GDPR I DEN NORSKE OPERA & BALLETT

Spekter, 13. desember 2017

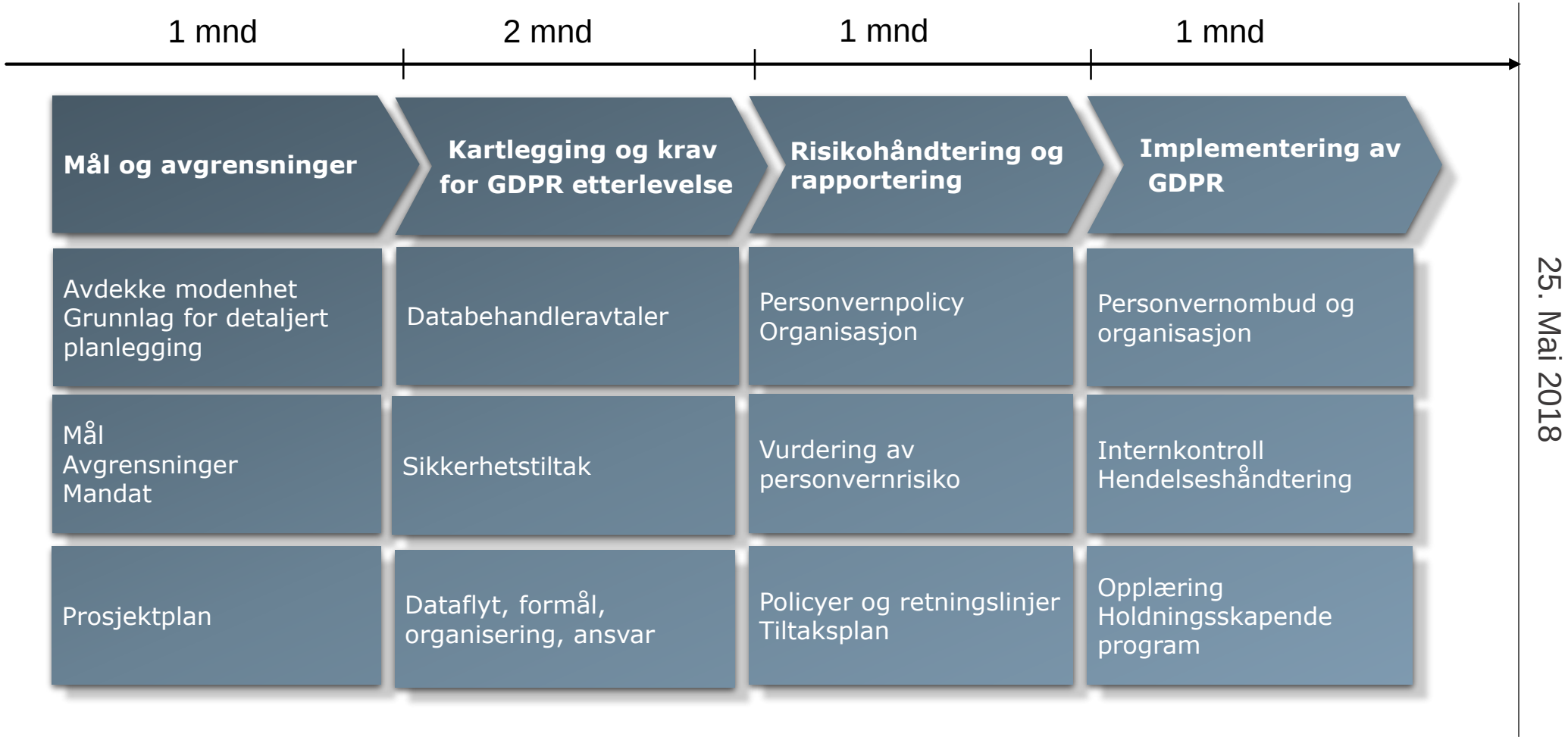
Overordnet - Hva er «The General Data Protection Regulation» (GDPR)?

- Definerer regler for all behandling av personopplysninger i virksomheter (regulering av personvern, personvernsikkerhet og personvernstyring).
- EU lov som erstatter eksisterende norsk personopplysningslov og –forskrift (fra 25. mai 2018).
- Omfatter både fysiske og digitale personopplysninger
- Det er viktig å merke seg er at GDPR handler like mye om prosessadministrasjon som det handler om datasikkerhet
  - For å være i samsvar med kravene til GDPR, og å kunne møte de registrertes krav til innsyn, må prosesser som behandler personopplysninger tilpasses eller utvikles
  - Applikasjoner som behandler personopplysninger må gjennomgås og evt. oppdateres for å oppfylle kravene om innebygd personvern. Databehandleravtaler må tilpasses

De syv styrende prinsippene for behandling/håndtering av personopplysninger iht. GDPR

1. Lovlighet, rimelighet og transparens
   - Personopplysninger skal behandles lovlig, rimelig og på en transparent måte.
2. Formålsbegrensning
   - Personopplysningene skal kun registreres for det angitte formålet (kan ikke benyttes til andre formål enn de er innsamlet for).
3. Dataminimering
   - Det skal ikke samles inn flere eller andre personopplysninger enn det som er nødvendig for det angitte formål.
4. Korrekthet
   - Personopplysningene som virksomheten behandler skal være korrekte (må oppdateres om nødvendig).
5. Lagringsbegrensning
   - Personopplysninger skal ikke lagres lenger enn nødvendig. Deretter skal opplysningene slettes.
6. Integritet og konfidensialitet
   - Personopplysninger skal behandles på en måte som sikrer tilstrekkelig sikkerhet.
7. Ansvarlighet
   - Behandlingsansvarlige skal kunne dokumentere at disse prinsippene er overholdt og at ansvaret for dette er plassert.

Prosjektmodell for å sikre GDPR etterlevelse i DNO&B



Noen sentrale spørsmål innledningsvis i kartleggingsfasen

- Hvilke prosesser og informasjonssystem behandler personopplysninger om **ansatte, kunder** og **leverandører**
- Hva benyttes personopplysningene til?
- Hvilke personopplysninger behandles og av hvilken kategori er de?
- Hvem har hvilke tilganger til personopplysningene?
- Hvordan er personopplysningene sikret?
- Hvor behandles og lagres personopplysningene (lokalt, sentralt, hos en driftsleverandør, i skyen)?
- Hvilke leverandører benyttet og hvilke avtaler er inngått om behandling av personopplysningene?
- Er det dokumentert et formål med behandlingen av personopplysningene og foreligger det samtykke fra de registrerte?

Kartlegging viser at DNOB har 29 fagsystemer med personopplysninger og behov for 21 nye databehandleravtaler

Marked (11)	Billettsystem, nyhetsbrevverktøy, CRM mot kunde og sponsorer, www.operaen.no, bildelagring/gjenfinning, video løsning, kontakt- og callsenter +++
Drift og sikkerhet (5)	Adgangskontroll, Videoovervåkning, Beredskapsverktøy, system for nøkkelkontroll, vaktjournal
HR (3)	Lønn, personal, rekruttering
Regnskap (2)	Økonomi/Regnskap, økonomirapporter
Plan (3)	Plansystem, produksjonsdatabasen i Maconomy, integrering og Rapporteringssystem
Teknisk drift (2)	Timeregistrering, kompetanseprogram
Ballett (1)	Helseoppfølgingssystem
IKT (2)	Arkivsystemet, fellesdisker/filområder

12 identifiserte gap mellom forordningens krav og dagens situasjon i DNOB

Nummer	Identifisert gap ift. etterlevelse av GDPR	Anbefaling og tiltak
1	En ansvarlig person som sikrer etterlevelse av GDPR i selskapet kreves	DNO&B må utpeke en personvernrådgiver
2	DNO&B mangler styringssystem for å håndtere lover og regler i henhold til GDPR (internkontroll)	Et internkontrollsystem må tydeliggjøres og rutiner for hvordan GDPR etterleves må utarbeides

12 identifiserte gap mellom forordningens krav og dagens situasjon i DNOB

Nummer	Identifisert gap ift. etterlevelse av GDPR	Anbefaling og tiltak
3	DNO&B har ikke en komplett oversikt over hvilke personopplysninger de har, hvordan de brukes og hvor de er lagret.	En oversikt over personopplysninger som behandles av DNO&B må etableres. Verktøy for å vedlikeholde GDPR dokumentasjon bør anskaffes.
4	Det finnes ingen dokumentert metode for vurdering av personvernkonsekvens og risiko. DNO&B har noe behandling av sensitive personopplysninger (helsedata Ballett)	Utarbeide metode for vurdering og forankring hos ledelsen, personvernrådgiver og systemeier

12 identifiserte gap mellom forordningens krav og dagens situasjon i DNOB

Nummer	Identifisert gap ift. etterlevelse av GDPR	Anbefaling og tiltak
5	Kundedata benyttes i noen grad for profilering uten samtykke.	Det må etableres prosedyrer for å sikre at personopplysningene som samles inn kun brukes som avtalt.
6	Manuelle rutiner øker risiko for ukorrekt data og data på avveie	Prosedyrer for å holde personopplysninger korrekte og oppdaterte må etableres med tilstrekkelig sikkerhet.
7	Informasjon om ansatte blir registrert ved ansettelse men blir aldri slettet.	Krav knyttet til lagringsbegrensning og sletting må beskrives og implementeres

12 identifiserte gap mellom forordningens krav og dagens situasjon i DNOB

Nummer	Identifisert gap ift. etterlevelse av GDPR	Anbefaling og tiltak
8	DNO&B benytter seg av flere drifts- og tjenesteleverandører som behandler personopplysninger uten databehandleravtale.	Databehandleravtaler må etableres og oppdateres for å etterleve GDPR artikkel 28. Prosedyre må etableres for å inngå databehandleravtaler som også inkludere underleverandører til leverandører.
9	Systemer skal ha en slettefunksjon for personopplysninger	Retningslinjer for lagrings- og sletteregime må etableres. Systemer som ikke støtter sletteregime må oppdateres.

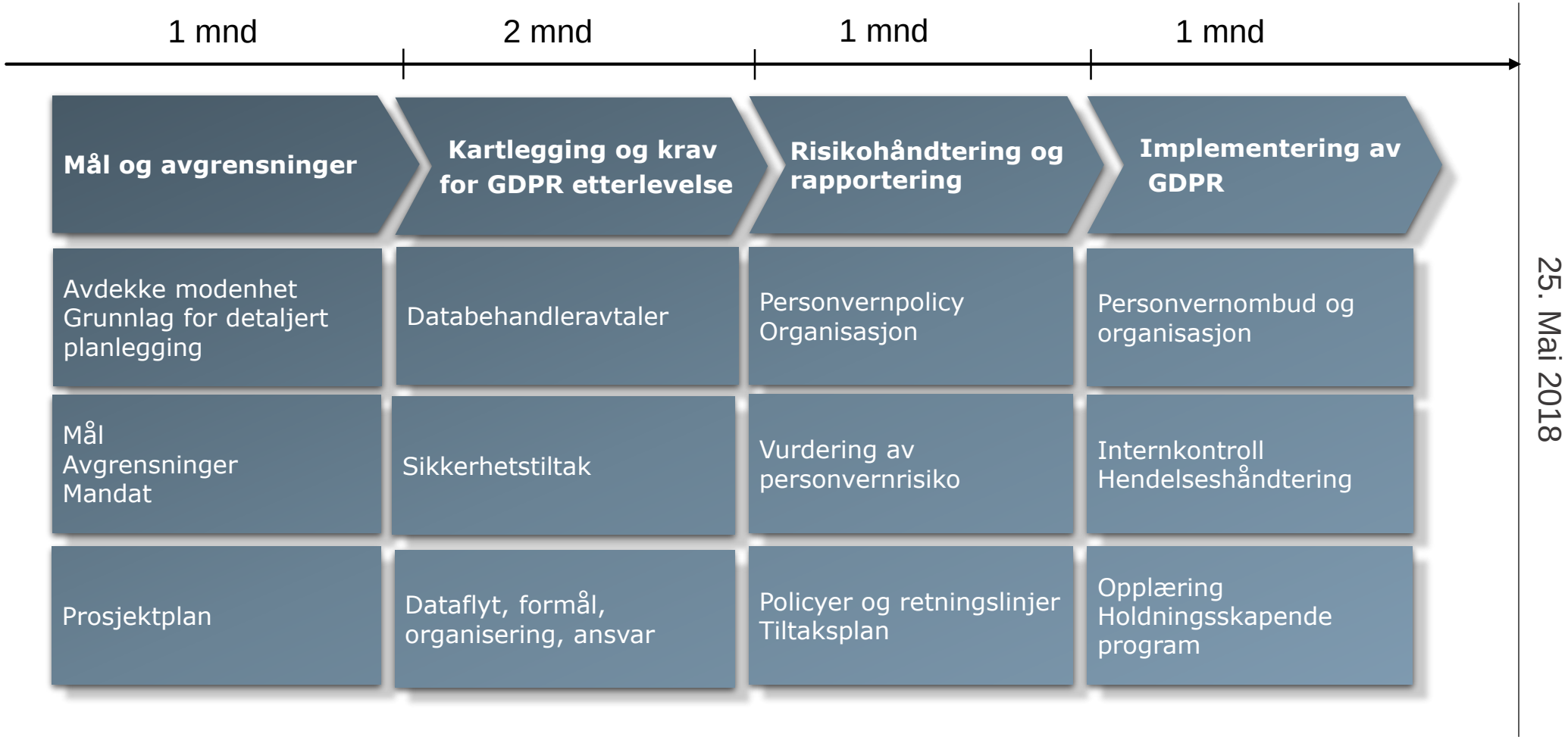
12 identifiserte gap mellom forordningens krav og dagens situasjon i DNOB

Nummer	Identifisert gap ift. etterlevelse av GDPR	Anbefaling og tiltak
10	DNO&B har ikke etablert retningslinjer for å sikre innebygget personvern i IKT-anskaffelser eller ved utvikling av IKT-systemene.	Retningslinjer som sikrer at innebygget personvern blir ivaretatt ved anskaffelser må utarbeides.

12 identifiserte gap mellom forordningens krav og dagens situasjon i DNOB

Nummer	Identifisert gap ift. etterlevelse av GDPR	Anbefaling og tiltak
11	DNO&B har ikke en dokumentert policy for informasjonssikkerhet med tilhørende styringssystem og ansvarliggjøring	En felles informasjonssikkerhetspolicy må etableres og ansvar må fordeles til nøkkelroller som vil utgjøre en sikkerhetsorganisasjon.
12	DNO&B har ikke prosedyrer for hendelseshåndtering ved sikkerhetsbrudd som berører personopplysninger.	DNO&B må etablere prosedyrer for hendelseshåndtering ved sikkerhetsbrudd, samt varsling til Datatilsynet innen 72 timer.

Prosjektmodell for å sikre GDPR etterlevelse i DNO&B



Læringspunkter

- Kom i gang – det er mer omfattende enn dere tror!
- Vurder ekstern bistand
- Ha minst like stort fokus på rutiner, prosesser og eierskap som på «det tekniske»