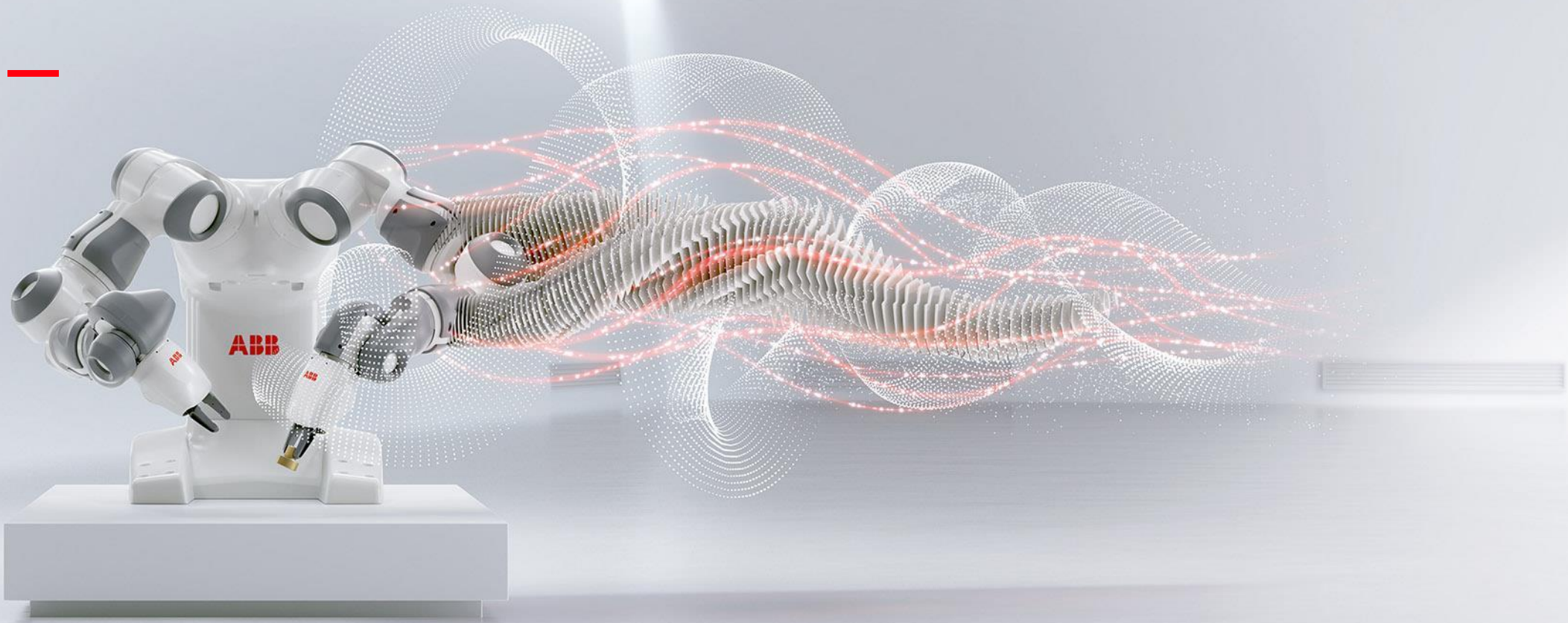


GDPR (General Data Protection Regulation) og Personopplysningeloven av 2018 og

De nye reglene sett fra en Pensjonskasses ståsted

PENSJONSKASSEKONFERANSEN 2019 – FRODE ONARHEIM

Fakta om ABB

2018

ABB i Norge:

- ❑ Driftsinntekter i Norge: **NOK 8,5 milliarder**
- ❑ Antall ansatte i Norge: **rundt 2 100**

ABB Globalt:

- ❑ Driftsinntekter ABB Group: **$ 27,66 milliarder**
- ❑ Antall ansatte ABB Group: **rundt 147 000**

- ❑ Leverer produkter, systemer, tjenester og programvare
- ❑ Opererer i mer enn 100 land – Asia, Midtøsten, Afrika, Americas og Europa

Attraktive markeder i omstilling:

Energirevolusjonen

Den fjerde industrielle revolusjonen

Energiforsyning	Industri	Transport og infrastruktur

Fakta om ABBs Pensjonsaksse

2018

- Forvaltningskapital: **NOK 3,3 milliarder**
- Beregnet solvenskapital dekning per 010119 – 189,3%

- Pensjoner under utbetaling: **NOK 99,0 millioner**
- Antall aktive medlemmer: 271
- Antall uførepensjonister: 126
- Antall pensjonsmottakere: 2088
- Antall fripolisekontrakter: 2774

- Styret består av 9 medlemmer hvorav 1 ekstern og 4 ansatte representanter
- Daglig leder, økonomiansvarlig og ansvarlig for pensjonsutbetaling er ansatt i ABB
- Pensjonskassen ble etablert I 1990

GDPR – Hva er personvern?

Personvern handler om retten til et privatliv og retten til å bestemme
over egne personopplysninger.

Alle mennesker har en ukrenkelig egenverdi.
Som enkeltmenneske har du derfor rett på
en privat sfære som du selv kontrollerer,
hvor du kan handle fritt uten tvang eller innblanding fra staten eller andre mennesker.

Dette prinsippet er blant annet forankret i
Den europeiske menneskerettighetskonvensjonen (EMK), hvor det heter:

**Enhver har rett til respekt for sitt privatliv og familieliv,
sitt hjem og sin korrespondanse.**
- *EMK artikkel 8*

GDPR – Fra tro på mestring til erkjennelse om at her må vi på «skolebenken»!

Fra «mapper» i sikre skap til digitale data i «bakke» og «sky» og kommunikasjon per brev til e-post, digipost og innlogging via min Id

Hvordan skulle vi tilpasse oss det nye regelverket?

- Den enkle tilnærmingen – «dette kan vi» – ble raskt erstattet av målrettet og innsats for omstilling til nye prosedyrer som er velfunderte og dokumenterte, men fortsatt har vi et stykke vei å gå!
- Underveis har vi innimellom opplevd noe av den samme frykten som kan minne om frykt for datasammenbrudd ved 1000 års skiftet! Med begrenset ressurstilgangs må det prioriteres.
- GDPR er IKKE vår kjernevirksomhet! Vi må være leveringsdyktige og tilgjengelige!
- Kunnskap og opplæring i fokus. «Autopilot» tilnærming holder IKKE!
- Ingen konsesjon å «lene» oss til!
- Alene ansvarlig for å begrunne hva slags informasjon vi skal kunne innhente og lagre, vite hvilke situasjoner som krever samtykke, samtykke krav og dokumentasjon for logging og rapportering av avvik etc.
- ***GDPR – integrert i alle prosesser – en naturlig del av vår hverdag.***

Det er styret's og daglig leder's ansvar å forsikre seg om og dokumentere at Pensjonskassen driver sin virksomhet i samsvar med ny lovgivning!

DATABESKYTTELSE GJELDER ALL BEHANDLING AV PERSONDATA

Persondata er all informasjon knyttet til en person, dvs. «data subjektet», som direkte eller indirekte kan identifisere personen

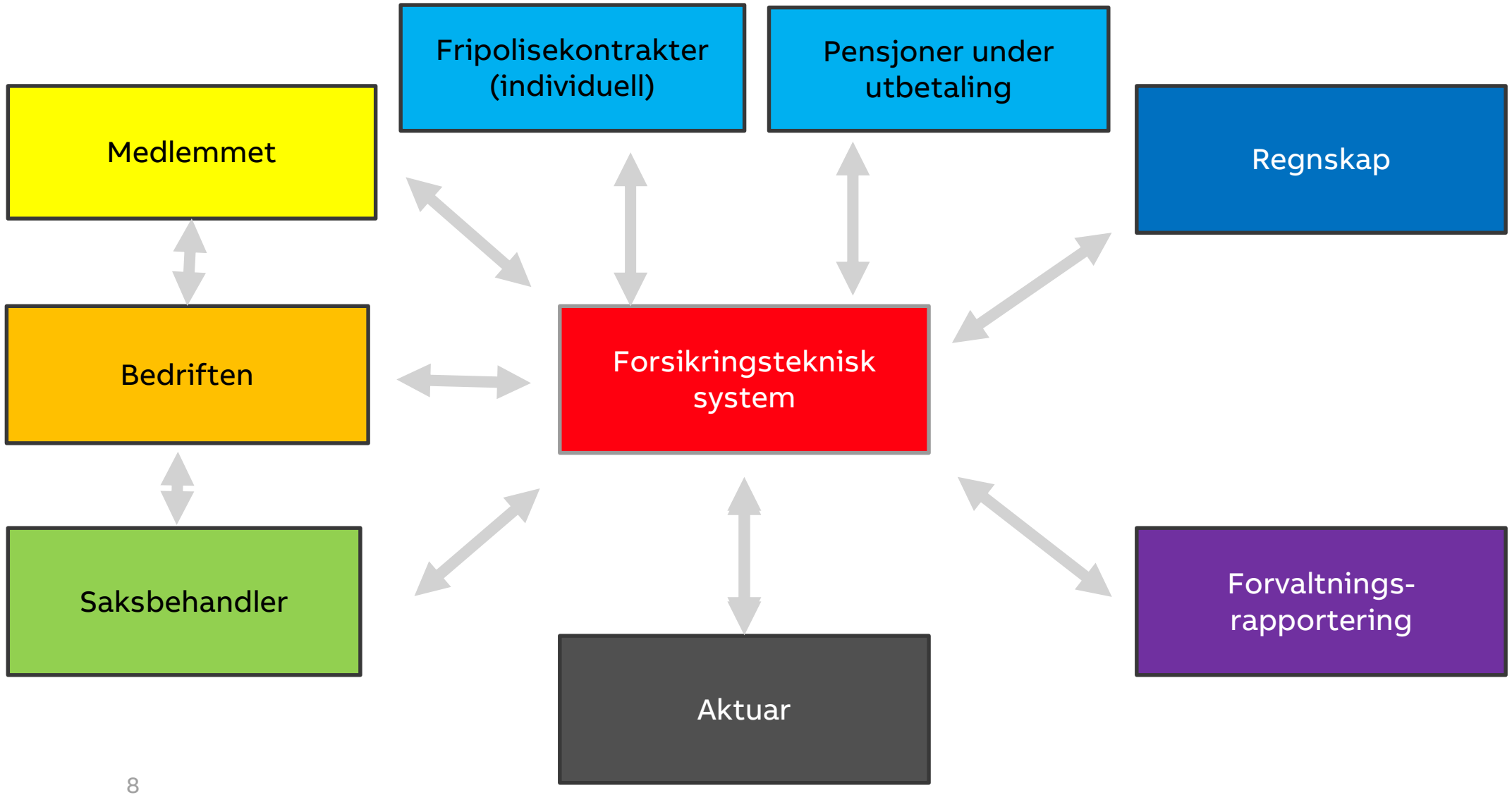
Pensjonskassen's informasjonsbehov direkte knyttet til rettighetshavers persondata

Avgjørende for å sikre at arbeidsgivers pensjonsavtale sikres korrekte medlemsdata for utbetaling av alders-, uføre-, ektefelle/samboer- og/eller barnepensjon gjennom løftets livsfase – opptil kanskje mer enn 100 år!!

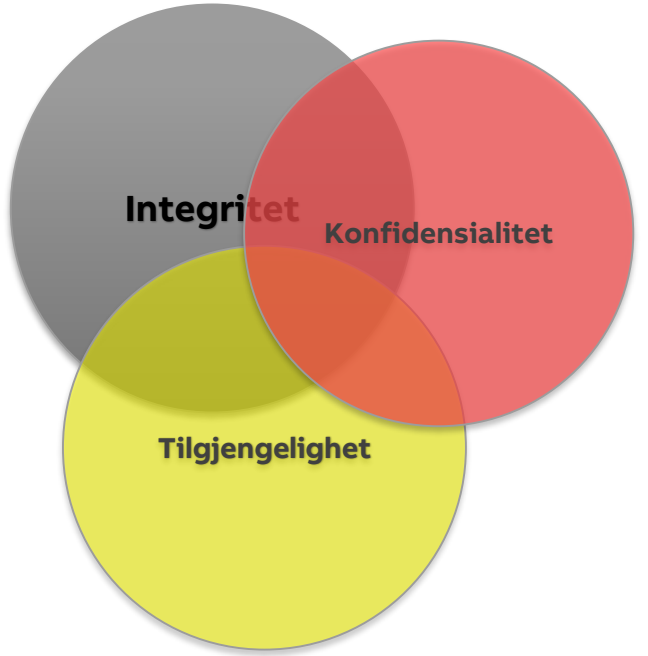
Relevante Persondata:

- Navn, kjønn, fødselsdato og år, personnummer, ansatte nummer, adresse, mail adresse, postnummer, pensjonsgrunnlag/lønn, opptaksdato, avgangsdato, sivil status, sykehistorikk, deltids prosenter, telefon nummer, navn på ektefelle/samboer/barn og tilleggsinformasjon som sikrer korrekt identifisering etc
- Vedtak innhentet fra NAV eller kontroll lege
- For pensjonister, uførepensjonister og etterlatte pensjonister – bankponti, skattenummer, utbetalingsdata, dato for utbetaling , etterkontroll og stop av ytelser, underlag knyttet til grunnlaget for ytelsens størrelse etc.
- I spesielle tilfeller trenger vi tilgang til sensitive persondata som helsedata og sykhistorikk fra behandlende lege/spesialist. I slike saker kreves innhenting av samtykke.

Pensjonskassens persondata er alle forankret i forsikringssystemet



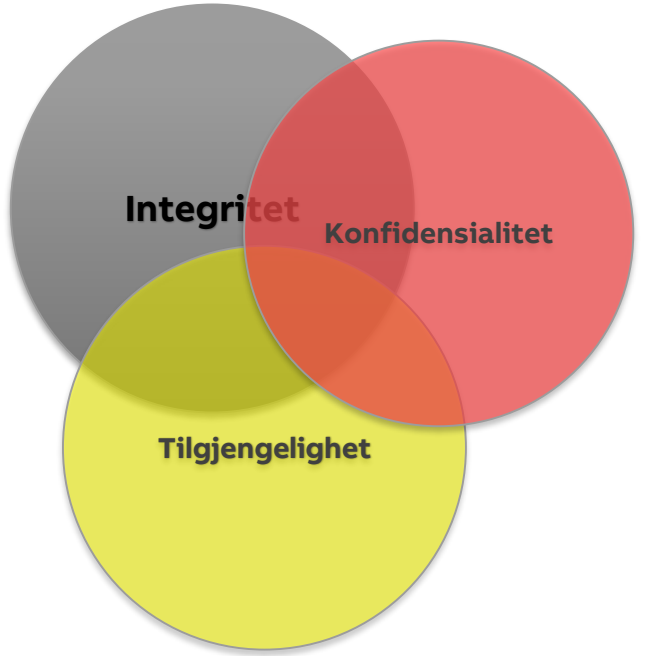
Integritet – Konfidensialitet - Tilgjengelighet



Pensjonskassens behov:

- Ansatte med nødvendig kunnskap til sikker kommunikasjon og lagring/sletting av «lovlig» informasjon og håndtering av avvik og varsling.
- Sikre et datagrunnlag som er tilstrekkelig for å levere korrekte ytelser til rettighetshaver(e) eller eventuelle etterlatte til rett tid gjennom hele livsløpet.
- Kostnadseffektiv administrasjon og service basert på sikker og rask tilgang til korrekte data.
- Sikkerhet for at lagret informasjon er tilgjengelig og beskyttet mot uautorisert tilgang og/eller tyveri/tapping av data, tap eller sletting av data gjennom feiloperasjon og «villet» ødeleggelse/sletting av data.
- Sikkerhet for at vi alltid kommuniserer med rett person og/eller fullmektig og at ytelsen(e) utbetales til riktige rettighetshaver(e)

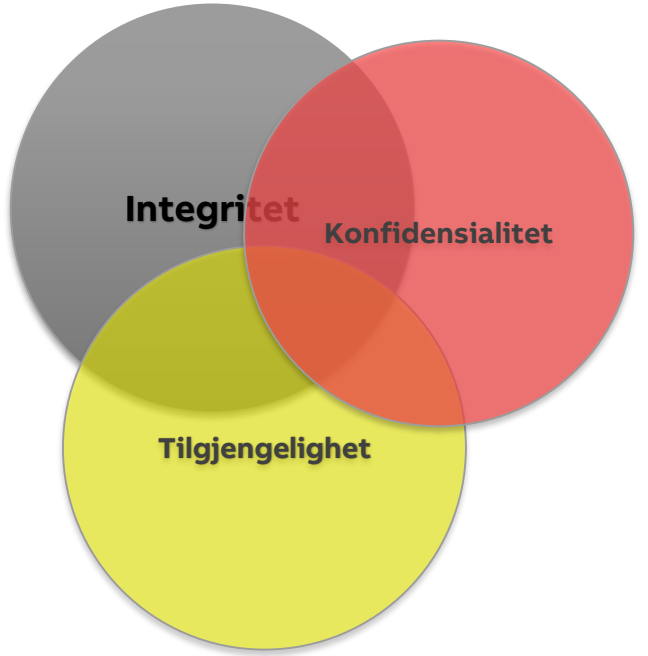
Integritet – Konfidensialitet - Tilgjengelighet



Rettighetshaver's behov:

- Pensjonen skal være korrekt beregnet basert på korrekt og oppdatert informasjon og iht til planbeskrivelse.
- Eventuelle etterlatte skal sikres korrekte ytelser ved rettighetshavers død.
- Service nivå som sikrer profesjonelle svar og veiledning.
- Tillitt til at personlig informasjon knyttet til ytelser, grunnlag for ytelsene, konto opplysninger og/eller andre personsensitiv informasjon ikke benyttes til annet formål eller kommer på av

Integritet – Konfidensialitet - Tilgjengelighet



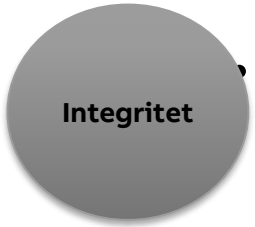
Arbeidsgivers behov:

- Kompetente ansatte med kunnskap innenfor sikker kommunikasjon og hvilke data som kan utveksles mellom foretaket og pensjonskassen.
- Rutiner for regelmessig å ajourføre medlemsdata for å sikre ansatte korrekt pensjon og at foretaket betaler riktig premie og holder kontroll med sine pensjonsforpliktelser.
- Taushetserklæringer for personell som skal ha tilgang til og/eller behandle personsensitiv informasjon.
- Sikre nødvendig «samtykke» fra ansatt ved informasjonsutveksling utover det som direkte er nødvendig for ajourhold av medlemsdata.

GDPR – Databehandleravtaler – Viktig å sikre kontroll m/avtalene!

- **Databehandleravtaler – Kapittel IV –** ***artikkel 24 – 31***
  - En pensjonskasse er en liten organisasjon som baserer seg på system løsninger og/eller tjenester som er utkontrahert.
  - Dersom databehandler benytter en underleverandør skal pensjonskassen ha kunnskap om dette. Det må foreligge en databehandlingsavtale mellom leverandøren og underleverandør som ivaretar pensjonskassens forpliktelser som behandlingsansvarlig (jf. personvernforordningen artikkel 28 og 29).
  - Fastsett klare krav til håndtering, logging og varsling av avvik. Det er Behandlingsansvarlige, dvs. Pensjonskassen, som har varslingsplikt ovenfor Datatilsynet (72 timers kravet) og ovenfor den eller de personer som er rammet dersom avviket ansees som vesentlig.

GDPR – utfordringer



- Sikre at eksisterende arkiv (historikk) inneholder informasjon som ikke bryter med GDPR
  - Omfattende kartleggingsjobb
  - Kan lett bli ressurskrevende

- Sikre en balanse mellom å jobbe effektivt og sikre at man til enhver tid er «compliant»
  - Vurdere arbeidsprosesser mht risiko og sårbarhet
  - Holde rutinebeskrivelser oppdatert
  - Krav til loggføring av aktiviteter

- Sikre at hele organisasjonen har tilstrekkelig kunnskap om GDPR og forståelse for hva forordningen «betyr for oss» - sikre at alle ledd er «compliant»


ABB