DOMSTOL-
ADMINISTRASJONEN

Rutine for håndtering av personvernavvik i DA

18.06.2021

Dok.type: Rutine for håndtering av personavvik	**Klassifisering**:	**Versjonsnr: 1.0**
Godkjent dato: 18.06.2001	**Godkjent av**: Solveig Moen	**Gyldig til**: Inntil videre
Revidert dato:	**Revisjonsansvarlig**: Personvernrådgiver	

Hva trenger du som vanlig medarbeider i DA å vite?

Målgruppen for denne rutinen er de som har definerte roller og oppgaver i arbeidet med håndtering av personvernavvik, herunder ledere. Den vanlige medarbeideren i DA trenger å vite følgende om dette:

Hva er et personvernavvik?

- Personvernavvik er behandling av personopplysninger i strid med lover eller interne rutiner i DA. Typiske eksempler er at
  - personopplysninger publiseres urettmessig
  - ansatte har tilgang til opplysninger de ikke har tjenstlig behov for
  - det mangler databehandleravtale med en underleverandør.

Når skal jeg rapportere et personvernavvik?

- I utgangspunktet skal du rapportere alt du tror kan være et personvernavvik. Så vil andre vurdere hvor alvorlig dette er og hvordan det skal håndteres videre. Du kan også snakke med personvernrådgiver eller personvernombud hvis du er i tvil om du skal registrere et personvernavvik.

Hvordan rapporterer jeg et personvernavvik?

- Bruk skjemaet på denne intranettsiden og send det på e-post til da.personvernavvik@domstol.no.
- Beskrivelsen av avviket skal identifisere hvilke/t krav det er brudd på, og må være forståelig for personell som ikke er involvert i avviket.

Innhold

1. Hensikt og formål

Formålet med rutinen er å bidra til

- at personvernavvik håndteres systematisk,
- at personvernlovgivning og interne bestemmelser blir fulgt,
- kontinuerlig læring og forbedring.

Registrering og håndtering av personvernavvik skal føre til positive konsekvenser for den enkeltes arbeidshverdag og virksomheten som helhet. Når personvernavvik følges opp systematisk bidrar dette til nyttig styringsinformasjon. Personvernavvik som avdekkes kan dermed effektivt bli lukket, og man hindrer at nye lignende avvik inntreffer på nytt.

2. Anvendelsesområder

Rutinen skal sikre forsvarlig og effektiv håndtering av personvernavvik i tråd med føringer som er gitt i:

- Personopplysningsloven
- DAs Personvernpolicy
- DAs Rutiner, som gjelder for alle ansatte og for alle områder og avdelinger i DA.

Personvernavvik skal aldri rettes mot person, men mot systemer, verktøy, interne rutiner, prosesser, lover og regler, etc.

Både ledere og medarbeidere er ansvarlige for å registrere personvernavvik som definert i denne rutinen.

3. Sentrale begrep

- **Personvernavvik**: Urettmessig behandling av personopplysninger og som er i strid med lover, interne rutiner og/eller retningslinjer som det er henvist til under punkt 4. Brudd på informasjonssikkerheten til personopplysningene, for eksempel ved urettmessig publisering eller tilgang til slike opplysninger.
- **Korrigerende tiltak**: Tiltak som er iverksatt for å fjerne årsakene til personvernavvik eller uønsket situasjon.
- **Preventive tiltak**: Tiltak som skal forhindre at personvernavvik oppstår på nytt.
- **Rotårsaksanalyse**: En mer dyptgående analyse som gjøres i alvorlige eller komplekse personvernavvik.

4. Roller og ansvar

4.1 Roller

- **Melder**: Melder kan være ansatt i DA, domstol, publikum, leverandør eller annen ekstern part.
- **Avviksteam**: Personvernrådgiver samt faste medlemmer fra INDU, HRK og IT. I tillegg vil andre ressurser som er relevant i hvert enkelt tilfelle også være en del av teamet. Avviksteamet skal sikre effektiv og forsvarlig behandling av avvik med middels og høy risiko for personvernet. Ref. vedlegg 3.
- **Avvikseier**: Den som har myndighet/ansvar i avdelingen/prosessen der personvern-avviket har oppstått. Avvikseier har myndighet til å ta beslutninger for å løse avviket, for eksempel hvis avviket utløser bruk av penger.
- **Utførende**: Den/de som skal gjennomføre korrigerende tiltak relatert til avviket.
- **DA-organisasjonen og domstolene**: Enhver nødvendig person, avdeling, prosess eller system i DA/domstolene som er identifisert for å hjelpe til med å løse avviket.
- **Personvernombud**: Rådgiver og den som rapporterer til Datatilsynet.
- **Datatilsynet**: Skal rapporteres til ved middels og høy risiko for personvernsikkerheten

4.2 Ansvar

Personvernrådgiver i DA

- Skal bidra til implementering og videreutvikling av denne rutinen, og sikre at den til enhver tid er oppdatert.
- Fører oversikt og dokumenterer saksbehandlingen av alle personvernavvik i eget Excel-skjema.
- Følger opp fremdrift i sakene og kaller inn til nødvendige oppfølgingsmøter der det ikke er nødvendig med avviksteam.
- Følger opp at avviksmeldingen blir håndtert i henhold til denne rutinen og ansvarsmatrise, samt at riktig mottaker blir informert der det ikke er nødvendig med avviksteam.
- Melder status tilbake til personen som opprinnelig meldte personvernavviket, samt påser at avviket blir lukket av ansvarlig person innen definert tid.
- Sammenstiller, analyserer og rapporterer oversikt over registrerte avvik til Avdelings-direktør Rett og styret. Ref. vedlegg 1.

Teamleder

- Fører oversikt og dokumenterer saksbehandlingen av alle avvik i eget Excel-skjema.
- Følger opp fremdrift i sakene og kaller inn til nødvendige oppfølgingsmøter.
- Personvernrådgiver er teamleder, men i dennes fravær ledes teamet av stedfortreder.

For avvik med *lav* risiko har leder, prosesseier eller andre som mottar avvik via personvern-rådgiver, ansvar for at tiltak blir iverksatt og at avviket blir «lukket». Ved *medium* og *høy* risiko for personvernsikkerheten, skal alltid avviksteam koples inn. Ref. vedlegg 7.1.

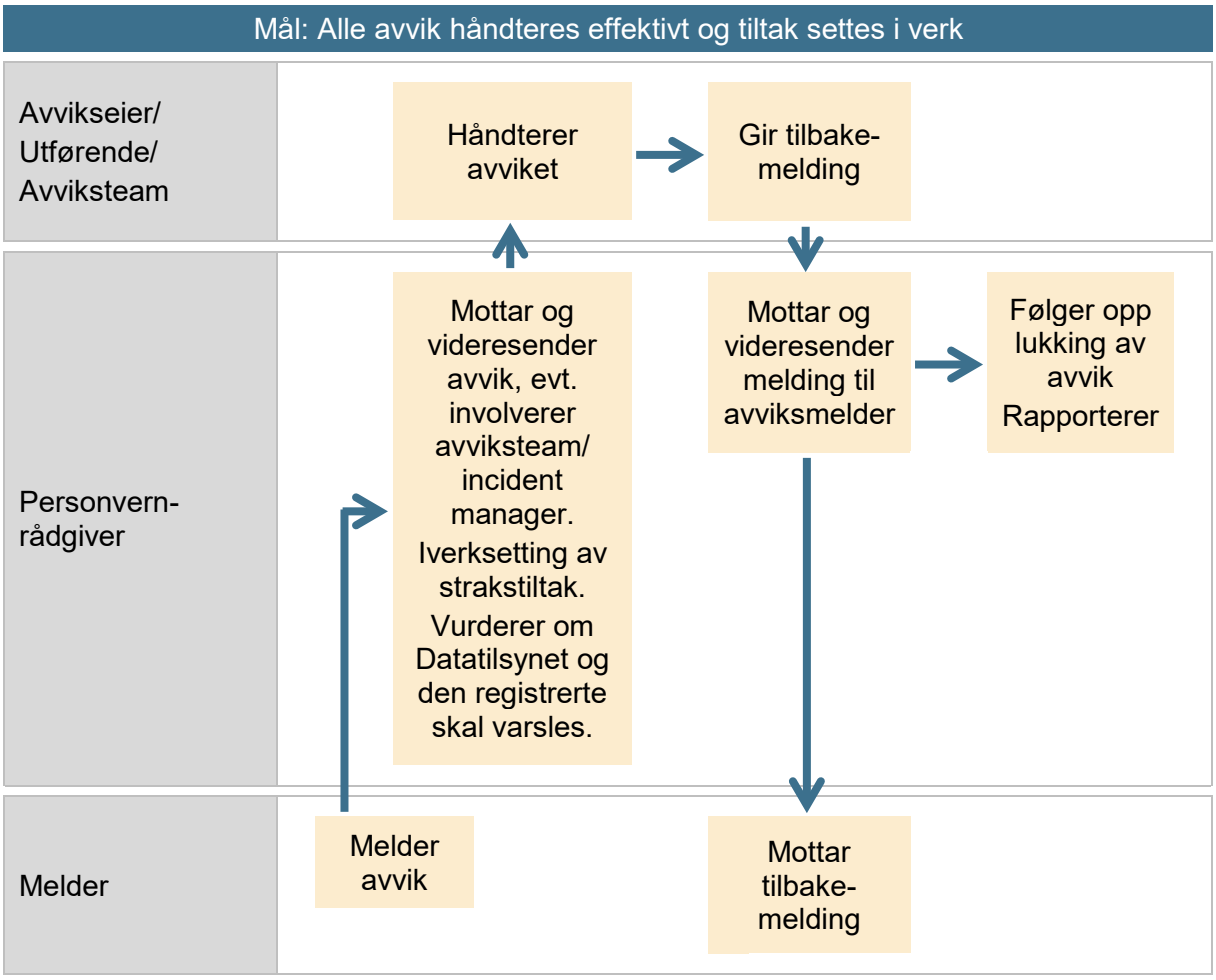
4.2.1 Ansvarlige

Avvikseier (A)	Den som har myndighet/ansvar i avdelingen/prosessen der avviket har oppstått.
Utførende (U)	Den/de som skal gjennomføre korrigerende tiltak relatert til avviket.
Konsulterende (K)	Den/de som kan bidra med hjelp og kunnskap for å løse avvik.
Informert (I)	Den/de som skal holdes orientert om progresjonen i håndteringen av avviket.

4.2.2 Ansvars- og involveringsmatrise

Prosessteg/ aksjoner	Melder	Avviks-team	Utfør-ende	Avviks-eier	DA-org.	Fagansvarlig informasjons-sikkerhet	PVO	Data-tilsynet
Første reaksjon					**U A**			
Registrering	**U**	**I**			**A**		**I**	**I**
Gjennomgå avviket	**U**	**A U I K**	**U**		**K**	**K I**		
Sette avviks-eier og tiltakseier		**U**	**I**	**I K**	**K**	**A**		
Håndtere avviket		**I**	**U**	**A**	**K**			
Bestemme tiltak som løser avviket	**I**	**I**	**U**	**A**				
Rotårsaks-analyse	**K**	**K I**	**U**	**A**		**I**	**I**	**I**
Evaluering og lukking	**I**	**U**		**A I**		**I**	**I**	**I**

4.3 Flytskjema prosess for avvikshåndtering



4.4 Personvernavvik i domstolene

Personvernombudet bistår i håndtering av personvernavvik som er oppstått i domstolene, og melder eventuelle avvik til Datatilsynet.

5. Prosess for håndtering av personvernavvik

Avhengig av alvorlighetsgrad, ta grep for å kontrollere og korrigere avviket umiddelbart hvis mulig.

5.1 Grensesnitt mot incidentprosessen

Incidentprosessen er IT sin prosess for å håndtere hendelser. I noen tilfeller vil en incident også være et brudd på personvernreglene. Brukersenteret skal da fylle ut skjema for personvernavvik med den informasjon som foreligger på dette tidspunktet og sende det til da.personvernavvik@domstol.no ref. punkt 5.2. Personvernrådgiver/avviksteamet er ansvarlig for videre oppfølging av avviket.

Hvis avviksteamet har behov for råd, veiledning eller trenger å komme i kontakt med ressurser på IT, kan produksjonsleder på Brukersenteret kontaktes på telefon 73 56 71 45 eller epost: produksjonsleder@domstol.no. Brukersenteret kan ved behov involvere driftspartner.

5.2 Rapporter avviket

- Bruk skjemaet på denne intranettsiden og send det på e-post til da.personvernavvik@domstol.no.
- Se pkt. 3 om definisjon på hva et personvernavvik er.
- Beskrivelsen av avviket skal identifisere hvilke/t krav det er brudd på.
- Beskrivelsen av avviket må være forståelig for personell som ikke er involvert i avviket.

5.3 Mottak av avvik

Avvik mottas hos personvernombud/personvernrådgiver.

- Personvernrådgiver vurderer, enten alene eller ved konsultasjon med medlemmer i avviksteamet, om avviksteam skal koples inn.
- Avviket skal kategoriseres hvis det er mulig på dette stadiet (alvorlighetsgrad – skal det for eksempel meldes til Datatilsynet?).
- Den relevante prosessen/avdelingen der avviket har skjedd involveres og avvikseier skal identifiseres.
- Personvernavvik med *lav* risiko for personvernsikkerheten behandles uten involvering av avviksteam (se vedlegg 1 og 2).
- Avviksteam samles hvis det er *medium* eller *høy* risiko for personvernsikkerheten (se vedlegg 1 og 2). Personvernrådgiver kaller inn aktuelle ressurser og eventuelt personvernombud. ***NB! Personvernombudet melder avviket til Datatilsynet via Altinn innen 72 timer. Vurder om den registrerte skal varsles.*** Ved *høy* risiko skal innkalling til avviksteam gå foran andre gjøremål.

5.4 Behandling av avvik

Det vil alltid være en undersøkende dialog i starten av prosessen avhengig av type avvik som har oppstått. Det vil derfor være vanskelig å sette opp en helt nøyaktig rekkefølge på når de forskjellige stegene i prosessen skjer. Punktene under er derfor bare ment som veiledende.

- Identifiser hvor avviket har oppstått og hvem som naturlig vil være avvikseier.

- Identifiser effektive korrigerende tiltak og sett tidsfrist for utførelse.
- Avklar hvilke ressurser som er nødvendige for å implementere korrigerende tiltak.
- Avvikseier kan utpeke andre til å utføre de konkrete tiltakene som er besluttet (utførende).
- Avviket lukkes når alle korrigerende/preventive tiltak er utført.
- Hvis avviket er alvorlig (høy risiko) og det er flere årsaker til at det har oppstått, vurder om en grundigere rotårsaksanalyse bør gjøres. Avhengig av resultatet av rotårsaksanalysen må en vurdere hvilke preventive tiltak som er hensiktsmessige å iverksette. Sett tidsfrist også på dette.
- Evaluering av avvikshåndteringen og det enkelte avvik er svært viktig. For å sikre læring etter personvernavvik vil etablering av «Lessons Learned» være nyttig.

6. Eierskap og implementering

Direktør RETT er den formelle eieren av denne rutinen. Rutinen er dynamisk og oppdateres ved behov.

7. Vedlegg

7.1 Kategorisering/prioritering av avvik

Risiko/ prioritet	Kriterier	Aksjon/eskalering	Melding Datatilsynet?	Informasjon til den registrerte?	Rotårsaks-analyse?
Høy	Data-tilsynet	Involvere: • Direktør • Ansvarlig avd.direktør • Avviksteam • Kommunika-sjonsavdeling	JA	JA	JA
Middels	Data-tilsynet	Involvere: • Ansvarlig avd.direktør • Avviksteam	JA	Må vurderes konkret	Må vurderes konkret
Lav	Data-tilsynet	Ingen eskalering	NEI	NEI	NEI

7.2 Veiledning vurdering av alvorlighet ved brudd på personopplysnings-sikkerheten

Personvern-konsekvens	Konfidensialitet	Integritet	Tilgjengelighet
Svært stor konsekvens	Uautorisert innsyn/tilgang til store mengder følsomme/sensitive opplysninger. Ingen logging. Stor spredningsfare.	Uopprettelig tap av data eller uautorisert endring av data uten at det oppdages.	Uopprettelig tap av tilgang eller svært lang nedetid. Viktige opplysninger utilgjengelige og lar seg ikke skaffe i overskuelig fremtid. Mangelen på tilgjengelighet kan føre til alvorlig økonomisk tap eller fare for helse.
Stor konsekvens	Uautorisert innsyn/tilgang til følsomme/sensitive personopplysninger. Ingen logging. Stor spredningsfare.	Betydelig tap av data for 24 timer eller mer eller uautorisert endring av data som er vanskelig å oppdage eller ikke varsles.	Svært krevende oppretting, lang nedetid, viktige opplysninger utilgjengelige. Opplysninger utilgjengelige på et tidspunkt det er viktig å ha de tilgjengelige.
Middels konsekvens	Uautorisert innsyn/tilgang til følsomme/sensitive opplysninger. Innsyn logges. Spredningsfare.	Tap av data for 6-24 timer tilbake eller uautorisert endring som varsles automatisk til administrator.	Krevende oppretting. Ikke uvesentlig nedetid. Potensielt viktige opplysninger som er utilgjengelige.
Liten konsekvens	Uautorisert innsyn/tilgang til følsomme opplysninger. Innsyn logges/varsles administrator. Liten spredningsfare.	Tap av data for 0-6 timer tilbake Uautorisert endring varsles automatisk til bruker og administrator.	Lett opprettelig, kort nedetid, lite viktige opplysninger som er utilgjengelige.
Svært liten konsekvens	Uautorisert innsyn/tilgang til lite følsomme opplysninger. Innsyn logges/varsles automatisk. Svært liten spredningsfare.	Tap av data men blir umiddelbart opprettet. Uautorisert endring varsles automatisk og er kun mulig på lite følsomme opplysninger.	Umiddelbar oppretting, svært kort nedetid, svært lite viktige opplysninger som er utilgjengelige.

7.3 Sammensetning av avviksteamet

Behov som må dekkes i teamet	Rolle	Fast eller innkalles ved behov?	Sted-fortreder?
Lede teamet, innkalle til møter, følge opp tiltak, gjøre innledende vurdering av avvik – spesielt prioritering	Teamleder	Fast person, personvernrådgiver	Ja
Ressurser fra INDU, HRK og IT	Utnevnte personer fra avdelingene	Faste personer	Ja
Kommunikasjon – hvordan på best mulig måte kommunisere avviket til omverdenen	Kommunikasjons-ansvarlig	Vurderes fra gang til gang	
Juridisk kompetanse knyttet til rettspleieunntaket, personvernregler, osv	Jurist	Dekkes av personvernombud ved behov	
Gjennomføre tiltak	Utførende	Rollen er fast, men det er alltid en vurdering hvem som skal delta	
Forankre beslutninger	Avvikseier	Rollen er fast, men det er alltid en vurdering hvem som skal delta	
Rotårsaksanalyse av avviket og logger disse for å sikre læring og forhindre at lignende avvik oppstår på nytt. Lage referat ang. avviket (?). Analysere, teste, spore og registrere avviksrapporter. Formidle informasjon om oppståtte avvik og hva som er viktig å passe på i organisasjonen.	Personvernrådgiver	Fast person – dekkes av teamleder	
Rolle som kjenner informasjonssikkerhet - kan gi verdifulle innspill til hvordan avviket skal bli håndtert. Søker aktivt etter sikkerhetshull i organisasjonen.	Fagansvarlig informasjonssikkerhet	Involveres ved behov, holdes orientert om avvik	
Incident manager – en rolle som skal følge spesielt kritiske IT-avvik. Tar kontakt med relevant systemansvarlig/ -ressurs, etc.	Incident manager	Fast person	Ja