GDPR-møte 24.01.18

Tema:

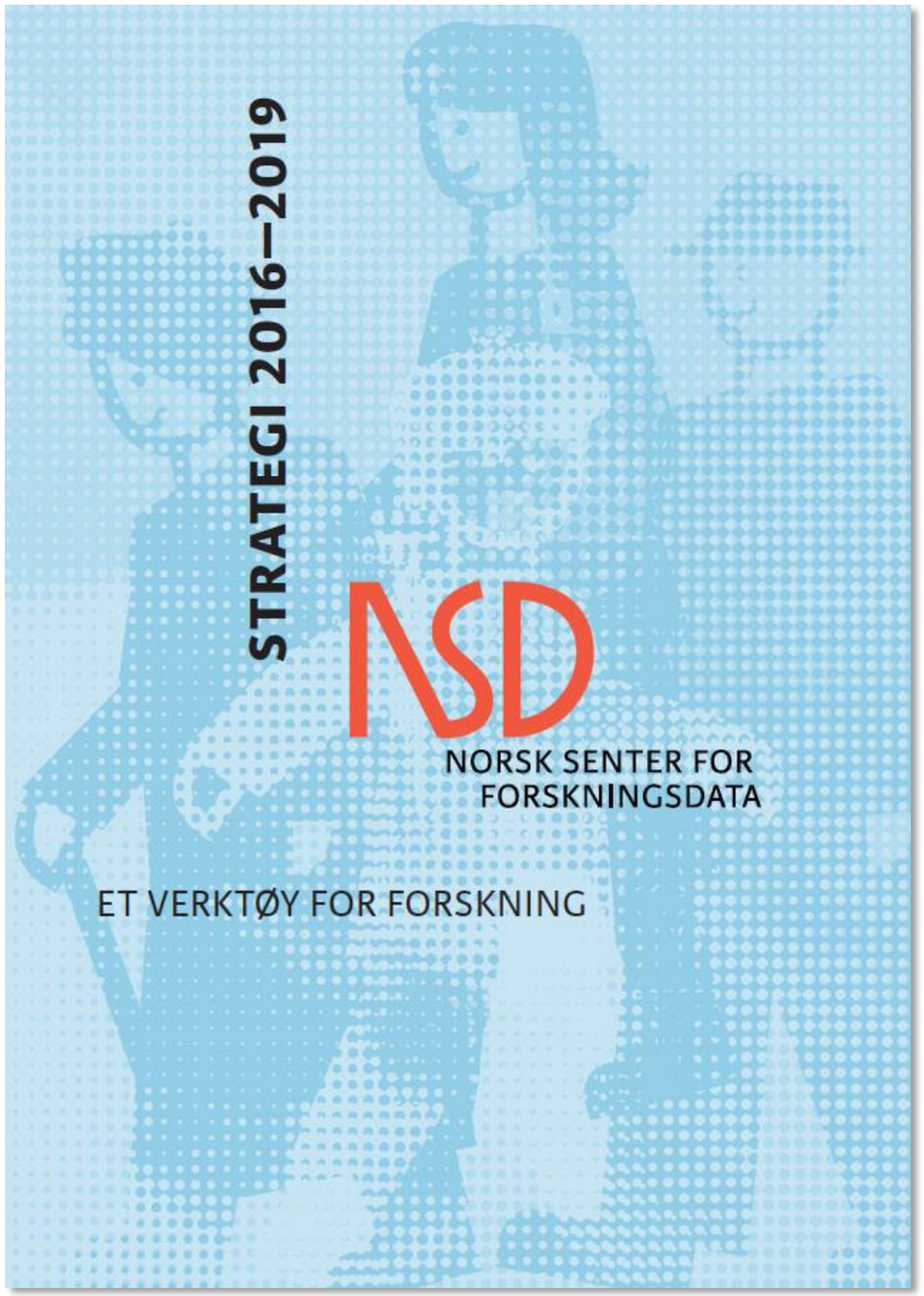
- Dagens avtale og hvilke personverntjenester NSD utfører i dag
- Hvilke krav stiller GDPR til forskningsinstitusjonene?
- Hva kan NSD gjøre for forskningsinstitusjonene videre og hvordan tilpasser vi våre tjenester?
- Hva bør institusjonene gjøre selv?

NSD
NORSK SENTER FOR FORSKNINGSDATA

Strategien

Forskningssektoren er målgruppe for alle tjenester NSD leverer.

Prinsippet om åpen tilgang, likebehandling og deling av forskningsdata er styrende for all virksomhet hos NSD.



NSD NSD NORDi (Norwegian Open R

NSD NORSK SENTER FOR FORSKNINGSDATA

Om NSD

I snart 50 år har NSD arkivert og formidlet forskningsdata. Vi jobber kontinuerlig for å gjøre tjenestene bedre

Her er noe av det vi jobber med i prosjektene NORDi og RAIRD:

ÅPEN - I BRUK

Datahåndteringsplan

Verktøy for å generere datahåndteringsplan. Maler for Horizon 2020 osv.

Status: I produksjon. Åpen for alle.

ÅPEN - I BRUK

Arkiveringsportal

Tjeneste for å arkivere data.

Status: I produksjon. Åpen for alle.

PILOT-TESTING

Registerdata (RAIRD)

Verktøy for å forenkle tilgang til registerdata - med innebygd personvern.

Status: Testing med pilot-brukere

BETA-VERSJON

Søkeportal

Skal gjøre det enklere å finne data hos NSD.

Status: Begrenset beta-versjon i produksjon. Åpen for alle.

PÅGÅR

Opplæring

Opplæringsprogram rettet mot forskere, studenter, administrasjon og videregående skole.

Status: Pågår og videreutvikles

UTVIKLING

Personvernportal: Institusjon

Tjeneste som gir institusjonene oversikt over prosjekter med persondata.

Status: Skal erstatte tidligere løsning i mai 2018

UTVIKLING

Personvernportal: Forsker/Student

Ny tjeneste for registrering av personvernprosjekt i forbindelse med GDPR.

Status: Skal erstatte tidligere løsning i mai 2018

UTVIKLING

Institusjonsportal

Skal gi institusjonene oversikt over all aktivitet knyttet til personvern, datahåndteringsplaner, arkivering og gjenbruk av data.

Status: Prototype sommer 2018

ALFA-VERSJON

Min side

Inngang til all aktivitet knyttet til NSD, for forskere, institusjoner osv.

Status: Skal erstatte tidligere løsning i mai 2018

NSD som personvernombud i dag

Avtalen omfatter:

- *Informasjon og veiledning* i spørsmål om forskning og personvern
- *Saksbehandling* av forskning og studentprosjekter som er regulert av personopplysningsloven eller helseregisterloven.

NSD/Ombudet skal:

- Kontrollere at behandling av personopplysninger skjer i henhold til regelverket
- Føre offentlig oversikt over prosjekter meldt til personvernombudet
- Bistå de registrerte med å ivareta deres rettigheter
- Påpeke brudd på reglene til institusjonen og varsle Datatilsynet om dette

Institusjonen skal:

- Informere forskere og studenter om meldeplikten (NSD bistår med informasjonsmateriell)
- Oppnevne kontaktperson med ansvar for informasjonsarbeidet
- Utarbeide, holde oppdatert og framvise dokumentasjon av institusjonens overordnede system for sikkerhetsrutiner og internkontroll som forskningsprosjektet gjennomføres i henhold til.

NSD som personvernombud i dag

Personverntjenestene våre i praksis:

- Informasjon og veiledning til forskere og studenter: foredrag, undervisning, møter, epost, telefon

- Forhåndskontroll:
- Institusjonen sørger for at forsker/student melder prosjekt som skal behandle personopplysninger
- NSD vurderer prosjektopplegget iht. lovkravene (personopplysningsloven og helseregisterloven)
- NSD påpeker evt. behov for korrigering av prosjektopplegget – ofte personlig kontakt
- NSD gir forsker skriftlig svar/tilrådning
- NSD vurderer om prosjektet er konsesjonspliktig
- NSD utformer søknad til Datatilsynet i samråd med forsker og bistår i dialogen med Datatilsynet
- NSD bistår forsker/institusjon ved klage på vedtak/vilkår til Datatilsynet eller Personvernnemnda

- Oppfølging/etterkontroll: sikre lovlig avslutning (anonymisering eller lovlig arkivering av persondata)
- NSD kontakter forsker eller veileder/student ved prosjektslutt
- NSD ber forsker/student oppgi status: er prosjektet avsluttet? data anonymisert? eller lovlig arkivert?
- NSD varsler institusjonens ledelse hvis forsker/student ikke svarer – får anledning til å rydde opp.

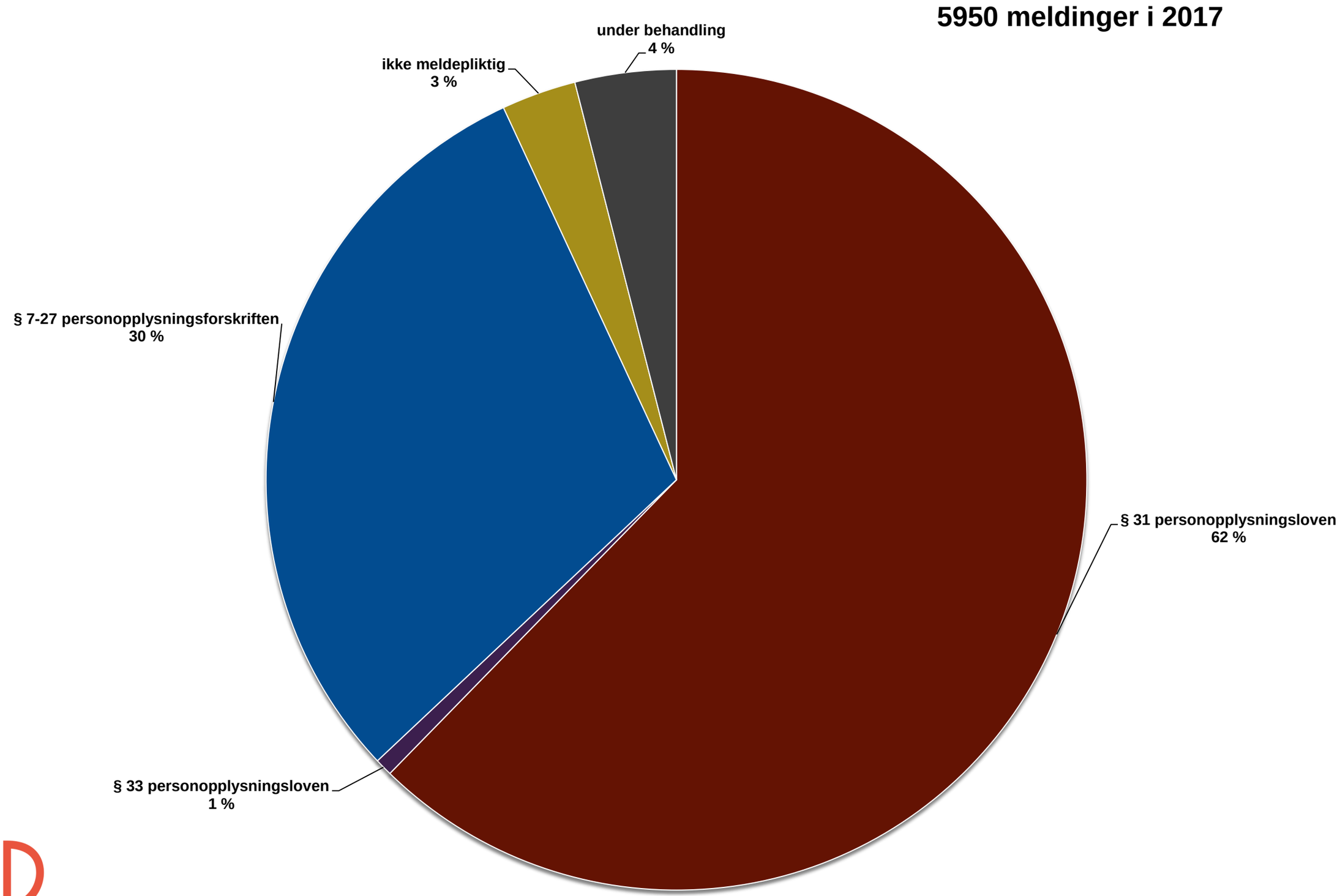
NSD som personvernombud i dag

- Meldingsarkivet:(Institusjonenes styringsverktøy)
- NSD gir institusjonen oversikt over alle forsknings/studentprosjekt med personopplysninger
- informasjon om hvert prosjekt: utvalg, data, lovlig behandlingsgrunnlag etc.
- alle relevante saksdokumenter: meldeskjema, endrings- og statusmeldinger fra forsker, skriftlige tilbakemeldinger fra ombudet, samtykkeskriv, eventuelle andre tillatelser

- Veiledning til institusjonen om
  - regelverk om personvern i forskning
  - internkontroll
  - håndtering av avvik
  - bistand ved tilsyn

- Offentlig søk: NSD offentliggjør oversikt over meldepliktige prosjekter på våre nettsider
- Henvendelser fra registrerte: NSD besvarer spørsmål fra forskningsdeltagere om prosjekter meldt til oss

Konsesjons- og meldeplikten i praksis avviklet



NSD
NORSK SENTER FOR FORSKNINGSDATA

@NSD

GDPR og nytt regelverk
Fra forhåndskontroll til internkontroll og oversikt

- Arbeidet med å sikre lovlig, forsvarlig og trygg bruk av personopplysninger kalles *internkontroll og er virksomhetens ansvar*
- Forskningsinstitusjonen plikter å legge til rette slik at forskere og studenter oppfyller lovkrav
- Forskningsinstitusjonen plikter å ha oversikt over behandlinger
- Forskningsinstitusjonen plikter å kontrollere at forskere og studenter oppfyller lovkrav
- **Forskningsinstitusjonen plikter å utpeke personvernombud og involvere ombudet i alle personvernspørsmål**
- **Personvernombudsrollen styrkes som et virkemiddel i internkontrollen**
- **Fra frivillig til obligatorisk**

NSD
NORSK SENTER FOR FORSKNINGSDATA

GDPRs krav til personvernombud – art. 37-39

Personvernombudet skal (som et minimum):

a) informere og gi råd om regelverk til virksomheten og ansatte,
b) kontrollere at virksomheten overholder personvernregelverk og virksomhetens personvernpolitikk og prosedyrer,
c) gi råd og delta i konsekvensanalyser,
d) samarbeide med tilsynsmyndighetene,
e) fungere som kontaktpunkt mellom Datatilsynet og virksomheten, inkl. forhåndsdrøftinger

«For Norges del er reglene langt på vei en kodifisering av eksisterende praksis»
Datatilsynet 23.06.2016

Ombudet skal prioritere innsatsen hvor personvernrisikoen er høyest

Virksomheten skal utpeke et personvernombud som:

- har nok kompetanse
- er uavhengig
- får nok ressurser

NORSK SENTER FOR FORSKNINGSDATA

NSDs kompetanse

- Har vurdert personvern i forskning i over 35 år
- I dag ombud for 137 forskningsinstitusjoner i Norge
- Behandler nå årlig ca. 6000 nye meldinger, 1000 endringsmeldinger, 7000 sluttmeldinger
- Alle forskningsområder – stor variasjon i utvalg, data og metode
- Forsknings- og studentprosjekter + kvalitetssikringsprosjekter (helse)
- Fra bachelorprosjekter til store befolkningsbaserte helseundersøkelser
- Erfaring med bistand i klagesaker, avvikssaker og ved tilsyn
- Seksjon med 20 ansatte – fagmiljø, bredde, stabilitet og kontinuitet i kompetansen
- Deltar jevnlig på kurs og konferanser om regelverk og etikk for personvern i forskning
- Nær dialog med Datatilsynet over tid - god kunnskap om tilsynets tolkninger
- Deltar i internasjonale prosjekter/fora som SERISS, CESSDA, BBMRI

Unik kompetanse om tolkning av personvernregelverket i forskning

- sikrer god kvalitet på tjenestene og rådgivningen vi leverer
- og likebehandling av forskningen

NSD – uavhengighet og ressurser

Uavhengighet ⇨ fordel for institusjonene, forskningen og personvernet

- eksternt ombud, stab av medarbeidere - gir en viss distanse til forsker
- unngår habilitetsproblemer og press
- lettere å gi «upopulære råd» i enkeltprosjekter
- lettere å varsle ledelsen om avvik

Ressurser ⇨ ordning som gir stordriftsfordeler

- Hver institusjon får «mye personvern for pengene», uten at det går på bekostning av forskningen
- Drar nytt av NSDs samlede kompetanse som dataarkiv, tilgangsforvalter og utvikler av tekniske løsninger for forskning
- Finansieres av institusjonene etter selvkostprinsippet
- Arbeidsmengden økt betraktelig – NSD har tilpasset seg ved oppbemanning, systemutvikling og omorganisering.

NSD – personvernombud eller kompetansesenter?

Justis- og beredskapsdepartementet i høringsnotat om ny personopplysningslov (§ 6):
«Det nevnes i denne forbindelse at ordningen der Norsk senter for forskningsdata (NSD) er personvernrådgiver for en rekke forskningsinstitusjoner når det gjelder forskningsvirksomhet, tilsynelatende fungerer godt, og at det er ønskelig at en slik ordning kan videreføres også under forordningen» (Høringsnotatet s. 39).

Departementet skisserer to hovedmodeller:

a) NSD fortsetter som sektorombud: en forskningsinstitusjon kan ha NSD som personvernombud for forskning, og et annet ombud som dekker behandling av personopplysninger til andre formål
b) NSD fortsetter som rådgiver for institusjonene – veileder og utfører tjenester for internt ombud

Vårt budskap:
Uansett om NSD fortsetter som ombud eller kompetansesenter, kan vi levere de samme tjenestene

Men vi mener forskningen, institusjonene og personvernet blir best ivaretatt ved å videreføre ordningen med NSD som personvernombud for forskning.

NSD
NORSK SENTER FOR FORSKNINGSDATA

Hvordan har vi gått frem for å tilpasse våre tjenester til GDPR?

Tre prosjekter:

- Internkontrollprosjektet: vi trapper opp veiledning til institusjonene
- Systemutvikling: vi oppdaterer meldeskjema, saksbehandling og Meldingsarkivet
- Saksbehandlingsprosjekt: Vi skyggesaksbehandler utvalgte prosjekter og oppdaterer saksbehandlingsrutiner og brevmaler.

Vårt kildegrunnlag:

- GDPR (artikkel for artikkel)
- DTs veiledere om GDPR
- Artikkel 29-gruppens veiledere
- Forslag til ny personopplysningslov
- Datatilsynets Veileder om internkontroll og informasjonssikkerhet
- Tilsynsrapporter (forteller noe om tilstanden i sektoren og hvordan DT tolker internkontrollkravene i praksis)
- Saksbehandling, inkl. avvik
- Kontakt med forskere, studenter, forskerstøtte og registrerte, Datatilsynet og andre aktører

NORSK SENTER FOR FORSKNINGSDATA

GDPRs krav til forskningsinstitusjonene - *sikre og påvise* at **hver behandling** av personopplysninger oppfyller lovkravene (art. 24)

NSD kvalitetssikrer at hvert prosjektopplegg:

- følger grunnleggende **prinsipper** (bl.a. formåls- og oppbevaringsbegrensning) – art. 5
- har lovlig **behandlingsgrunnlag** – art. 6, 9 og 10 (evt. med supplerende hjemmel i nasjonal lovgivning)
- oppfyller **vilkår om samtykke** (hvis samtykkebasert forskning) – art. 7
- ivaretar den **registrertes rettigheter** (art. 12-22) eller dokumenterer hjemmel for unntak
- gjennomgår **personvernkonsekvensvurdering** hvis høy personvernrisiko – art. 35
- **forhåndsdrøftelse med Datatilsynet** hvis fortsatt høy personvernrisiko etter konsekvensvurdering – art. 36

…og at hvert prosjektopplegg følger nasjonal lovgivning når det gjelder:

- **tilrådning fra personvernombud** før behandling av sensitive personopplysninger – jf. utkast til ny personopplysningslov § 6
- **noen av tilleggskravene i særlovgivningen** (helseregisterloven og helseforskningsloven)
- **andre forhåndstillatelser** som dispensasjon fra taushetsplikten - forvaltningsloven

GDPRs krav til forskningsinstitusjonene - *sikre og påvise* at **hver behandling** av personopplysninger oppfyller lovkravene (art. 24)

NSD innhenter informasjon i meldeskjema og veileder forsker/student om:

- **informasjonssikkerhet** – art. 32
- lovkravene dersom personopplysninger **overføres til andre institusjoner:**

- databehandler – art. 28 og 29
- felles behandlingsansvarlig – art. 26
- overføring til utlandet – art. 44-49

Men på disse punktene må vi legge til grunn at forsker følger institusjonens retningslinjer….

- Vi ønsker å få inn institusjonens retningslinjer,
- slik at vi kan bruke disse i saksbehandlingen
- for å bistå med å implementere rutinene for informasjonssikkerhet i hvert prosjekt

NSD kvalitetssikrer og dokumenterer prosjektopplegget

Oppdatert meldeskjema

- sikrer at institusjonen får nødvendig info om hvert prosjekt iht. GDPR

Saksbehandling

- sikrer at prosjektopplegget oppfyller lovkrav

Forhåndskontroll - mest ressurser på prosjekter med høy personvernrisiko:

1) Forenklet saksbehandling 2) Tilrådning 3) Personvernkonsekvensvurdering 4) Forhåndsdrøfting

Underveiskontroll *(automatiseres)*

- Kontakter forsker/student underveis i langvarige prosjekter om status
- Vurderer dersom endringer

Etterkontroll *(automatiseres)*

- Kontakter forsker/student når behandlingen av personopplysninger er planlagt avsluttet
- Vurderer dersom endringer
- Varsler institusjonen hvis forsker/student ikke gir tilbakemelding

Meldingsarkivet - verktøy for å dokumentere krav i art. 30 og (delvis) art. 24

NSD
NORSK SENTER FOR FORSKNINGSDATA

GDPRs krav til forskningsinstitusjonene - system:

- Den behandlingsansvarliges ansvar (internkontroll) – art. 24
- Innebygd personvern (privacy by design and by default) – art. 25
- Felles behandlingsansvar med andre institusjoner krever «ordning»/avtale – art. 26
- Risikovurdering av, og skriftlig instruks til, databehandlere – art. 28
- **Protokoll over behandlinger av personopplysninger – art. 30**
- **Samarbeid med tilsynsmyndigheten – art. 31**
- Sikkerhet ved behandlingen – art. 32
- Brudd på persondatasikkerheten (avvik): internt register, varsel til Datatilsynet og de registrerte – art. 33 og 34
- Utpeke personvernombud – art. 37
- Oppfordrer til atferdsnormer og sertifisering (frivillig) – art. 40-43
- Regler om overføring til tredjestater (utenfor EU/EØS) – art. 44-49

NSD trapper opp støtte og veiledning til institusjonene

- Helhetlig opplæringstilbud:

- Foredrag, kurs, nettverkssamlinger og digitale ressurser om nytt regelverk
- Om kravene i hvert forskningsprosjekt og kravene til institusjonen (internkontroll)
- For ulike organisasjonsnivåer: ledelse, forskerstøttepersonell (fakultet/institutt) og forskere/studenter

- Veiledning om internkontroll / bidra til mal eller bransjenorm

- Bistand til å forebygge, oppdage og håndtere avvik

- Kurs, saksbehandling av enkeltprosjekter, Meldingsarkivet

- Meldingsarkivet i ny form

- Verktøy for dokumentasjon - art. 30 og (delvis) art. 24
- Ønsker å få inn institusjonens retningslinjer for informasjonssikkerhet, bruke i saksbehandlingen
- Verktøy for risikovurdering (oversikt over prosjekter med ulik grad av personvernrisiko) – art. 32

- Bistand ved kontroll fra Datatilsynet

Hva med helseforskningen?

Departementet i høringsnotat om ny personopplysningslov:

- Den generelle konsesjonsplikten til Datatilsynet forsvinner,
- men kan "gjeninnføres" i særlovgivningen

- Trolig fortsatt krav om etisk vurdering fra REK (jf. forskningsetikkloven),
- Usikkert om REK fortsatt skal gi juridisk forhåndsgodkjenning av behandling av helseopplysninger (iht. helseforskningsloven)

To postkasser?

Uansett:

- All behandling av sensitive personopplysninger til forskning skal tilrås av personvernombud (jf. utkast til ny personopplysningslov § 6)
- Institusjonen må ha oversikt over alle behandlinger, og sikre og påvise at behandlingene er i samsvar med GDPR.

Vårt budskap er at institusjonene bør pålegge sine forskere og studenter å melde helseforskningsprosjekter til NSD

NSD arbeider for å forbedre forskerhverdagen og vil utvikle APIer som gjør det mulig å gjenbruke informasjon i våre systemer

Avtalen – hva må revideres?
Hva er egentlig nytt?

- Personvernombud blir obligatorisk, oppgaver og ansvar utvides
- NSD oppdaterer meldeskjema, saksbehandlingsprosedyrer og Meldingsarkivet iht. ny lov
- NSD trapper opp veiledning til institusjonene på leder/adm.nivå
- Vil på sikt hjelpe institusjonene med å implementere deres retningslinjer for informasjonssikkerhet i hvert prosjekt.

- Institusjonen må sørge for at forskerne melder forskningsprosjekter (inkl. helseforskning) til NSD
- Institusjonen må oppdatere internkontrolldokumentet iht. ny lov
- Institusjonen må sørge for å ta i bruk Meldingsarkivet
- Finansiering

NSD
NORSK SENTER FOR FORSKNINGSDATA

Hva er klart 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)

NORSK SENTER FOR FORSKNINGSDATA

NSD

NORSK SENTER FOR FORSKNINGSDATA