Ready or not, here we come

Hvordan var NAV forberedt på GDPR?
Internrevisjonens angrepsvinkel

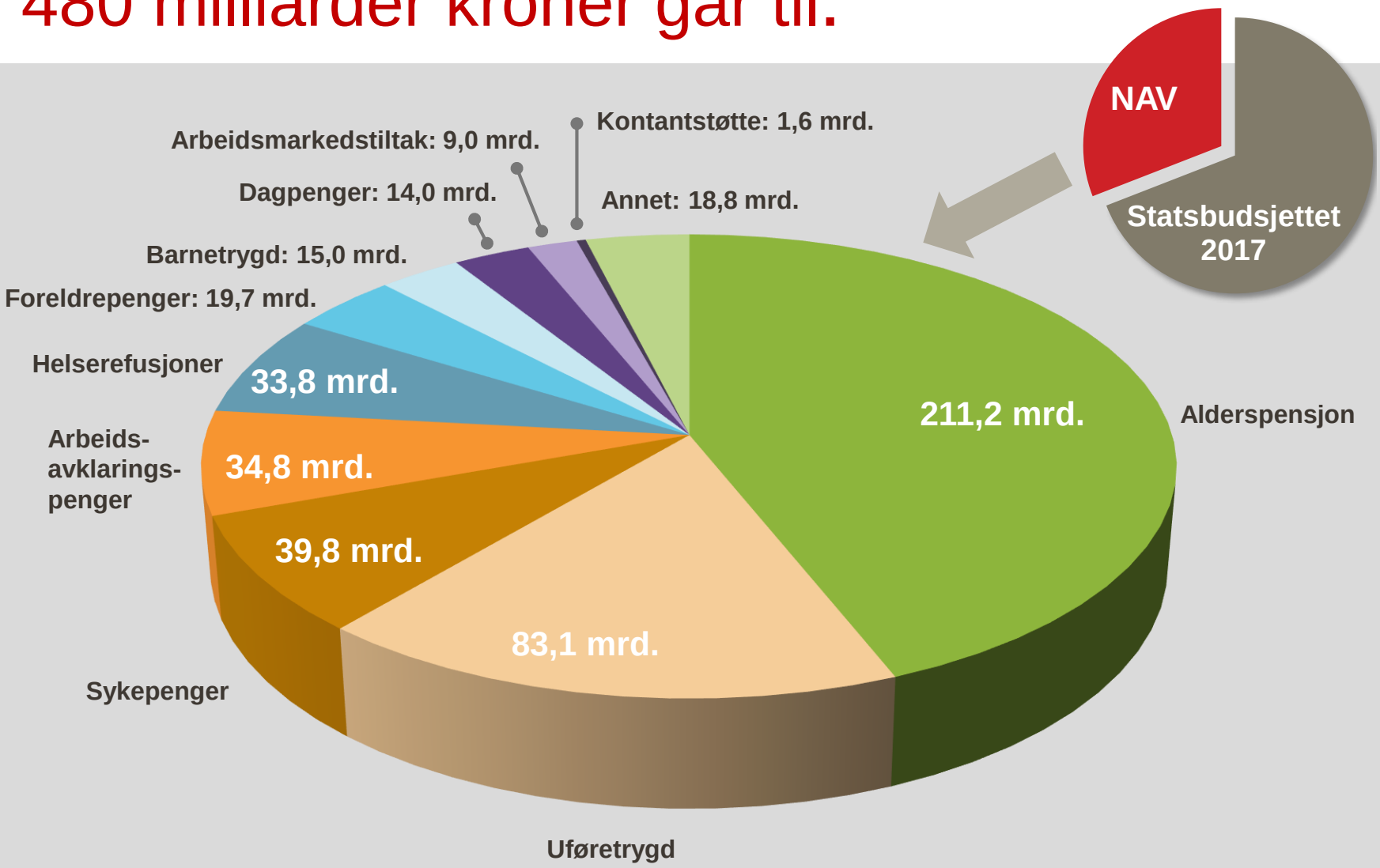
19.03.2019//Terje Klepp

Hvem er jeg?

- Siviløkonom og statsautorisert revisor fra NHH
- Arthur Andersen (1981-2002)
- Ernst & Young/EY (2002-2016)
- Partner siden 1990
- IT-revisjon siden 1984
- Internrevisjon siden tidlig 90’ tallet
- Begynte i NAV 15.8.2016

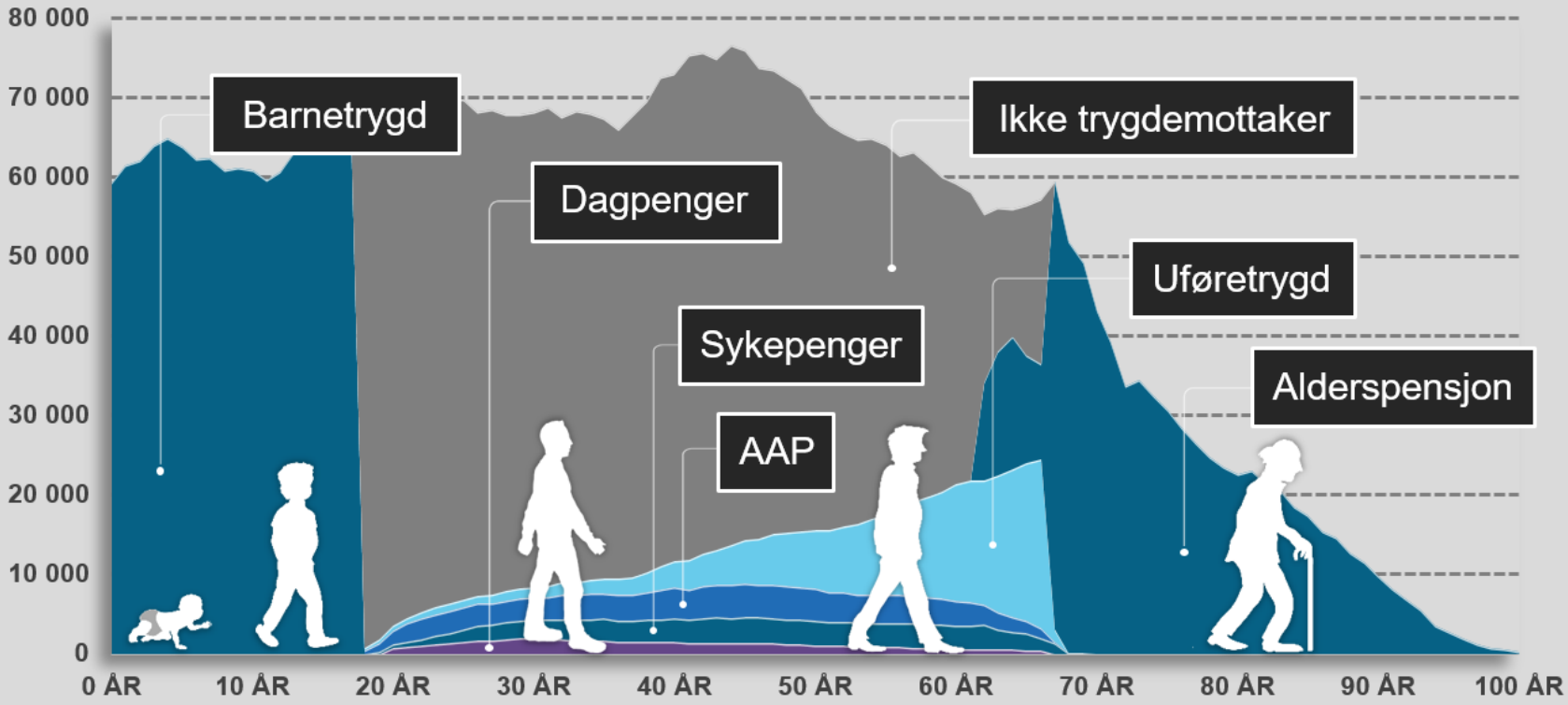
NAV i tall og fakta 2017

480 milliarder kroner går til:



I tillegg utbetalte NAV 25,5 milliarder kroner på vegne av Statens pensjonskasse. Totalt utbetalte dermed NAV 505,8 milliarder kroner i 2017.

NAV er med fra vugge til grav



Den norske befolkningen per januar 2014, og koblingen hvert årskull har til noen av trygdeordningene i NAV. Statistikk fra NAV finnes på nav.no/kunnskap

NAVs GDPR utfordringer
(for ca. 2 år siden)

«Snokesaken» - Rapport fra oktober 2016

Rapport: Nav-ansatte snoker på venner og kjendiser

Nav-ansatte snoker på seg selv, familie og venner – og på kjendiser. De risikerer sjelden å bli oppdaget, viser en ny rapport.

SNOKER: Andelen Nav-ansatte som snoker mer enn Nav kan akseptere, ifølge ny rapport.
FOTO: HOLM, MORTEN / SCANPIX

Kari Stokke Nilsen
Journalist

Hans Jørgen Solli
Journalist

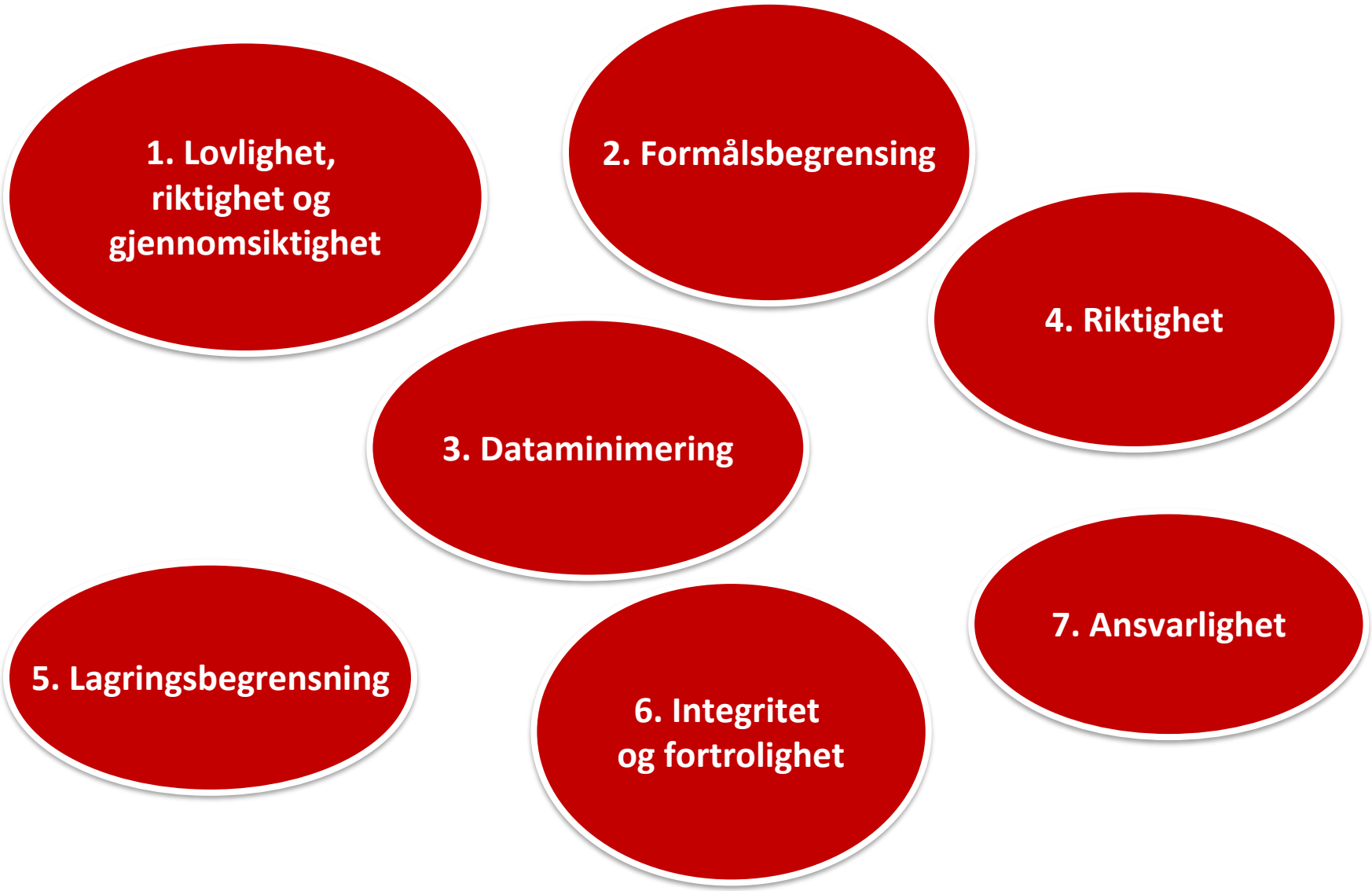
Publisert 1. nov. 2016 kl. 15:00

Artikkelen er mer enn to år gammel.

Hva er et personvernombud - og NAV

- Ombudet skal **involveres** i **alle saker** som handler om behandling av personopplysninger i virksomheten.
- Virksomheten har ansvar for at ombudet har **tilstrekkelige ressurser** og mulighet til å utføre sine oppgaver og opprettholde sin ekspertise.
- Ombudet skal være **uavhengig,** og det er virksomhetens ansvar …
- Ombudet kan **ikke avskjediges** eller straffes for å utføre sine oppgaver.
- At det ikke **skapes bindinger**, slik at en har en så «fri» og uavhengig rolle at personvernombudet har reell påvirkning
- Personvernombudet skal **rapportere til […] øverste ledelse**.
- Ombudet skal være bundet av **taushetsplikt eller konfidensialitet** under utførelsen av sine plikter.
- Ombudet skal være **kontaktpunkt for de registrerte**.

Diapsalmata – Personvern i et nøtteskall (Artikkel 5)

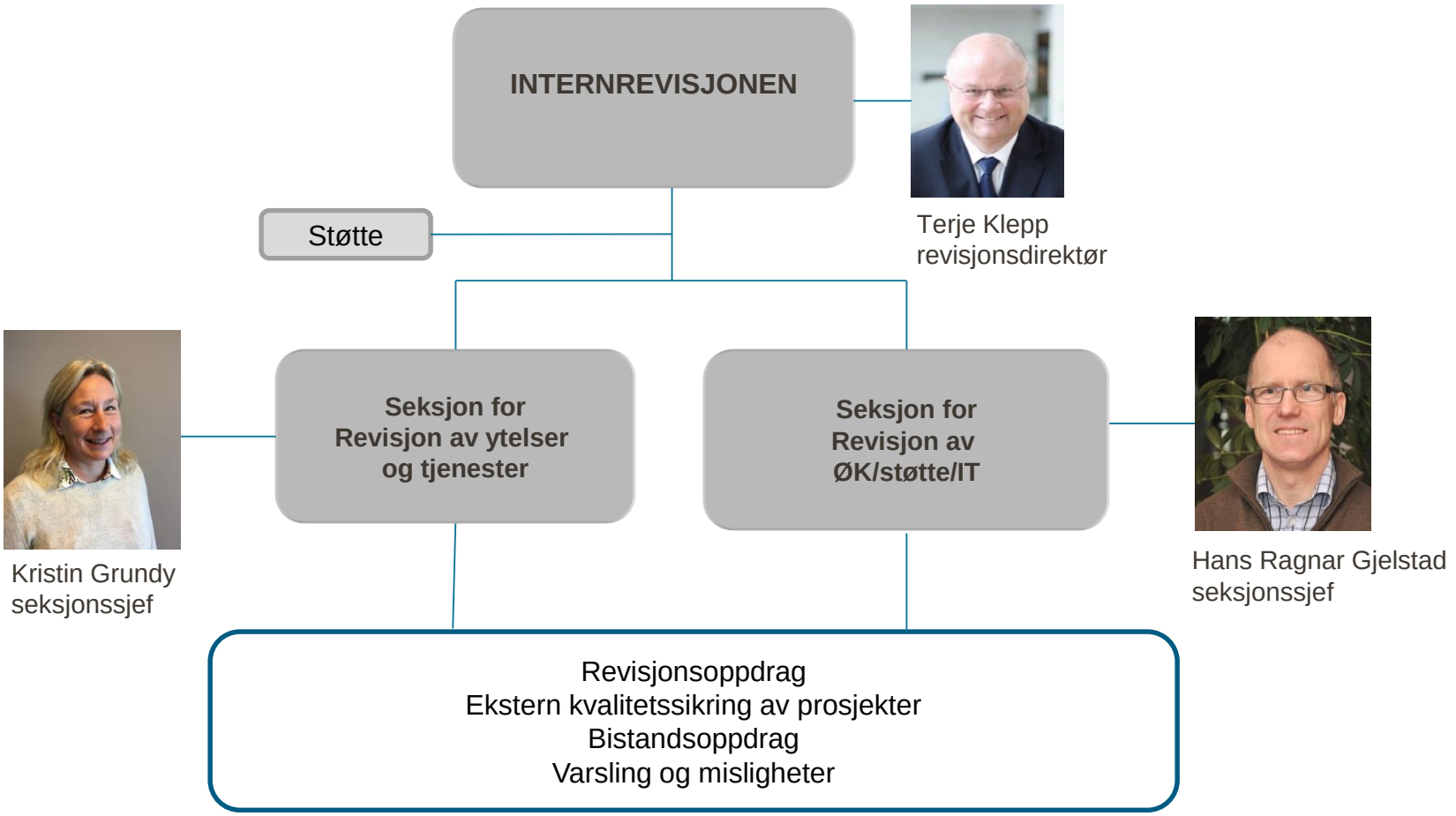


NAVS GDPR utfordringer (PVO for 20 måneder siden)

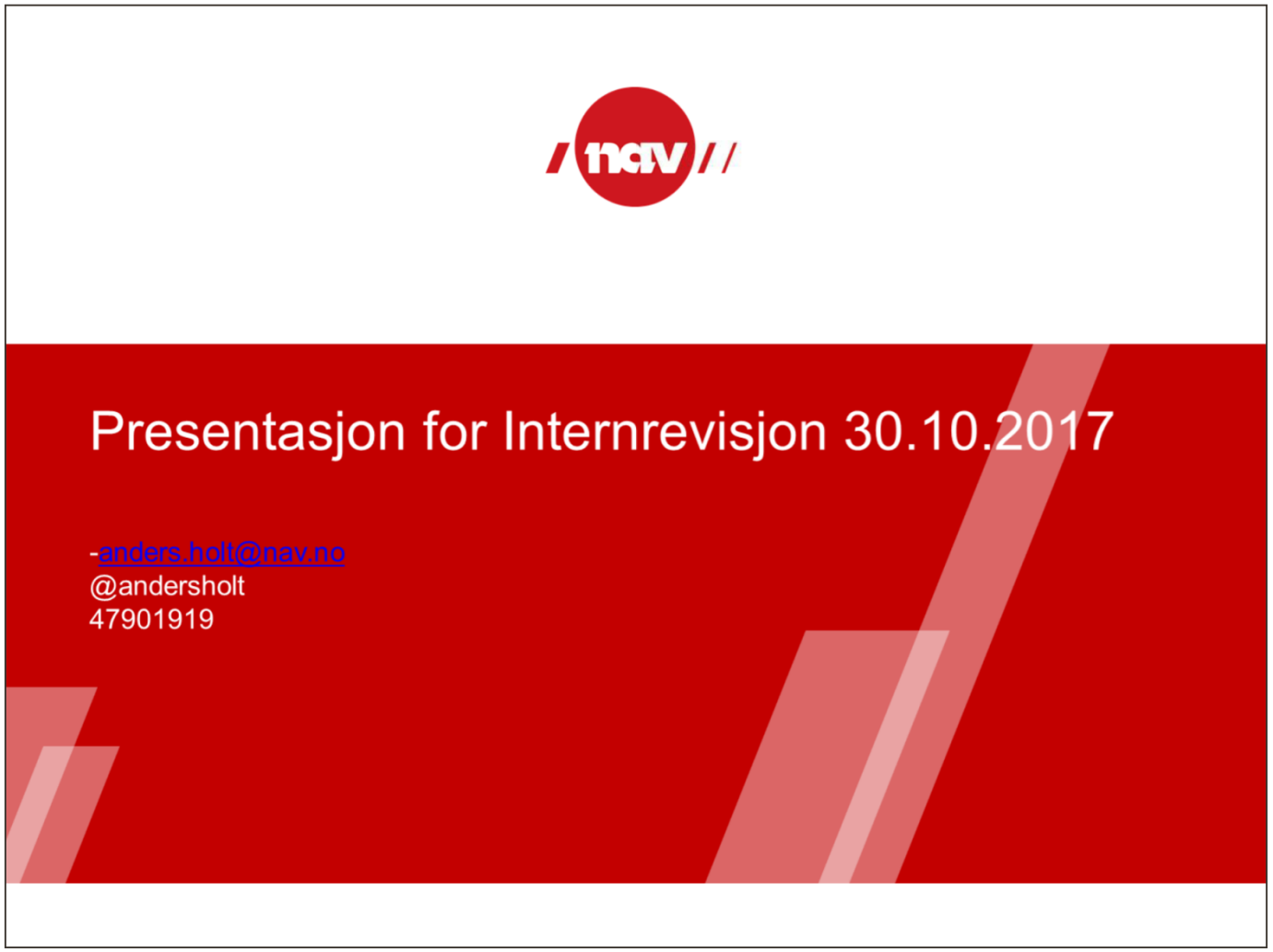
- NAV er en stort sted
- Desentralisert og sentralisert organisering (740 lokasjoner)
- Livsløps personopplysninger - Stort omfang av PO - Mange brukere
- Tredjeparter - Fra store etater til hjelpemiddelsentraler til små tolker
- Mye IT – nytt og gammelt (Infotrygd fra 1978)
- Sterkt fokus på Sikkerhet og Taushetsplikt – mindre på personvern
- Uklare rutiner på en del områder
- Litt mangelfull kompetanse ifm personvern
- Manglet personvernombud

Hva gjorde så internrevisjonen med dette, og hva fant vi?

Internrevisjonen organisering 2018/2019



Vi inviterte PVO til et møte med hele IR



Revisjonsplan 2018 (ledergodkjent 12/2017)

Navn på revisjonen	Målet og temaer	Begrunnelse, bakgrunn	Priori-tering	Område (ABKV)+Rx
Implementering av Personvernforordningen	Kartlegge hvor langt NAV er kommet for å være klar til forordningen trer i kraft 25.5.2018. Tema: Policy, retningslinjer, rutiner Kommunikasjon/opplæring	GDPR «readiness». Nytt PVO kan ha behov for å få dette kartlagt. Bør gjøres veldig tidlig i 2018. Revisjonen bør gjøres av flere team, et team på IT, et team på ytelser, et team på tjenester osv…	1	R5,R10 B
HR, Kom, Kunnskap				
Håndtering av egne ansatte/familie som er brukere av NAV	Sjekk etterlevelse av rutine Risiko for snoking Personvern for de ansatte	Hvordan fungerer NAV for ansatte/familie som blir brukere av NAV? Fylkene har ulike rutiner for håndtering av ansattesaker. Ansatte, barn og ektefeller kan bli sperret i ulike fagsystemer, men navnene deres er likevel synlige og tilgjengelige også for ansatte som ikke har tilgang til	1	R10 V

- Vi brukte 540 + 230 = 770 timer på de to prosjektene, dvs 110 dagsverk (plan var 100 + 40 dagsverk)

Internrevisjonsoppdragene – egne ansatte

1. Bakgrunn
NAV har ca. 14 000 statlig og 5 000 kommunalt ansatte medarbeidere. Når medarbeidere i NAV, og deres familie/nærstående, søker om ytelser eller har behov for oppfølging fra NAV kommer etaten og enkeltmedarbeidere i en dobbeltrolle som arbeidsgiver, kollega og forvaltningsorgan. Sykefraværet i NAV var i 2017 på 7,2 prosent.

3. Revisjonsformål og -tema
Formålet med revisjonen er å vurdere om NAVs rutiner for håndtering av saker som gjelder egne ansatte ivaretar personvern, samt om de i tilstrekkelig grad er egnet til å ivareta tilliten til NAV.

Tema for revisjonen er:

- Gjeldende rutiner for sperring og bruk av alternativt behandlingskontor

Internrevisjonsoppdragene – GDPR klar

Internrevisjonen / **Oppdragsdefinisjon**

Revidert enhet: NAV	Utarbeidet av: KB/Team
Revisjonsoppdrag (referanse og navn): C2018-03 - Implementering av personvernforordningen	Utarbeidet dato: 06.03.18

2. Overordnet risikovurdering

Det er risiko for at

- NAV ikke klarer å imøtekomme kravene i GDPR
- NAVs omdømme blir redusert og brukere mister tillit til NAV
- NAV kan få store bøter ved overtredelse

3. Revisjonsformål og -tema

Internrevisjonen skal kartlegge om NAV er i rute med implementeringen av GDPR før reglene trår i kraft.

Revisjonsrapportene

Revisjonsrapport C2018-04

Egne ansatte som brukere av NAV

Rutiner for skjerming og bruk av alternativt behandlingskontor

31. mai 2018

Rapportmottaker:
Inger-Johanne Stokke, HR-direktør; Geir Axelsen, økonomi- og styringsdirektør; Kjersti Monland, ytelsesdirektør; Kjell Hugvik, arbeids- og tjenestedirektør; Torbjørn Larsen, IT direktør;
Kopimottakere:
Sigrun Vågeng, arbeids- og velferdsdirektør; Anders Holt, Personvernombud; Yngvar Åsholt, Kunnskapsdirektør; Ingrid Nikolic, HR-Partner; Anja Hildonen, Juridisk seksjon; Terje Andre Olsen, Sikkerhetsseksjonen; Michael Nielsen, Ytelsesavdelingen; Ole Morten Pünther, Arbeid- og tjenesteavdelingen; Øyvind Mogen, seksjon for program- og utvikling; Kari W. Ebbesen, Økonomiseksjonen; Evelyn Bendiktsen, Ytelsesavdelingen; Petter Hafskjold, IT-arkitektur.

Versjon 1.0

Revisjonsrapport - C2018-03

Implementering av personvernforordningen

29. juni 2018

Rapportmottakere:
Yngvar Åsholt, kunnskapsdirektør; Geir Axelsen, økonomi- og styringsdirektør; Anders Holt, Personvernombud; Kjell Hugvik, arbeids- og tjenestedirektør; Torbjørn Larsen, IT-direktør; Kjersti Monland, ytelsesdirektør; Inger-Johanne Stokke, HR-direktør; Hege Turnes, kommunikasjonsdirektør

Kopi:
Sigrun Vågeng, arbeids- og velferdsdirektør

Versjon 1.0

…og våre vurderinger…

2.3. Overordnet vurdering

Rutinene for å sikre diskresjon/skjerme personopplysninger for NAVs ansatte har store svakheter	**ORANGE**

1.3. Overordnet vurdering

Etaten er i gang med forberedelser for å imøtekomme GDPR krav, men arbeidet er ikke helhetlig og systematisk og mye gjenstår. Samtidig er det ikke avsatt nok ressurser til arbeidet. Etaten vil ikke etterleve alle sentrale GDPR krav når forordningen trer i kraft.

De 8 kriterier som ble vurdert («GDPR klar»)

4. Implementering av personvernforordningen

Implementering av personvernforordningen er ikke på plass innen 6. juli 2018, men det gjennomføres et prosjekt, Nye personvernregler i NAV, fase 3. Prosjektet er foreløpig forsinket og mangler ressurser.

1. Det er gjort en overordnet kartlegging av etatens personopplysninger og formålet disse brukes til, men det bør gjøres en grundigere kartlegging.
2. NAV mangler en fullstendig oversikt over hjemler for behandling av personopplysninger. Videre mangler NAV i noen tilfeller hjemler for behandlinger vi utfører (eksempelvis for automatiserte vedtak og noen grunnlagsregistre mm.)
3. Nødvendigheten av personopplysningene er ikke vurdert i tilstrekkelig grad og bør detaljeres ytterligere. Hvor dypt man skal gå i denne kartleggingen bør adresseres.
4. Personvernkonsekvensvurdering og risikoanalyse for brukers/registrertes forhold er kun gjennomført i nye prosjekter, men i liten grad for gamle systemer i NAV.
5. Det finnes i varierende grad regler og rutiner for lagring, retting og sletting, men disse er i liten grad revidert med hensyn til om de imøtekommer krav i Personvernforordningen.
6. Det finnes regler for innsyn, men rutiner er ikke godt nok kjent og innsynslogger og innsynsløsninger er under arbeid. Mye må i dag løses manuelt ved innsynsbegjæring fra brukere og dagens løsning er ikke tilfredsstillende.
7. Informasjon om rettigheter og plikter til bruker er utarbeidet.
   Etaten mangler oppdaterte rutiner for varsling av Datatilsynet og bruker ved brudd på personvernet.
8. Mal for databehandleravtaler er utferdiget, men alle eksisterende avtaler er ikke oppdatert og malen må tilpasses de enkelte kontraktene. Databehandleravtaler vil i stor grad være på plass før 06.07.18.

Bevisst valg å være transparente

GDPR – Ready or not, here we come

Ovenstående tittel var også tittel på et innlegg på den nasjonale fagkonferansen i offentlig revisjon, avholdt på Lillestrøm den 23. oktober. Innlegget ble holdt i to-spann av NAVs personvernombud, Anders Holt, og undertegnede. Hensikten var å gi en overordnet status på GDPR og fortelle hva internrevisjonen gjorde våren 2018 for å vurdere hvor langt fra å oppfylle GDPR forordningens krav NAV ville være ved forventet ikrafttredelsesdato ultimo mai 2018.

AV TERJE KLEPP
Revisjonsdirektør, NAV

Det hele starter noen år tilbake. NAV har som mange andre organisasjoner vært underlagt personvernlovgivningen som har eksistert i Norge i en år-rekke. Tidlig i 2016 ble det avdekket at en betrodd medarbeider hadde gjort en rekke uberettigede oppslag i NAVs fagsystemer på personer vedkommende ikke hadde tjenstlig behov for å undersøke. NAV valgte i dette tilfelle å anmelde vedkommende.

På bakgrunn av denne saken valgte Arbeids- og velferdsdirektøren å engasjere et eksternt advokatfirma, som i samarbeid med et revisjonsselskap gjennomførte undersøkelser av blant annet hvordan NAV forholdt seg til regelverket om behandling av personopplysninger. I slutten av oktober 2016 avga disse en omfattende rapport til ledelsen i NAV, som valgte å offentliggjøre hele rapporten.

En av anbefalingene i rapporten var at NAV etablerer et personvernombud. På dette tidspunktet var det kjent hvilke krav som ville komme i GDPR forordningen som var ventet å tre i kraft ca 1,5 år etter at rapporten til NAV ble presentert. Ett av disse kravene var at NAV måtte ansette et personvernombud senest i annet halvår 2018. På bakgrunn av rapportens anbefaling ble arbeidet med å ansette et personvernombud igangsatt, og høsten 2017 hadde NAV ansatt sitt første personvernombud, Anders Holt, som kom fra tilsvarende stilling i Telenor-konsernet.

Internrevisjonen i NAV starter planleggingsarbeidet for kommende kalenderår på høsten. Ett av prosjektene som ble diskutert med ledelsen og vedtatt av Arbeids- og velferdsdirektøren sent i 2017 het; «Implementering av personvernforordningen». Målet for denne revisjonen var å kartlegge hvor langt NAV var kommet med hensyn til implementering av GDPR ved forventet ikrafttredelsesdato 28.05.2018 (denne fristen ble som kjent senere utsatt flere ganger sist til 28.07.2018). Dette revisjonsoppdraget, som vi i kortversjon kalte *«GDPR readiness»*, måtte derfor gjennomføres tidlig i 2018.

Vi startet revisjonsprosjektet vinteren 2018, og i vår oppdragsdefinisjon valgte vi følgende innfallsvinkel; «Internrevisjonen vil i denne revisjonen undersøke om:

- NAV har kartlagt hvilke personopplysninger de har og hvilket formål disse brukes til
- Hjemmel for behandling av personopplysninger er på plass
- Nødvendigheten av personopplysningene er vurdert
- Risikoanalyse for brukers forhold er gjennomført
- Det finnes regler og rutiner for lagring, retting, sletting av personopplysninger
- Det finnes regler og rutiner for innsyn
- Det finnes rutiner for informasjon om rettigheter og plikter til bruker
- Avtaler (eks. databehandleravtaler ol.) er på plass»

Revisjonen ble basert på intervjuer og dokumentgjennomgang, og vi tok sikte på å levere vår revisjonsrapport før sommerferien.

Rapporten ble sendt på høring tidlig i juni, og den endelige revisjonsrapporten ble datert 29. juni 2018. På det tidspunktet var det klart at implementeringstidspunktet for GDPR forordningen hadde blitt utsatt til 6. juli, slik at vår rapport ble sendt til toppledelsen i NAV før reglene trådte i kraft. Fordi Norge fulgte implementeringstidspunktet for EØS land ble ikrafttredelsen ytterligere utsatt til 28. juli, uten at det hadde noen praktisk betydning.

Internrevisjonen hadde en hypotese om at NAV ikke ville klare å oppfylle alle forordningens krav ved implementeringstidspunktet. Denne hypotesen ble da bekreftet gjennom revisjonsarbeidet, og vi trakk følgende hovedkonklusjon i vår rapport: *«Etaten er i gang med forberedelser for å imøtekomme GDPR krav, men arbeidet er ikke helhetlig og systematisk og mye gjenstår. Samtidig er det ikke avsatt nok ressurser til*

arbeidet. Etaten vil ikke etterleve alle sentrale GDPR krav når forordningen trer i kraft.»

Som det fremgår av hovedkonklusjonen hadde NAV iverksatt mye arbeid, og flere av tiltakene ble også nevnt i vår hovedoppsummering hvor vi skrev;

«Følgende er utført:

- Personvernombud er ansatt
- Det er utarbeidet en oversikt over etatens behandlinger av personopplysninger på et overordnet nivå
- Det er gjennomført personvernkonsekvensvurderinger for alle nye systemer, om enn av forskjellig detaljgrad og kvalitet
- Det er laget informasjonspakker for NAV kontaktsenter og NAV kontorene og egen side på Navet (som er NAVs interne intranettside)
- Klageinstansen i Bergen har fått delegert ansvaret for forespørsler om retting og sletting
- Styringsdokumenter for personvern er utarbeidet
- Mal for Databehandleravtaler er oppdatert
- Det er gitt opplæring til flere personer i direktoratet
- Det er opprettet Personvernforum som møteplass og for læring i direktoratet
- Personvernerklæring er publisert på nav.no (NAVs eksterne kilde til informasjon)
- Rutiner for varsling til Datatilsynet og bruker ved brudd på personvernet lages av Sikkerhetsseksjonen og vil være på plass fra 01.08.18

En god del arbeid var altså igangsatt før eller under perioden vi gjennomførte vår revisjon. Imidlertid var det relativt mye arbeid som gjenstod på det tidspunkt vi avga vår revisjonsrapport. De forhold vi valgte å fremheve i vår konklusjon var følgende;

- Vi kommer ikke i mål på alle punkter med implementeringen av GDPR i etaten før fristen 06.07.18
- Prosjekt fase 3 er ennå ikke fullstendig oppbemannet og prosjektet er forsinket
- Det gjenstår å gjøre personvernkonsekvensvurderinger for så å si alle gamle systemer med høy risiko
- Etatens kompetanse på området er mangelfull og det er ikke satt av tilstrekkelige ressurser til arbeidet

- Noe testing foregår fortsatt på reelle brukerdata
- Når det gjelder automatisering og sammenstilling av opplysninger på utviklingssiden må GDPR krav ivaretas og det er krevende
- Det er utfordringer med fortolkningen av kravene i det nye regelverket, og dette påvirker spesielt utviklingssiden
- Systematisk opplæringsløp for etaten er ikke på plass
- Etatens arbeid for å imøtekomme GDPR krav er skriftlig dokumentert i varierende grad
- Det synes å mangle en helhetlig koordinering av etatens arbeid, enheter adresserer GDPR separat, noe som ikke er effektivt og innebærer risiko for ulik adressering og tolkning

Ovenstående kan synes som en lang liste med mangler. Det er imidlertid et meget omfattende regelverk som nå er gjeldende. Selv om forordningen ble vedtatt i EU våren 2016, er nok erkjennelsen at de fleste kom sent i gang med arbeidet for å tilpasse seg regelverket, og at det vil være mange andre instanser i Norge som nok opplever å ha mye gjenstående arbeid før alt er på plass, selv mange måneder etter forordningens ikrafttredelse.

Etter at vår rapport ble publisert har NAV satt ekstra ressurser på arbeidet – og også engasjert eksterne konsulenter med spisskompetanse på forordningen. En del av tiltakene vi anbefalte i vår rapport hadde forfall først mot slutten av året. Så selv om det fremdeles er en del gjenstående arbeid når denne artikkelen skrives, vil NAV ved inngangen til 2019 være langt bedre stilt enn da internrevisjonen startet sin gjennomgang av *«GDPR Readiness»*.

…men kanskje ikke så transparente…

8.1.2019

Innsyn i internrevisjonsrapporter

Media: NRK Nyheter
Journalist: Marianne Johansen

Beskrivelse:
Hei!

Jeg ber om innsyn i alle internrevisjonsrapporter fra 2018.

På forhånd takk for hjelpen!

Oppfølging:
Følges opp i morgen.

Ansvarlig avd: Internrevisjonen
Fagansvarlig: Terje Klepp
Status: Åpen

Hva er GDPR status i NAV nå?

NAVS GDPR Status nå (dvs pr. oktober 2018):

- Ansatt personvernombud
- …

GDPR prosjektet løper fremdeles!

Leverer videre på det følgende:

Er i fase 3 – flyttet fra IT, som nå er et delprosjekt under hovedprosjektet

NAVS GDPR status nå

- Styring (internkontroll):
  - Sikkerhet versus Personvern
  - Styringsdokumenter
  - Implementering
- Full oversikt – alltid – løpende - Behandlingsoversikt
  - Behandlingsoversikt og systemoversikt
  - Oversikt over manuell behandling –implementering
- Rettigheter og plikter
  - Eksempel: Rett til innsyn: Innsynsbegjæring
- Informasjonssikkerhet versus personvernsikkerhet
  - Risikoanalyser
  - Personvernkonsekvensvurdering (DPIA)
- Tredjeparter
  - Hvem er de – Databehandleravtaler, små og store leverandører
- Avvik – Brukere – Ansatte – Kombinasjoner av ansatte / brukere
- Kompetanse – diverse løp.

NAVS GDPR status nå - Oppsummert

NAV jobber videre for fullt både med

- Videre implementering av ansvar / kompetanse / implementering
- Et GDPR-prosjekt som vokser og har en lang hale

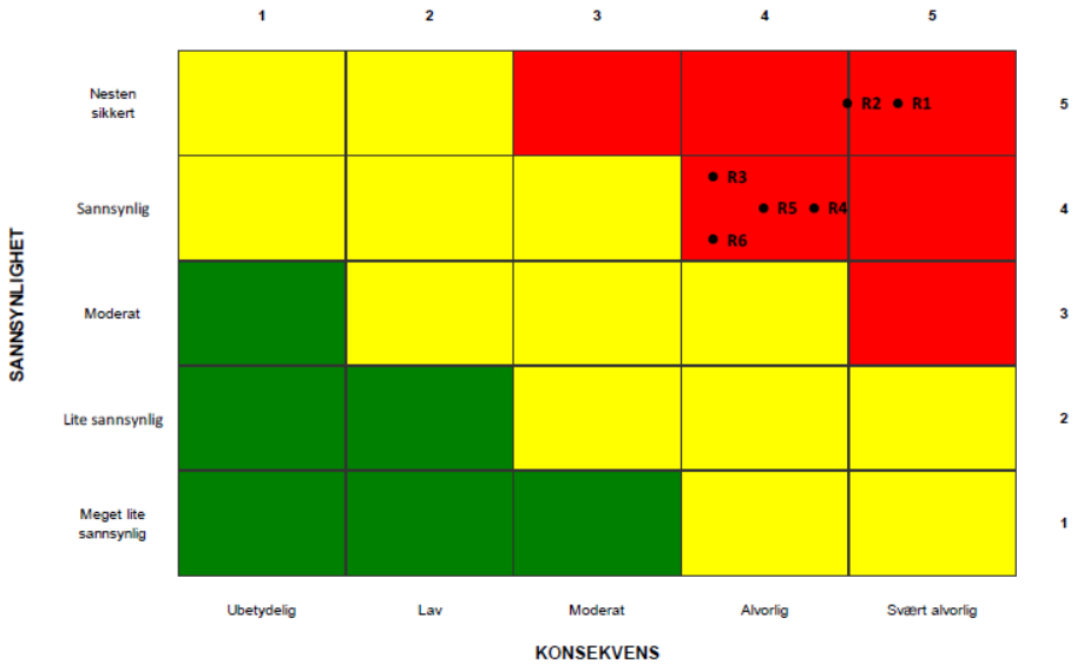
Arbeid med personvern er krevende – og morsomt:

1. Ingen kompetanse – hjelp til alt, spør om alt
2. Litt kompetanse – hjelp til alt, spør om like mye
3. Mye kompetanse – behøver ikke hjelp til alt, men spør kanskje mer
4. Tung kompetanse – ikke hjelp til noe, spør sjeldnere, men mer krevende spørsmål

Men ting tar lenger tid enn man tror…

Seks risikoer klassifiseres som høye Mars 2019

Risikomatrise for høye risikoer



Forklaring

R1	Uavklart lovlig oppbevaringstid
R2	Mangel på faktisk sletting
R3	Relevans og konsekvenser av nye rettigheter for de registrerte er uavklart
R4	Gjenstående arbeid med inngåelse og forvaltning av databehandleravtaler
R5	Gjenstående arbeid med systematisk opplæring
R6	Mangel på systematisk internkontroll

Et lite a-propos mht reaksjonsmønster…

Tidligere NAV-leder dømt for snoking

En tidligere NAV-leder må betale bot, men slipper fengsel etter å ha snoket i opplysninger om flere enn 30 personer i sitt nærmiljø.

SØKTE PÅ NABOEN: Dette er loggene der det går fram dato, og hvilket tidspunkt på dagen den tidigere Nav-lederen gjorde oppslag på nabo-ekteparet.
FOTO: TORMOD STRAND / NRK

Svein Vestrum Olsson
Journalist

Publisert 11. mars kl. 21:13
Oppdatert 11. mars kl. 21:17

Takk for meg!