Personvern

Fastsette behandlingsgrunnlag | Behandle opplysninger | Rette og slette opplysninger | Håndtere avvik på personopplysnings-sikkerheten

Personvern

Prosesseier: Annette Ansteensen | Godkjent av: Ann-Cathrin Becken | Godkjent dato: 7.11.2023 | Publisert versjon: 1

Hensikt:

Dette prosessområdet er til for å sikre at NND ivaretar fysiske personers rett til vern av sine personopplysninger i henhold til personvernloven og GDPR-forordningen.

Omfang:

NND behandler personopplysninger og er dermed behandlingsansvarlig i henhold til loven. Som behandlingsansvarlig må NND sørge for å være i samsvar med personvernlovgivningen.

Videre omfatter dette området flere prosesser som samlet skal bidra til at prosessens hensikt blir oppfylt. Dette forutsetter blant annet kunnskap om lovgivningen og interne prosedyrer for gjennomføring og kontroll, varsel til Datatilsynet og varsel til de registrerte.

Informasjon om rettigheter for de registrerte skal gis uoppfordret og er beskrevet i personvernerklæringene.

Behandlingsinformasjon skal gis på forespørsel.

Inngang:

Prosessen starter med at NND mottar, lagrer og behandler personopplysninger.

Resultat:

Når prosessen er gjennomført oppfyller NND lovens krav til ivaretagelse og behandling av personopplysninger.

Roller og rollenes ansvar i prosessen

Utførende roller i prosessen	***Rollens oppgaveansvar/myndighet i denne prosessen***
Behandlingsansvarlig/informasjonseier	Den som eier/forvalter/behandler opplysningene til de registrerte. Skal være ansvarlig for behandling av avvik på personopplysningssikkerheten. Øverste behandlingsansvarlig er direktør i NND.
Personvernombud	Rådgivende part for både registrerte og behandlingsansvarlig. Bistår ved avvik. Kravstiller og kontrollerende part.
Prosesseier	Forvalter prosessen og dens bruk i NNDs daglige virke. Er kontaktperson ved brudd.

Systemeiere	Må ved innsyn bistå med uthenting av opplysninger fra systemet de er systemeier for. Sørge for systemspesifikke sletteprosedyrer.

Eksterne krav/føringer til prosessen:

Kravdokument (lovverk, standarder o.l.)
Lov om behandling av personopplysninger (personopplysningsloven)
GDPR-forordningen
Internkontrollforskriften
Flere relevante fra Datatilsynet
Lov om Schengen informasjonssystem (SIS)
Forskrift om behandling av personopplysninger
Overgangsregler om behandling av personopplysninger
Forskrift om kameraovervåking i virksomhet
Forskrift om arbeidsgivers innsyn i epostkasse og annet elektronisk lagret materiell
Forskrift om Schengen informasjonssystem (SIS-forskriften)

Virksomhetskrav:

Kravdokument (Politikk, strategi og program o.l.)
NNDs vurdering av GDPR i virksomheten – siste godkjente versjon
Personvernerklæring

Dokumentert informasjon (styrende dokumentasjon)

Prosedyre

- Prosedyre for håndtering av avvik på personvernsikkerheten

Øvrig

- Personvernerklæring for ansatte og innleide
- Varsling om brudd på personopplysningssikkerheten - avvik

Fastsette behandlingsgrunnlag

Prosesseier: Annette Ansteensen | Godkjent av: Ann-Cathrin Becken | Godkjent dato: 7.11.2023 | Publisert versjon: 1

Inngang:

NND igangsetter en prosess som involverer personopplysninger og trenger behandlingsgrunnlag.

Omfang/Aktiviteter:

NND behandler personopplysninger og særlige sensitive personopplysninger, og dette gjør vi for å kunne utføre ulike arbeidsprosesser o.l.

NND har definert følgende formål:

1. Drift av administrative rutiner (som lønn, HR etc)
2. Drift av IT systemer (som nettverk og VPN)
3. IT sikkerhetsmekanismer og gjennomganger, eventuelle hendelsesundersøkelser
4. Gi allmenn og rettet informasjon om NNDs virksomhet til interesserte parter, herunder forbedre informasjon som gis basert på bruksmønster

NND behandler personopplysninger basert på følgende grunnlag i GDPR-forordningen:

- Artikkel 6, bokstav a: Den registrerte har samtykket til behandling av sine personopplysninger for ett eller flere spesifikke formål
- Artikkel 6, bokstav b: Nødvendig for å oppfylle en avtale som den registrerte er part i
- Artikkel 6, bokstav c: Nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige
- Artikkel 6, bokstav f: Nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger
- Artikkel 9, bokstav g: Behandlingen er nødvendig av hensyn til viktige allmenne interesser, på grunnlag av unionsretten eller medlemsstatenes nasjonale rett som skal stå i rimelig forhold til det mål som søkes oppnådd, være forenlig med det grunnleggende innholdet i retten til vern av personopplysninger og sikre egnende og særlige tiltak for å verne den registrertes grunnleggende rettigheter og interesser

Resultat:

Fastsatt formål og behandlingsgrunnlag for innsamling av personopplysninger på følgende registrerte:

- Ansatte i NND
- Gjester og innleide hos NND
- Besøkende ved NND
- Mottaker av informasjon fra NND
- Andre NND mottar informasjon fra

Behandle opplysninger

Prosesseier: Annette Ansteensen | Godkjent av: Ann-Cathrin Becken | Godkjent dato: 7.11.2023 | Publisert versjon: 1

Inngang:

NND innhenter eller mottar personopplysninger

Omfang/Aktiviteter:

Omfatter alle situasjoner hvor personopplysninger skal behandles.

NND samler inn personopplysninger på følgende registrerte:

- Ansatte i NND
- Gjester og innleide hos NND
- Besøkende ved NND
- Mottaker av informasjon fra NND
- Andre NND mottar informasjon fra

Disse opplysningene behandles og lagres flere steder – se egen behandlingsprotokoll for å se hvilke typer personopplysningskategorier som er lagret hvor.

Resultat:

NND har samlet inn og behandlet personopplysninger

Rette og slette opplysninger

Prosesseier: Annette Ansteensen | Godkjent av: Ann-Cathrin Becken | Godkjent dato: 7.11.2023 | Publisert versjon: 1

Inngang:

En registrert ber om at personopplysninger blir rettet eller slettet

Omfang/Aktiviteter:

Dersom den registrerte mener at vi har registrert uriktige personopplysninger, kan vedkommende kreve at NND retter eller supplerer opplysningene. Den registrerte må kunne sannsynliggjøre at opplysningene er uriktige og hva som er korrekt.

En registrert kan i noen tilfeller kreve at personopplysninger slettes, så lenge opplysningene ikke er omfattet av unntak.

En registrert kan kreve sletting av opplysninger ved følgende tilfeller:

- Dersom den registrerte benytter seg av sin rett til å protestere mot bruk av personopplysningene sine, og det ikke finnes tungtveiende grunner til behandlingen
- Dersom NND behandler personopplysninger basert på gitt samtykke og dette trekkes tilbake
- Dersom det ikke lenger er nødvendig å beholde opplysningene – dvs at formålet med opplysningene er oppnådd
- Dersom NND innhenter opplysningene ulovlig
- Dersom NND har sletteplikt etter loven

Dette skal normal gjennomføres uten ugrunnet opphold og normalt senest innen én måned.

I personopplysningsloven finnes det unntak for sletting, og det er i følgende tilfeller:

- Lagring er nødvendig for arkivering i allmenhetens interesse, vitenskapelige eller historiske forskningsformål eller statistiske formål. Unntaket gjelder bare dersom sletting i alvorlig grad vil hindre at målene nås. Videre sier personvernforordningen artikkel 89 at disse typene behandling av personopplysninger må ha tiltak og garantier for å ivareta den enkeltes personvern
- NND har lagringsplikt etter lov (f.eks. bokføringsplikt)
- Lagring er nødvendig for å fastsette, gjøre gjeldende eller forsvare rettskrav
- Personopplysningene inngår i en ytring som er vernet av ytrings- og informasjonsfriheten

Resultat:

Den registrerte får tilbakemelding om sine rettigheter og utfallet av saksbehandlingen.

Behandlingen ender med at opplysninger blir supplert/rettet, slettet eller lagret videre.

Håndtere avvik på personopplysnings-sikkerheten

Prosesseier: Annette Ansteensen | Godkjent av: Ann-Cathrin Becken | Godkjent dato: 7.11.2023 | Publisert versjon: 1

Inngang:

Det har oppstått et avvik på personopplysningssikkerheten.

Omfang/Aktiviteter:

Brudd på personopplysningssikkerheten blir heretter kalt avvik, og er et 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.

Typiske avvik er:

- **Konfidensialitetsavvik**, uautorisert bruk eller tilfeldig avsløring av personopplysninger
- **Integritetsavvik**, uautorisert eller tilfeldig endring av personopplysninger
- **Tilgangsavvik**, uautorisert eller tilfeldig tap av tilgang til eller ødeleggelse av personopplysninger Slike avvik kan skyldes:
- **Tekniske feil**, for eksempel at et nettsted eller en database gir åpen tilgang til personopplysninger
- **Menneskelige feil**, for eksempel feilhåndteringer eller -vurderinger, som mangelfull nedlåsing av personopplysninger, at personopplysninger sendes til uvedkommende og at dokumenter eller lagringsenheter med personopplysninger forelegges
- **Ekstern trusselaktør**, som hackere eller andre stater, som forsøker å få tak i eller ødelegge sikkerhetsgradert informasjon, som inneholder personopplysninger

Når det foreligger brudd på personopplysningssikkerheten, skal følgende gjøres:

- **Intern varsling** – Når en ansatt, innleid eller andre med tilgang til våre lokaler eller systemer oppdager avvik, skal dette varsles internt iht varslingsknappen i Kjernen. Innmelder skal ikke melde saken i Better, dette for å unngå at varsel ikke leses/mottas omgående, men ringe iht ringeliste. Det er informasjonseier som er ansvarlig for å registrere saken i Better.

- **Varsel til Datatilsynet** – Det skal gis 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. Meldingen til Datatilsynet skal baseres på informasjon som registreres i Better, hvor det også er egne felter/oppgaver ved brudd på personopplysningssikkerheten.

Merk – fristen for melding til Datatilsynet er 72 timer etter å ha fått kjennskap til avviket.

- **Varsel til de berørte** – Det skal gis melding til de registrerte personene som er rammet av avviket (heretter «de berørte») iht prosedyre. En eventuell meldeplikt til de berørte kommer i tillegg til meldeplikten til Datatilsynet. Dette gjøres i samarbeid med Personvernombud.

- **Dokumentere avviksbehandlingen** – NND skal dokumentere ethvert avvik, inkludert avvik hos databehandlere, uavhengig av om avviket er meldepliktig til Datatilsynet eller ikke. Prosedyren beskriver hvordan behandling skal skrives og dokumenteres.

- **Læring og oppfølging** – NND ønsker å forebygge og forhindre 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 eksiterende systemer/prosedyrer bør tilpasses/endres for å hindre nye avvik
  - om det har vært tilstrekkelig kontroll med systemene/prosedyrene
  - om leverandører/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 avviket

Resultat:

NND har behandlet avvik i tråd med regelverket og eventuelt gitt melding til Datatilsynet og de berørte.

Videre er det også evaluert hvilke forbedrings- og læringspunkter NND skal jobbe videre mot.