerheten, samt bidra til virksomhetens oversikt over alle hendelser og avvik. Personvernkoordinator skal rapportere alvorlige hendelser og avvik til virksomhetsleder, og bistå ved rapportering av hendelser og avvik til Datatilsynet, til overordnet byrådsavdeling, til Byrådsavdeling for finans og til personvernombudet.

---

[1] Lov om behandling av personopplysninger (Personopplysningsloven) m/EUs personvernforordning artikkel 4 nr. 12

Informasjonssikkerhetskoordinator i virksomheten skal bidra til å håndtere informasjonssikkerhetshendelser- og brudd, samt bidra til oversikt over alle avvik og sikkerhetsbrudd. Videre skal koordinatoren rapportere alvorlige sikkerhetsbrudd til virksomhetsleder og bistå ved rapportering av alvorlige sikkerhetsbrudd til overordnet byrådsavdeling og til Byrådsavdeling for finans.

Hver enkelt **virksomhet** i Oslo kommune skal etablere sine egne rutiner for å avdekke, håndtere, rapportere avvik. Dette er virksomhetsleders ansvar. Ved etablering av gode avviksrutiner vil årsak til avviket, korrigerende tiltak og rapportering bli dokumentert, og virksomheten sikrer dermed at personvernregelverket følges. Det er også viktig at virksomhetsleder anskaffer verktøy hvor ansatte kan rapportere avvik gjennom.

Videre skal **virksomheten** gjennomføre opplæring for alle ansatte, slik at avviksrutinen er kjent og blir tatt i bruk av alle ansatte. Dette vil kunne bidra til at avvik oppdages, håndteres og lukkes på en rask og effektiv måte.

Virksomhetsleder bør sørge for å plassere ansvar for håndtering av avvik til dedikerte ressurser, som for eksempel personvern-/informasjonssikkerhetskoordinator, og påse at disse har tilgang til nødvendig verktøy og digitale løsninger. For å kunne rapportere avvik til Datatilsynet kan virksomhetsleder påse at en (eller flere) ressurser tildeles et ansvar og at rollen som «Utfyller/innsender» i www.altinn.no . Som oftest er det virksomhetens leder som kan tildele disse rollene.

Avvikshåndtering

Hvordan melde avvik?
Hvordan ansatte skal melde avvik er opp til den enkelte virksomhet i kommunen å avgjøre.

Avvik kan for eksempel meldes inn via et egnet elektronisk verktøy eller muntlig til virksomhetens leder eller andre dedikerte ansatte som har ansvaret for avvikshåndteringen. Noen virksomheter har pr. i dag allerede føringer for hvilket rapporteringsverktøy som skal benyttes for registrering av uønskede hendelser og avvik. For eksempel skal virksomheter under Byrådsavdeling for helse-, eldre- og innbyggertjenester (HEI) benytte EQS for rapportering av avvik.

Dersom virksomheten har lav terskel og aksept for å melde avvik vil det kunne bidra til å skape god kultur og gjøre det lettere for de ansatte å melde fra om avvik som oppdages.

I den videre veiledningen vil vi se nærmere på hvilke vurderinger og handlinger som må foretas etter at avviket er meldt inn til virksomheten. For den enkelte ansatte vil dette trolig ikke være relevant, men for dedikerte ressurser kan de beskrevne handlingene være til hjelp i håndteringen.

Hvordan håndtere innmeldte avvik?
Virksomhetsleder bør utpeke en eller flere ansatte som er mottaker og/eller ansvarlig for håndtering avviksmeldinger internt i virksomheten. Når et avvik er rapportert inn til virksomheten er det viktig at virksomheten legger til rette for at disse ressursene kan dokumentere avvikshåndteringen skriftlig og forankre konklusjonen i virksomheten. Denne prosessen skal beskrives i virksomhetens egen avviksrutine og rutinen skal gjøres kjent for alle av virksomhetens ansatte.

Når virksomheten mottar en avviksmelding må følgende vurderinger og handlinger utføres:

1. **Er personopplysninger berørt?**
   Det første man må gjøre er å vurdere om personopplysninger er berørt i avviket. For eksempel kan det være navn, adresse, mobilnummer, fødselsnummer mv. til en eller flere registrerte. Eller det kan være at helseopplysninger, etnisk opprinnelse, religionstilhørlighet sammen med navn og adresse eller liknende er berørt. Da snakker man om særlige kategorier av personopplysninger. Den ansvarlige vurderer dette og dokumenterer resultatet.

2. **Iverksette strakstiltak og langsiktige tiltak?**
   Videre må man vurdere hvilke strakstiltak som må iverksettes slik at avviket kan lukkes så raskt som mulig. Ofte vil det være nødvendig å involvere andre ressurser i virksomheten som kan bidra inn i dette arbeidet. Dette fordi disse personene kan kjenne løsningen eller prosessen rundt behandlingen av personopplysningene godt. Eksempel på slike ressurser kan være IT-ansvarlig, saksbehandlere i egen organisasjon, men også andre ressurser på tvers av avdelinger og/eller sektorer.

   Dersom man har anledning til det må man også se nærmere på om det er nødvendig å iverksette eller planlegge for langsiktige tiltak slik at man kan hindre at samme type avvik oppstår senere. Dette kan for eksempel være etablering av nye eller endring av eksisterende rutiner, opplæring av de ansatte i virksomheten mv.

3. **Hvilken risiko utgjør avviket for den registrertes rettigheter og friheter?**

   Parallelt med at man vurderer tiltak for å lukke avvik, bør man også vurdere hvilken risiko avviket har hatt for de berørte registrertes rettigheter og friheter, siden virksomheten har en plikt til å melde fra til Datatilsynet innen 72 timer dersom avviket *utgjør en risiko* for den registrertes rettigheter og friheter.

   Med «risiko» menes en vurdering av forholdet mellom sannsynligheten for at en uønsket hendelse vil inntreffe og konsekvenser av at en slik hendelse inntreffer.

   I en vurdering av risikoen må man se på de konkrete omstendighetene rundt avviket. Dette vil blant annet være avvikets alvorlighetsgrad og potensielle innvirkning avviket vil ha for den enkelte registrerte.

Hvilket nivå avviket medfører for den berørte registrertes rettigheter og friheter vil innebære at virksomheten må foreta en vurdering av den registrertes personopplysningsvern og personvern. Dette omfatter også en vurdering av andre grunnleggende menneskerettigheter som retten til privatliv, ytringsfrihet m.m. etter den Europeiske menneskerettighetskonvensjonen.

Byrådsavdeling for finans har utarbeidet en mal for nærmere vurdering av risiko som kan være til hjelp for virksomhetene[2].

Virksomhetene må dokumenter og oppsummere vurdering og slå fast hvilket nivå risikoen for den enkelte registrerte er på. Avviket kan enten være av lav, middels eller høy risiko for den registrertes rettigheter og friheter.

Dersom avviket utgjør en risiko for den registrertes rettigheter og friheter skal virksomheten melde avviket til Datatilsynet. Dersom risikoen er høy skal den berørte registrerte informeres. Det er viktig at konklusjonen av vurderingen alltid dokumenteres skriftlig og forankres på rett ledernivå, uavhengig av nivå på risiko.

Når må virksomheten sende melding til Datatilsynet?

Dersom det oppstår et avvik hvor det er sannsynlig at bruddet medfører en risiko for de registrertes rettigheter og friheter, skal virksomheten som nevnt sende melding til Datatilsynet[3].

Det er viktig å merke seg at personvernregelverket stiller krav om at meldingen til Datatilsynet skal sendes senest 72 timer etter at virksomheten har fått kjennskap til at det foreligger et avvik. For å ivareta dette kravet er det viktig at virksomheten har gode og effektive avviksrutiner.

Dersom bruddet ikke meldes innen 72 timer, skal årsakene til forsinkelsen oppgis. Hvis det ikke er mulig å gi all informasjon samtidig til Datatilsynet, kan meldingen gis trinnvis. Det innebærer at virksomheten oppdaterer meldingen til Datatilsynet flere ganger via www.Altinn.no[4] til avviket anses håndtert og lukket. Dette gjelder særlig for de tilfeller avviket er omfattende.

Er virksomheten usikker på om personopplysninger er berørt ved en hendelse, kan det likevel være hensiktsmessig å informere Datatilsynet om dette, og senere oppdatere meldingen når ytterligere informasjon foreligger. Om virksomheten ikke har anledning til å melde avviket

[2] Vedlegget vil revideres og publiseres høsten 2021

[3] Lov om behandling av personopplysninger (Personopplysningsloven) m/EUs personvernforordning artikkel 33

[4] https://www.altinn.no/skjemaoversikt/datatilsynet/melding-om-avvik-datatilsynet/

skriftlig til Datatilsynet innen fristen på 72 timer, kan Datatilsynet også kontaktes pr. telefon. Virksomheten bør da be om at meldingen registreres og en bekreftelse på dette[5].

Oslo kommunes personvernombud er tilgjengelig for rådgivning dersom virksomheten er usikker på håndtering av avviket, og kan kontaktes før melding sendes til Datatilsynet. Personvernombudet og ansvarlig byrådsavdeling skal alltid informeres når virksomheten sender melding til Datatilsynet. Kopi av meldingen kan også sendes til Byrådsavdeling for finans ved seksjon for Informasjonssikkerhet og IKT. Meldingen til Datatilsynet skal dokumenteres og journalføres ihht. til arkivlovens bestemmelser.

Informasjon til de registrerte

Når må virksomheten gi informasjon til de registrerte?
Dersom det foreligger et brudd på personopplysningssikkerheten som medfører høy risiko for den registrertes rettigheter og friheter, har virksomheten plikt til å gi informasjon så raskt som mulig til de berørte registrerte[6].

Virksomheten kan også vurdere om det er hensiktsmessig å informere de berørte registrerte dersom avviket har en lavere risiko for den enkelte.

Fordelen ved å involvere de berørte registrerte tidlig er at disse kan bidra til å forhindre misbruk av personopplysningene, begrense omdømmetap, skape tillit m.m. Det kan derfor i noen tilfeller være hensiktsmessig å kontakte den berørte registrerte selv om virksomheten ikke melder avviket til Datatilsynet. Dersom dette gjøres må virksomheten oppfylle minimumskravene etter personvernregelverket, se nedenfor om krav til hva den registrerte må opplyses om.

I noen tilfeller vil ikke virksomheten være pliktig til å informere de berørte registrerte[7]. Dette gjelder dersom:

- *Det er gjennomført egnede tekniske og organisatoriske sikkerhetstiltak for å sikre personopplysningene i forkant av bruddet, særlig tiltak som gjør personopplysningene uleselige for personer som ikke har autorisert tilgang til dem – f.eks. kryptering.*

- *Det er gjort etterfølgende tiltak som sikrer at det ikke lenger er sannsynlig at den høye risikoen vil oppstå. For eksempel, avhengig av omstendighetene, hvis virksomheten umiddelbart har identifisert og iverksatt tiltak mot en enkeltperson som har fått tilgang til personopplysningene før vedkommende har hatt mulighet til å gjøre noe med dem. Det*

5 For mer informasjon om hvordan melde avvik til Datatilsynet, se Datatilsynets nettsider: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvikshandtering/melde-avvik-til-datatilsynet/

6 Lov om behandling av personopplysninger (Personopplysningsloven) m/EUs personvernforordning artikkel 34 nr. 1

7 Lov om behandling av personopplysninger (Personopplysningsloven) m/EUs personvernforordning artikkel 34 nr. 3

må allikevel vurderes hvor høy restrisiko som er igjen og hvilke konsekvenser det kan medføre for de berørte.

- *Det vil innebære en uforholdsmessig stor innsats. Eksempler på dette er når kontaktopplysninger har blitt borte som et resultat av bruddet eller i utgangspunktet ikke har vært kjent for den behandlingsansvarlige (virksomheten). Dersom det er tilfelle, skal man i stedet informere offentlig, eller det skal treffes et lignende tiltak som sikrer at de registrerte underrettes på en like effektiv måte.*

- *Informasjon om sikkerhetsbruddet vil avsløre opplysninger av betydning for Norges utenrikspolitiske, forsvars- og sikkerhetsinteresser, forebygging og etterforskning av straffbare handlinger, og opplysninger underlagt lovpålagt taushetsplikt, jf personopplysningsloven § 16 fjerde ledd, jf. § 16 første ledd bokstav a, b og d*

En vurdering av når informasjon til den registrerte er nødvendig må gjennomføres for hvert enkelt avvik.

Hva må de registrerte vite om avviket?
Dersom virksomheten har konkludert med at den registrerte skal informeres, er det visse krav til innhold som må være oppfylt.

Informasjon til de registrerte skal som minimum inneholde[8]:

- *en nærmere beskrivelse av avviket,*
- *navn og kontaktinformasjon til virksomhetens kontaktpunkt hvor ytterligere informasjon kan innhentes, samt kontaktinformasjon til Oslo kommunes personvernombud,*
- *nærmere beskrivelse av hvilke sannsynlige konsekvenser bruddet har medført for den registrerte,*
- *nærmere beskrivelse av de tiltakene som virksomheten har truffet eller som foreslås iverksatt for å håndtere bruddet. Dette gjelder også tiltak for å redusere eventuelle skadevirkninger som følge av bruddet (dersom relevant).*

Ved utforming av informasjon til de registrerte er det viktig at virksomheten tilpasser informasjonen til hvem som er mottakere, for eksempel om det er eldre, pasienter, barn/ungdom m.m. som skal motta denne.

Hvilke kanaler kan vi benytte for å kontakte de registrerte?
Virksomheter bør ta direkte kontakt med de personene som er berørt av avviket. For å finne frem til riktig kontaktinformasjon kan virksomheten benytte kontakt- og reservasjonsregister[9].
Hvordan personer skal kontaktes bør vurderes konkret ut fra hvilke metoder og kanaler som er

[8] Lov om behandling av personopplysninger (Personopplysningsloven) m/EUs personvernforordning artikkel 34 nr.2

[9] https://www.difi.no/fagomrader-og-tjenester/difis-felleslosninger/kontakt-og-reservasjonsregisteret

mest hensiktsmessige og effektive basert på hensynet til den enkelte person og hva virksomheten er tjent med.

For at informasjonen om avviket skal være så åpen og tydelig som mulig bør informasjonen være ment for nettopp dette formålet og bør derfor ikke sendes sammen med annen informasjon fra kommunen.

Dersom avviket berører et avgrenset antall registrerte kan SvarUt benyttes for sikker digital utsendelse av brev. Hvis dette ikke lar seg gjøre kan virksomheten vurdere å bruke e-post eller SMS, men husk at disse er usikre kanaler.

Hvis avviket omfatter en betydelig mengde registrerte, eller man er usikker på omfanget av berørte registrerte, kan virksomhetene vurdere om det er andre kanaler som kan benyttes for å nå ut til så mange som mulig.

Dette kan for eksempel være:

- Informasjon på Oslo kommunes og virksomhetens/skolens o.l. nettsted som er godt synlig for de registrerte, f.eks. informasjon på nettstedets første side.
- Annonsering i trykte medier eller andre medier.
  Dersom dette alternativet benyttes er det viktig at virksomheten tar en vurdering av andre mulige konsekvenser som kan oppstå, f.eks. risikoen for omdømmetap, medieomtale m.m.

Oppsummering

Huskeliste ved håndtering av avvik

- ✓ Alle ansatte i Oslo kommune
  - har et ansvar for å rapportere avvik de selv oppdager.
  - skal gis tilstrekkelig opplæring i avviksrutinene og verktøy som benyttes.

- ✓ Dedikerte ressurser i avvikshåndteringen
  - skal ha tilstrekkelig kompetanse og kapasitet til å håndtere avvik.
  - må vurdere og skriftlig dokumentere avvikets omfang, tiltak og risikonivå avviket har for den registrerte.
  - vurdere hvorvidt Datatilsynet skal varsles og om informasjon til de berørte registrerte skal gis.

- ✓ Virksomhetsleder skal sørge for at
  - det etableres rutiner for avvikshåndtering i virksomheten, melding til Datatilsynet, samt informasjon til den berørte registrerte.
  - det foreligger verktøy for melding og rapportering om avvik.
  - dedikerte ressurser er satt til rollen(e) for videre håndtering av avviket.

- ✓ Kopi av melding til Datatilsynet skal sendes til ansvarlig byrådsavdeling og personvernombud, samt Byrådsavdeling for finans v/seksjon for Informasjonssikkerhet og IKT.

Vedlegg

Mal for risikovurdering ved avvikshåndtering – under arbeid

Eksempel på avviksrutiner for en virksomhet – under arbeid