Rutiner for personvernbrudd og varsling

*[KOMMENTAR: Dette er et eksempel/mal som må tilpasses den enkelte virksomhet. Alle punkter satt i firkantklammer, må endres, og kommentarer må fjernes. Så må rutinene besluttes av den øverste ledelse i virksomheten. Spesielt punktet om hvordan intern varsling skal gjøres, i punkt 5.1 må tilpasses. Det er brukt «personvernansvarlig» i rutinene om den som har en del plikter og ansvar etter rutinene. Denne rollen kan erstattes med «personvernombud» «daglig leder» eller andre som er ansvarlig avhengig av hvordan man har organisert rollene i virksomheten. I mindre virksomheter har man ofte ikke en person som er ansvarlig for personvern, og da er det naturlig at daglig leder har rollen. Er virksomheten offentlig virksomhet eller andre som ikke har «daglig leder», kan dette erstattes med tilsvarende rolle i virksomheten.]*

**Disse rutinene gjelder for håndtering av personvernbrudd og varsling i [VIRKSOMHET] og er besluttet av daglig leder. Rutinene er en del av internkontrollrutinene i [VIRKSOMHET] og alle ansatte og andre som har befatning med personopplysninger i [VIRKSOMHET] plikter å sette seg inn i rutinene og følge disse.**

# Bakgrunn for rutinen

Avvik fra våre rutiner og personvernregelverket må håndteres på riktig måte for å sikre at personvernet til de vi behandler personopplysninger om ivaretas og sikres. Det er derfor etablert rutiner for å sikre at avvik og brudd på personvernet fanges opp, varsles riktig internt, varsles til Datatilsynet og de som er berørt av et eventuelt brudd, og at vi iverksetter tiltak for å begrense konsekvensene av brudd og reduserer risikoen for senere brudd.

For å sikre at avvik fra våre rutiner og lov-/regelverk håndteres riktig og at vi sikrer personopplysninger, skal alle avvik varsles internt til personvernansvarlig. Personvernansvarlig vil så vurdere om Datatilsynet og/eller til de som er rammet av bruddet (dvs. de personene som personopplysningene som bruddet omfatter kan knyttes til, som omtales som de «registrerte»).

# Rutine – Oversikt

* Et personvernbrudd er et brudd på sikkerheten som har betydning for personopplysninger som behandles, eller brudd på rutiner eller regelverk knyttet til personopplysninger, se nærmere i punkt 3 nedenfor.
* Ethvert brudd skal meldes umiddelbart etter dette oppdages til personvernansvarlig
* Bruddene skal loggføres og dokumenteres
* Personvernansvarlig vurderer om brudd skal meldes til Datatilsynet
* Personvernansvarlig vurderer også om bruddet skal meldes til de som personopplysningene gjelder (de registrerte)
* Er [VIRKSOMHET] databehandler, skal behandlingsansvarlig varsles om personvernbrudd uten ugrunnet opphold etter bruddet oppdages

Nærmere beskrivelse og forklaring av de enkelte punkter og begreper i rutinen følger nedenfor.

# Hva er personvernbrudd?

Et personvernbrudd er et brudd sikkerheten til personopplysninger ved at rutiner og prosedyrer (som våre interne rutiner eller personvernregelverket) for å sikre personopplysninger brytes, og at dette har ført til:

* Brudd på **konfidensialitet**, som at personopplysninger blir tilgjengelig (ved tilgang, overføring, lagring, spredning osv.) for personer eller i systemer hvor opplysningene ikke skal være tilgjengelig,
* brudd på **integritet**, som utilsiktet eller ulovlig tilintetgjøring, sletting, tap, endring osv. av personopplysninger, eller
* brudd på **tilgjengelighet**, som at personopplysninger som skal være tilgjengelig ikke er tilgjengelige for de som skal ha tilgang til opplysningene.

(Se personvernforordningen artikkel 4 nr. 12).

For at det skal være et personvernbrudd, må forholdet:

1. Gjelde **personopplysninger**, dvs. opplysninger som kan knyttes til fysisk person enten direkte eller indirekte,
2. **sannsynligvis ha ført til en risiko for personvernet** til personene som personopplysningene gjelder, og
3. ha **hatt virkning for konfidensialiteten, integriteten eller tilgjengeligheten** til personopplysningene.

Et personvernbrudd kan også være annet enn at rutiner eller prosedyrer brytes, bare kravene ovenfor gjelder.

Foreligger det en situasjon som dekkes av det ovenfor, eller du er usikker på om en slik situasjon foreligger, skal du melde fra til personvernansvarlig.

# Utbedring av personvernbrudd

Så snart brudd er avdekket, skal det vurderes tiltak for å utbedre bruddet. Rask utbedring av bruddet reduserer konsekvensene for de bruddet berører, og kan ha betydning for f.eks. Datatilsynets vurdering av konsekvenser av bruddet på personvernregelverket (som bøter).

Utbedring vil både være å redusere konsekvensene av bruddet som foreligger, og tiltak for å redusere sannsynligheten for at tilsvarende eller lignende brudd oppstår senere.

**Utbedring iverksettes umiddelbart**, og skal involvere personvernansvarlig (så snart det lar seg gjøre).

For alle brudd som ikke anses å være ubetydelige og ha ingen eller meget liten betydning for personvernet, skal det vurderes tiltak for utbedring.

Det skal så snart som mulig undersøkes hva som er konsekvensene av bruddet, herunder foretas risikovurdering av bruddets konsekvenser for de som er berørt av bruddet (de registrerte), som kan ha betydning for prioriteten for utbedring av bruddet. Det skal eventuelt lages en plan for å avdekke konsekvensene og årsaken til bruddet, som skal ha klare ansvarsforhold og et klart tidspunkt for når utbedring skal være gjennomført. **Tiltak for utbedring skal imidlertid prioriteres om det er nødvendig for å redusere konsekvensene av bruddet.**

Utbedring kan være teknisk utbedring, endring av rutiner, bedring av opplæring, endring i organisasjon mv. Tiltakene bør ha som mål å redusere risikoen for at tilsvarende brudd, eller brudd med samme årsak, skjer igjen. Det skal vurderes hvilke tiltak som er hensiktsmessige for å sørge for tilfredsstillende utbedring i det enkelte tilfelle.

Foreligger det eventuell restrisiko etter utbedring, skal daglig leder beslutte om restrisikoen kan aksepteres.

Plan for utbedring og tiltak som er iverksatt, samt dokumentasjon/bekreftelse på at utbedring er gjennomført skal lagres/arkiveres for å senere kunne dokumenteres.

# Varsling av brudd

## Intern varsling

**Alle personvernbrudd og andre avvik** fra våre rutiner og annet regelverk vi er underlagt **skal meldes** til personvernansvarlig. Det er en **meget lav terskel** for hva som skal meldes internt, og det skal ikke foretas noen nærmere vurdering om dette er et brudd som skal varsles til Datatilsynet eller de som bruddet gjelder før bruddet varsles internt.

Personvernbrudd og avvik skal **meldes umiddelbart** etter de oppdages/avdekkes.

Du melder ved å sende en e-post eller ta kontakt med personvernansvarlig på andre måter [KOMMENTAR: Kan erstattes med andre måter å varsle på, som f.eks. skjema eller meldingstjeneste]. Tas det kontakt per telefon, skal det sendes skriftlig melding så snart det lar seg gjør. Kontaktopplysninger til finner du her:

[TA INN].

Alle personvernbrudd skal logges, se skjema vedlagt denne rutinen. Den som melder inn brudd/avvik skal oppdatere loggen, men personvernansvarlig er ansvarlig for at loggen er oppdatert.

Personvernansvarlig skal etter intern melding er mottatt vurdere om Datatilsynet skal varsles, se punkt 5.2, om de registrerte skal varsles, se punkt 5.3, eller om behandlingsansvarlig skal varsles, i tilfelle det foreligger databehandlerforhold, se punkt 5.4.

## Varsling til Datatilsynet

### Vurdering om varsel skal skje

Personvernansvarlig er ansvarlig for å vurdere og beslutte om varsel skal sendes til Datatilsynet for det enkelte brudd. Det skal skje varsling til Datatilsynet dersom bruddet:

1. Gjelder **personopplysninger**, dvs. opplysninger som kan knyttes til fysisk person direkte eller indirekte.
2. Er et brudd på **sikkerheten** for personopplysningene, se ovenfor om hva som er et personvernbrudd under punkt 3.
3. Bruddet må **sannsynligvis medføre en risiko** for de personopplysningene gjelder, altså det er en sannsynlighet for at forholdet som beskrevet i punkt 3 har ført til brudd på sikkerheten for personopplysningene (brudd på konfidensialitet, integritet eller tilgjengelighet).
4. Hatt en **virkning for** **personvernet** til de personopplysninger gjelder. Dette medfører at de rettigheter som de personopplysningene gjelder har etter GDPR må ha vært skadelidende. Dette omfatter enhver og alle rettighetene som følger av GDPR, og finnes i det vesentlige i GDPR kapittel III.

(Se GDPR artikkel 33).

Det skal kun foretas varsel til Datatilsynet dersom bruddet **har eller vil** **medføre** en **risiko** for **personvernet** til de som personopplysningene gjelder. Det er derfor slik at **ikke alle brudd skal meldes**, og det må gjøres en vurdering til før bruddene meldes, og denne vurderingen skal dokumenteres. Datatilsynet skriver i sin veiledning at man må være tilnærmet helt sikker på at bruddet ikke vil medføre eller har medført noen risiko for de berørte, for at unntaket skal være oppfylt. Er man derfor usikker på om unntaket er oppfylt, er det bedre å melde til Datatilsynet for sikkerhets skyld.

### Hvordan varsel skal gjøres

Varsel til Datatilsynet skal gjøres **uten ugrunnet opphold** (dvs. varsel skal gis umiddelbart dersom det ikke foreligger grunner til at varsel ikke kan gis så snart) og senest innen 72 timer fra bruddet oppdages. Det kan også varsles før man har all informasjon om bruddet, f.eks. før man har avdekket årsaken til bruddet, (foreløpig melding) og at det deretter sendes oppdateringer om bruddet og tiltak som fattes.

Varsel gjøres **gjennom Altinn** av den som har varslingsfullmakt i Altinn for melding av personvernbrudd. Det bør avklares hvem som har varslingsfullmakt *før* det oppstår en situasjon hvor det skal skje en varsling.

Det er krav til **hva meldingen til Datatilsynet skal inneholde** (se GDPR artikkel 33 (3)). Før varsling skjer bør det lages en «kladd» av varselet for å involvere de rette personene og samle den riktige informasjonen for bruddet. Arbeidsskjemaet inntatt i vedlegg 2 til rutinene kan benyttes i denne sammenheng og inneholder også informasjon om hvilke opplysninger som skal meldes.

## Varsel til de berørte (de registrerte)

Dersom det er sannsynlig at bruddet vil kunne føre til **høy risiko**for de som person­opplysningene gjelder (de «registrerte»), skal disse varsles, se GDPR artikkel 34. Vurderingen er derfor lik som vurderingen over om varsling skal skje til Datatilsynet, men her må det være høyere risiko for at konsekvensen ved bruddet har betydning for personvernet til de personopplysningene gjelder.

Varsel til de registrerte skal imidlertid gjøres **uten ugrunnet opphold**, dvs. varsel skal gis umiddelbart dersom det ikke foreligger grunner til at varsel ikke kan gis så snart. Det må være gode/gyldige grunner for slik utsettelse – det er ikke tilstrekkelig at det ikke passer eller man skal avvente situasjonen til man vet mer.

Det skal allikevel ikke sendes varsel til de som personopplysningene gjelder dersom:

* Det er gjort egnede sikkerhetstiltak (tekniske og organisatoriske, dvs. endringer i rutiner mv.) for opplysningene som er berørt av bruddet, som f.eks. som å gjøre personopplysningene uleselige for personer som ikke har autorisert tilgang til dem, som ved kryptering,
* det er gjort etterfølgende tiltak som sikrer at det ikke lenger er sannsynlig at det foreligger høy risiko for personvernet til de som personopplysningene gjelder, eller
* det å varsle de personopplysningene gjelder vil innebære en uforholdsmessig stor innsats, f.eks. at det gjelder for mange personer. Dersom dette gjelder, så skal det i stedet bruddet offentliggjøres, f.eks. ved pressemelding eller gjennom media, eller at det gjøres lignende tiltak for effektiv informasjon.

Varselet til de personopplysningene gjelder skal inneholde det samme som varselet til Datatilsynet, se punkt 5.2 ovenfor. .

## Varsel til den behandlingsansvarlig som databehandler

Omfatter bruddet personopplysningene som [VIRKSOMHET] er **databehandler** for, dvs. personopplysningene behandles på vegne av en annen person eller selskap (som er behandlingsansvarlig), så skal bruddet varsles til den som er behandlingsansvarlig. Slik varsel skal skje **uten ugrunnet opphold**, dvs. varsel skal gis umiddelbart dersom det ikke foreligger grunner til at varsel ikke kan gis så snart. Det skal dokumenteres at varsel er gitt, dvs. varsel må skje skriftlig (eventuelt etter muntlig varsel er gitt om det må gjøres av tidshensyn).

Er det avtalt i databehandleravtalen med behandlingsansvarlig eller gitt andre instrukser/fullmakter om at varsel skal gjøres av databehandler, så skal vi melde til Datatilsynet og eventuelt til de personopplysningene gjelder (de berørte). Databehandleravtalen skal også gjennomgås for å se om det er andre krav overfor behandlingsansvarlig i tilfelle personvernbrudd.

# Kontroll og etterlevelse

Personvernansvarlig skal sørge for at denne rutinen er enkelt tilgjengelig for alle medarbeidere og at alle medarbeidere er kjent med rutinen. Rutinene skal også være tilgjengelig og kjent for andre enn medarbeidere som kan bli involvert i eller avdekke personvernbrudd eller avvik, som f.eks. innleide konsulenter.

Personvernansvarlig skal regelmessig, og minst årlig, kontrollere at rutinen er tilgjengelig, samt at alle som må være kjent med rutinen er kjent med denne og etterlever rutinen.

Personvernansvarlig skal følge opp utbedringstiltak og -planer for personvernbrudd og avvik for å kontrollere om disse er etterlevd og at risikoen for senere brudd er redusert.

Alle avvik og personvernbrudd skal rapporteres til daglig leder minst årlig, hvor det skal fremkomme hvilke personvernbrudd som er meldt til Datatilsynet og/eller de registrerte, samt følger av bruddene, tiltak for å utbedre og forhindre senere brudd og annet som er relevant for daglig leders vurdering av risikoen knyttet til behandling av personopplysninger i virksomheten.

# Dokumentasjon

All dokumentasjon knyttet til avvik og brudd skal arkiveres og være tilgjengelig til senere. Det skal føres logg for avvik og brudd fra disse oppdages og frem til tiltak er iverksatt og bruddet er utbedret (se vedlegg 1: Logg for personvernbrudd), inklusiv vurdering av om brudd skal meldes og melding til Datatilsynet og eventuelt de som personopplysningene gjelder.

# Mer informasjon

Se Datatilsynets veiledning for håndtering av avvik: <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvik/>.

# Vedlegg 1: Logg for personvernbrudd

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Dato loggføring** | **Beskrivelse (beskrivelse av hendelsen, hva skjedde, personopplysninger involvert, registrerte berørt, type brudd mv.). Eget dokument kan benyttes, med henvisning herfra.** | **Tidspunkt/-periode for avviket/bruddet** | **Meldt av (navn)** | **Vurdering om melding Datatilsynet og eventuelt de registrerte (hvis meldt, se ytterligere dokumentasjon).** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Vedlegg 2: Arbeidsskjema for varsling av brudd til Datatilsynet

Dette er et arbeidsdokument for å kunne arbeide mer effektiv på å utforme varsel til Datatilsynet. Endelig melding må sendes via Altinn. Husk at den som skal sende meldingen i Altinn må ha rettigheter til å sende varsler til Datatilsynet i Altinn. Det bør undersøkes hvem i virksomheten som har slike rettigheter før bruddet oppstår.

|  |  |
| --- | --- |
| **Hendelsen ble oppdaget:** | 06.06.2023 kl 00:00 |
| **Meldefrist:** | **06.06.2023 kl 00:00** |
| **Skjema utarbeidet av:** |  |
| **Tittel:** | (Kunde, oppdrag, beskrivelse mv.) |
| **Andre involvert:** | (Databehandlere, leverandører, kunder mv.) |

## Innsender

| **Felt i Altinn** | **Fylles inn i Altinn** | **Intern kommentar (tas ikke inn i Altinn)** |
| --- | --- | --- |
| Melder din virksomhet som behandlingsansvarlig eller databehandler | Behandlingsansvarlig  Databehandler |  |

Foretas innsendelse som databehandler, må det også fylles ut følgende:

|  |  |  |
| --- | --- | --- |
| Er avviket meldt til behandlingsansvarlig? | Ja  Nei |  |
| Legg inn navn på de virksomheter som er behandlingsansvarlige for personopplysningene som er berørt av avviket. |  |  |

## Beskrivelse av avviket

| **Felt i Altinn** | **Fylles inn i Altinn** | **Intern kommentar (tas ikke inn i Altinn)** |
| --- | --- | --- |
| Hovedårsak til avviket | Brudd på rutiner  Manglende rutiner  Menneskelig svikt  Teknisk svikt  Annet |  |
| Tidsrom for avviket | 06.06.2023 til 06.06.2023 |  |
| Når ble avviket oppdaget | 06.06.2023 kl 00:00 |  |
| Angi hvor mange personer som kan være berørt av avviket |  |  |
| Beskriv hva som har skjedd.  Begrunn her om det er behov for å unnta fra offentlighet hele/deler av meldingen, og hvilke hjemler som ligger til grunn. Datatilsynet vil gjøre en selvstendig vurdering av dette.  *Beskriv hva som har skjedd. Hvis mulig, beskriv hvor det skjedde.* | Dersom meldingen skal unntas fra offentlighet, kan dette inntas her, f.eks. på følgende måte (merk at det er opp til Datatilsynets egen vurdering om meldingen unntas fra offentlighet):  Unntatt fra offentlighet jf. offentlighetslovens § 13, jf. forvaltningslovens § 13 siden meldingen inneholder forhold om personlige forhold og/eller bedriftshemmeligheter, herunder informasjon om tekniske innretninger og forhold av betydning for informasjonssikkerheten i virksomheten. |  |
| Hvordan oppstod avviket?  *Beskriv hvordan avviket oppstod eller hva som er årsaken til at dette kunne skje. Dersom det er uklart, beskriv hva dere tror er årsakene til at avviket har skjedd.* |  |  |
| Beskrivelse av hva slags type personopplysninger som ble berørt |  |  |
| Hvilken relasjon har virksomheten til de personene som er berørt av avviket?  *Eksempler på relasjoner: Kunder, klienter, pasienter, ansatte, studenter, elever mv.* |  |  |
| Beskriv hvor personopplysningene befinner seg etter avviket. Skriv også hvor mange og hvilken type mottakere som kan ha fått eller sett opplysningene.  *Her kan virksomheten også oppgi om man ikke vet hvor personopplysningene er, om de er mottatt av andre brukere, eller om de er indeksert av søkemotor eller liknende.* |  |  |

## Konsekvenser

| **Felt i Altinn** | **Fylles inn i Altinn** | **Intern kommentar (tas ikke inn i Altinn)** |
| --- | --- | --- |
| Beskriv mulige konsekvenser avviket har medført for de berørte personene.  *Konsekvenser for personer kan for eksempel være:*   * *følsomme, fortrolige eller private opplysninger er eksponert,* * *fare for misbruk av personopplysninger,* * *fare for diskriminering,* * *fare for identitetstyveri eller bedrageri,* * *fare for økonomisk tap,* * *fare for omdømmetap, eller* * *annen betydelig ulempe for personen som er berørt.* |  |  |

## Tiltak

| **Felt i Altinn** | **Fylles inn i Altinn** | **Intern kommentar (tas ikke inn i Altinn)** |
| --- | --- | --- |
| Beskriv hvilke tiltak som er gjort og planlagt for å hindre gjentakelse, og hva som er gjort for å redusere potensielle skadevirkninger.  *Beskriv her hvilke rutiner som er innført eller endret, hva slags opplæring som er gitt, hvilke tekniske og fysiske tiltak som er iverksatt eller planlagt.* |  |  |

## Informasjon

| **Felt i Altinn** | **Fylles inn i Altinn** | **Intern kommentar (tas ikke inn i Altinn)** |
| --- | --- | --- |
| Har de berørte personene blitt informert? | Ja  Nei |  |
| Hvis ja, hvordan? | Avisoppslag  E-post  Personlig brev  Virksomhetens nettside  Annet |  |
| Hvis nei, forklar hvorfor de ikke har blitt informert |  |  |

## Kontaktinformasjon

| **Felt i Altinn** | **Fylles inn i Altinn** | | **Intern kommentar (tas ikke inn i Altinn)** |
| --- | --- | --- | --- |
| Navn og kontakt­informasjon til personvern­ombud eller kontakt­person hos virksomheten som kan gi mer informasjon om avviket. | Navn: |  |  |
| E-post: |  |  |
| Telefon: |  |  |
| Referanse  (Oppgi referansenummer som dere vil at skal følge saken. Dersom dette feltet er tomt, vil Datatilsynet sette navn på kontaktperson som deres referanse). |  |  |
| Alternativ kontaktperson | Navn: |  |  |
| E-post: |  |  |
| Telefon: |  |  |

## Vedlegg

Følgende vedlegg skal sendes inn:

(F.eks. skjermbilder, dokumenter, beskrivelse mv.)

*Vedlegg lastes opp ved å trykke på arkfanen «Oversikt – skjema og vedlegg».*