Avvikshåndtering ved brudd på personopplysningssikkerheten og melding til Datatilsynet

HENSIKT

Sikre at lovbestemt meldeplikt til Datatilsynet følges ved brudd på personopplysningssikkerheten.

MÅLGRUPPE

Alle som har tilgang til, og/eller bearbeider og forvalter personopplysninger for VID

DEFINISJONER

Avvik - Brudd på personopplysningssikkerheten, brudd på lover og regler, samt brudd på VID interne rutiner, som regulerer enten direkte eller indirekte, behandling av personopplysninger.

Et brudd på personopplysningssikkerheten er 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, jf personvernforordningen artikkel 4 nr. 12.

Personopplysninger – alle opplysninger som kan knyttes til enkelt person (f eks navn, adresse, telefonnummer, e-post og fødselsnummer (11 siffer), se personvernforordningen artikkel 4.

Avvikseier: Den linjeleder som eier arbeidsutførelsen som avviket gjelder.

Tiltakseier: Den eller de som er ansvarlig for implementering av de tiltak som avvikseier har utformet. Tiltakseiere kan være en eller flere ansatte, systemeiere, prosesseiere, ledere på et annet nivå eller annen enhet, eller tiltakseier og avvikseier kan i noen tilfeller være samme person.

Bruddene kan deles i brudd på:

- **Konfidensialitet** - At informasjon har konfidensialitet betyr at det er sikret at informasjonen

og informasjonssystemene bare er tilgjengelige for de som har et tjenstlig behov. Eks. utilsiktet eller ulovlig utlevering av, eller tilgang til, personopplysninger

- **Integritet** - informasjon har integritet betyr at det er sikret at informasjonen er korrekt, gyldig og fullstendig og at den ikke kan endres utilsiktet eller av uvedkommende. Eks. utilsiktet eller ulovlig endring av personopplysninger.

- **Tilgjengelighet** - At informasjon og informasjonssystemer har tilgjengelighet betyr at det er

sikret at informasjonen og informasjonssystemene er tilgjengelige ved behov innenfor de tilgjengelighetskrav som er satt. Eks. utilsiktet eller ulovlig tap av tilgang til eller tilintetgjøring av personopplysninger.

Eksempel på avvik:

- feilsendt e-post og vedlegg, særlig der det er personopplysninger
- innsamling av data i skjema med personopplysninger som gjør informasjonen søkbar på internett
- feilutlevering eller feilpublisering av personopplysninger
- feil i tilganger, utstyr eller programvare som gjør at informasjons tilgjengelighet er svekket, og som igjen kan svekke personopplysningssikkerheten
- rutiner vedrørende personopplysningssikkerhet som mangler, ikke fungerer, eller som ikke følges
- manglende grunnlag eller vurdering av grunnlag for å behandle personopplysninger
- personnummer (11 siffer) som er sendt ukryptert per e-post til eksterne (Et enkelt dokument som inneholder et personnummer (11 siffer) sendt mellom ansatte gjennom VIDs e-post løsning anses ikke som avvik, men anbefales imidlertid ikke
- Utskift med personopplysninger som kommer på feil skiver
- Elektronisk utstyr med personopplysninger som blir stjålet eller på avveie
- bruker går fra arbeidsstasjonen usikret/låser ikke PC-en når forlater arbeidsplassen
- bruker låner ut brukernavn og passord til andre
- brukers tilgang blir ikke fjernet ved fratredelse
- helseopplysninger blir sendt i usikret (ikke kryptert) e-post
- autorisert bruker får ikke tilgang
- urettmessig tilegnelse av taushetsbelagte opplysninger (snoking)

1. MELDING OG OPPFØLGNING AV AVVIK

1.1. Informere, melde og igangsette strakstiltak

Dersom avvik oppdages og det er behov for strakstiltak, skal den som oppdager avviket også umiddelbart informere nærmeste leder som igjen skal varsle systemeier dersom det gjelder systemer (i samarbeid med IT seksjonen ved behov). Systemeier/avdelingssjef som avvikseier der hendelsen har skjedd har ansvaret for å sørge for at det iverksettes risiko reduserende tiltak umiddelbart dersom det er behov for det.

Den som oppdager avviket, eventuelt vedkommende nærmeste leder, skal straks varsle avvik til direktør administrativ og personvernombudet.

Utenfor ordinær arbeidstid, hvis avviket gjelder IKT, så IT-sjef og direktør administrativ støtte kontaktes som da har ansvaret for de oppgavene som i denne rutinen tilligger personvernombudet.

Avvikseier skal etter beste evne kartlegge og analysere årsaken til avviket og vurdere bakenforliggende årsaksfaktorer (ved behov i samarbeid med IT seksjonen) som medførte at avviket fant sted. Dette gjør at det kan utvikles målrettede og effektive tiltak knyttet til både kompetanse, ressurser, ledelse og rutiner. Tiltak skal distribueres til en eller flere tiltakseiere som har ansvar for oppfølging og implementering av de tiltak som er utarbeidet.

VID har plikt til å melde avvik til Datatilsynet dersom bruddet kan ha medført middels eller høy risiko for de berørte. Dersom det er ingen eller lav risiko, er det ikke behov for å melde fra til Datatilsynet.

Avviket skal meldes Datatilsynet så raskt som mulig og senest innen 72 klokketimer fra avviket oppdages, jf personvernforordningen artikkel 33 nr. 1.

Den som oppdager avviket skal også melde avviket i (intern avvik system).

1.2. Innholdet i meldingen til personvernombudet

Det skal gis nødvendige opplysninger til personvernombudet om:

- Beskrivelse av avviket.
  - Hovedårsak
  - Tidsrom
  - Når avviket ble oppdaget
  - Antall berørte personer
  - Beskrivelse av hva som har skjedd
  - Hvordan avviket oppsto
  - Beskrivelse av hva slags type personopplysninger som ble berørt
  - Hvilken relasjon VID har til personene
  - Beskrivelse av hvor personopplysningene befinner seg etter avviket

Dersom det er mulig skal det kun gis anonymiserte personopplysninger i meldingen til personvernombudet.

1.3. Personvernombudets ansvar:

Personvernombudet beslutter om avviket skal rapporteres til Datatilsynet etter personvernforordningen art 33 nr.1. se Datatilsynet - Når og hvor skal jeg melde avvik

Dersom det gjelder et teknisk avvik skal IT-sikkerhet kontakts i tillegge for rådgivning.

Personvernombudet sender elektronisk melding via Altinn til Datatilsynet innen 72 klokketimer.

Dersom det er viktig at Datatilsynet blir raskt kjent med avviket, for eksempel stor sannsynlighet at Datatilsynet vil motta henvendelser fra andre vedrørende avviket, skal personvernombudet først varsle tilsynet på telefon.

Meldingen til Datatilsynet skal inneholde beskrivelse av avviket (se over), konsekvenser, tiltak om det er gitt informasjon til de berørte og kontaktinformasjonen til personvernombudet eller annen kontaktperson ved VID.

Dersom VID ikke har all informasjon som trengs på dette tidspunktet, sendes meldingen trinnvis og det opplyses i første meldingen at den manglende informasjon vil bli ettersendt.

Dersom bruddet ikke meldes innen 72 timer, skal årsakene til forsinkelsen oppgis til Datatilsynet.

1.4. Informasjon til berørte personer

Dersom det foreligger et avvik som meldes til Datatilsynet, skal de som har fått personopplysningene sine på avveier så raskt som mulig informeres skriftlig dersom det er sannsynlig at avviket vil medføre en *høy risiko for deres rettigheter og friheter*, jf. personvernforordningen artikkel 34 nr. 1.

Personvernombudet avgjør om det medfører en høy risiko og dermed at de berørte skal informeres.

Systemeier, der avviket er knyttet til system, har ansvaret for å informere de berørte. Er ikke avviket knyttet til et system, har avdelingssjef i avdelingen der avviket har skjedd dette ansvaret.

Informasjon til de berørte skal minst inneholde:

- Klar og tydelig beskrivelse av arten av bruddet på personopplysningssikkerheten
- Kontaktopplysning til personvernombudet
- Sannsynlige konsekvenser
- Beskrive skadebegrensende tiltak som er iverksatt eller planlagt iverksatt

1.5. Avviksbehandling

Hendelsen vurderes og registreres i det interne avviksbehandlingssystemet for videre intern saksbehandling. Dersom avviket ikke meldes til Datatilsynet, skal det i interne avviksbehandlingssystemet begrunnes hvorfor avviket ikke er meldt.

Systemeier har, der avviket er knyttet til system (i samarbeid med *IT seksjonen* ved behov), ansvaret for å vurdere og iverksette tiltak for å hindre gjentakelse, og for å redusere potensielle skadevirkninger av bruddet. Er ikke avviket knyttet til et system, har avdelingssjef i avdelingen der avviket har skjedd dette ansvaret.

Avvikseier skal avdekke og analysere årsaken til avviket. Med utgangspunkt i årsaksfaktorer skal avvikseier vurdere hvordan avviket bør håndteres, og utforme forslag til tiltak. Avvikseier dokumenter foreslåtte tiltak i avvikssystemet med fastsatt frist og ansvarlig person for implementering av tiltak. Tiltakene skal konkretisere ønsket effekt. Avvikseier kan underveis i avvikshåndteringen, basert på egen vurdering, endre nivå for kritikalitet.

Gjennomføring av tiltak etter fastsatt frist gitt av avvikseier, tiltakseier (en eller flere) skal vurdere foreslåtte tiltak. Ved tiltak som medfører omfattende endringer eller ressurser, skal tiltakseier utforme forslag til løsning med et grovt estimat for ressursbehov. Dette godkjennes av Avvikseier før tiltak iverksettes. Tiltakseier rapporterer fremdrift på implementering av tiltaket til avvikseier i avvikssystemet. Tiltakseier rapporterer til avvikseier når tiltak er implementert.