

GDPR-møte 24.01.18

Tema:

- Dagens avtale og hvilke personverntjenester NSD utfører i dag
- Hvilke krav stiller GDPR til forskningsinstitusjonene?
- Hva kan NSD gjøre for forskningsinstitusjonene videre og hvordan tilpasser vi våre tjenester?
- Hva bør institusjonene gjøre selv?

Hva bør dere gjøre selv?

Oppdatere internkontrollsystemet

Internkontroll er...

- En infrastruktur av rutiner for ledere, forskerstøtte, forskere og studenter
- som ledelsen gir
- for å sikre at personopplysninger behandles lovlig og sikkert

Ledelsen skal beskrive rutinene i et dokument (internkontrolldokumentet)

- som gjøres kjent for alle ledere, forskerstøtte, forskere og studenter
- og kan fremvises for Datatilsynet ved kontroll

Krav til protokoll – art. 30

Protokollen - institusjonens oversikt over alle behandlinger av personopplysninger.

Protokollen skal inneholde kjerneopplysninger om hver behandling:

- navn og kontaktopplysninger til behandlingsansvarlig og personvernombud,
- formålene med behandlingen,
- kategoriene av registrerte
- kategoriene av personopplysninger,
- kategoriene av mottakere
- eventuelle overføringer av personopplysninger til tredjestat eller internasjonal organisasjon (med navn på virksomhet),
- planlagte tidsfrister for sletting
- en generell beskrivelse av tekniske og organisatoriske sikkerhetstiltak

Hva bør internkontrolldokumentet inneholde?

Ledelsen (styrende rutiner):

Kartlegge personopplysninger + lovkrav + fordele oppgaver + sikkerhetsorganisering + lage skriftlige rutiner for ledere og ansatte + sikre at rutinene implementeres

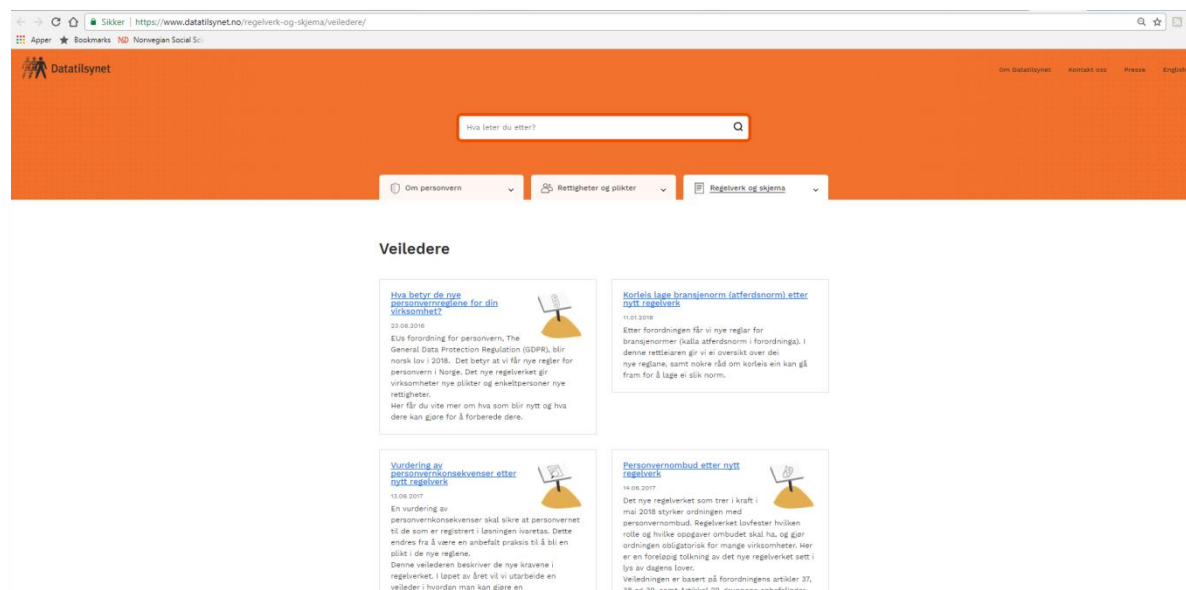
Forskere (gjennomførende rutiner):

Skal få rutiner for behandling av personopplysninger - «håndbok» og følge disse

Forskningsadministrasjonen (kontrollerende rutiner):

Rutiner for opplæring av forskere + rutiner for egenkontroll + rutiner for avvikshåndtering

Nyttige veiledere om internkontroll



www.datatilsynet.no/regelverk-og-skjema/veiledere/



Øverste administrative leder

Juridisk ansvar. Skal sørge for:

- å sikre og påvise at hver behandling følger lovkravene
- dokument som beskriver virksomhetens internkontrollrutiner
- at rutinene er kjent for alle ansatte og studenter

Forskningsadministrasjon

Praktisk arbeid med internkontroll:

- informere forskere/studenter om rutiner
- kontrollere at rutinene blir fulgt
- forebygge og følge opp avvik

Forskere og studenter

Skal behandle personopplysninger i tråd med rutinene

NSD Personverntjenester

Rådgivende rolle:

- veilede forskere, studenter, ledelse og forskningsadministrasjon i personvernspørsmål
- forhånds- underveis og etterkontroll av hvert prosjekt
- personvernkonsekvensvurderinger og forhåndsdrøftinger med Datatilsynet
- Meldingsarkivet gir institusjonens ledelse oversikt og kontroll med prosjektene
- varsler ledelsen om avvik

Meldingsarkivet

Hva er Meldingsarkivet?

- Gir din institusjon oversikt over alle forskningsprosjekter meldt til NSD
- Om hvert prosjekt: daglig ansvarlig, formål, utvalg, type opplysninger, lagringsmåte, varighet, behandlingsgrunnlag + alle sakspapirer (vilkår)
- Et verktøy for forebygge, avdekke og håndtere avvik (egenkontroll)
- Et verktøy for å *påvise* (dokumentere) at hver behandling er i tråd med lovkravene (f.eks. ved tilsyn)

Hvem bør ha tilgang?

- Ledelsen bestemmer hvilke ansatte som skal ha tilgang
- Ledelsen utpeker en brukeransvarlig som administrerer tilgangen for de andre brukerne
- Alle ledere og ansatte med internkontrolloppgaver bør ha tilgang

Hvordan bruke Meldingsarkivet?

Ansatte med internkontrolloppgaver bør ha faste rutiner for å etterse:

- at alle prosjekter som skal behandle personopplysninger meldes til NSD
- at alle innmeldte prosjekter er forankret ved institusjonen
- at prosjektene har nødvendige tillatelser
- at krav/vilkår i tillatelsene følges opp
- at forskere/studenter som skal slutte rydder opp i aktive prosjekter
- at avvik meldes til ledelsen og følges opp

Ledelsen må sørge for at Meldingsarkivet blir tatt i bruk

- fordel internkontrolloppgaver til forskerstøtten (hva, hvorfor og hvordan)
- gi konkrete rutiner for jevnlig bruk av Meldingsarkivet (hva, hvorfor og hvordan)
- gi instruks til brukeransvarlig om å gi tilgang til Meldingsarkivet til alle personer med internkontrolloppgaver

NSD har laget brosjyrer og gir kurs i bruk av Meldingsarkivet.

Spørsmål til salen:

- Hvordan jobber dere med personvern/internkontroll?
- Hvordan forbereder dere GDPR?
- Hvilke behov har dere mht. de personverntjenestene vi utfører for dere?

Oppsummering – hva gjør NSD for dere 25.mai?

- Meldeskjema – sikrer institusjonen nødvendig informasjon om prosjektet, som formål, utvalg, data, sikkerhetstiltak, varighet
- Saksbehandling av hvert prosjekt:
 - sikrer at prosjektopplegget oppfyller GDPRs krav til prinsipper, behandlingsgrunnlag, registrertes rettigheter,
 - veileder forsker/student om informasjonssikkerhet
 - foretar konsekvensvurdering og forhåndsdrøfting når påkrevd
 - følger opp underveis og ved prosjektslutt for å sikre lovlig grunnlag for eventuelle endringer
- Meldingsarkivet
 - landingsside for hvert prosjekt (prosjektopplegg og vår vurdering)
 - gir oversikt over behandlingene (protokoll jf. art. 30)
- Veiledning og kurs om internkontroll



NSD

NORSK SENTER FOR
FORSKNINGSDATA