NAV – Risikovurderinger og databehandleravtale

Høye ambisjoner, store muligheter

November 2018 // Jørgen Holmsen / Leif Tore Løvmo

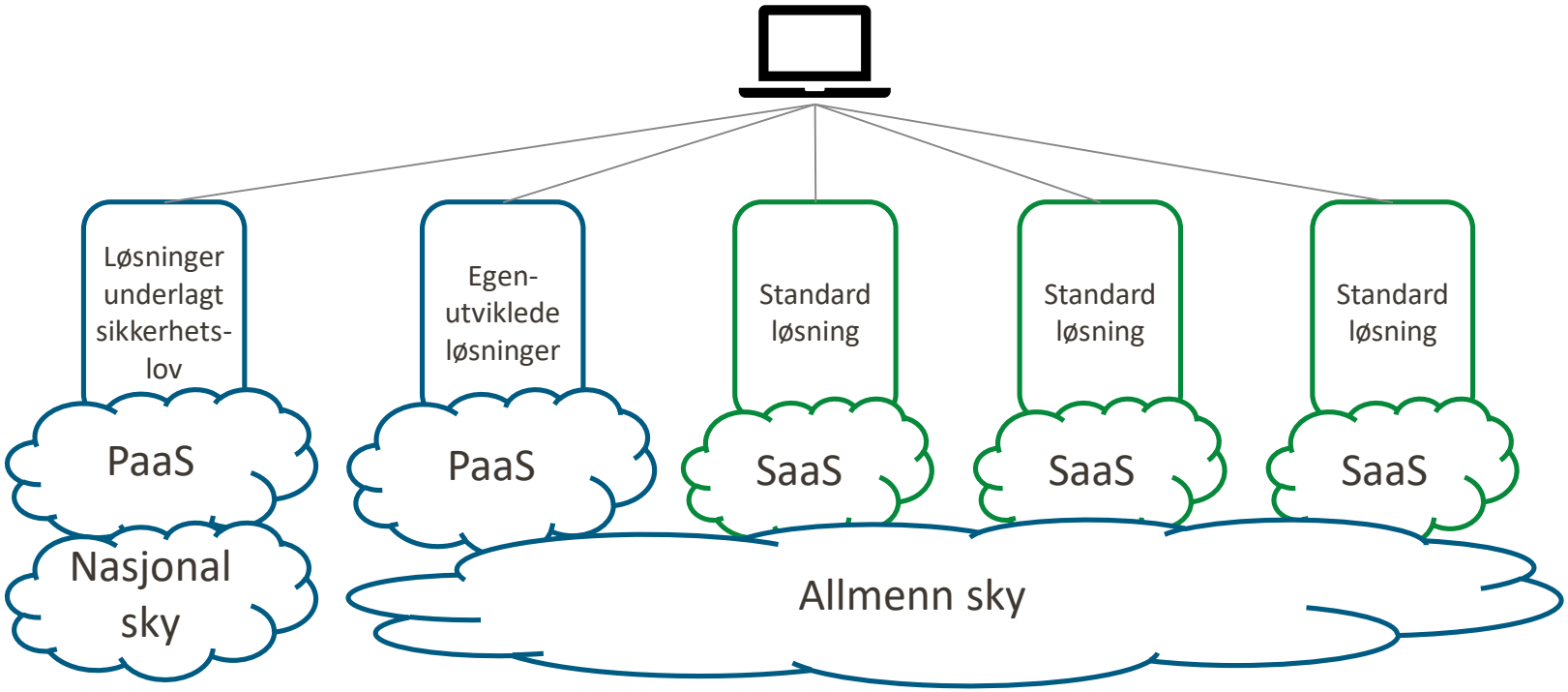
Innhold

- Skystrategi/Målbilde
- Risikovurderinger og personkonsekvensvurderinger
- Databehandleravtale

Bakgrunn

- NAVs sourcingsstrategi og Nasjonal strategi for skytjenester tilsier bruk av skytjenester
- Skytjenester har funksjonalitet og innovasjonstakt som langt overgår hva NAV selv kan levere
- Skytjenester er i sin natur smidige, skalerbare og kostnadseffektive (Agility, elasticity, efficency – ser at funksjonalitet går foran kost)
- Standardløsninger leveres i større og større grad som skytjenester og leverandørene prioriterer skytjenester foran programvare som installeres hos kundene
- Plattform- og infrastrukturtjenester leveres som skytjenester i stor skala, forutsigbare kostnader og mye funksjonalitet
- Sikkerhet er kritisk for skyleverandørene og de bruker mye ressurser på dette

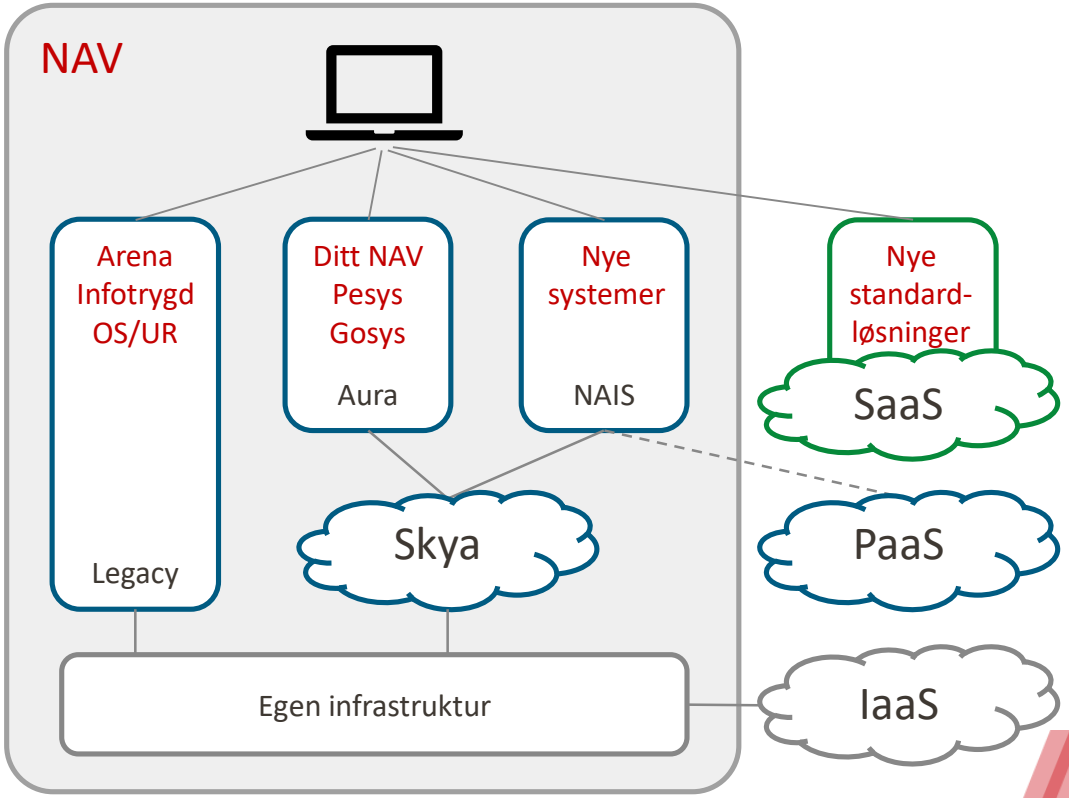
Målbilde



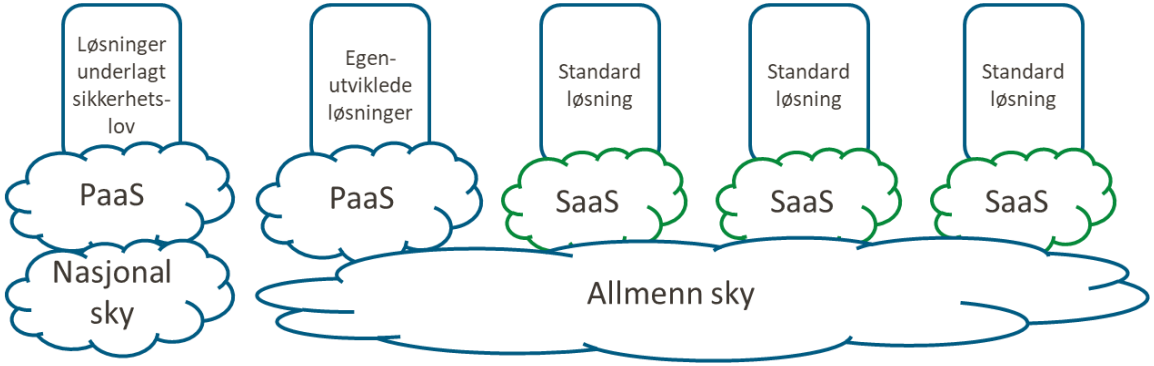
Sikkerhetsloven vil kunne stille krav om at noen av NAVs systemer må være plassert i Norge, men det antas at det kun vil gjelde noen få systemer.

Forslag til prinsipper og overgangsarkitektur

- Egenutviklede løsninger, hyllevare og SaaS skal være sømløst integrert i brukernes arbeidsflate
- Hyllevare er foretrukket og skal fortrinnsvis leveres som skytjeneste
- Nye egenutviklede løsninger skal ikke ha sterke bindinger til NAVs plattform og infrastruktur
- Eventuell bruk av plattform- og infrastrukturtjenester (IaaS) for eksisterende egenutviklede løsninger (legacy) baseres på kostnadsvurdering



Oppsummering



- Skytjenester vil bli en viktig del av NAVs systemportefølje
  - Kostnadseffektiv tilgang til standardfunksjonalitet som stadig videreutvikles
  - Nye, innovative løsninger som integreres med løsningene / skytjenestene
  - Omfattende sikkerhetsfunksjonalitet NAV ikke kan lage selv
- Nødvendig sikkerhet kan ivaretas i skytjenester
  - NAV må ha kontroll på informasjonen som behandles, vurdere risiko og dokumentere hvordan sikkerheten ivaretas
  - Vi må gjøre endringer på dagens løsninger før de legges ut i skyen
- Vi tar i bruk skytjenester kontrollert, stegvis og over tid

- Skystrategi/Målbilde
- **Risikovurderinger og personkonsekvensvurderinger**
- Databehandleravtale

Dette er NAV

1/3 av stats-budsjettet

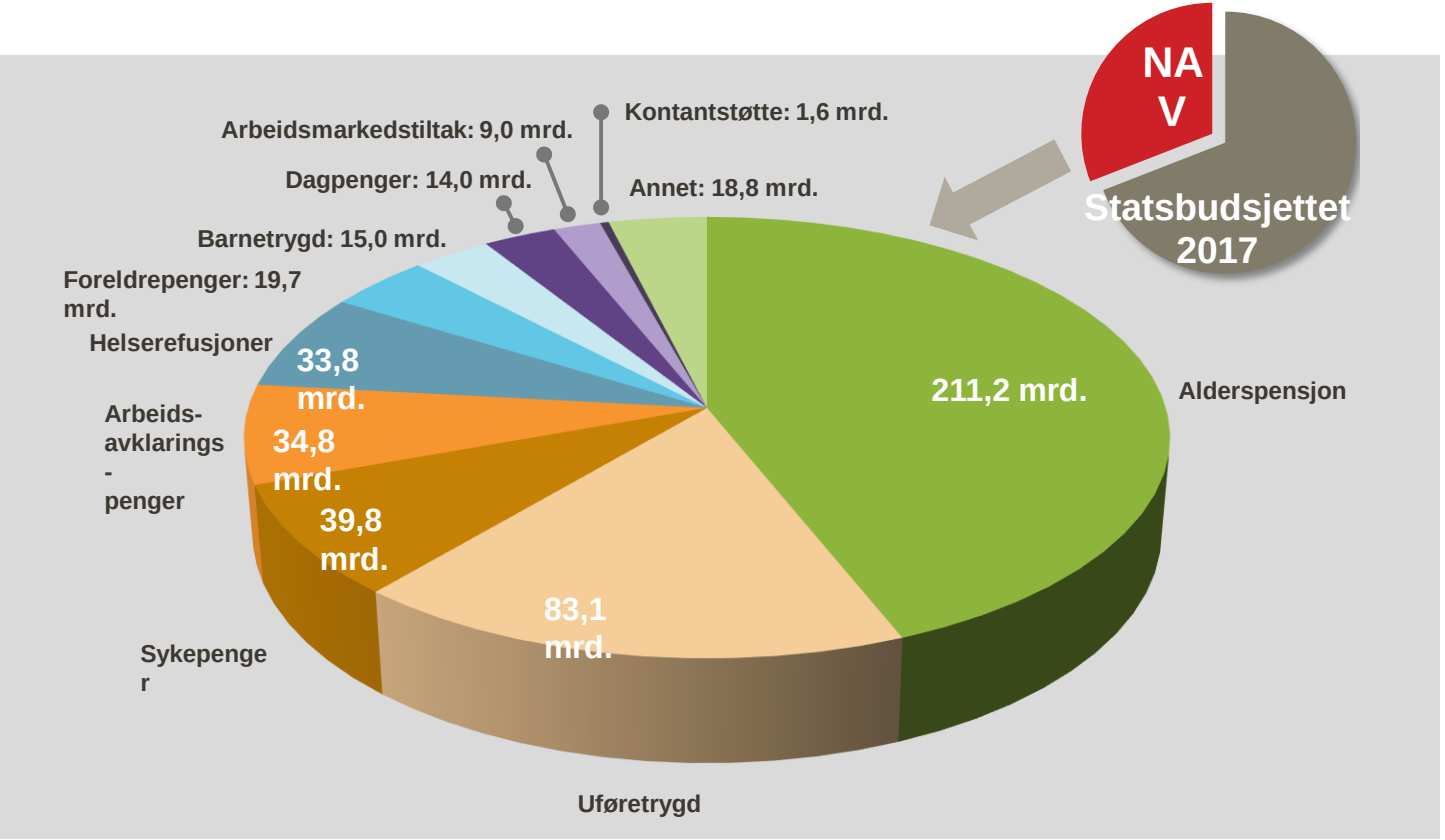
Tjenester til 2,8 mill. mennesker

60 ulike stønader og ytelser

Tjenester mot arbeid

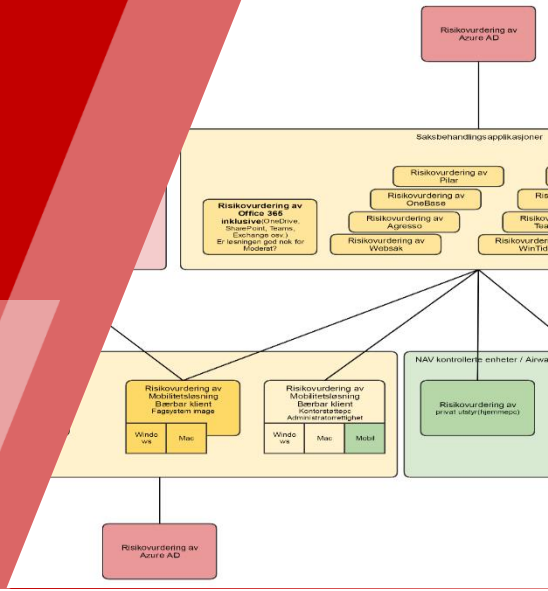
Sosiale tjenester

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.

Risikovurderinger og personvernkonsekvensvurderinger



Leif Tore Løvmo

Hvordan vurderte vi sikkerhet tidligere

- Klassifisering av informasjon(inklusive personverr
- Kravstilling basert på informasjon
- Eventuelt risikovurdering
- Eksterne tjenester – Kravstilling og anskaffelse
- Godkjenning/anbefaling av løsningen av sikkerhetsseksjonen

Abstrakte krav hvordan oppfylles de?

Generell e krav er strenge

Vanskelig for behandlings-ansvarlig å vurdere avvik

Abstrakte krav Hva om man ikke oppfyller kravet?

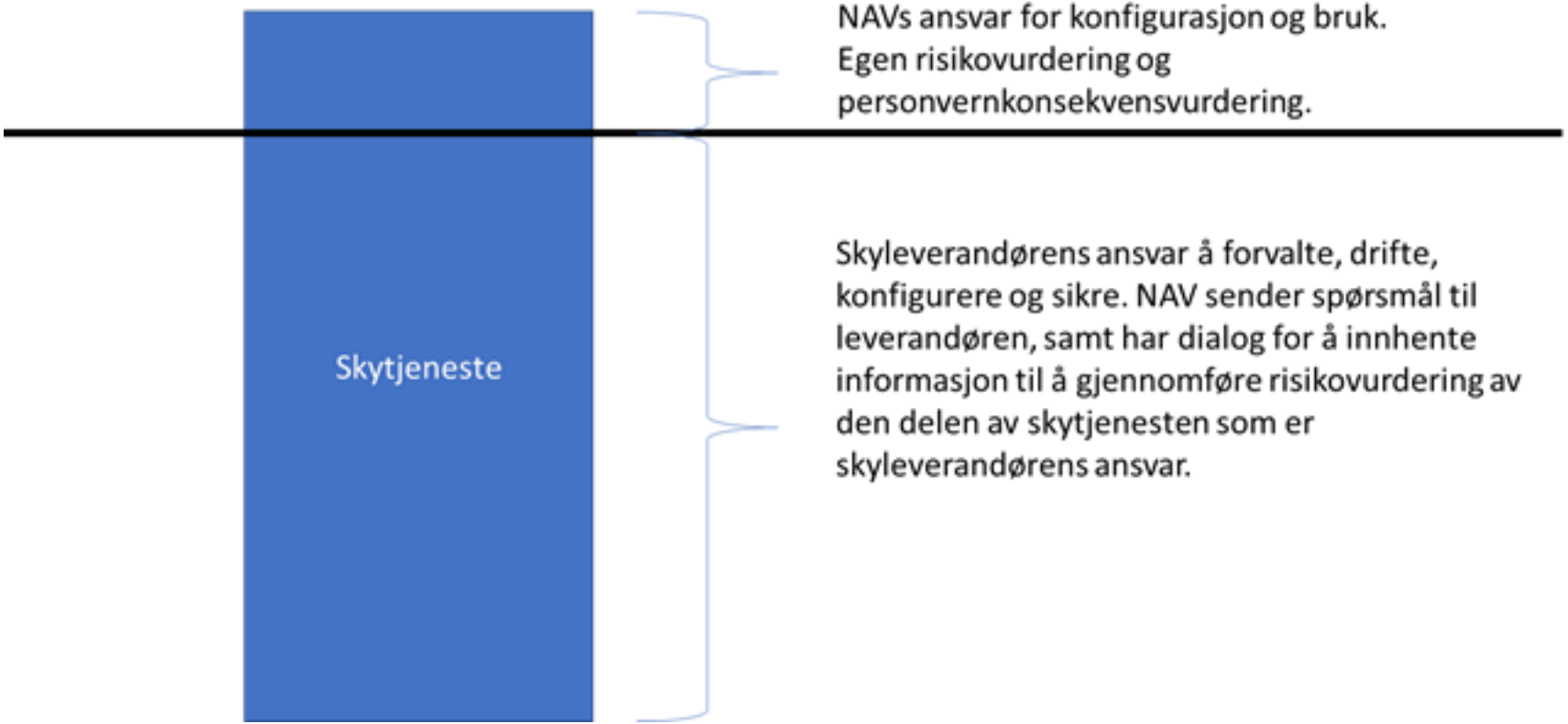
Endringer

- Teamene ansvarlig for sikkerheten
- Behandlingsansvarlig aksepterer restrisiko
- PaaS – Ikke vite hva den skal brukes til
- Kan ikke påvirke sikkerhetsnivået til leverandøren i noen stor grad
- Ansette egne utviklere
- Etablert utvikler-sikkerhetsmiljø
- Ansatt personvernombud
  - Gjennomfører Personvernkonsekvensvurdering

Risikovurderinger – Team ansvarlig

- Fokus på gjennomføring, og innspill fra mange
- Skrive om krav til risikoer(under arbeid)
- Kommunisere risiko istedenfor å stille krav
- Identifisere muligheter

Skytjenester og risikovurderinger



Gjennomføring risikovurdering av leverandør

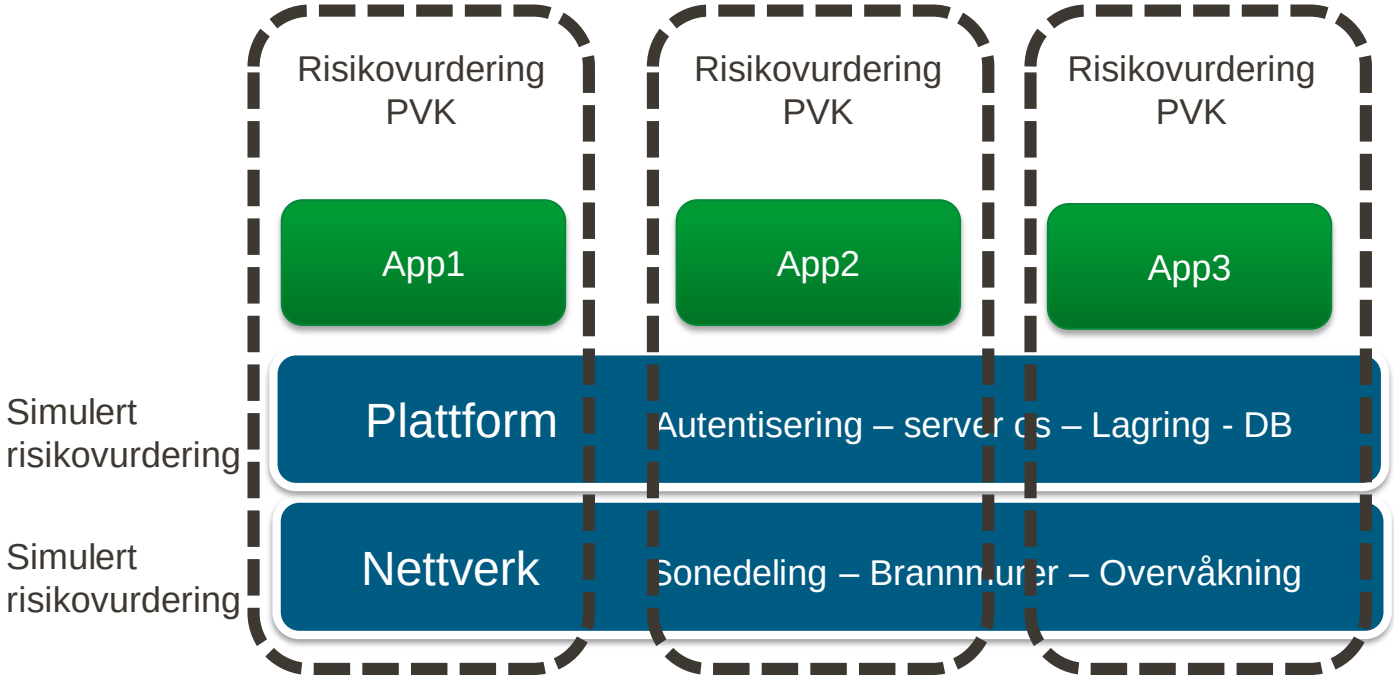
- Innhente svar på spørsmål
- 2 timers presentasjon fra leverandør
- 1-2 timer risikovurdering med (2 personer).
- Kort oppsummering

- Eksempler på funn:
  - Administratorrettigheter
  - Backup
  - Support(Utenfor EU-område)
  - Herding ikke relevant

Gjennomføring risikovurdering av applikasjon

- Felles arbeidsområde(Office 365 Teams) hvor relevante blir informert.
- Ha med deltakere fra forskjellige fagmiljøer(eksempler under):
  - Applikasjon
  - Microsoft Azure AD
  - Sikkerhet/overvåkning
  - Applikasjonssikkerhet
  - Nettverkssikkerhet
  - Database
- Få frem fakta
- Hva er forskjellen fra On-Prem(Muligheter)
- Gjennomføre typisk i workshoper(1-3) 1 t. møter.
- Oppsummering til beslutning

Fra godkjenning plattform til risikovurdering av applikasjon

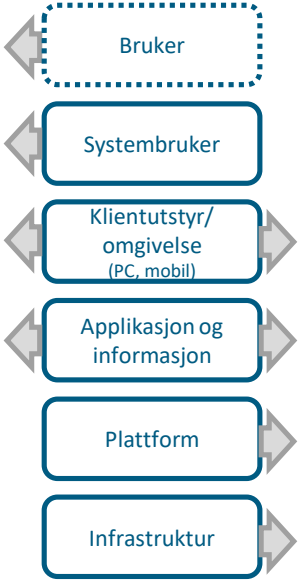


Ansvar - Restrisiko

Fagsiden

Den behandlingsansvarlige (fagsiden) har ansvar for å vurdere risikoen knyttet til hvordan informasjon behandles – hvem bruker IT-løsningen, hvor brukes den og hvilken risiko er det for at informasjon kommer på avveie.

Behandlingsansvarlig har ansvar for personvern og risiko i løsningen og at det er utarbeidet personvernkonsekvens-vurdering. Behandlingsansvarlig tar beslutning om det er akseptable risiko knyttet til behandlingen.

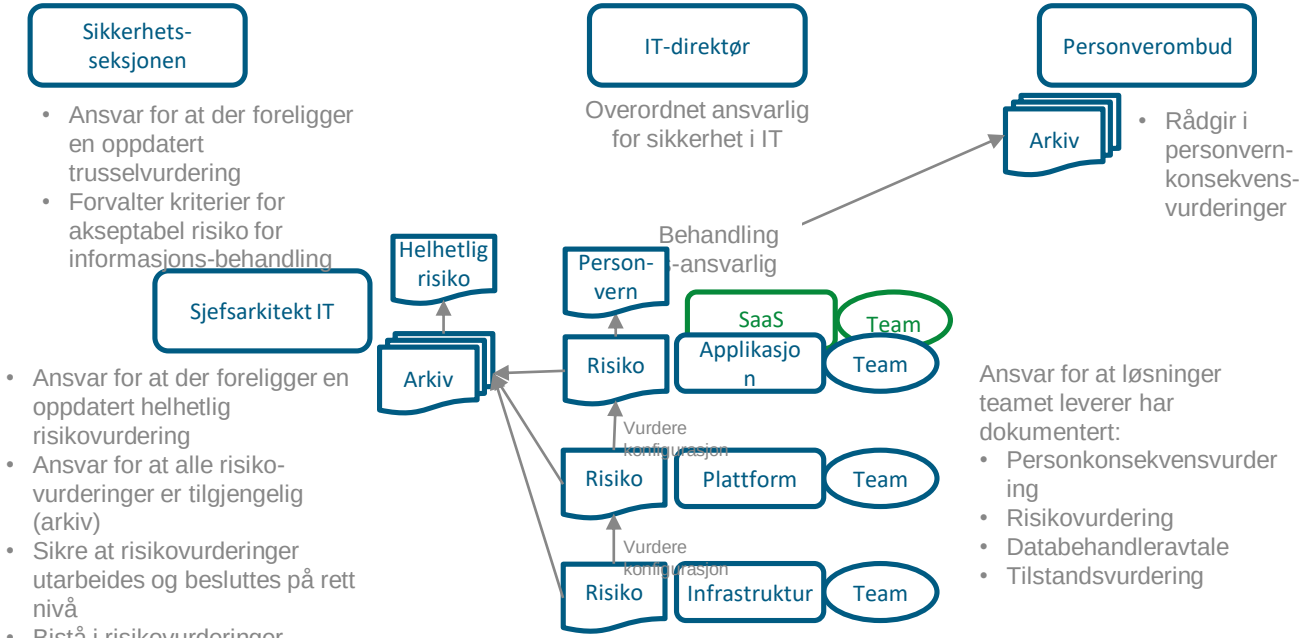


IT-avdelingen

Teamet har ansvar for å sikkerheten og å vurdere risikoen knyttet til sine løsninger basert på risiko i tilgrensende og underliggende løsninger (applikasjon, plattform, infrastruktur). Teamet tar beslutning om løsningen har akseptabel risiko. Ved behov rådfører teamet seg med sjefsarkitekt IT.

Teamet skal også forsikre seg om at det er utarbeidet personvern-konsekvensvurdering og databehandleravtaler der det er nødvendig.

Roller knyttet til risikovurderinger i IT

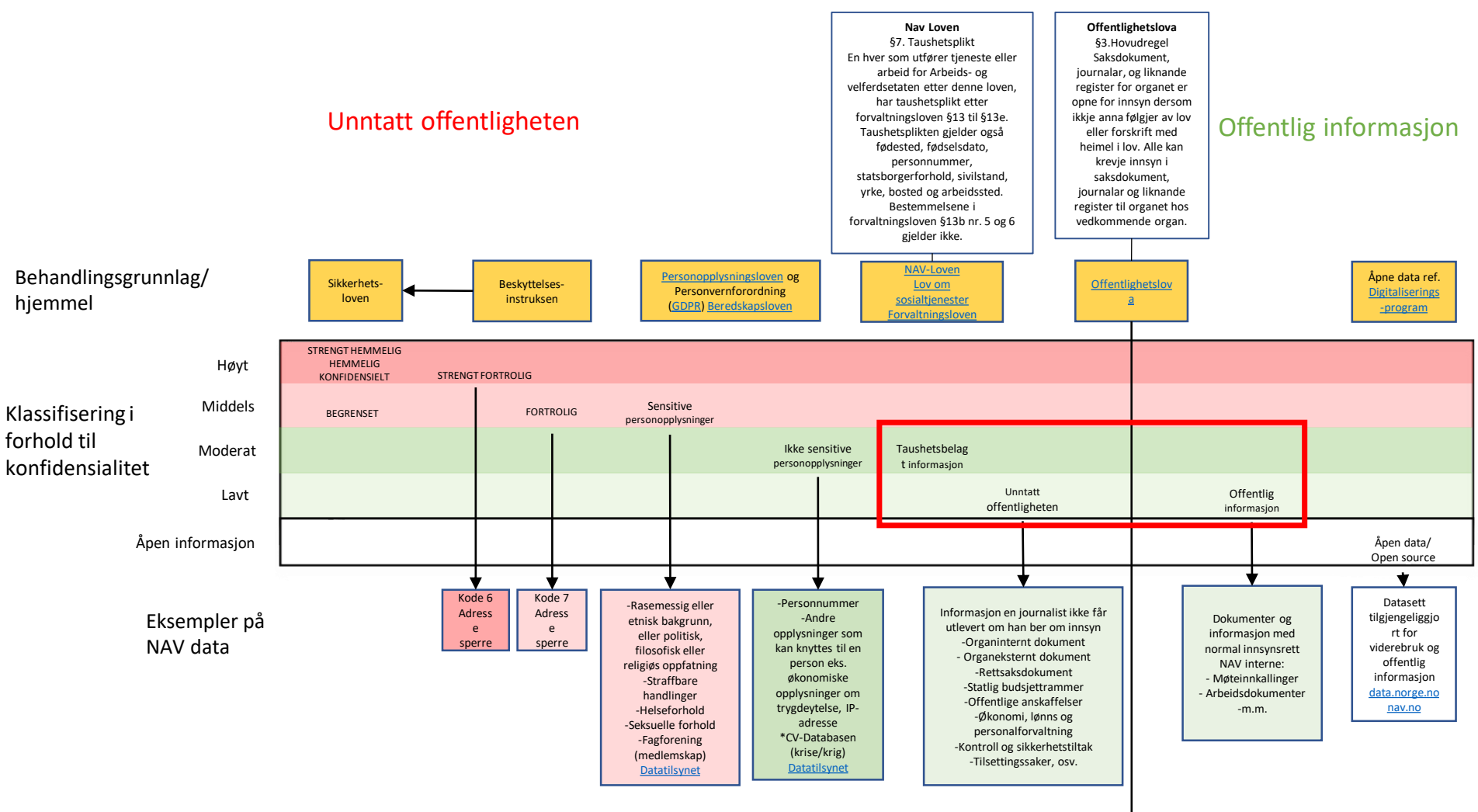


- Ansvar for at der foreligger en oppdatert trusselvurdering
- Forvalter kriterier for akseptabel risiko for informasjons-behandling

- Ansvar for at der foreligger en oppdatert helhetlig risikovurdering
- Ansvar for at alle risiko-vurderinger er tilgjengelig (arkiv)
- Sikre at risikovurderinger utarbeides og besluttes på rett nivå
- Bistå i risikovurderinger

Ansvar for at løsninger teamet leverer har dokumentert:

- Personkonsekvensvurder ing
- Risikovurdering
- Databehandleravtale
- Tilstandsvurdering


Unntatt offentligheten
Offentlig informasjon
Nav Loven
§7. Taushetsplikt
En hver som utfører tjeneste eller arbeid for Arbeids- og velferdsetaten etter denne loven, har taushetsplikt etter forvaltningsloven §13 til §13e. Taushetsplikten gjelder også fødested, fødselsdato, personnummer, statsborgerforhold, sivilstand, yrke, bosted og arbeidssted. Bestemmelsene i forvaltningsloven §13b nr. 5 og 6 gjelder ikke.
Offentlighetslova
§3.Hovudregel
Saksdokument, journalar, og liknande register for organet er opne for innsyn dersom ikkje anna følgjer av lov eller forskrift med heimel i lov. Alle kan krevje innsyn i saksdokument, journalar og liknande register til organet hos vedkommende organ.
Behandlingsgrunnlag/ hjemmel
Sikkerhets-loven
Beskyttelses-instruksen
Personopplysningsloven og Personvernforordning (GDPR) Beredskapsloven
NAV-Loven Lov om sosialtjenester Forvaltningsloven
Offentlighetslov a
Åpne data ref. Digitaliserings -program
Klassifisering i forhold til konfidensialitet
Høyt
Middels
Moderat
Lavt
Åpen informasjon
STRENGT HEMMELIG
HEMMELIG
KONFIDENSIELT
STRENGT FORTROLIG
BEGRENSET
FORTROLIG
Sensitive personopplysninger
Ikke sensitive personopplysninger
Taushetsbelagt informasjon
Unntatt offentligheten
Offentlig informasjon
Åpen data/ Open source
Eksempler på NAV data
Kode 6 Adresse sperre
Kode 7 Adresse sperre
-Rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning
-Straffbare handlinger
-Helseforhold
-Seksuelle forhold
-Fagforening (medlemskap)
Datatilsynet
-Personnummer
-Andre opplysninger som kan knyttes til en person eks. økonomiske opplysninger om trygdeytelse, IP-adresse
*CV-Databasen (krise/krig)
Datatilsynet
Informasjon en journalist ikke får utlevert om han ber om innsyn
-Organinternt dokument
- Organeksternt dokument
-Rettsaksdokument
-Statlig budsjettrammer
-Offentlige anskaffelser
-Økonomi, lønns og personalforvaltning
-Kontroll og sikkerhetstiltak
-Tilsettingssaker, osv.
Dokumenter og informasjon med normal innsynsrett NAV interne:
- Møteinnkallinger
- Arbeidsdokumenter
-m.m.
Datasett tilgjengeliggjort for viderebruk og offentlig informasjon
data.norge.no
nav.no

- Skystrategi/Målbilde
- Risikovurderinger og personkonsekvensvurderinger
- Databehandleravtale

Avtalestruktur og databehandleravtale

- Databehandleravtale inngår som en del av avtalerammeverket knyttet til skytjenesten
- Databehandleravtalen må vurderes som en del av anskaffelsesprosessen før avtalen inngår/aksepteres
- Hvert team som ønsker ta i bruk allmenn skytjenester (les legge ut data), der det er inngått avtale, må lese og forstå hvilke avvik som finnes og hva det betyr for dem
- I NAV er det etablert felles oversikt over hvilke databehandler brukes til hvilke formål/type data (gjelder også hvilken brukerdata som lagres)

Databehandleravtale

- NAV har laget seg en mal basert på Datatilsynet sin med tillegg. Den er såkalt behandlingsansvarligvennlig
- Består av
  - Hoveddel - Sier noe om bruk av underdatabehandlere, revisjon, bistand, lovvalg og verneting, meldingsflyt etc
  - Vedlegg 1 - Databehandlingens omfang
  - Vedlegg 2 - Tekniske og organisatoriske sikkerhetstiltak
  - Vedlegg 3 - Oversikt over godkjente underdatabehandlere
- Fungerer fint mot mindre leverandører som ikke har egen databehandleravtale
- Fungerer ikke så bra mot store leverandører har sine egne databehandleravtale som er såkalt databehandlervennlig
  - Avtaleteksten i både hoveddel, Vedlegg 1, 2 og 3 ligger fast i utgangspunktet (kan ikke endres)

Databehandleravtale

- Databehandleravtalen er en del av avtalerammeverket og eies således av IT-avtaler i NAV
- Selve databehandleravtalen er ikke stor, men det er mange henvisninger til tjenester som omfattes og hvor det er forskjeller (f.eks globale tjenester)
- Må være veldig klar på hvilke tjenester man skal ta i bruk før man starter gjennomgang av databehandleravtalen slik at service-terms for de tjenester man skal ta i bruk også vurderes

Avtaleform – en skog av avtaler

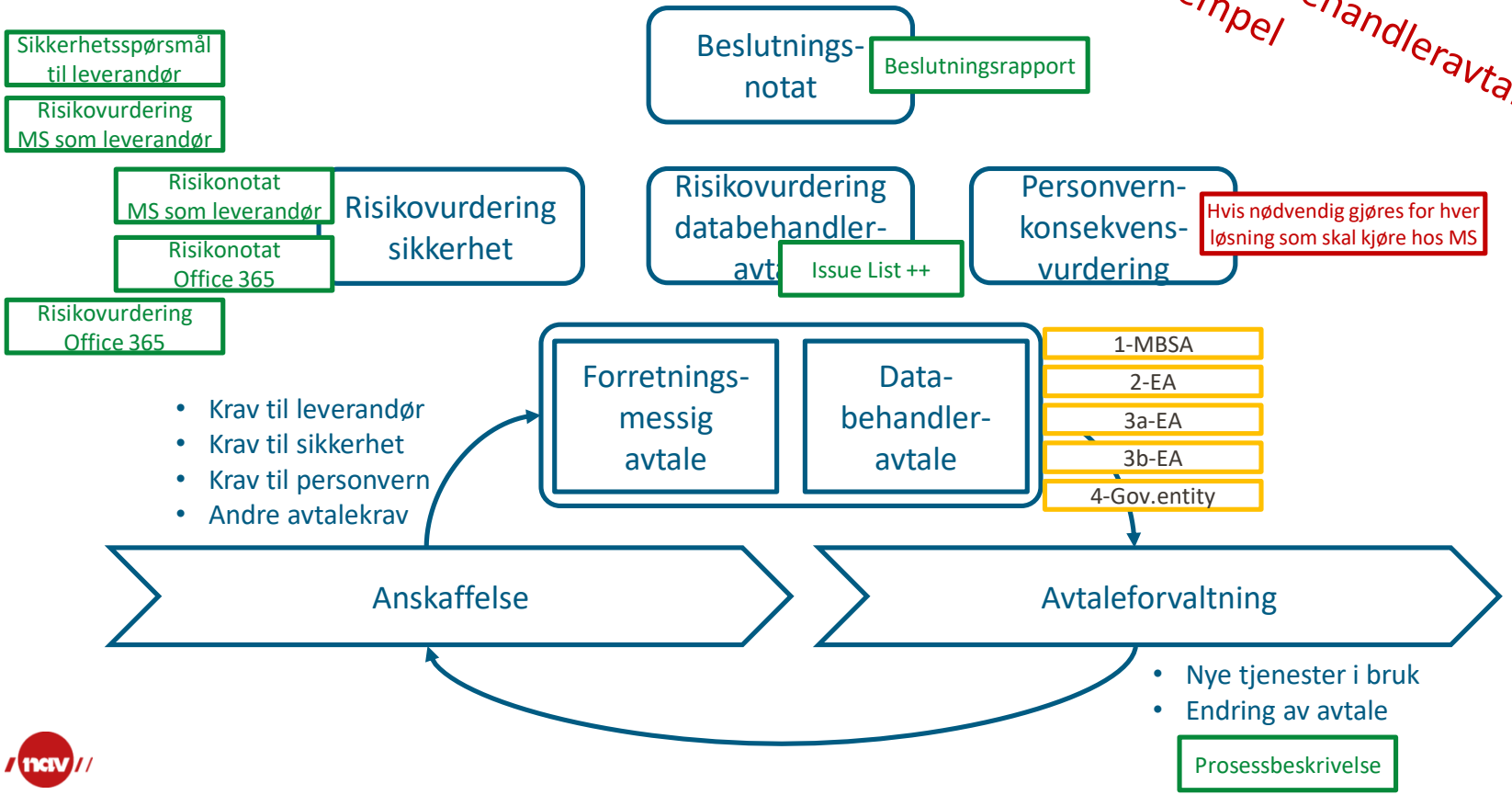
- For gjennomgangen av Microsoft sin OST (som er Microsoft sin databehandleravtale) gikk NAV også igjennom følgende dokumenter (senere referert til som «Avtalen»):
  - Vilkår for Elektroniske Tjenester («OST»), herunder særlig Vilkår for Personvern og Q&A fra Microsoft («Q&A»),
  - Tillegg for kvalifiserte offentlige enheter («TOE»),
  - Microsoft Business and Services Agreement («MBSA»),
  - Server- og Skyregistrering («SS»),
  - Skjema for Produktvalg for Foretak og Foretaksregistrering for Abonnement («Skjema»),
  - Foretaksregistrering (Indirekte) («Foretaksregistrering»),
  - Enterprise-avtale («EA»),
  - Programsignaturskjema («Signaturskjema»),
  - Server- og Skyregistrering (Indirekte) («SSI»),
  - Microsofts personvernerklæring («Personvernerklæringen»).

Arbeidsform – første versjon

- NAV har vurdert («nærlest») alle dokumentene («Avtalen») opp mot NAV sin mal for databehandleravtaler og personvernforordningen 2016/679 («GDPR») – spesielt betingelsene som berører personvern og personvernrettslige forhold.
- NAV har også gjennomgått øvrig relevant lovgivning, og der det foreligger eventuelle utfordringer knyttet til avtaleinngåelsen er dette kommentert
- Igjennom arbeidsmøter med deltakere fra juridisk (jurister og personvernombudet), IT-avtaler, drift, utvikling og arkitektur ble funn diskutert
- Resultatet er en liste med funn/krav NAV har presentert leverandør og som NAV må gjøre en vurdering av risiko på gitt NAV ikke får medhold
- Leverandøren har vært involvert hele veien
  - Utfordret med behov og krav – både skriftlig og muntlig

Overordnet prosess (er i støpeskjea)

MS databehandleravtale som eksempel



Funn MS avtalen

- Der NAV har ansett de norske versjonene av dokumentene for å være uklare, har NAV foretatt en gjennomgang av engelsk versjon av dokumentene.
- NAVs vurdering av Avtalen i sin helhet er at denne er i samsvar med GDPR, og at Avtalen er databehandlervennlig.
  - Der GDPR gir handlingsrom til det går vilkårene i Microsofts favør, eksempelvis ved revisjon, lovvalg og verneting.
- Gjennomgangen av Avtalen synliggjør flere forhold som avviker fra NAVs Databehandleravtale, uten at disse forholdene er i strid med GDPR.

Avvik fra NAVs databehandleravtale (1)

- Lovvalg og verneting
- Overføring til tredjeland (kontroll på EU Model Clauses - EMC)
- Databehandlingens omfang (vedlegg 1)
- Bruk av underdatabehandlere (kontroll av nye)
- Revisjon (egen, tid etc)
- Rutiner ved opphør (hva skjer dersom NAV pga avvik ønsker å terminere tjenesten)

Avvik fra NAVs databehandleravtale (2)

- Hvilken taushetserklæring som skal benyttes
- Ansvarsfraskrivelser for indirekte tap - erstatningsbestemmelsen
- Varsling av avvik/sikkerhetsbrudd
- Vilkår i Avtalen kan ensidig endres av leverandør
- Sikkerhetstiltak (vedlegg 2), tekniske og organisatoriske, er ikke detaljspesifisert i Avtalen, informasjon er i andre dokumenter og på leverandørens nettsider

Oppsummering

- Teknisk risiko avklart tidlig
- Databehandleravtalen viste seg å være ressurskrevende og ta lang tid
- NAV har avdekket uklarheter, foreslått endringer og må dokumentere restrisiko og konsekvens
- Forvaltning og oppfølging av Avtalen er sentralt for å ivareta personvern
  - NAV må detaljere rutiner og prosesser
  - NAV har sett at det må på plass flere ressurser