	Tittel Prosedyre for håndtering av avvik på personvernsikkerheten	
	Dokumentnummer 2023-1467	Dokumenttype Prosedyre
Forfatter Ole-Alexander Reinfjell	Godkjent av Ann-Cathrin Becken	Godkjent dato 14.11.2023
Versjon 1	**Dokumentet er ukontrollert dersom skrevet ut eller nedlastet**	

PROSEDYRE FOR HÅNDTERING AV AVVIK PÅ PERONSVERNSIKKERHETEN

1 HENSIKT

Denne prosedyren beskriver hvordan NND håndterer avvik på personopplysningssikkerheten. En tilfredsstillende personopplysningssikkerhet forutsetter at avvik avdekkes, håndteres og unngås for fremtiden ved at NND iverksetter passende tiltak.

2 ANSVAR OG MYNDIGHET

Alle ansatte, sekonderte og innleide har ansvar/plikt til å varsle ved avvik på personvernsikkerheten.

Personvernombudet skal involveres ved avvik, mens det er informasjonseier som skal behandle avvik og saksbehandle dette.

Det er juridisk avdeling som eier prosedyren, mens behandlingsansvarlig/informasjonseier er utførende part.

3 OMFANG

Hva er et avvik:
Brudd på personopplysningssikkerheten (avvik), er sikkerhetsbrudd som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på en annen måte behandlet i NND.

Typiske avvik:

a. **Konfidensialitetsavvik**, uautorisert bruk eller tilfeldig avsløring av personopplysninger
b. **Integritetsavvik**, uautorisert eller tilfeldig endring av personopplysninger
c. **Tilgangsavvik**, uautorisert eller tilfeldig tap av tilgang til eller ødeleggelse av personopplysninger

Slik avvik kan skyldes:

d. **Tekniske feil**, for eksempel at et nettsted eller en database gir åpen tilgang til personopplysninger
e. **Menneskelige feil**, for eksempel feilhåndtering eller -vurderinger, som mangelfull nedlåsing av personopplysninger, at personopplysninger sendes til uvedkommende og at dokumenter eller lagringsenheter med personopplysninger forelegges
f. **Eksterne trussel aktører**, som hackere eller andre stater, som forsøker å få tak i eller ødelegge sikkerhetsgradert informasjon, og informasjon som inneholder personopplysninger

4 PROSESSTILKNYTNING

Prosedyren er knyttet til prosessområdet for Personvern.

5 BESKRIVELSE

Nr.	Rekkefølge på aktivitet/oppgave	Ansvar
1	**Intern varsling:** Intern varsling av avvik er avgjørende for å håndtere avvik på en tilfredsstillende måte. Alle ansatte har en plikt til å gi melding om avvik og mistanke om avvik for å sikre at disse avdekkes og håndteres av NND. Mulige avvik skal umiddelbart varsles iht varslingsknappen i Kjernen (ringeliste). Videre skal informasjonseier eller den som mottar varslet gjennomgå avviket og registrere det i Better. NNDs personvernombud regnes som en relevant ressursperson ved ethvert avvik. Informasjonseier, personvernombudet og juridisk avdeling er ansvarlig for håndteringen av avviket, herunder etterfølgende dokumentasjon og læring/oppfølging. Varslet i Better skal inneholde en beskrivelse av: - Avviket, herunder hva det innebærer og hvordan det har oppstått - Når avviket ble oppdaget - Hvem avviket ble oppdaget av - Hvilket system som er rammet av avviket - Hvilken skade som har eller kan ha oppstått som følge av avviket - Hva som er gjort innledningsvis for å stanse eller begrense skaden Alle interne varsler skal dokumenteres i samsvar med punkt 4. Dersom NND kommer til at virksomheten kan stå overfor et avvik, skal følgende tiltak vurderes umiddelbart, i den grad de er relevant og nødvendig: - Kartlegge hendelsesforløpet - Finne ut hvordan eventuelle skader kan begrenses - Slå av eventuelle systemer som har eller kan ha ført til avviket, i den grad det er nødvendig for å begrense eventuelle skader og det ikke medfører skade på andre viktige interesser - Stanse ytterligere uautorisert adgang til det aktuelle systemet, for eksempel ved å endre passord eller avvikle brukerprofiler - Iverksette tiltak for å gjenopprette tapte data og begrense eventuelle skar forårsaket av avviket	

	- Dersom det er mistanke om kriminell aktivitet, varsle/anmelde forholdet til politiet - Sikre bevis for etterforskning, for eksempel ved hacking eller uautorisert tilgang fra en ansatt Særlig om databehandlere: NNDs databehandlere skal gi en melding til NND *uten ugrunnet opphold* dersom de har fått kjennskap til et avvik. NND skal selv ta stilling til om et innmeldt avvik er meldingspliktig til Datatilsynet, se punkt 2 og 3. Databehandlere kan etter omstendighetene gi melding til Datatilsynet, men dette forutsetter at hver enkelt databehandler har fått fullmakt til dette. NND gir eventuelt slik fullmakt i databehandleravtale.	
2	**2 Varsel til Datatilsynet:** **2.1 Hvilke avvik skal varsles om til Datatilsynet?** NND skal gi melding til Datatilsynet dersom avviket vil medføre *en risiko for fysiske personers rettigheter og friheter.* Spørsmålet beror på en objektiv og konkret risikovurdering, hvor risikoens sannsynlighets- og alvorlighetsgrad er relevante momenter. I vurderingen av om slik risiko foreligger, skal NND ta hensyn til: - Hvilke personopplysninger avviket gjelder, herunder om det er særlige personopplysninger eller ordinære personopplysninger - Hvor mange personer som er berørt av avviket - Hvorvidt avviket medfører en risiko for omdømme tap, identitetstyveri, økonomisk tap og/eller sikkerhetsrisiko for de berørte - Hvorvidt det er viktig å iverksette tiltak for å redusere virkningen av avviket - Hva som forårsaket avviket - Hvem som har fått eller kan ha fått tilgang til personopplysningene Merk at melding til Datatilsynet ikke er nødvendig dersom det *sannsynligvis ikke* vil medføre slik risiko. Situasjoner det er avvik sannsynligvis ikke vil medføre risiko kan for eksempel være at personopplysningene allerede er offentlig tilgjengelig, eller at de er kryptert slik at informasjonen er uleselig for uautoriserte personer. Alle avvik, uavhengig av om avviket skal meldes til Datatilsynet eller ikke, skal dokumenteres i samsvar med punkt 4. Dersom NND kommer til at det ikke foreligger slik risiko, har NND bevisbyrden for å bevise dette. NNDs risikovurderinger skal dermed også dokumenteres i samsvar med punkt 4.	

2.2 Prosedyre for varsel til Datatilsynet

Dersom NND kommer til at avviket vil medføre risiko for fysiske personers rettigheter og friheter, har NND meldeplikt til Datatilsynet. Datatilsynet skal varsles med eget skjema via Altinn, evt i form av brev.

<u>Meldingspliktige avvik skal meldes til Datatilsynet innen fristen</u>
Avviksmeldingen til Datatilsynet skal gis *uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til avviket.* Begrepet *kjennskap til* innebærer imidlertid at ikke enhver mistanke om brudd vil utløse friststarten. NND ha en viss anledning til å gjøre undersøkelser med sikte på å avklare hvorvidt det faktisk foreligger et avvik. Det er derfor avgjørende at alle ansatte følger varslingsrutinen.

Dersom en databehandler har gitt NND melding om et avvik, løper fristen i utgangspunktet fra det tidspunktet databehandleren ble klar over avviket. NND har derfor inntatt i sine databehandleravtaler at databehandlere skal gi melding om eventuelle avvik umiddelbart.

<u>Eventuelle fristoversittelser skal begrunnes</u>
Dersom NND ikke gir Datatilsynet melding om avviket innen fristen på 72 timer, skal årsakene til forsinkelsen oppgis. NNDs vurdering skal dokumenteres i samsvar med punkt 4.

<u>Adgang til å gi trinnvis informasjon</u>
Dersom og *i den grad* det ikke er mulig å gi all informasjon samtidig, kan Datatilsynet få informasjon i flere omganger, for eksempel hvis hendelsesforløpet er uklart eller mer informasjon må innhentes.

Dersom det er behov for trinnvis informasjon, skal NND:

- Gi informasjon om behovet for trinnvis informasjon i det første varslet til Datatilsynet
- Gi ytterligere informasjon uten ugrunnet opphold

NND kan også gi utfyllende informasjon hvis ny informasjon som Datatilsynet bør vite om kommer frem.

<u>Innhold</u>
Ifølge GDPR art. 33 nr. 3 skal meldingen til Datatilsynet inneholde minst:

a. Beskrive arten av avviket, herunder, når det er mulig
    I. Kategoriene av og omtrentlig antall registrerte som er berørt
    II. Kategoriene og omtrentlig antall registreringer av personopplysninger som er berørt
b. Inneholde navnet og kontaktopplysninger til personvernombudet eller annet kontaktpunkt
c. Beskrive de sannsynlige konsekvensene av avviket
d. Beskrive tiltakene som den behandlingsansvarlige har truffet eller foreslår for å treffe for å håndtere avviket, herunder,

	dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger som følge av avviket Se egen veiledning under lenker – Datatilsynet og hvordan melde avvik	
3	**3 Varsel til de berørte** **3.1 Hvilke avvik skal varsles om til de berørte?** NND skal gi melding til de registrerte personene som er rammet av avviket (heretter «de berørte») dersom det er sannsynlig at avviket *vil medføre en høy risiko* for deres *rettigheter og friheter*. En eventuell meldeplikt til de berørte kommer i tillegg til meldeplikten til Datatilsynet, se punkt 2. Vurderingen skal bestå av en objektiv og realistisk kartlegging og vurdering av uønskede hendelser som kan ramme de berørte. Ifølge Datatilsynet skal formuleringen *rettigheter og friheter* forstås vidt, slik at den omfatter: - Rettigheter og friheter etter GDPR, for eksempel retten til sletting - Rettigheter g friheter etter annen lovgivning, for eksempel retten til privatliv og frihet fra diskriminering - Avtaler, for eksempel retten til å motta lønn Det europeiske Personvernrådets (EDPB) retningslinjer for hvilke avvik som er meldepliktig og ikke er tilgjengelig under veiledning. Vurderingen skal dokumenteres i samsvar med punkt 4. **3.2 Prosedyre for varsel til de berørte** Dersom NND kommer til at avviket vil medføre høy risiko for fysiske personers rettigheter og friheter, se punkt 3.1, har NND meldeplikt til de berørte, med mindre det er grunnlag for unntak, se punkt 3.3. Avviket skal kommunisere direkte til den berørte på en enkel og tilgjengelig måte, slik at det gir størst sjanse for at alle de berørte får vite om bruddet. Det er viktig at meldingen ikke sendes sammen med annen informasjon, for eksempel felles e-post, slik at meldingen blir mindre synlig. <u>Meldingspliktige avvik skal meldes til de berørte innen fristen</u> Melding til de berørte skal gis *uten ugrunnet opphold*, som betyr at meldingen skal gis så snart som mulig. <u>Innhold:</u> Ifølge GDPR art. 34 nr. 2 skal meldingen til den berørte inneholde: a. En klar og tydelig beskrivelse av arten av avviket og minst	.

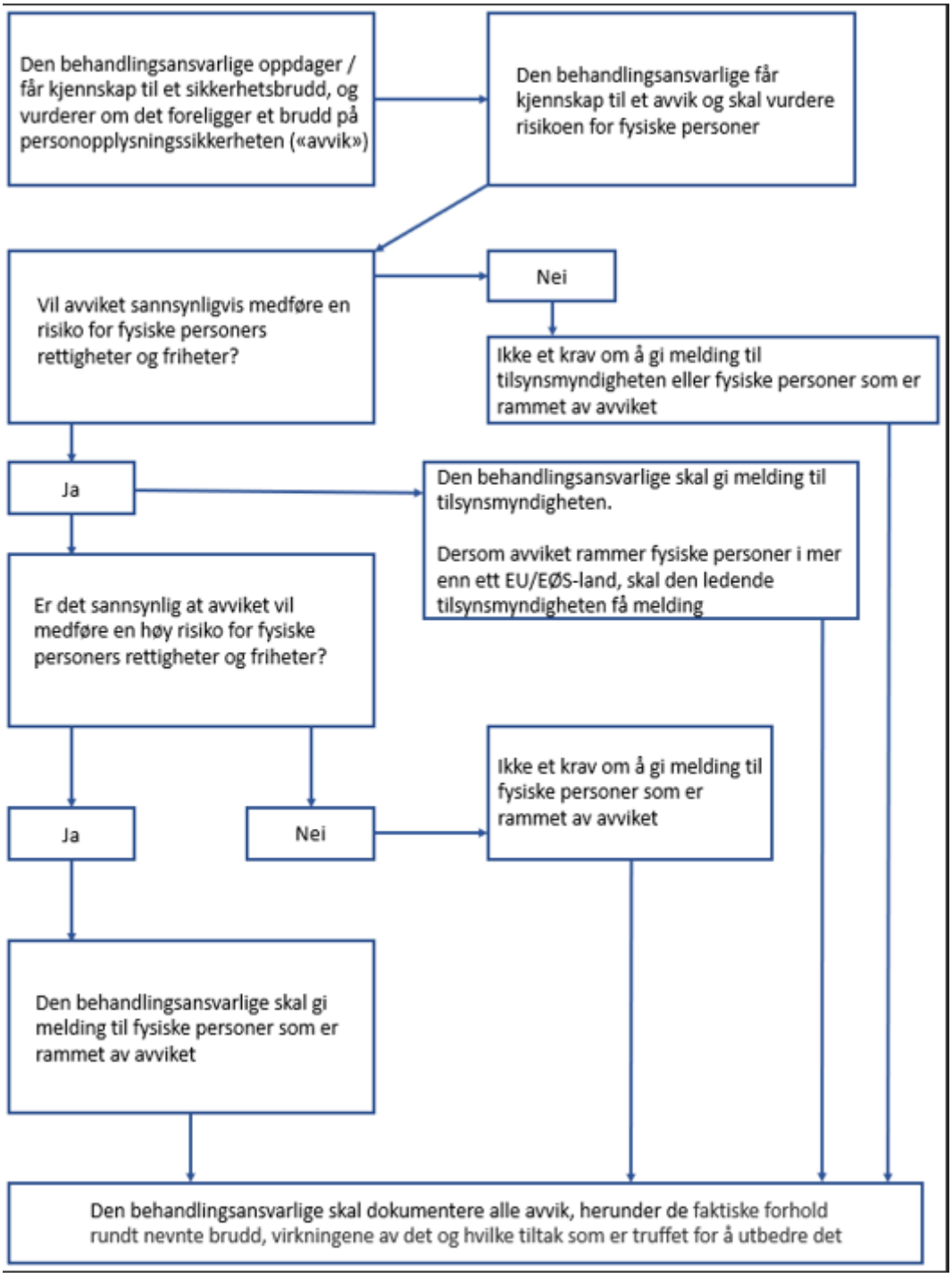
	b. Inneholde navnet og kontaktopplysningene til personvernombudet eller annet kontaktpunkt c. Beskrive de sannsynlige konsekvensene av avviket d. Beskrive tiltakene som den behandlingsansvarlige har truffet eller foreslår å treffe for å håndtere avviket, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger som følge av avviket **5.3 Unntak fra meldeplikten til de berørte** Ifølge GDPR art. 34 nr. 3 gjelder ikke meldeplikten dersom a. NND har gjennomført egnede tekniske og organisatoriske sikkerhetstiltak som er blitt anvendt på personopplysningene som er berørt av avviket, sørlig tiltak som gjør personopplysningene uleselige for enhver person som ikke har autorisert tilgang til dem, for eksempel kryptering b. NND har truffet etterfølgende tiltak som sikrer at det ikke lenger er sannsynlig at den høye risikoen for de registrertes og friheter vil oppstå *Eller* c. Det vil innebære uforholdsmessig stor innsats – allmennheten skal isteden underrettes, eller det skal treffes et lignende tiltak som sikrer at de registrerte underrettes på en like effektiv måte Et egnet sikkerhetstiltak kan for eksempel være bruk av fjernsperringssystemer til å beskytte personopplysninger. Blir systemet kort tid etter at en jobbtelefon kommer på avveie, kan forholdene tale for at det ikke er sannsynlig at slik risiko foreligge. NND skal kunne dokumentere ovenfor Datatilsynet at ett av alternativene er oppfylt, herunder hvordan unntakene ble vurdert, se punkt 4.	
4	**4 Dokumentasjon av avvik** NNS skal dokumentere *ethvert* avvik, inkludert avvik hos databehandlere, uavhengig av om avviket er meldepliktig til Datatilsynet eller ikke. Ett av formålene med dokumentasjonsplikten er at Datatilsynet skal kunne kontrollere om NND har handlet i samsvar med GDPR art. 33, jf. GDPR art. 5 nr. 2. Ifølge GDPR art 33. nr. 5 skal NND dokumentere a. De faktiske forholdene rundt avviket b. Virkningen avviket har c. Tiltakene som er truffet for å utbedre avviket Vurderingen/begrunnelser for avgjørelser som blir tatt i forbindelse med avvik, skal også dokumenteres, og NND skal også dokumentere	

	- Begrunnelse for hvorfor NND mener det ikke er meldeplikt, herunder risikovurderinger - Begrunnelse for forsinket varsling NND skal også dokumentere interne varslinger og varslinger fra databehandlere. NNDs rapporter skal arkiveres i Documaster, og det er behandlingsansvarlig/informasjonseier som er ansvarlig for at rapporten utarbeides og arkivers i samsvar med denne prosedyren. Saksbehandlingen av avvik skal følge prosess for «Forbedring- og avvikshåndtering» og behandles i Better.	
5	**5 Læring og oppfølging** NND ønsker å forebygge og forhindre fremtidige avvik. Etter at et eventuelt avvik er håndtert, skal NND vurdere om eksisterende tiltak er tilstrekkelige for å hindre nye, lignende avvik. NND skal vurdere - Hvorfor eksisterende tiltak ikke hindret avviket - Om eksisterende systemer/styrende dokumenter bør tilpasses/endres for å hindre nye avvik - Om det har vært tilstrekkelig kontroll med systemene/styrende dokumenter - Om leverandør/tjenestetilbydere bør byttes ut - Om ansatte og/eller innleide ressurser var klar over at avviket kunne oppstå - Om det er behov for ytterligere opplæring for å hindre fremtidige avvik - Om det var satt av nok ressurser til å håndtere avvik NNDs vurderinger skal være en del av etterkontrollen i Better og rapporten i sin helhet skal arkiveres i Documaster. Dersom vurderingen avdekker et behov for nye tiltak og/eller endringer i denne prosedyren, skal dette iverksettes innen rimelig tid.	

6 REFERANSE

<Referanse til eksterne krav, evt. interne krav (policy) som styrer prosedyren>

VEDLEGG 1 - FLYTSKJEMA



7 ENDRINGSLOGG

Dato	Vers. nr.	Angi endringen og årsaken. Referer til hvor i dokumentet endringen er foretatt
14.11.2023	1	Første versjon
	2	
	3	
	4	
	5	
	6	
	7	